UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE FILOSOFIA E CIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ELAINE PARRA AFFONSO

A INSCIÊNCIA DO USUÁRIO NA FASE DE COLETA DE DADOS: PRIVACIDADE EM FOCO

Marília - SP
2018

ELAINE PARRA AFFONSO

A INSCIÊNCIA DO USUÁRIO NA FASE DE COLETA DE DADOS: PRIVACIDADE EM FOCO

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação da Faculdade de Filosofia e Ciências, da Universidade Estadual Paulista – UNESP – Campus de Marília, como requisito para obtenção do título de Doutorado em Ciência da Informação.

Área de Concentração: Informação, Tecnologia e Conhecimento.

Linha de Pesquisa: Informação e Tecnologia.

Orientador: Prof. Dr. Ricardo César Gonçalves Sant'Ana.

Marília - SP
2018

Affonso, Elaine Parra.
A257i A insciência do usuário na fase de coleta de dados: privacidade em foco / Elaine Parra Affonso. – Marília, 2018.
325 f. ; 30 cm.

Orientador: Ricardo César Gonçalves Sant'Ana.
Tese (Doutorado em Ciência da Informação) - Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, 2018.
Bibliografia: f. 249-277.

1. Sistema de coleta automática de dados. 2. Direito à privacidade. 3. Proteção de dados. 4. Sigilo. I. Título.

CDD 005.73

Ficha catalográfica elaborada por Telma Jaqueline Dias Silveira - CRB 8/7867

ELAINE PARRA AFFONSO

A INSCIÊNCIA DO USUÁRIO NA FASE DE COLETA DE DADOS: PRIVACIDADE EM FOCO

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação, da Faculdade de Filosofia e Ciências, da Universidade Estadual Paulista – UNESP – Campus de Marília, na área de concentração Informação, Tecnologia e Conhecimento.

BANCA EXAMINADORA

Orientador: _____

Dr. Ricardo César Gonçalves Sant'Ana
Universidade Estadual Paulista – Unesp/Marília

2º Examinador: _____

Dra. Plácida L. V. A. da Costa Santos
Universidade Estadual Paulista – Unesp/Marília

3º Examinador: _____

Dr. Guilherme Ataíde Dias
Universidade Federal da Paraíba (UFPB)

4º Examinador: _____

Dra. Silvana Drumond Monteiro
Universidade Estadual de Londrina (UEL)

5º Examinador: _____

Dra. Ângela Maria Grossi de Carvalho
Universidade Estadual Paulista – Unesp/Bauru

Aprovada em 05 de julho de 2018.

Marília
2018

Dedico este trabalho aos meus pais Osvaldo e Iolanda,

Ao meu esposo Edgar e a ela:

...benção na minha vida: *Maria Clara*, o ser humano mais lindo que Deus poderia ter escolhido para ser minha filha!

AGRADECIMENTOS

A Deus, luz para minhas escolhas, suas palavras sussurram incessantemente, por isso eu não desanimei, por isso eu tive ânimo e por isso eu continuei a caminhada...Obrigada meu Deus por ter marchado a minha frente!

Ao meu esposo Edgar por sempre acompanhar meus sonhos, pelo amor e carinho com a nossa família.

A minha filha Maria Clara, que cresceu junto com este trabalho, obrigada pela compreensão nas minhas ausências, mesmo eu estando tão próxima. Que a jornada que eu percorri seja exemplo de que tudo é possível quando existe perseverança.

Aos meus pais, Osvaldo e Iolanda, vocês fizeram o que eu não pude fazer, estiveram onde eu não pude estar, deram carinho no momento da minha ausência....gratidão é pouco....

A minha cunhada e amiga Sandra C. de Oliveira, pelo incentivo ao ingresso no doutorado e por todos os conselhos e paciência durante minhas crises de angústias...

Ao meu irmão Clayton, por toda ajuda e acolhida em sua casa em Marília.

Ao meu orientador, Profº Dr. Ricardo C. G. Sant'Ana por ter acreditado que seria possível, sua competência profissional foi fundamental para todas as minhas conquistas!

As minhas companheiras de grupo de pesquisa que compartilharam de muitos momentos durante esse percurso no doutorado: Elizabete Monteiro, Jacquelin T. Camperos Reyes, Diana V. B. S.Aleixo, e, especialmente a minha amiga Cristina Toyoko Hashimoto.

Aos professores membros da banca, Guilherme Ataíde Dias, Plácida L. V. A. da Costa Santos, Silvana Drumond Monteiro, Ângela Maria Grossi de Carvalho, e suplentes, Cristiane H. C. Bernardo, Douglas D. J. de Macedo e Leonardo C. Botega, por sua disposição em participar da avaliação deste trabalho.

Ao Centro de Educação Tecnológica Paula Souza pelo afastamento concedido para que eu pudesse me dedicar ao doutorado e aos colaboradores da Fatec Presidente Prudente – SP, especialmente ao meu coordenador Marcelo Buscioli Tenório e a minha amiga Daiane Marcela Piccolo.

Muito obrigada!

Cada indivíduo é visto, mas não vê; objeto de uma informação, nunca sujeito de uma comunicação. (...) o panoptismo faz funcionar ao arrepio do direito, uma tecnologia que vai além dos limites traçados
(FOUCAULT, 1987, p.224)

RESUMO

A coleta de dados tem se tornado uma atividade predominante nos mais diversos meios digitais, em que as redes de computadores, principalmente a Internet, são essenciais para essa fase. A fim de minimizar a complexidade envolvida no uso de aplicações e de meios de comunicação, a relação usuário-tecnologia tem sido apoiada por interfaces cada vez mais amigáveis, o que contribui para que a coleta de dados, muitas vezes, ocorra de forma imperceptível ao usuário, tornando-o insciente sobre a coleta realizada pelos detentores de dados, situação que pode ferir o direito à privacidade de usuários e de referenciados. Para proporcionar consciência sobre a coleta de dados aos usuários, ambientes digitais disponibilizam políticas de privacidade com informações sobre essa fase, buscando conformidade às leis e aos regulamentos que amparam a proteção de dados pessoais, muito representada na literatura acadêmica por meio de modelos e técnicas para anonimização. A insciência sobre a coleta de dados pode estabelecer como o indivíduo se preocupa em relação às ameaças à sua privacidade e quais são as atitudes que ele deveria ter para ampliar a proteção de seus dados, que também pode ser estimulada pela carência de ações e de pesquisas de diversas áreas do conhecimento. Diante do exposto, o objetivo desta tese é caracterizar o contexto que favorece a insciência do usuário enquanto alvo de fases de coleta de dados em ambientes digitais, considerando implicações de privacidade. Para tanto, adotou-se a pesquisa exploratória-descritiva, com abordagem qualitativa. Utilizou-se a triangulação metodológica, a partir do referencial teórico que abarca a anonimização na fase de coleta de dados; legislações que amparam a proteção de dados pessoais e a coleta de dados realizada por tecnologias. Em relação às pesquisas no âmbito de proteção de dados por anonimização, observou-se que existe uma carência de trabalhos na fase de coleta de dados, uma vez que, muitas pesquisas têm concentrado esforços no contexto de medidas para compartilhar dados anonimizados, e quando a anonimização se efetua na coleta de dados, a ênfase tem sido em relação a dados de localização. Muitas vezes, as legislações ao abordarem elementos que estão envolvidos com a fase de coleta, apresentam esses conceitos de modo generalizado, principalmente em relação ao consentimento sobre a coleta, inclusive, a própria menção a atividade de coleta, emerge na maioria das leis por meio do termo tratamento. A maior parte das leis não possui um tópico específico para a coleta de dados, fator que pode fortalecer a insciência do usuário no que tange a coleta de seus dados. Os termos técnicos como anonimização, *cookies* e dados de tráfego são mencionados nas leis de modo esparso, e muitas vezes não estão vinculados especificamente a fase de coleta. Os dados semi-identificadores se sobressaem na coleta de dados pelos ambientes digitais, cenário que pode ampliar ainda mais as ameaças a privacidade devido à possibilidade de correlação desses dados, e com isso, a construção de perfis de indivíduos. A opacidade promovida pela abstração na coleta de dados pelos dispositivos tecnológicos vai além da insciência do usuário, ocasionando incalculáveis ameaças à privacidade e ampliando, indubitavelmente, a assimetria informacional entre detentores de dados e usuários. Conclui-se que a insciência do usuário sobre sua interação com os ambientes digitais pode diminuir a autonomia para controlar seus dados e acentuar quebras de privacidade. No entanto, a privacidade na coleta de dados é fortalecida no momento em que o usuário tem consciência sobre as ações vinculadas aos seus dados, que devem ser determinadas pelas políticas de privacidade, pelas leis e pelas pesquisas acadêmicas, três elementos evidenciados neste trabalho que se configuram como participativos no cenário que propicia a insciência do usuário.

Palavras-chave: Coleta de dados. Insciência. Anonimização. Privacidade. Proteção de dados.

ABSTRACT

Data collection has become a predominant activity in several digital media, in which computer networks, especially the internet, are essential for this phase. In order to minimize the complexity involved in the use of applications and media, the relationship between user and technology has been supported by ever more friendly interfaces, which oftentimes contributes to that data collection often occurs imperceptibly. This procedure leads the user to lack of awareness about the collection performed by the data holders, a situation that may harm the right to the privacy of this user and the referenced users. In order to provide awareness about the data collection to the user, digital environments provide privacy policies with information on this phase, seeking compliance with laws and regulations that protect personal data, widely represented in the academic literature through models and techniques to anonymization in the phase of data recovery. The lack of awareness on the data collection can establish how the individual is concerned about threats to its privacy and what actions it should take to extend the protection of its data, which can also be stimulated by the lack of action and researches in several areas of the knowledge. In view of the above, the objective of this thesis is to characterize the context that favors the lack of awareness of the user while the target of data collection phases in digital environments, considering privacy implications. For that, the exploratory research was adopted, with a qualitative approach. The methodological triangulation was used, from the theoretical referential that includes the anonymization in the phase of the data collection; the legislation that supports the protection of personal data and the data collection performed by technologies. The results show that, regarding researches on data protection by anonymization, it was observed that there is an absence of works about the data collection phase, since many researches have concentrated efforts in the context of measures to share anonymized data. When anonymization is done in data collection, the emphasis has been on location data. Often, legislation when addressing elements that are involved with the collection phase, present these concepts in a generalized way, mainly in relation to the consent on the collection, including the very mention of the collection activity, emerges in most laws through the term treatment. Most laws do not have a specific topic for data collection, a factor that can strengthen user insight regarding the collection of their data. Technical terms such as anonymization, cookies and traffic data emerge in the laws sparingly and are often not specifically linked to the collection phase. The quasi-identifiers data stands out in the data collected by the digital environments, a scenario that can further extend the threats to privacy due to the possibility of a correlation of this data, and with this, the construction of profiles of individuals. The opacity promoted by abstraction in data collection by computer networks goes beyonds the lack of awareness of the user, causing incalculable threats to its privacy and undoubtedly widening the informational asymmetry among data keepers and users. It is concluded that user insight about their interaction with digital environments can reduce the autonomy to control their data and accentuates privacy breaches. However, privacy in data collection is strengthened when the user is aware of the actions linked to its data, which should be determined by privacy policies, laws and academic research, i.e, three elements evidenced in this work that are constitute as participatory in the scenario that provides the lack of awareness of the user.

Keywords: Data Collect. Lack of awareness. Anonymization. Privacy. Data protection.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

APEC	*Asian Pacific Economic Cooperation*
APIs	*Application Programming Interfaces*
APPs	*Australian Privacy Principles*
ASCII	*American Standard Code for Information Interchange*
CEP	Código de Endereçamento Postal
CI	Ciência da Informação
CVD	Ciclo de Vida dos Dados
DEC	*Digital Equipment Corporation*
E2EE	*End-To-End Encryption*
EFF	*Electronic Frontier Foundation*
EMD	*Earth Mover Distance*
EU	União Europeia
EUA	Estados Unidos
FBI	*Federal Bureau of Investigation*
FERPA	*Family Educational Rights and Privacy Act*
FIPPs	*Fair Information Practice Principles*
FTP	Protocolo para Transferência de Arquivos (*File Transfer Protocol*)
GCI	Comitê Gestor da Internet no Brasil
GDPR	General Data Protection Regulation
GPL	*General Public Licence*
GUID	*Globally Unique Identifier*
HIPPA	*Health Insurance Portability and Accountability Act*
HTTP	*HyperText Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
I	Identificadores
ICCID	*Integrated Circuit Chip Card Identification*
IMEI	*International Mobile Equipment Identity*
IP	*Internet Protocol*
IPX	*Internetwork Packet Exchange*
ISO/TS	*International Organization for Standardization/Technical Specification*
LAI	Lei de acesso à informação
LBS	*Location Basead Service*
MAC	*Media Access Control*
NS	Não sensíveis
NSA	*National Security Agency*

OECD	*Organization for Economic Co-operation and Development*
OSI	*Open System Interconnection*
P2P	*Peer-to-Peer*
PAMIA	*Privacy Act Modernization for the Information Age*
PETs	*Privacy-Enhancing Technologies*
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PL	Projeto de Lei
PLS	Projeto de Lei do Senado
RFID	*Radio-Frequency Identification*
RPC	*Remote Procedure Call*
SE	Sensíveis
SI	Semi-Identificadores
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SPX	*Sequenced Packet Exchange*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TIC	Tecnologia da Informação e Comunicação
TLS	*Transport Layer Security*
TOR	*The Onion Router*
TTL	*Time-to-Live*
UDP	*User Datagram Protocol*
URI	*Uniform Resource Identifier*
URL	*Uniform Resource Locator*
WWW	*Word Wide Web*

SUMÁRIO

1 INTRODUÇÃO

> *Da mesma forma, uma vez dentro, tornamo-nos reféns do destino. [...] Tudo o que é privado agora é feito, potencialmente, em público e está potencialmente disponível para consumo público e continua sempre disponível, até o fim dos tempos, já que a Internet "não pode ser forçada a esquecer" – nada que tenha sido registrado em algum de seus inumeráveis servidores (BAUMAN, 2014, p. 20).*

Há uma grande discussão na atualidade sobre os aspectos que permeiam a privacidade do indivíduo pertencente à sociedade da informação, uma vez que com o uso exponencial das tecnologias da informação, ampliam-se também as atividades que realizam coleta de dados. A coleta de dados passa ser uma atividade comum durante a interação do usuário com as tecnologias, tais como: aplicações no ambiente Web; aplicativos para dispositivos móveis; sistemas de informação empresariais, incluindo a coleta pelas câmeras de vigilância nos estabelecimentos públicos e privados.

As ameaças à privacidade do indivíduo são decorrentes da constante vigilância proporcionada pelos dispositivos tecnológicos, da grande quantidade de dados coletados, da velocidade com que eles podem ser transferidos, da duração que podem ser vistos e armazenados, incluindo as possibilidades de recuperação por usuários e por outras aplicações (MASON, 1986; TAVANI, 2008).

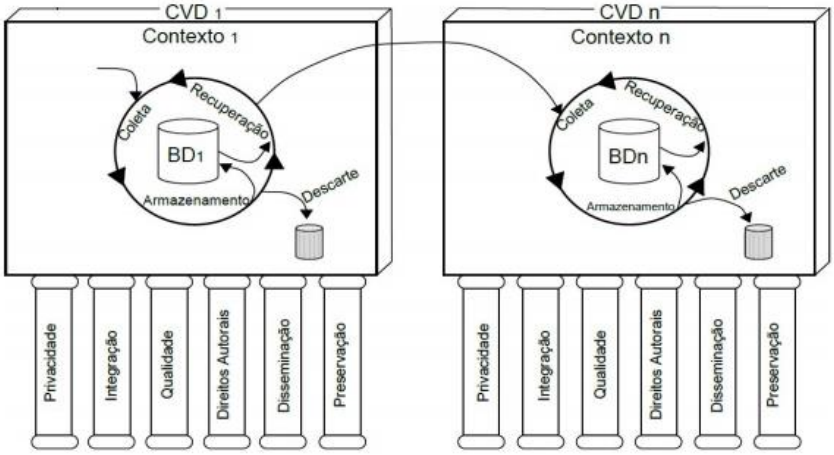
> [...] no mundo atual, a tecnologia atua em dois flancos distintos e adversos: por um lado, ajuda a moldar uma sociedade mais evoluída e mais bem informada; em contrapartida, conduz as pessoas a uma maior fragilidade quanto às suas informações pessoais, expondo-as, muitas vezes, a abusos de toda ordem, tendo por suporte seus próprios dados pessoais (GAMIZ, 2012, p. 26).

Bennett (1992) ressalta que embora o termo "privacidade" seja ambíguo e polêmico, configurando-se, em determinado momento, como a necessidade de exclusividade do espaço físico, evitando a intromissão, e em outro momento, como o controle da informação pessoal, é essencial que a abordagem da privacidade da informação esteja sempre vinculada à proteção de dados. Pereira (2003) também afirma que a doutrina jurídica quando envolvida com estudos de direito no contexto das tecnologias da informação, costuma relacionar a privacidade com a ideia de proteção de dados pessoais.

O momento em que se tem como objetivo obter dados é representado pela fase de coleta do Ciclo de Vida dos Dados (CVD) (SANT'ANA, 2013). Na fase de coleta é realizado o

planejamento e a execução de diversas atividades, por exemplo: a identificação da necessidade informacional; o reconhecimento da necessidade da coleta; a definição dos dados que serão coletados; os procedimentos para realização da coleta; o formato dos dados; a localização das fontes desses dados, e o tratamento necessário para que esses dados estejam alinhados à finalidade da coleta (SANT'ANA, 2016). A fase de coleta no CVD está permeada pelos fatores privacidade, integração, qualidade, direitos autorais, disseminação e preservação dos dados (SANT'ANA, 2016), conforme Figura 1.

Figura 1 - Ciclo de Vida dos Dados para a Ciência da Informação



Fonte: Sant'Ana (2016, p. 123)

Dentre essas fases, apresentadas na Figura 1, a coleta de dados pode se tornar imperceptível e ocasionar quebras de privacidade dos sujeitos que são agentes alvos de processos de coleta. Para Tanenbaum e Wetherall (2011) o rápido crescimento tecnológico fez com que as diferenças entre as fases de coleta, armazenamento e processamento desaparecessem rapidamente, tornando as questões ocorridas nesse processo intangíveis e abstraídas para o usuário.

A abstração no âmbito do uso das tecnologias da informação é fundamental para minimizar a complexidade resultante da interação do usuário com os ambientes digitais, e a sua finalidade é omitir certos detalhes desse processo, uma vez que, abstração eficiente é aquela que realça detalhes que são importantes para o usuário, omitindo os que são insignificantes para a interação (KORTH; SILBERSCHATZ, 1993; SCLAVOS; SIMONI; ZNATY, 1994).

Para O'hara e Shadbolt (2014) cada vez que emerge uma nova tecnologia que permite que o usuário interaja com o ambiente digital sem a necessidade de presença física, cria-se uma nova abstração, pois, quando não existe a presença física, o indivíduo deixa suas representações

(dados) nesse ambiente, tornando impossível esconder suas ações e, consequentemente, não tendo a percepção de quais dados estão sendo coletados.

Em relação à coleta de dados nos ambientes digitais a abstração se efetua apenas para o usuário, ao contrário do detentor de dados[1] que pode possuir conhecimento do resultado de todas as interações usuário-ambiente digital.

Ao abordar sobre tecnologias da inteligência, Lévy (1993) define abstração no contexto de suas relações com as tecnologias intelectuais, e exemplifica que a representação da situação por meio de tabelas, quadros, mapas ou diagramas visam simbolizar dados complexos e numerosos, difíceis de serem compreendidos em informação imediatamente perceptível. Assim, "[...] é abstrato todo o problema fora de nossas capacidades de manipulação e de reconhecimento imediato" (LÉVY, 1993, p. 159).

No entanto, a abstração torna mais difícil o conhecimento sobre os elementos presentes na fase de coleta de dados e a ação dos detentores de dados com fruto da interação usuário-ambiente digital, assim, o usuário pode não possui consciência sobre esse processo. Consciência que pode ser definida como "[...] capacidade humana para conhecer, para saber que conhece e para saber o que sabe que conhece. A consciência é um conhecimento (das coisas e de si) e um conhecimento desse conhecimento (reflexão)" (CHAUÍ, 1995, p. 147).

Neste trabalho, adota-se o conceito de consciência atrelada à "situação de consciência", que é definida como saber o que está acontecendo, ou mais precisamente, a "[...] percepção dos elementos no ambiente dentro de um volume de tempo e espaço, a compreensão de seu significado e a projeção de seus status no futuro próximo[2]" (ENDSLEY, 1988, p. 97, tradução nossa).

O usuário passar a ter consciência da coleta de dados a partir do momento que ele identifica quais dados estão sendo coletados e distingue os dados que ele mesmo transmite e aqueles que são coletados pelo ambiente digital ou pelo dispositivo tecnológico. A percepção da coleta deve estar vinculada a "quando" essa coleta acontece e em qual "lugar" do ambiente a coleta está sendo realizada, compreendendo a "justificativa" e o que "será" realizado com esses dados. A partir do momento em que o usuário compreender claramente os elementos que estão envolvidos nessa atividade, esse contexto deixa de ser abstrato para tornar-se perceptível. Para Lévy (1993, p. 159), "[...] um problema que permanecesse abstrato seria simplesmente insolúvel".

---

[1] Aquele que detém os dados e gerencia dados.

[2] "[...] *the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future*".

Quando o usuário não perpassa por essas fases, ele se torna insciente sobre a coleta de dados e, consequentemente, isso impacta na possibilidade de controlar as questões vinculadas a essa atividade, principalmente no que tange a proteção da privacidade. Segundo Vygotsky (1995), para que seja possível controlar uma atividade é preciso ter consciência sobre ela.

Neste trabalho adota-se o termo insciente como a falta de conhecimento, percepção ou consciência sobre os elementos envolvidos no processo de coleta de dados durante a interação do usuário com o ambiente digital, nessa interação o usuário é sujeito alvo da coleta realizada pelos detentores de dados.

As representações (dados) deixadas no ambiente digital, fruto das atividades de coleta de dados e da interação usuário-ambiente digital resulta na informação vinculada a um indivíduo, que pode ser composta pelos dados provenientes de seus atos, consumos, cadastros e opiniões, que contribuem para o conhecimento do sujeito, inclusive para a descoberta de seus dados sensíveis. Esse cenário implica tanto em ameaças à privacidade, quanto conduz a ampliação da assimetria de informação[3] entre detentores de dados e os sujeitos que utilizam de ambientes digitais. Mason (1986) chama esse cenário de exposição por descrição minuciosa, que é fruto da coleta de "nós mesmos" com o uso do conector "e", relatado na seguinte situação:

> Posso autorizar uma instituição a coletar informações "A" sobre mim e outra instituição a coletar informações "B" sobre mim; mas eu não quero que ninguém possua "A" e "B" sobre mim ao mesmo tempo. Quando "C" é adicionado à lista de conjunções, o dono da nova informação saberá ainda mais sobre mim. E então "D" é adicionado e assim por diante. Cada atributo que vai adicionando na minha tecelagem revela cada vez mais sobre mim. No processo, o tecido criado é uma ameaça à minha privacidade (MASON, 1986, p. 2, tradução nossa)[4].

O conhecimento obtido por meio da coleta de dados pode ser visto na matéria *online* da revista Vogue, na qual Read (2017) aborda que os dados coletados pelos aplicativos de namoro são muito maiores do que as informações listadas no perfil do usuário. Read (2017) relata a história da jornalista Judith Duportail da *Guardian* que, ao solicitar ao Tinder[5] os dados que eles possuíam sobre ela na sua conta, obteve um relatório de 800 páginas, contendo dados referentes à suas preferências, datas, lugares e comportamentos, dados que faziam parte da sua

[3] Conceito baseado na teoria da informação assimétrica desenvolvida por Akerlof (1970), que analisa o mercado de carros usados e as implicações de informações assimétricas, nas quais o vendedor de um bem sabe mais do que o comprador em relação à qualidade desse produto.

[4] "*I may authorize one institution to collect information "A" about me, and another institution to collect information "B" about me; but I might not want anyone to possess "A and B" about me at the same time. When "C" is added to the list of conjunctions, the possessor of the new information will know even more about me. And then "D" is added and so forth. Each additional weaving together of my attributes reveals more and more about me. In the process, the fabric that is created poses a threat to my privacy*".

[5] Aplicativo que por meio de dados de localização permite encontros entre pessoais.

interação com o aplicativo, mas que ela não havia percebido tê-los transmitido para o aplicativo, além da presença das suas fotos do *Instagram* (mesmo depois de ela ter excluído sua conta), suas preferências do *Facebook* e os locais físicos onde esteve durante as conversas no aplicativo.

Como proferido no provérbio de Salomão, capítulo 17, versículo 27, "Quem retém as palavras tem saber" (PROVÉRBIOS, 1999). Correlacionando essa afirmação aos ambientes digitais e à coleta de dados de usuários, compreende-se que quem armazena os dados tem saber e, consequentemente, o poder de ação com esses dados. Os dados, portanto, representam valor e poder comercial para muitas organizações que os detêm.

Para Mason (1986) uma ameaça à privacidade dos indivíduos tem sido o valor que os dados têm apresentado na tomada de decisões, pois cada vez mais os dados se tornam valiosos para o meio comercial. Em relação ao poder, o sociólogo francês Vance Packard (1967) alarma a respeito do apoderamento de dados pessoais. Para o autor,

> [...] o maior perigo em um banco de dados centralizado seria a possibilidade de colocar um poder tão grande nas mãos de pessoas que podem apertar alguns botões de computadores. Quando os detalhes de nossas vidas são armazenados em um computador central ou em outros grandes sistemas de armazenamentos, todos nós nos sujeitamos, de certa forma, ao controle exercido pelos operadores destas máquinas[6] (PACKARD, 1967, p. 40, tradução nossa).

Destarte, os dados pessoais representam muito dinheiro para os anunciantes, pois, com posse desses dados, os detentores podem segmentar consumidores e utilizar para estratégias de marketing e outros fins. Por outro lado, caso um *site* que coleta dados do usuário seja invadido por um *hacker*, também estaria disponível a terceiros, havendo indesejáveis novas quebras de privacidade (READ, 2017).

No livro "*The hidden persuaders",* de Vance Packard (1982), já era descrito como as estratégias de marketing eram moldadas de acordo com o comportamento do usuário:

> Muitos de nós estamos sendo influenciados e manipulados – muito mais do que percebemos – nos padrões de nossas vidas cotidianas. Estão sendo feitos esforços em larga escala, muitas vezes com sucesso impressionante, para canalizar nossos hábitos não pensativos, nossas decisões de compra e nossos processos de pensamento pelo uso de *insights* extraídos da psiquiatria e das ciências sociais. Normalmente, esses esforços ocorrem sob o nosso nível de

[6] "*The most disquieting hazard in a central data bank would be the placing of so much power in the hands of the people in a position to push computer buttons. When the details of our lives are fed into a central computer or other vast file-keeping systems, we all fall under the control of the machine's managers to some extent*".

> consciência; de modo que os recursos que nos movem sejam muitas vezes, em certo sentido, "escondido" [7] (PACKARD, 1982, p. 11, tradução nossa).

Nesse cenário, a Internet tem sido facilitadora no processo de coleta e retenção de grandes quantidades de dados sobre indivíduos, e por meio de metadados[8] é possível obter de seus usuários dados de localização, navegação, contatos, comunicações ou hábitos de compras *online*, possibilitando aos detentores de dados obterem conhecimento que vai além do conteúdo semântico presente nas comunicações (KURBALIJA, 2016).

Para Schuster et al. (2017), embora os metadados não revelem o conteúdo de uma mensagem ou coleta, sua combinação e análise podem revelar informações extraordinárias sobre a coleta de dados e sobre o titular desses dados. Esses dados são aqueles que podem estar mais distantes da percepção do usuário durante a fase de coleta de dados nos ambientes digitais.

Desta forma, o usuário pode ser insciente sobre a coleta desses metadados quando interage com ambientes digitais, insciência que pode refletir nas atitudes e ações para controlar seus dados, acentuando os danos à privacidade, e ainda, sem o conhecimento do usuário sobre esses danos.

Essa situação pode ser vista na coleta realizada pelos carros do *Street View* da *Google* entre os anos 2008 a 2010, que ilegalmente coletou dados das redes *wi-fi* ao andar pelas ruas de cidades, atividade que a empresa alegou não ter sido proposital. No entanto, a quebra de privacidade ocorreu não apenas pelas fotos de ruas e casas que o serviço da *Google Street View* coletou, mas pelos dados de redes sem fio que estavam ao alcance dos veículos, de onde foi coletado um conjunto de dados pessoais tais como: e-mails, senhas, fotos e protocolos de bate papo. Ressalta-se que essa atividade realizada pelo *Google* ocorreu sem o conhecimento e consentimento do usuário.

A própria *Google* confirmou que seus carros coletavam dados de conteúdo de conexão *Wi-fi* não criptografadas, dentre os dados coletados havia uma grande quantidade de dados pessoais. Após esses fatos serem revelados, o Ministério Público de Hamburgo iniciou investigações e aplicou multa ao *Google* de 145 mil euros por coletar dados por meio do *Street*

---

[7] "*The way many of us are being influenced and manipulated – far more than we realize – in the patterns of our everyday lives. Large-scale efforts are being made, often with impressive success, to channel our unthinking habits, our purchasing decisions, and our thought processes by the use of insights gleaned from psychiatry and the social sciences. Typically these efforts take place beneath our level of awareness; so that the appeals which move us are often, in a sense, 'hidden'*".

[8] Um conjunto de dados - atributos - referenciais, metodologicamente estruturados e codificados, conforme padrões internacionais, para localizar, identificar e recuperar pontos informacionais de textos, documentos e imagens disponíveis em meios digitais ou em outros meios convencionais (ALVES; SANTOS, 2013, p. 40).

View. Esse foi um dos casos mais sérios de violação dos regulamentos de proteção de dados pessoais (RIGG, 2013).

Caso similar também aconteceu no Brasil, pois a empresa *Google*, por meio do *Street View*, coletou indevidamente dados sigilosos de cidadãos pelas ruas de cidades, o que fez com que 23ª Vara Cível de Brasília solicitasse que a empresa justificasse a coleta de dados realizada. No entanto, a *Google* não autorizou acesso aos equipamentos e aos dados coletados (ALECRIM, 2013).

A revelação de informações por meio de metadados também está presente nos recursos imagéticos. Affonso e Sant'Ana (2015) evidenciaram metadados de imagem digital que podem revelar informações sensíveis do indivíduo, e metadados que quando combinados com outros dados tornam possível a identificação do titular dos dados ou do sujeito referenciado na imagem. Ainda que a imagem em si nem sempre seja uma ameaça à privacidade, ressalta-se que os metadados que ela carrega podem potencializar brechas de privacidade.

O reflexo da coleta de dados e as consequências para os indivíduos referenciados nos dados podem ser retratados no caso da Equifax[9], que em setembro de 2017 anunciou a violação de privacidade ocorrida entre meados de maio e julho do mesmo ano, que implicou na quebra de privacidade por meio de roubo de dados pessoais de aproximadamente 143 milhões de americanos. Os cibercriminosos acessaram nomes de pessoas, números de segurança social[10], datas de nascimento, endereços e, em alguns casos, números de licenças de motoristas. Eles também roubaram números de cartões de crédito de mais ou menos 209 mil pessoas, incluindo dados de identificação pessoal de cerca de 180 mil clientes dos Estados Unidos envolvidos em relatórios de créditos, e ainda, dados pessoais de cidadãos do Reino Unido e do Canadá (GRESSIN, 2017; O'BRIEN, 2017).

Johnson (2017) ressalta que a preocupação principal na violação de dados da Equifax foi o roubo de dados de adultos. Apesar disso, não foram especificados quantos dos afetados eram menores de idade, uma vez que, dados pessoais de crianças se tornam itens valiosos para ladrões de dados, pois o número de segurança social não apresenta dívidas de cartão de crédito ou empréstimos. McGee (2017) alerta que embora essa violação de dados esteja entre as mais agravantes, devido ao alcance e ao tipo de informação exposta ao público, como dados

[9] Serviço de proteção ao crédito dos Estados Unidos, considerada uma das três maiores *bureau* de crédito americano.

[10] Nos Estados Unidos esse número tem o objetivo de rastrear indivíduos para fins de Previdência Social, no entanto, tornou-se um número para identificação do cidadão utilizado para diversos fins.

sensíveis, os cidadãos americanos não parecem estar cientes sobre as consequências da violação de dados e quebras de privacidade.

No início de setembro de 2017, o *Instagram* também alertou seus usuários que, devido uma falha de segurança em seus sistemas, *hackers* poderiam ter tido acesso aos dados pessoais de seus usuários. A consequência dessa violação é a venda de dados do usuário, tais como e-mail e número de telefones pertencentes às contas de usuário do *Instagram*, e que por meio desses dados é possível obter conhecimento valioso sobre um indivíduo (LARSON, 2017).

Considerada a maior violação de dados da história, o *Yahoo* emerge em seguidas declarações de violações de dados. Em setembro de 2016, a empresa confirmou que os dados associados a aproximadamente 500 milhões de contas de usuários foram roubados, violação que ocorreu no final de 2013. Segundo o *Yahoo*, dentre os dados coletados estão: nomes, endereços de e-mail, números de telefones, datas de nascimento e, em alguns casos, perguntas e respostas de segurança usados na autenticação de e-mail (FIEGERMAN, 2016a). Três meses depois, a empresa descobriu uma segunda infração, revelando que a invasão afetou mais de um bilhão de contas de clientes (FIEGERMAN, 2016b). Em 2017, a *Verizon*, que comprou o Yahoo em junho, revelou que a violação de contas do Yahoo foi três vezes maior do que fora divulgado, totalizando três bilhões de contas violadas (MULLEN; FIEGERMAN, 2017).

Como consequência da coleta de dados pessoais, outras empresas famosas estão na lista das que sofreram violações de privacidade, tais como: *Myspace*, que em 2016 confirmou a violação dos nomes de usuários de, aproximadamente, 360 milhões de contas; *Linkedln*, que teve, em 2012, seus dados hackeados, resultando em mais 100 milhões de dados de usuário afetados; *Target*, que em 2013 teve, aproximadamente, 40 milhões de dados de seus clientes violados, dentre eles dados de cartões de crédito e de débito (FIEGERMAN, 2016b).

As violações não estão presentes apenas nas empresas privadas, instituições governamentais também aparecem envolvidas em quebras de privacidade. Em 2014, Snowden, um analista de sistema, ex-contratado da Agência de Segurança Nacional dos Estados Unidos (*National Security Agency* - NSA), ao fazer delações a respeito de coleta de dados e de vigilância em massa, revelou que a NSA e o *Federal Bureau of Investigation* (FBI) estariam recebendo informações de nove empresas americanas que possuem aplicações na Internet sobre as comunicações de usuários da Web em países de todo o mundo (POLICARPO; BRENNAND, 2017). Essa coleta se dava por meio de um portal e pelo programa secreto PRISM. Esse programa sigiloso permitiu que a NSA coletasse dados diretamente dos servidores de grandes empresas, tais como *Google, Facebook, Yahoo, Microsoft, Apple*, entre outras (POLICARPO; BRENNAND, 2017).

Nessas revelações do caso Snowden, observa-se que ao coletar dados dessas empresas, a vigilância governamental amplia-se para o contexto do cidadão comum, público extremamente participante das aplicações providas por empresas, tais como, *Google, Facebook* e *Yahoo*, uma vez que, notoriamente, essa coleta por agências governamentais não é explícita e perceptível para o usuário.

Para Policarpo e Brennand (2017), as revelações de Snowden promoveram repercussões importantes que implicam em discussões e desdobramentos políticos, sociais, econômicos e jurídicos, e que necessita de "[...] adequação do Direto às inovações aportadas pelas constantes inovações tecnológicas" (POLICARPO; BRENNAND, 2017, p. 270).

Essas violações são alguns exemplos que relatam a implicação da coleta de dados e as ameaças à privacidade, destacando o usuário em uma posição desprivilegiada e insciente sobre a coleta e o que será feito com seus dados, incluindo as consequências de uso por terceiros, fatores que impactam diretamente no comportamento do usuário em relação a essa situação.

Bauman (2011) compara o comportamento dos nossos ancestrais com a sociedade atual ao defender a esfera privada. Para o autor, o ser humano era incentivado a vigiar e a partir para o combate para defender o domínio privado em relação à intromissão indevida pelos detentores do poder. Hoje, há a inversão de hábitos e de valores, pois os indivíduos perderam boa parte da coragem, energia e vontade de ir à defesa da esfera privada (BAUMAN, 2011). A insciência, considerada neste trabalho como a falta de conhecimento sobre a fase de coleta de dados, pode colaborar para que não exista o comportamento de defesa ao direito de privacidade.

> Por esse motivo, 'a intenção de esconder … é muito mais forte quando se choca com a intenção de revelar'. Se essa 'maior intensidade' não se manifesta, se não há o desejo de defender com unhas e dentes um tema sigiloso contra os bisbilhoteiros, intrusos e importunos, ou não é respeitada, a privacidade corre perigo (BAUMANN, 2011, p. 40).

A justificativa para a coleta de dados nos mais diversos ambientes digitais, tais como mecanismos de busca, redes sociais, plataformas de comércio eletrônico ou aplicativos móveis é a de oferecer melhores resultados para o usuário durante sua interação com os ambientes digitais.

> Coletamos informações para fornecer serviços melhores a todos os nossos usuários, desde descobrir coisas básicas, como o idioma que eles falam, até coisas mais complexas, como anúncios que o usuário pode considerar mais úteis, as pessoas on-line que são mais importantes para o usuário ou os vídeos do *YouTube* dos quais o usuário poderá gostar (GOOGLE, 201-).

Similarmente, em sua política de privacidade, a rede social *Facebook* descreve que realiza coleta de dados referente às atividades dos usuários e às informações disponibilizadas por eles quando utilizam de seus serviços, incluindo informações presentes no conteúdo, tipo de conteúdo visualizado, dados sobre pessoas e grupos com os quais se conectam; além de interações e informações de: pagamento, dispositivo, *sites* e de aplicativos que utilizam serviços do *Facebook*, bem como informações de parceiros externos e de empresas dessa rede social (FACEBOOK, 201-).

Desta forma, o benefício proporcionado pelos ambientes digitais determina a justificativa para coleta de dados e, consequentemente, sobrepõe as questões de privacidade. Para Woo (2006), os usuários acabam por desistir voluntariamente do seu direito à privacidade em troca dos privilégios providos pelos ambientes digitais, que em troca do serviço exige dados do usuário. Assim, pode ser uma decisão do usuário permitir a coleta dos dados; no entanto, prevalece a relação custo-benefício quando o usuário está inserido nesse contexto.

> O problema passa a ser, então, a troca de dados pelo privilégio de acesso a *websites*. A maioria das pessoas abre mão de seus direitos à privacidade para ter condições de usar a Internet. Uma vez que se renunciou a esse direito à proteção da privacidade, os dados pessoais tornam-se propriedade legítima das firmas de Internet e de seus clientes (CASTELLS, 2003 p. 143).

A dicotomia consciência e atitude podem incidir nas questões relacionadas à privacidade, pois a consciência induz a se preocupar com ameaças à privacidade dos dados, embora o usuário possa se comportar de maneira diferente dependendo do contexto (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015). Essa situação é denominada de paradoxo de privacidade (NORBERG; HORNE; HORNE, 2007), marcada pela contradição entre as intenções do usuário em relação à privacidade (na divulgação de seus dados pessoais) e o comportamento real assumido por ele.

Em relação à coleta realizada pelos mecanismos de busca, Affonso et al. (2017) ressaltam que a consciência do usuário está associada aos dados que ele mesmo envia para o ambiente. No entanto, uma coleta silenciosa pode ocorrer sem o usuário tenha ciência, e para que esse usuário se torne menos insciente sobre o processo, é necessária a leitura e a interpretação das políticas de privacidade.

Os ambientes digitais disponibilizam políticas de privacidade com a intenção de proporcionar aos usuários informações sobre a coleta de dados, podendo ampliar a sua consciência sobre o processo. No entanto, a percepção do usuário sobre a coleta de dados pode estar vinculada à descrição que a empresa disponibiliza nas políticas de privacidade ou nos

dados que o usuário, cientemente, disponibiliza durante a utilização do serviço, como nome de usuário, senhas, preenchimentos de campos de cadastros, termos de busca, entre outros (AFFONSO; SANT'ANA, 2018, no prelo).

> [...] a consciência quanto à coleta de dados envolve o conhecimento que o usuário tem sobre a forma e como seus dados serão coletados, pois o objetivo das políticas de privacidade deveria ser a de sanar, de modo claro e evidente, insciências sobre a coleta de dados, de forma a ampliar a percepção do usuário em relação a esse processo (AFFONSO; SANT'ANA, 2018, no prelo)[11].

Assim, pode-se considerar que assumir um posicionamento em relação à coleta de dados é fruto da consciência que os indivíduos têm a respeito desse momento. Para Kurbalija (2016) os usuários devem ter consciência sobre como seus dados pessoais serão usados pelos detentores, fato que deve ocorrer sem que haja a indisponibilidade do serviço ou aplicação caso esse usuário não aceite a coleta de dados, ou apresente dúvidas sobre como seus dados pessoais serão utilizados.

Nesse contexto, permeado pelas questões de insciência do usuário sobre a coleta de dados por detentores, as possíveis ameaças à privacidade e à necessidade de proteção de dados pessoais, apresentam-se, a seguir, o problema, a tese, a hipótese, os objetivos, a justificativa, a delimitação do tema e a metodologia desta pesquisa.

1.1 Problema de pesquisa

A intensa coleta de dados nos ambientes digitais, cuja justificativa pelos detentores de dados é prover melhores serviços para o usuário, resulta em um maior conhecimento sobre os sujeitos alvos de coleta e, indubitavelmente, leva a quebra de privacidade desses usuários ao interagir com o ambiente digital.

A coleta de dados se torna tão tênue e com detalhes técnicos totalmente abstraídos para os usuários, que os transformam em atores inscientes em relação aos elementos envolvidos nesse processo, de forma a não distinguir a figura do detentor como o primeiro a violar sua privacidade.

> Mais graves e traiçoeiros que as formas clássicas de invasão, os atuais mecanismos de intromissão podem ser dirigidos por controle remoto e **sem conhecimento** da pessoa que é atingida. A informação e os dados podem ser extraídos sem que a lesão cause uma deformidade aparente ou determine um confronto entre o agressor e a vítima (DOTTI, 1982, p. 36, grifo nosso).

[11] [...] *awareness about data collection involves the user's knowledge about how their data will be collected. The purposes of privacy policies should be to make information about data collection more clear and accessible and to broaden the user's perception of this process*.

A falta de conhecimento sobre a coleta de dados surge em algumas abordagens: Pereira (2003) argumenta que o fornecimento de dados pelos usuários pode ser facilitado por ele próprio, mas também parte desses dados pode ser coletada nas redes de computadores de forma dissimulada, isto é, sem que seus titulares estejam conscientes de tal atividade. Fairfield (2005) também afirma que atividades realizadas por meio das tecnologias farão com que as pessoas não saibam o que está acontecendo com seus dados. A *World Wide Web Consortium* (W3C) (2015) ao abordar sobre *fingerprinting*[12] relata que o usuário não tem consciência sobre a coleta de dados quando interage com ambientes digitais.

Da mesma forma, Machado e Bioni (2016, p. 352, grifo nosso) ao explorarem sobre a coleta de dados por programas sociais, especificamente o nota-fiscal paulista, afirmam que "é espantoso notar que o armazenamento, a transmissão, o processamento e o cruzamento dessas informações geram um fluxo de informação totalmente **opaco** ao cidadão". Abade e Alves (2017) ao indagarem se os usuários fornecem seus dados para acessar serviços *online* e redes sociais, tiveram como resultado uma quantidade considerável de usuários que acreditam que 'não' fornecem dados para portais de serviços, tal como o *Google*, e ainda, que desconhecem os termos de uso e a principais leis que amparam a proteção de dados pessoais.

Na Ação Civil Pública, julgada em 27/04/2018 pela 9ª Vara Cível Federal de São Paulo, o ministério público ao versar sobre a coleta de dados realizada pelo Windows 10, afirma que o fato da opção para a coleta de dados já estar marcada como padrão durante a instalação do Windows 10, se torna mais fácil, pois basta o usuário clicar e instalar, sem ter que ficar lendo e habilitando preferências. No entanto, ressalta que, "imperioso lembrar que alguns usuários poderão nem mesmo **identificar as consequências das suas escolhas**" (BRASIL, 2018c, p. 3, grifo nosso), ainda o autor da ação menciona que:

> A desativação dessa coleta de dados, apesar de ser parcialmente possível, é tarefa complexa e trabalhosa, e, certamente, usuários domésticos que não possuem familiaridade em customizar aplicativos (ou seja, a esmagadora maioria das pessoas) terão dificuldades para impedir o envio dos seus dados e, conforme esclareceu a Assessoria Técnica do Ministério Público Federal em São Paulo (Informação Técnica de fls. 06/10), último parágrafo de fl. 09, os consumidores/usuários, na maioria das vezes, **desconhecem o real impacto desta falta de privacidade** [...] a coleta de dados pelo Windows 10 é informação de suma importância, que deve ser pronta e claramente percebida pelo consumidor [...] (BRASIL, 2018c, p. 3, grifo nosso).

[12] Meio de rastreamento digital, tal como o *fingerprinting* de navegador Web, que consiste na coleta de dados e configurações do navegador e do sistema de um usuário quando este visita um site (LAPERDRIX; RUDAMETKIN; BAUDRY, 2016).

Desta forma, a insciência do usuário, enquanto alvo de fases de coleta de dados, sobre a ação dos detentores desses dados coletados, pode ser fator importante na precarização de seu direito à privacidade, e pode ser potencializada por características inerentes aos ambientes digitais ao encapsular complexidade em camadas de abstração, incluindo a falta de foco e especificidade nas questões vinculadas a coleta de dados.

1.2 Tese

Existem fatores que contribuem para um cenário que propicia insciência do usuário na fase de coleta de dados nos ambientes digitais, insciência esta que pode ter impactos em questões importantes como a da privacidade.

1.3 Hipótese

Este trabalho levanta a seguinte hipótese: O cenário que favorece a insciência do usuário na fase de coleta de dados pode ser determinado pelos seguintes fatores:

a) Carência de pesquisas sobre proteção de dados pessoais na fase de coleta de dados

Presume-se que o meio acadêmico, ao abordar questões de privacidade em relação à proteção de dados pessoais, tem concentrado esforços em pesquisas que visam proteger a privacidade do indivíduo no âmbito da disponibilização de dados por parte das organizações, a fim de permitir o compartilhamento e reuso de dados pela sociedade e diversas áreas do conhecimento. Então, no que tange a coleta de dados, acredita-se que exista uma carência de pesquisas nessa fase, o que pode implicar no desenvolvimento de medidas para proteção de dados, incluindo a disseminação de informações sobre as ameaças da coleta realizada pelo detentor, sujeito que muitas vezes passa despercebido pelo usuário em relação à violação de sua privacidade, seja o usuário alvo de coleta ou referenciado no conjunto de dados.

Sweeney (2002), ao iniciar o artigo que tem sido base para diversas pesquisas[13] na área de proteção de dados pessoais, intitulado "*k-anonymity: a model for protecting privacy"*, faz a seguinte reflexão:

> Os detentores de dados, operando de forma autônoma e com conhecimento limitado, tem dificuldades de **liberar informações** que não comprometem a privacidade, confidencialidade ou interesses nacionais. [...] a sobrevivência do banco de dados depende da capacidade do titular de dados em produzir dados anônimos, pois não liberar essas informações pode diminuir a necessidade dos

[13] Até o presente momento o *Google Scholar* traz que esse artigo foi citado por 4.855 trabalhos.

> dados, enquanto por outro lado, a falta de proteção adequada pode criar circunstâncias que prejudicam os indivíduos (SWEENEY, 2002, p. 4, tradução nossa, grifo nosso)[14].

A preocupação da autora é criar meios que impeçam a identificação do indivíduo em uma base de dados publicada. O k-anonimato tem sido base para diversos modelos para proteção de dados pessoais, tais como o *l-diversity* (MACHANAVAJJHALA et al., 2006) e *t-closeness* (LI; LI; VENKATASUBRAMANIAN, 2007). Além desses modelos, emerge a privacidade diferencial (DWORK, 2008), proposta que visa garantir a privacidade dos sujeitos referenciados nos conjuntos de dados para uma possível disponibilização.

Para Martínez, Sánchez e Valls (2013), o objetivo dos métodos de proteção da privacidade é evitar a reidentificação de indivíduos a partir dos dados publicados. Vários métodos de controle de divulgação para mascarar dados publicados foram desenvolvidos, e por meio de métodos para verificar os riscos de divulgação é possível mensurar a capacidade de um atacante vincular os registros do conjunto de dados que recebeu operações de anonimização. A anonimização é definida no Art. 5, inciso XII do Projeto de Lei 5.276 de proteção de dados pessoais como "[...] qualquer procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (BRASIL, 2016a).

Destarte, se existe carência de pesquisas sobre privacidade no momento da coleta, então, esse fator pode configurar o contexto que leva a insciência dos usuários e impactar no desenvolvimento de novas aplicações e técnicas para minimizar quebras de privacidade. Cenário que também pode implicar no desenvolvimento de novas leis e políticas de informação.

b) Generalização dos aspectos de coleta de dados em legislações

Acredita-se que legislações tendem a ser genéricas ao tratar a coleta de dados pessoais, especificamente no que tange a detalhes técnicos computacionais, uma vez que, a existência de leis específicas para proteção de dados pessoais se torna essencial para promover atitudes que visam garantir a privacidade de sujeitos alvos de coleta ou referenciados em conjunto de dados. Ao exigir essas atitudes colabora-se para minimizar a insciência do usuário sobre a fase de coleta de dados.

[14] "*Data holders, operating autonomously and with limited knowledge, are left with the difficulty of releasing information that does not compromise privacy, confidentiality or national interests. In many cases the survival of the database itself depends on the data holder's ability to produce anonymous data because not releasing such information at all may diminish the need for the data, while on the other hand, failing to provide proper protection within a release may create circumstances that harm the public or others*".

c) Abstração na fase de coleta de dados, promovida pela própria interface das redes de computadores e pela falta de clareza das políticas de privacidade

Pressupõe-se que as características inerentes dos ambientes digitais contribuem para enredar a percepção do usuário sobre a coleta de dados, impactando diretamente na consciência sobre esse processo e atitudes na busca pelo seu direito a privacidade, pois mesmo quando os ambientes relatam em suas políticas de privacidade informações sobre a coleta, os detalhes dos metadados de comunicação podem não estarem explícitos e claros para o usuário.

1.4 Objetivo geral

Caracterizar o contexto que favorece a insciência do usuário enquanto alvo de fases de coleta de dados em ambientes digitais, considerando implicações de privacidade.

1.5 Objetivos específicos

- ✓ Contextualizar os aspectos envolvidos na proteção de dados pessoais, tais como as definições de privacidade, os modelos e as técnicas no âmbito da anonimização;
- ✓ Verificar como a proteção de dados pessoais, por meio de anonimização, tem sido abordada na fase de coleta de dados pelas pesquisas científicas;
- ✓ Identificar a legislação que versa sobre proteção de dados pessoais no Brasil e as principais leis e princípios internacionais, enfatizando a abordagem dada à coleta de dados pessoais;
- ✓ Explicitar os possíveis dados coletados por ambientes digitais, indicando ameaças à privacidade no âmbito da coleta de dados;
- ✓ Descrever o processo de coleta de dados mediante análise de dados de tráfego resultante da interação do usuário com o ambiente digital, descrevendo os níveis de abstração e as possíveis ameaças à privacidade.

1.6 Motivação e justificativa

A motivação da autora deste trabalho para investigar acerca de privacidade e especificamente em relação à insciência do usuário surgiu durante suas pesquisas no decorrer do doutorado (AFFONSO; SANT'ANA, 2015; AFFONSO; OLIVEIRA; SANT'ANA, 2017; AFFONSO; SANT'ANA, 2017).

Nessas pesquisas foram averiguados aspectos de privacidade no domínio da recuperação de dados, e notou-se que muitos métodos de proteção de privacidade são desenvolvidos e aplicados com foco na fase de recuperação de dados, fato que instigou a verificar como essas

medidas tem se efetuado na fase de coleta. Outra observação foi em relação à falta de clareza nas políticas de privacidade disponibilizadas pelos ambientes digitais, que podem conduzir o usuário a insciência sobre a coleta de dados. Essas políticas de privacidade são muitas vezes descritas para atender a vários serviços, tornando-as subjetivas, visto que, ações que poderiam colaborar para o usuário compreender melhor essa fase, se tornam revelações omissas (AFFONSO et al, 2017). Notou-se também uma coleta de dados além do necessário para o uso do serviço quando o usuário utiliza de aplicativos móveis (AFFONSO; MONTEIRO; CAMARGO, 2016) e, que políticas de privacidade não estão presentes em muitos aplicativos, ampliando a insciência do usuário sobre os dados coletados (AFFONSO, MONTEIRO; SANT'ANA, no prelo).

Esses relatos conduziram ao desenvolvimento da pesquisa sobre dados que são coletados de forma explícita e de forma implícita quando o usuário interage com ambientes digitais (AFFONSO; SANT'ANA, 2018, no prelo), o que levou a pesquisadora a investigar o cenário que propicia a insciência do usuário, buscando amparo nas pesquisas acadêmicas, no ordenamento jurídico e na interação com uso de aplicações no ambiente Web.

É notório que as questões vinculadas à privacidade se tornam extremamente relevantes em um cenário onde a coleta de dados tem se tornado presente nas mais diversas atividades dos indivíduos, cuja razão está vinculada ao oferecimento de melhores serviços, resultando em usuários cativados com os benefícios proporcionados pelas tecnologias. Os dados se tornam moeda de troca entre usuários-detentores; no entanto, o volume de conhecimento gerado nesses detentores se torna mais valioso do que qualquer serviço por ele ofertado.

A opacidade estabelecida no processo de coleta de dados faz com que o usuário se limite a identificar o papel do detentor de dados, que não é visto como um atacante ou um ator que irá se beneficiar com o acesso aos dados. Assim, as ameaças aos dados pessoais não estão apenas na disponibilização desses para a sociedade, mas o próprio detentor passa a ter o apoderamento dessa coleta, caracterizando a quebra de privacidade. Quando detentor passa a ter posse dos dados, o usuário transfere para ele o controle e a confiança de que sejam aplicadas medidas de segurança ao coletar os mais diversos tipos de dados.

Entretanto, o usuário pode não ter consciência sobre a coleta e as consequências derivadas dela quando interage com aplicações na Internet, isso pode ser comprovado pelos fatos ocorridos recentemente, dentre eles, a coleta de dados no *Facebook.*

A rede social foi alvo de escândalos devido alegações que a *Cambridge Analytica*[15] coletou e usou dados de 50 milhões de perfis de usuários do *Facebook*, para atingir os eleitores nas eleições dos Estados Unidos em 2016. A *Cambridge Analytica* que trabalhou com a equipe de eleição de Donald Trump foi acusada de realizar análise com os dados coletados de perfis de usuários para prever e influenciar a escolha do presidente dos Estados Unidos, a fim de direcioná-los para anúncios políticos personalizados, principalmente os eleitores que estavam indecisos em relação ao candidato (CADWALLADR; GRAHAM-HARRISON, 2018). Evidentemente, a maioria dos usuários da rede social não imaginou que seus dados estavam sendo objeto de análise para ser usado na formação de sua própria opinião.

Outra situação de relevo que remete a insciência de usuário quando se trata de coleta de dados, é um julgado do Tribunal de Justiça de São Paulo (TJSP), na qual se observa o posicionamento do relator ao explanar sobre a coleta de dados pelo *Facebook*. O referente processo teve como solicitação por parte da agravante, que o *Facebook* fornecesse o código *International Mobile Equipment Identity* (IMEI) de usuários que proferiram ofensas a sua pessoa na rede social *Facebook*. Ao defender sua tese, o relator afirma que os dados coletados pela rede social são apenas os exigidos no cadastro do usuário, não sendo possível disponibilizar esse dado para a agravante. No entanto, o fato do dado não ser coletado durante o cadastro não significa que não existe uma coleta sendo realizada de forma silenciosa para o usuário.

> Ementa: Internet. Publicações ofensivas no Facebook. Decisão agravada que determinou o fornecimento do código IMEI dos usuários que proferiram as ofensas. Impossibilidade. O provedor dos *sites* não está obrigado a fornecer dados pessoais dos usuários que **sequer são exigidos no momento do cadastro**, inexistindo provas de que esses dados são armazenados pelo Facebook. Fornecimento do IP dos usuários que é suficiente para sua identificação. Jurisprudência deste E. TJSP. Decisão reformada para afastar a obrigatoriedade de fornecimento do IMEI. Recurso provido (BRASIL, 2016c, grifo nosso).

Esse cenário de falta de percepção sobre o processo de coleta de dados pode também ser explicitado pelo parecer de um artigo submetido a um evento da Ciência da Informação, em que fica evidente que a insciência sobre as questões envolvidas na fase de coleta também está presente no meio acadêmico. Ao dar parecer sobre o trabalho que trazia no teor a abstração na fase de coleta, resultante dos dados de comunicação, o (a) parecerista justifica a recusa do trabalho por meio do seguinte fragmento de texto: “A temática está centrada no aspecto técnico de tráfego de dados, falta maior inserção na área [...]”. Considerando que a Ciência da

[15] Empresa privada que realizava mineração e análise de dados.

Informação é a área que estuda os fenômenos relacionados à informação e dados, não é justificável que os metadados representantes do tráfego de dados não estejam vinculados à área e não careçam de amplitude de estudos para que se possa verificar as possíveis ameaças à privacidade.

> A Ciência da Informação pode e deve contribuir para que este cenário de acesso e uso intenso de dados se desenvolva da melhor maneira possível, buscando identificar e estudar fatores e características que propiciem ampliação do equilíbrio entre os atores envolvidos no processo e a máxima otimização do uso dos dados (SANT'ANA, 2016, p.119).

A falta de percepção em relação à coleta de dados decorre do indivíduo ser mais consciente a ameaças a privacidade quando algo tangível acontece - como alguém abrir a caixa de correio para ler uma carta. Ao contrário, pode parecer-lhes menos intrusivo se alguém navega remotamente no seu histórico de pesquisa ou na sua caixa de e-mail (KIFT, 2013). A insciência sobre a coleta de dados faz com que as preocupações dos usuários, em relação à privacidade, sejam voltadas para o contexto da segurança da informação, tais como a invasão de computadores e de contas de e-mail, ou o roubo de conteúdo digital (fotos, arquivos, número de cartão de crédito). No entanto, isso não significa que os dados têm salvaguarda de acesso não autorizado ou que seu uso será de acordo com a vontade e ciência dos seus titulares.

Diante do exposto, o presente trabalho justifica-se, dada sua relevância científica e acadêmica, no desenvolvimento de um estudo sistemático para caracterizar o cenário que propicia a insciência do usuário na fase de coleta de dados, uma vez que essa insciência pode refletir diretamente sobre a percepção e comportamento em relação à privacidade enquanto o usuário é agente alvo de processos de coleta. A partir do momento que o usuário não sabe o que acontece, a tendência é não haver maiores preocupações e adoção de medidas para garantir que não ocorra a exposição de seus dados. Como diz a o ditado popular, "o que os olhos não veem, o coração não sente". Assim, se o indivíduo não tem a percepção do processo de coleta de dados, não há motivos para se preocupar com as implicações dessa atividade.

Esta pesquisa também se justifica pela relevância social, pois ao identificar e tornar explícitos fatores que propiciam a insciência do usuário colabora-se para ampliação de estratégias para prevalecer os direitos a privacidade, que podem ser realizadas tanto pelo meio acadêmico, quanto pelo ordenamento jurídico no desenvolvimento de leis.

> [...] entendemos que tanto os governos quanto a Academia devam continuamente investigar as tecnologias digitais da informação e comunicação, o avanço da ciência da informação e cotejá-las permanentemente com o previsto nos vários ordenamentos jurídicos e com as

> estratégias e investimentos de proteção aos dados, como forma predominante de salvaguardar a sociedade e suas várias formas de organização nessa nova realidade da era da informação (DIAS; VIEIRA, 2015, p. 182).

A importância do envolvimento da Ciência da Informação nas questões vinculadas à privacidade pode ser resgatada pelo trabalho de Wersig e Neveling (1975, p. 129), ao afirmarem que a gênese da Ciência da Informação pode ser orientada a partir de quatro perspectivas: "[...] visão orientada para o fenômeno; visão orientada para os meios; visão orientada para a tecnologia e; visão orientada para os fins".

Assim, os elementos vinculados à tecnologia passam a ser uma preocupação da Ciência da Informação, portanto, essa ciência pode amparar, por meio de estudos e pesquisas, os aspectos vinculados desde a coleta até a recuperação de dados, contribuindo para novas descobertas em relação à proteção de dados pessoais. No entanto, a privacidade perpassa as questões de tecnologias e, quando ameaçada, impacta a esfera social do indivíduo. Então, "[...] existem determinadas necessidades sociais a serem preenchidas, e que a Ciência da informação deve servir a essas necessidades e desenvolver o trabalho prático com elas relacionado" (WERSIG; NEVELING, 1975, p. 130, tradução nossa)[16].

1.7 Delimitação

O universo de pesquisa está delimitado na fase de coleta do CVD (SANT'ANA, 2013), com ênfase no fator privacidade, considerando a privacidade no domínio da proteção de dados pessoais. A Figura 2 ilustra a fase de coleta de dados e os níveis de abstração na relação usuário-detentor de dados, para tanto, utilizou-se do conceito em camadas do modelo OSI. O modelo OSI é uma proposta desenvolvida pela *International Organization for Standardization* (ISO) para padronizar os conceitos envolvidos na comunicação em redes de comunicação, tornando explícita a distinção entre serviços, interfaces e protocolos (TANENBAUM, 2003). O modelo OSI é referenciado neste trabalho como uma orientação para o entendimento do processo de comunicação nas redes de computadores, especificamente, no que tange ao conceito de abstração proporcionado pela sua estrutura em camadas.

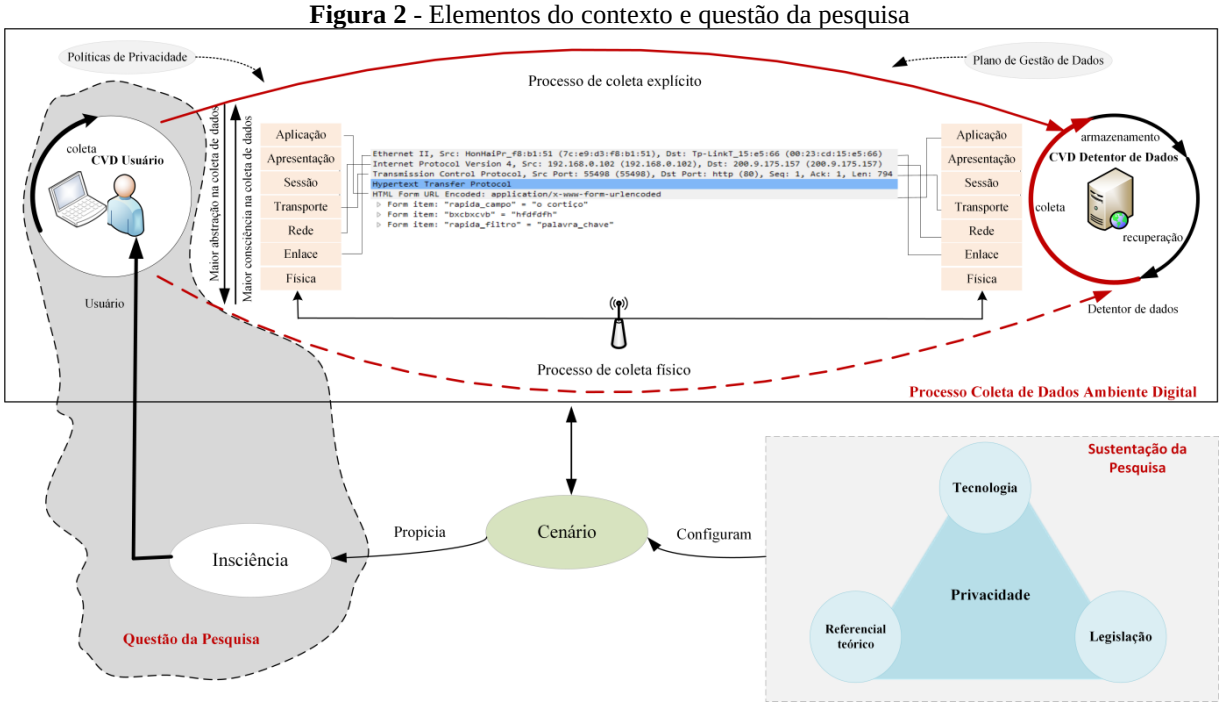
> Uma arquitetura em camadas nos permite discutir uma parcela específica e bem definida de um sistema grande e complexo. Essa simplificação tem considerável valor intrínseco, pois provê modularidade fazendo com que fique mais fácil modificar a implementação do serviço prestado pela camada. Contanto que a camada forneça os mesmos serviços para a que está acima dela e use os mesmos serviços da camada abaixo dela (KUROSE; ROSS, 2010, p.36).

[16] "[...] *there are some social needs which have to be fulfilled and that 'information science1 should serve and develop the practical work related to those needs*".

No contexto prioritariamente associado a Web, a coleta de dados se inicia quando o usuário (Ciclo de Vida dos Dados do Usuário – CVD Usuário) solicita uma página ao servidor de aplicação (Ciclo de Vida dos Dados do Detentor – CVD Detentor de Dados). A interação do usuário com esse ambiente digital se efetua a partir dos dados que ele fornece explicitamente (processo de coleta explícito) e implicitamente (processo abstraído para o usuário) (Figura 2). Assim, nesse cenário o usuário é alvo de fases de coleta pelos detentores de dados, no qual considera-se que o usuário é insciente em relação a muitos dados coletados por essa atividade.

A arquitetura das redes de computadores, caracterizada por meio das camadas do modelo de referência OSI, determina as interfaces onde a abstração se faz presente, tornando esse processo opaco para o usuário. Essa abstração se perfaz por meio do encapsulamento da coleta de dados, efetivado pelos protocolos que proporcionam a transição de dados entre as camadas (AFFONSO; SANT'ANA, 2018, no prelo).

Figura 2 - Elementos do contexto e questão da pesquisa

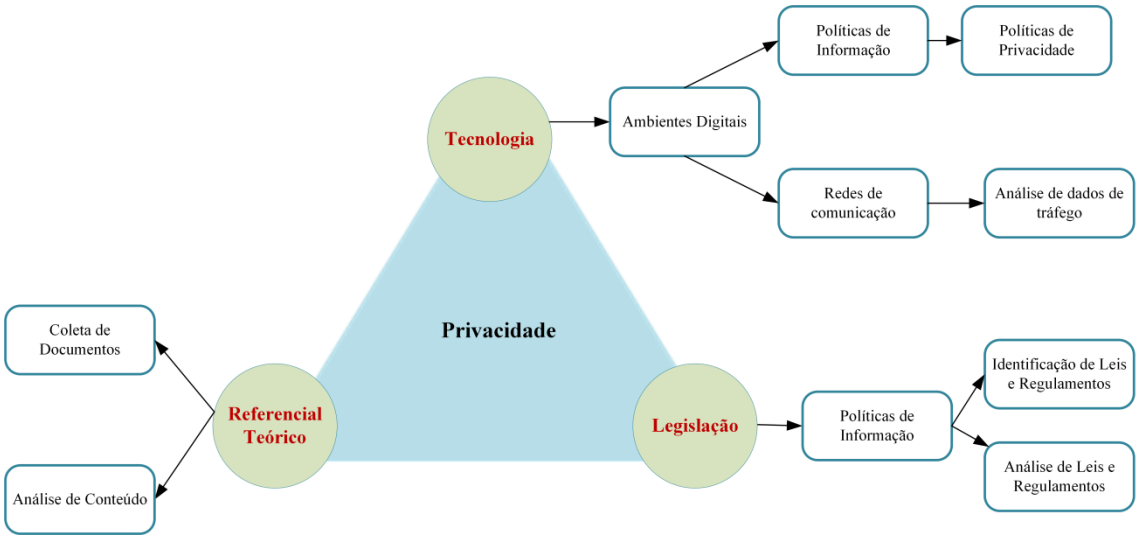


Fonte: Adaptado de Affonso e Sant'Ana (2018, no prelo)

Além disso, esta pesquisa é sustenta por três elementos: a) referencial teórico, por meio da publicação de trabalhos que abarcam a proteção de dados pessoais no domínio da anonimização; b) legislações, que amparam as questões envolvidas com proteção de dados pessoais e; c) a coleta realizada por meio de tecnologias, especificamente em ambientes digitais

(Figura 3). Desta forma, considera-se que esses elementos configuram o cenário que propicia a insciência do usuário sobre o momento da coleta de seus dados.

Figura 3 - Elementos participantes da pesquisa



Fonte: Elaborado pela autora

Considera-se ainda, que no cenário de coleta de dados, os ambientes digitais dispõem de políticas de privacidade e/ou de planos de gestão de dados com a intenção de informar seus usuários sobre as atividades realizadas com os dados.

1.8 Metodologia

Esta pesquisa é de cunho descritivo, com abordagem qualitativa. Adotou-se a triangulação metodológica, determinada por Denzin (1988) como o uso de múltiplos métodos para estudar e analisar, de forma interpretativa, determinado problema de pesquisa.

A triangulação tem o objetivo de combinar diferentes métodos de investigação para coleta de dados e análise do objeto de estudo (FLICK, 2008). Para Denzin e Lincoln (2006, p. 16), "[...] o uso de múltiplos métodos, ou da triangulação, reflete em uma tentativa de assegurar uma compreensão em profundidade do fenômeno em questão".

> A triangulação é uma abordagem metodológica que requer um desenho de pesquisa, cujo desenvolvimento pode contar com técnicas de recolha de dados diferentes, tanto com instrumentos para a pesquisa quantitativa quanto para a pesquisa qualitativa ou ainda mobilizando instrumentos quantitativos e qualitativos em uma mesma pesquisa. Ela tem se mostrado competente porque permite coletar informações a partir de fontes, espaços e tempos diferentes. Pode ainda triangular teorias e pesquisadores de distintas áreas do conhecimento (FIGARO, 2014).

A fim de evidenciar elementos que levam a insciência do usuário sobre a fase de coleta de dados e as implicações nas questões de privacidade, este trabalho utiliza os métodos descritos a seguir.

1.8.1 Pesquisa bibliográfica

Utilizou-se da pesquisa bibliográfica, que é "[...] elaborada com o propósito de fornecer fundamentação teórica ao trabalho, bem como a identificação do estágio atual do conhecimento referente ao tema" (GIL, 2010, p. 29), para explanar sobre:

a) As principais definições de privacidade e contextualizar os aspectos envolvidos na proteção de dados pessoais, tais como técnicas e modelos para anonimização;
b) Elementos envolvidos com os mecanismos de busca;
c) Camadas de abstração de dados relacionadas ao modelo de referência OSI e ferramentas para análise de pacotes de dados em redes de comunicação.

1.8.2 Revisão sistemática de literatura

Por meio de coleta de documentos na base de dados *Web of Science*, buscou-se evidenciar como a anonimização de dados tem sido abordada na fase de coleta de dados. "Uma revisão sistemática da literatura é um meio de identificar, avaliar e interpretar pesquisas disponíveis relevantes para uma determinada questão de pesquisa, área de tópico ou fenômeno de interesse" (KITCHENHAM, 2004, p. 1, tradução nossa) [17].

O motivo de uma revisão sistemática decorre da necessidade de pesquisadores sintetizarem informações existentes sobre algum fenômeno de forma detalhada e de maneira imparcial. Por meio da revisão sistemática, torna-se possível identificar carências na pesquisa atual, a fim de sugerir áreas para mais investigação, fornecer uma estrutura para posicionar adequadamente novas atividades de pesquisa, tirar conclusões gerais sobre algum fenômeno ou auxiliar na geração de novas hipóteses (KITCHENHAM, 2004).

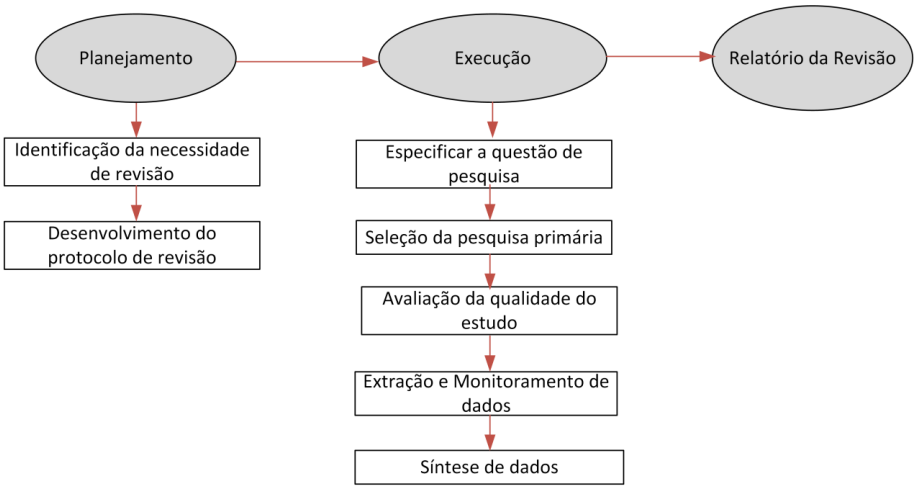
Para Dyba, Dingsoyr e Hanssen (2007), uma revisão sistemática é, ao contrário de uma revisão tradicional, um recurso conciso que utiliza de métodos rigorosos para identificar, avaliar criticamente e sintetizar estudos relevantes sobre um tópico específico. A pesquisa realizada em uma revisão sistemática pode ser limitada por data, por revista, por bases de dados, e assim por diante, desde que os procedimentos de pesquisa sejam transparentes e replicáveis.

---

[17] "*A systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest. Individual studies contributing to a systematic review are called primary studies; a systematic review is a form a secondary study*".

O objetivo desta revisão foi verificar se a proteção da privacidade, por meio da anonimização, está presente na fase de coleta do ciclo de vida dos dados, buscando evidenciar, especificamente, os elementos envolvidos nessa fase. A seguir, descrevem-se o planejamento do protocolo de revisão sistemática e os métodos utilizados nesta revisão, constituindo a primeira fase do protocolo de revisão sistemática (Figura 4), baseado em Kitchenham (2004).

Figura 4 - Etapas da revisão sistemática



Fonte: Baseado em Kitchenham (2004).

O protocolo de revisão sistemática é composto por três fases principais (KITCHENHAM, 2004):

a) Planejamento: consiste em identificar qual a necessidade da realização da revisão e estruturação do protocolo.
b) Execução: tem a finalidade de determinar a questão principal e secundária que a revisão busca atender, identificando os itens relacionados ao escopo da pesquisa; estratégias para selecionar os documentos (processo de inclusão e exclusão de documentos); procedimento para avaliar a qualidade dos estudos (são definidos critérios para justificar a inclusão dos trabalhos); estratégias para a extração dos dados (definição de atributos para estruturar os documentos recuperados); e síntese dos dados extraídos (utiliza-se de representações por meio de gráficos e quadros para visualização dos resultados obtidos com a revisão sistemática).
c) Relatório da revisão: apresentação dos resultados e discussão dos conteúdos revelados por meio da recuperação dos documentos.

1.8.2.1 Planejamento

Nessa fase realiza-se a “identificação da necessidade de uma revisão sistemática”, desta forma, ressalta-se que o motivo dessa revisão decorre da necessidade de explanar sobre privacidade, especificamente no âmbito de proteção de dados pessoais mediante anonimização de dados, de forma detalhada e de maneira imparcial. Assim, essa revisão tem por objetivo identificar e analisar estudos que abordam a anonimização na fase de coleta de dados incluindo a verificação dos principais modelos e técnicas. A coleta de documentos foi realizada no mês de abril de 2017.

1.8.2.2 Execução

1.8.2.2.1 Especificação da questão de pesquisa

Questão Primária: Anonimização de dados pessoais tem sido abordada na fase de coleta dos dados?

Questão Secundária: Quais os elementos envolvidos na anonimização de dados na fase de coleta dos dados?

O escopo e as especificidades das questões de pesquisa estão envolvidos com os seguintes elementos:

- ✓ População: pesquisadores e o legislativo que realizam pesquisas no domínio da proteção de dados pessoais, por meio de anonimização de dados;
- ✓ Intervenção[18]: modelos e técnicas que abordam anonimização de dados;
- ✓ Resultados[19]: incentivos ao desenvolvimento de técnicas e modelos que permitem a anonimização de dados na fase de coleta e, consequentemente, ampliam-se questões voltadas à proteção de dados pessoais, inclusive tornando-se base para o desenvolvimento de novas leis.

1.8.2.2.2 Estratégias que foram utilizadas para seleção de pesquisas primárias

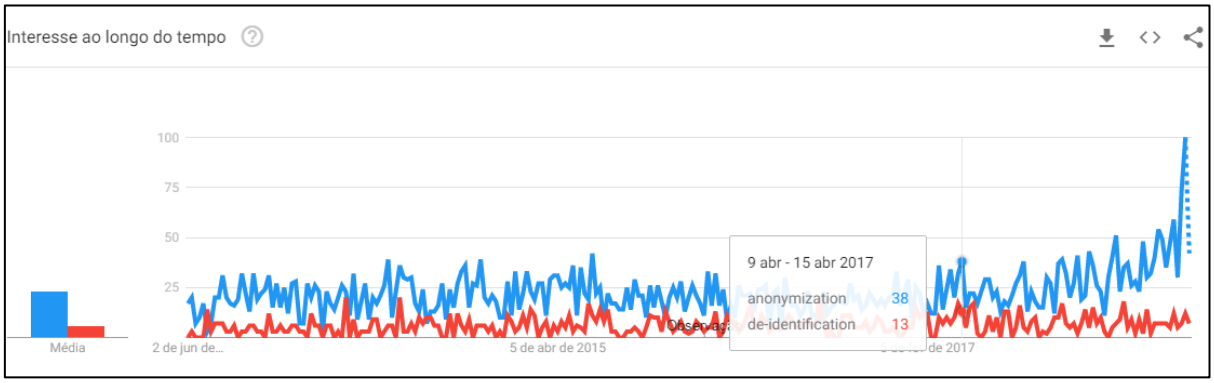
a) Base de dados: Foi escolhida a base de dados *Web of Science*, pois ela proporciona uma investigação eficiente e a recuperação de artigos relevantes de periódicos renomados, buscando, assim, o que há de melhor na ciência em relação às pesquisas sobre anonimização de dados, incluindo a credibilidade nos documentos disponibilizados, a fim de garantir resultados com qualidade. Além disso, permite a recuperação de trabalhos de diversas áreas do conhecimento e apresenta esses resultados de forma estruturada.

[18] Definida por Kitchenham (2004) como as tecnologias ou *software* que abordam questões específicas.
[19] Devem estar relacionados com fatores de importância para profissionais (KITCHENHAM, 2004).

b) Termo descritor: A busca foi realizada por meio do termo anonimização nos idiomas inglês, espanhol e português, determinado respectivamente por: *anonymisation*, *anonimización* e anonimização. O termo foi escolhido devido à intensa relação com as questões de proteção da privacidade e dos dados pessoais. Segundo a ISO 25237:2017, anonimização[20] refere-se "[...] ao processo pelo qual os dados pessoais são irreversivelmente alterados, de tal forma que um sujeito não pode ser mais ser identificado direta ou indiretamente [...]" (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2017). Conforme citam Sheth, Kaiser e Maalej (2014), a anonimização é a técnica mais conhecida de proteção de privacidade e parece ser percebida como uma medida importante e efetiva tanto por usuários quanto por desenvolvedores.

As questões de proteção de dados pessoais estão envolvidas com outros termos como *de-identification* ou de-identificação, definida como o processo de remover associação entre um conjunto de dados e o indivíduo referenciado nesses dados (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2017). No entanto, o termo anonimização ainda se sobressai, como pode ser observado pelos termos pesquisados no *Google Trends*[21] (Figura 5). A Figura 5 ilustra a comparação entre os termos *anonymization* e *de-identification* no período de 2014 a 2018, em que o termo *anonymization* se destaca pelas ocorrências de buscas no período. A análise com o termo anonimização e de-identificação apresentaram também maiores ocorrências para o termo anonimização, no entanto, o termo *anonimización* não teve ocorrência suficiente para gerar o gráfico.

Figura 5 - Recorte indicando ocorrências dos termos *anonymization* e *de-identification*



Fonte: *Google Trends*

[20] *Anonymization: process that removes the association between the identifying data set and the data subject* (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2017)
[21] Disponível em: https://trends.google.com.br/trends/. Acesso em: 8 jul. 2017.

Na *Web of Science*, a busca ocorreu por meio da digitação do termo descritor no campo pesquisa (pesquisa básica), opção da ocorrência do termo descritor no documento (seleção tópico), considerando 50 documentos por páginas, exibidos por ordem de citação, da maior para a menor.

Em relação aos índices de citação, foram mantidas a seleção padrão dos seguintes índices de citações: *Science Citation Index Expanded (SCI-EXPANDED)* -- 1900-presente*; Social Sciences Citation Index* (SSCI) --1900-presente; *Arts & Humanities Citation Index* (A&HCI) --1975-presente*; Conference Proceedings Citation Index* - Science (CPCI-S) --1991-presente; *Conference Proceedings Citation Index - Social Science & Humanities* (CPCI-SSH) --1991-presente*; Emerging Sources Citation Index* (ESCI) --2015-presente. E os seguintes índices químicos: *Current Chemical Reactions* (CCR-EXPANDED) --1985-presente (Inclui os dados de estrutura do *Institut National de la Propriete Industrielle* até o ano de 1840) e *Index Chemicus* (IC) --1993-presente.

c) Tipos de documentos: Na opção do ambiente da *Web of Science,* foram selecionados os tipos de documentos: *proceedings papers*; *article; review* e *book chapter* para a recuperação dos trabalhos.

d) Ano de publicação: Este trabalho não considerou valor temporal, foram recuperados todos os documentos disponibilizados pela base de dados. Dessa forma, foi selecionado no campo "tempo estipulado" a opção todos os anos.

e) Exibição dos documentos recuperados: A classificação dos documentos recuperados foi realizada por meio do número de citações (do maior para o menor). Além disso, os metadados referentes aos documentos foram resgatados por meio do item salvar em outros formatos de arquivo. Ao selecionar a opção "salvar em outro formato", no item gravar conteúdo, escolheu-se a opção registro completo, no formato de arquivo "separado por tabulação (*Windows*)". Posteriormente, esse arquivo foi aberto em *software* de planilha, utilizou-se o *software Microsoft Excel* para extrair os campos de interesse.

f) Critérios para seleção dos estudos

Nesse item são apresentados os critérios de inclusão e exclusão, incluindo os processos de seleção preliminar e final dos estudos. Durante a seleção, foram avaliados os resumos, introduções e conclusões dos trabalhos, seguindo os critérios de inclusão e exclusão definidos no protocolo de pesquisa. Assim, só foram selecionados artigos dos quais se pudesse acessar o artigo completo.

- ✓ Critérios de inclusão

Foram considerados exclusivamente artigos de periódicos, trabalhos de conferências/congressos, capítulos de livros e revisões que tivessem pelo menos uma citação. Para atender as questões de pesquisa, os seguintes critérios de inclusão foram determinados:

Questão primária: aspectos de privacidade, especificamente a anonimização de dados realizada na fase de coleta de dados.

Questão secundária: elementos, tais como técnicas e modelos de proteção de dados pessoais, envolvidos na fase de coleta de dados.

- ✓ Critérios de exclusão

A fim de compor a amostra de trabalhos para análise, foram adotados os seguintes critérios de exclusão:

Questão primária: anonimização de dados não foi empregada na fase de coleta de dados;

Questão secundária: anonimização apenas citada no contexto da psicologia, filosofia, direito ou medicina, em que a anonimização não foi foco principal do documento. Foram excluídos também os documentos que abordaram técnicas para segurança da informação no cenário apenas de impedir a intercepção por terceiros; medidas para prevenir ataques em redes de computadores; e o uso de *softwares* para tornar o usuário anônimo, como o uso do TOR[22] e similares.

- ✓ Processo de seleção preliminar

O termo descritor é submetido na base de dados *Web of Science* e, posteriormente, são coletados os atributos disponibilizados pela base de dados referentes a cada documento, armazenando-os em *software* de planilhas. No processo de seleção preliminar, os documentos selecionados foram apenas os que tinham pelo menos uma citação.

- ✓ Processo de seleção final

Todos os documentos que passaram no processo de seleção preliminar tiveram resumo, introdução e conclusão lidos, buscando identificar se o processo de anonimização ocorreu na fase de coleta ou de recuperação de dados e se eles atendiam aos critérios de inclusão determinados nessa revisão sistemática. Para a identificação da fase em que a pesquisa descrita em cada trabalho se encontra, utilizou-se o Ciclo de Vida dos Dados para Ciência da Informação (CVD-CI) (SANT'ANA, 2013). Posteriormente, os trabalhos selecionados foram lidos buscando identificar o escopo e as características principais da anonimização realizada.

[22] [22] Software livre com a finalidade de proporcionar ao usuário meios de se defender contra a análise de tráfego de dados (TOR, 201-).

1.8.2.2.3 Procedimentos para avaliar a qualidade dos estudos

A avaliação da qualidade permite aos pesquisadores verificar as diferenças na execução dos estudos selecionados, contribuindo para síntese de dados e interpretação de resultados (KITCHENHAM, 2004). Para comprovar a qualidade dos documentos selecionados, eles foram classificados com base nos critérios de qualidade definidos por Dyba, Dingsoyr e Hanssen (2007). A classificação dos documentos em relação aos critérios foi realizada por meio da escala dicotômica "sim" ou "não". Utilizou-se os seguintes critérios de qualidade:

[1] O documento é baseado em pesquisa ou um relato de opinião de especialista?

[2] Os objetivos da pesquisa foram definidos de forma clara?

[3] Existe uma descrição adequada do contexto em que a pesquisa foi realizada?

[4] O projeto de pesquisa é apropriado para abordar os objetivos da pesquisa?

[5] Existe uma declaração clara de resultados?

[6] O estudo representa valor para pesquisa ou prática?

1.8.2.2.4 Estratégias de extração de dados

Com a recuperação dos documentos que abordaram anonimização apenas na fase de coleta dos dados, foram extraídas as seguintes informações:

- ✓ Ano da publicação;
- ✓ Título do documento;
- ✓ Quantidade de citação;
- ✓ Resumo;
- ✓ Origem: País (s) de origem das instituições de afiliação dos autores dos trabalhos;
- ✓ Fonte: Periódico ou evento no qual o trabalho foi publicado;
- ✓ Tipo de documento: artigos em eventos; artigos em periódicos; artigos de revisão ou capítulos de livros;
- ✓ Área da pesquisa: área em que os trabalhos foram definidos na *Web of Science*;
- ✓ Abordagem/característica principal (síntese descritiva);

Para a extração de informações do texto para o atributo abordagem/característica principal foi realizada a leitura de cada publicação que atendeu os critérios de inclusão, buscando identificar os elementos que caracterizam a anonimização de dados na fase de coleta.

1.8.2.2.5 Síntese dos dados extraídos

Nos resumos dos documentos foi aplicada a análise de conteúdo[23], por meio do estudo do código do texto, verificando o número total de palavras ou ocorrências (BARDIN, 1977)[24]. Para isso, utilizou-se a ferramenta *textalyser.net*[25], que permite a contagem e a análise estatística de grupos de palavras, tornando possível determinar a densidade de palavras-chave e a análise de proeminência de palavras e expressões.

Segundo Bardin (1977), a análise de conteúdo pode ter as seguintes funções:

- ✓ Heurística: cuja finalidade é ir descobrindo o conteúdo por meio da tentativa exploratória. "É a análise de conteúdo para ver o que dá" (BARDIN, 1977, p. 30);
- ✓ Administração da prova: As hipóteses, sob a forma de questões, serão verificadas no sentido de confirmação. "É a análise de conteúdo para servir de prova" (BARDIN, 1977, p. 30).

Desta forma, por meio da análise de palavras, buscou-se confirmar a abordagem principal/características dos documentos definida pelo pesquisador (administração da prova) e descobrir novos conteúdos (heurística).

Esses resultados contribuíram para a confirmação e a determinação dos elementos para a caracterização dos documentos analisados, resultando na construção do sumário dos documentos incluídos na revisão sistemática.

Com os resultados obtidos no processo de extração de dados - leitura dos trabalhos selecionados - e a análise de conteúdo por contagem de palavras e expressões para verificar a frequência de termos, elaborou-se as seguintes sistematizações:

- ✓ **Sistematização 1:** Os trabalhos foram categorizados nos seguintes atributos: Artigo (para identificação do trabalho); autor (es); ano de publicação; quantidade de citação; e abordagem/característica principal (síntese descritiva, elaborada a partir da leitura e interpretação dos documentos);
- ✓ **Sistematização 2:** Os trabalhos foram caracterizados nos seguintes atributos: Artigo (identificação do trabalho); origem; fonte; tipo de documento; área, contexto (cenário em que a anonimização de dados foi abordada ou realizada); modelos (modelos para

[23] "Um conjunto de técnicas de análises das comunicações visando obter, por procedimentos, sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não), que permitam a inferência de conhecimento relativos às condições de produção/recepção (variáveis inferidas) destas mensagens" (BARDIN, 1977, p. 31).

[24] Fase de Tratamento dos resultados obtidos e interpretação, na qual Bardin (1977) afirma que "os resultados brutos são tratados de maneira a serem significativos (<falantes>) e válidos. Operações estatísticas simples (percentagens), ou mais complexas (análise fatorial), permitem estabelecer quadros de resultados, diagramas, figuras e modelos, os quais condensam e põem em relevo as informações fornecidas pela análise".

[25] Disponível em: <http://textalyser.net/index.php?lang=en#analysis>. Acesso em: 2 set. 2017.

anonimização de dados); técnicas (técnicas para anonimização de dados) e arquitetura de redes de computadores adotada.

Os atributos contexto, modelos, técnicas e arquitetura de rede de computadores que compuseram o quadro de sistematização dos trabalhos foram determinados por meio da leitura dos documentos e da análise estatística por contagem de palavras com a ferramenta *textalyser.net* Para ilustrar os termos frequentes nos documentos e seus relacionamentos, utilizou-se o minerador de texto *Sobek*[26].

Os dados extraídos dos documentos também foram representados por meio de gráficos, a fim de evidenciar a quantidade de trabalhos e de citação por ano; a quantidade de documentos por tipo de produção e citação; frequência das áreas de pesquisas; frequência dos países nos trabalhos; predominâncias de modelos e técnicas para anonimização de dados; contexto em que a anonimização foi aplicada e a frequência das arquiteturas de redes. Por meio desses dados quantitativos torna-se possível análise e inferências a respeito do objeto de estudo da revisão sistemática. Conforme cita Bardin (1977, p. 38, grifo do autor) o interesse do pesquisador "não reside na descrição dos conteúdos, mas sim no que estes nos poderão ensinar após serem tratados [...] e relativamente a 'outras coisas'".

Para a visualização da distribuição geográfica dos países das instituições a que pertencem os autores dos documentos recuperados, foi utilizada a ferramenta *Google Fusion Tables*[27], por meio da inserção da latitude e da longitude dos países dos autores que constituíram a *corpus* dessa revisão.

1.8.2.3 Relatório da revisão

Será apresentado o resultado da revisão sistemática de acordo com as etapas descritas nas seções anteriores. Para Dyba, Dingsoyr e Hanssen (2007), o resultado de uma revisão sistemática inclui: quadros que resumem todos os artigos incluídos; quadros que mostram como os estudos foram classificados e os temas que foram encontrados nos documentos.

1.8.3 Pesquisa documental

a) **Documento jurídico**

Utilizou-se de pesquisa documental mediante análise de documento jurídico (leis, regulamentos e jurisprudências) para identificar como tem sido aborda a proteção de dados

[26] Ferramenta gratuita apoiada no conceito de mineração de texto, que permite extrair conceitos pertinentes de dados não estruturado, ou semiestruturado, por meio da análise de frequência de termos (SOBEK, 2017).
[27] Disponível em: <https://support. google.com/fusiontables/answer/2571232>. Acesso em: 2 jan. 2017.

pessoais. Segundo Gil (2008, p. 51) a pesquisa documental é muito próxima à pesquisa bibliográfica, no entanto, a diferença está na natureza das fontes, pois "[...] a pesquisa documental vale-se de materias que não receberam ainda um tratamento analítico [...] tais como: documentos oficiais, reportagens de jornal, cartas, contratos, etc." (GIL, 2010, p. 51). Para execução da pesquisa e análise considerou-se os seguintes cenários:

- ✓ Cenário internacional: Foram identificadas e explanadas as principais leis e os principais regulamentos que abordam as questões de proteção de dados pessoais da Austrália, Canadá, Estados Unidos, determinados países da Europa, Hong Kong e Coreia do Sul. A identificação da legislação foi por meio de busca nos *sites* governamentais dos países supracitados. A escolha por esses países foi baseada no *site* da DLA Piper (2017), que os apresentam como fortes nas questões de privacidade;
- ✓ Cenário nacional: Foram identificadas e explanadas as leis e os projetos de leis no contexto da proteção de dados pessoais. A identificação ocorreu por meio de consulta nos *sites* do governo federal, especificamente no portal da legislação[28], no item "Pesquisa de Legislação". A busca ocorreu por meio dos termos descritores: dados pessoais, proteção de dados, privacidade, banco de dados, informática, sigilo, anonimização. As jurisprudências foram identificadas mediante busca no sítio do Observatório do Marco Civil[29], especificamente na categoria "privacidade" e "dados pessoais". As leis e os projetos de leis foram categorizados nos seguintes atributos: lei, ator (sujeito envolvido na Lei), processo (regulamentos, princípios ou direitos relacionados à proteção de dados pessoais) e conceitos (definição de termos envolvidos com privacidade e proteção de dados pessoais). Por meio dessa categorização, gerou-se uma síntese das leis que abarcam proteção de dados pessoais e uma síntese do Projeto de Lei 5.276/2016.

Posteriormente, por meio de análise das leis e regulamentos especificou-se como esses documentos tratam as questões vinculadas especificamente à coleta de dados pessoais.

A coleta no sítio do governo federal ocorreu no mês de novembro de 2016. No cenário internacional a coleta de dados ocorreu no mês de setembro de 2017 e no mês de maio de 2018[30]. A coleta de dados realizada no sítio do Observatório do Marco Civil foi realizada nos meses de março e abril de 2018.

---

[28] Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/_Lei-principal.htm>. Acesso em: 20 dez. 2016.
[29] Disponível em: <http://www.omci.org.br/jurisprudencia/> Acesso em: 10 mar. 2018.
[30] Especificamente para a identificação de leis dos países pertencentes à União Europeia devido à implantação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

b) **Políticas de Privacidade**

Foi utilizada pesquisa documental para explorar e analisar a política de privacidade do mecanismo de busca *DuckDuckgo* [31] a fim de identificar os possíveis dados coletados por esse ambiente digital. A identificação se deu pela interpretação dos itens "informação que coletamos" e "informações que não coletamos" presentes na política de privacidade do *DuckDuckgo.*

Realizou-se uma adaptação na categorização dos dados coletados pelos mecanismos de busca *Google* e *Bing* presente no trabalho de Affonso et al. (2017), acrescentando os dados coletados pelo mecanismo de busca *DuckDuckgo.* Posteriormente, os dados foram classificados em Identificadores (I), Semi-Identificadores (SI) e Sensíveis (SE) (CIRIANI et al., 2009). Essa categorização tem a finalidade de explicitar como a coleta de dados pelos mecanismos de busca causam ameaças à privacidade.

Para demonstrar as possíveis ameaças a privacidade quando usuários interagem com ambientes digitais, especificamente com os mecanismos de busca, adotou-se a taxonomia de privacidade proposta por Solove (2006).

1.8.4 Coleta de dados em ambiente Web

A fim de demonstrar a coleta de dados de tráfego nas redes de computadores (metadados) durante a interação do usuário com os mecanismos de busca e a abstração presente nesse processo, realizou-se:

- ✓ A identificação e análise de dados de tráfego com a ferramenta *Wireshark*[32] para ilustrar o fluxo de dados durante a interação do usuário com o ambiente digital;
- ✓ Correlação dos dados de interação coletados pela ferramenta *Wireshark* com a camada OSI, indicando as possíveis quebras de privacidade e insciência do usuário sobre o processo.

Para a realização da coleta de dados, utilizou-se um notebook que possui sistema operacional Windows 7, com conexão sem fio, acessando as páginas Web dos mecanismos de busca *Bing*, *Google* e *DuckDuckgo*.

A análise dos dados do mecanismo Bing se deu via protocolo HTTP (*HyperText Transfer Protocol)*, e a análise dos dados dos mecanismos *Google* e *DuckDuckgo* foi realizada via protocolo HTTPS (*HyperText Transfer Protocol Secure)*. Os pacotes de dados trafegados

[31] Disponível em: <https://duckduckgo.com/?q=&t=i>. Acesso em: 12 set. 2017.
[32] *Software* livre que permite acompanhar e analisar os dados de tráfego de redes de computadores durante a interação do usuário com aplicações na Internet.

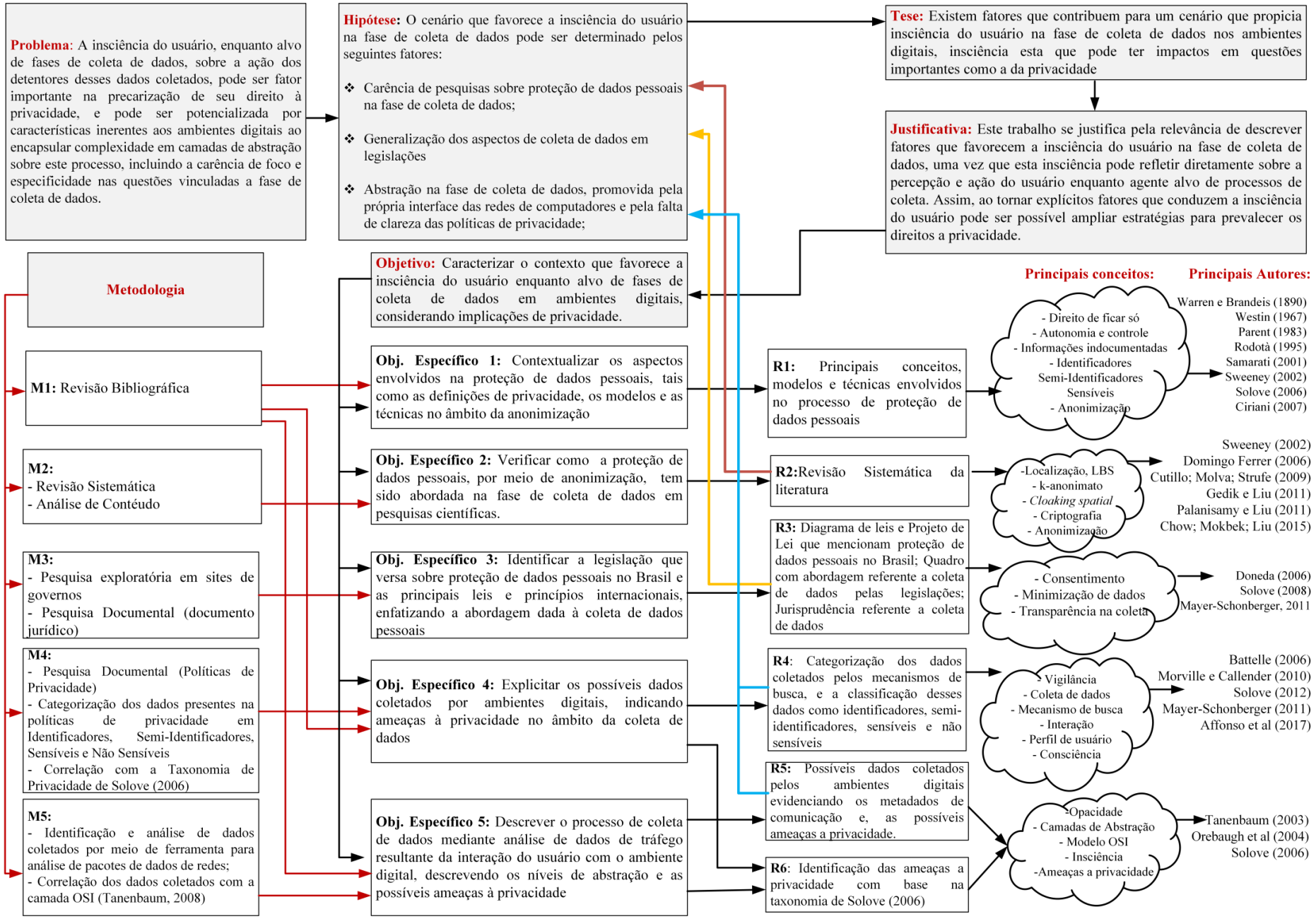
durante o acesso foram coletados e selecionados para análise, a fim de demonstrar os possíveis dados coletados durante a interação do usuário com ambientes digitais.

Ressalta-se que a coleta de dados se efetuou no equipamento da própria autora e em rede *wi-fi* doméstica. Os dados foram coletados no dia 09 de dezembro de 2017.

1.9 Estrutura do trabalho

Na Figura 6, apresentam-se o problema, as hipóteses, a tese, a justificativa, os objetivos, objetivos específicos, a metodologia empregada e os principais conceitos e autores que emergiram durante o desenvolvimento do trabalho.

Figura 6 - Estrutura da tese



Fonte: Elaborado pela autora

Este capítulo apresentou a contextualização da temática, indicando as implicações da coleta de dados pelos seus detentores, o problema de pesquisa, a tese, hipótese, o objetivo geral, os objetivos específicos, a justificativa, a metodologia e a estrutura do trabalho.

O capítulo 2 é constituído de referencial teórico, em que são explanadas as principais definições de privacidade e a taxonomia de privacidade determinada por Solove (2006).

O capítulo 3 versa sobre os aspectos envolvidos na proteção de dados pessoais, tais como: anonimização de dados, dados identificadores, dados semi-identificadores e dados sensíveis. Apresentam-se, também, os principais modelos (k-anonimato, l-*diversity,* t-*closeness*) e as técnicas (generalização, supressão, adição de ruídos, entre outras) para a proteção da privacidade.

No capítulo 4 é apresentada uma revisão sistemática de literatura, a fim de explicitar como tem sido abordada a proteção da privacidade por meio de anonimização de dados na fase de coleta nas pesquisas científicas. Apresenta-se como resultado a síntese de cada trabalho, os principais modelos e técnicas de anonimização empregados nas pesquisas analisadas; os países que mais se destacaram com trabalhos de pesquisa no âmbito da coleta de dados; o principal cenário em que a anonimização foi empregada; e as áreas do conhecimento que mais se evidenciaram na amostra analisada.

O capítulo 5 explora as principais leis e os principais regulamentos internacionais, que abarcam questões vinculadas à proteção de dados pessoais, e a legislação brasileira que ampara essa questão. Ressalta-se neste capítulo a abordagem dada especificamente à coleta de dados, e a jurisprudência brasileira em relação à privacidade e proteção de dados pessoais.

No capítulo 6 explana-se sobre os mecanismos de busca e as suas consequências nos aspectos de privacidade, para tanto realizou uma análise a partir da interpretação das políticas de privacidade e uma análise mediante os dados de tráfego da interação usuário ambiente digital. E por fim, são explicitados os possíveis dados coletados pelos mecanismos de busca Bing, Google e *DuckDuckgo*.

O capítulo 7 versa sobre as possíveis ameaças a privacidade, para tanto, utilizou-se como ponto norteador o framework de Solove (2006).

Por último, o capítulo 8 apresenta as conclusões e trabalho futuro.

2 PRIVACIDADE

Pode haver uma janela alta de onde eu veja o céu e o mar, mas deve haver um canto bem sossegado em que eu possa ficar sozinho, quieto, pensando minhas coisas, um canto sossegado onde um dia eu possa morrer.
(BRAGA, 2001)

As questões vinculadas à privacidade do indivíduo pelo uso de tecnologias não são apenas de agora, a repercussão e os conceitos iniciais sobre a privacidade emergiram devido à utilização de novas tecnologias no século XIX, que sutilmente começaram a permitir o acesso e a divulgação de momentos relativos à vida privada do indivíduo. Neste contexto, esse capítulo objetiva-se por meio de revisão bibliográfica resgatar definições e abordagens de privacidade que foram se adequando juntamente com a evolução dos aparatos tecnológicos.

O fortalecimento da necessidade de privacidade em relação à divulgação de fatos da vida privada foi evidenciado pela publicação do artigo intitulado "Direito a privacidade" dos autores Warren e Brandeis, em 1890, na *Harvard Law Review*. Esse artigo aflorou a doutrina e jurisprudência para questões de privacidade, cujo foco principal foi às preocupações com o surgimento de dispositivos e as atividades que poderiam invadir a vida privada dos indivíduos, tais como as máquinas fotográficas e as empresas jornalísticas, que ameaçavam tornar real a predição de que "o que é sussurrado no armário deve ser proclamado no telhado". O impulso para os autores foi à intrusão pela imprensa na vida familiar e social de Warren, que revelou detalhes de eventos na sua casa, tal como o casamento de sua filha. Para Pereira (2003) o direito a privacidade declarado por Warren e Brandeis faz uma acepção ao direito de defesa, tendo como núcleo o direito a intimidade com caráter de exclusão.

> A doutrina jurídica, e também a jurisprudência, e tendo em vista a natureza negativa do direito à intimidade, atribuíram a este direito um status de defesa contra intromissões que poderiam ser realizadas tanto pelos Poderes Públicos, como por particulares (PEREIRA, 2003, p. 127).

Para Doneda (2006) é importante não ignorar que a privacidade emergiu como um direito vinculado à classe burguesa[33], no entanto, foi potencializada pelo crescimento do fluxo

[33] "A possibilidade de aproveitar plenamente a própria intimidade é uma característica que diferencia a burguesia das demais classes: e o forte componente individualista faz com que esta operação se traduza, posteriormente, em um instrumento de isolamento do indivíduo burguês em relação à sua própria classe [...] portanto, o nascimento da privacidade não se apresenta como a realização de uma experiência "natural" de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo. Não é por acaso que seus instrumentos jurídicos de tutela foram predominantemente modelados com base naquele característico do direito burguês por excelência: a propriedade;

de informação que acentuou a importância da privacidade como uma necessidade para outras liberdades fundamentais.

Para Warren e Brandeis (1890), ninguém tem o direito de publicar algo sem o consentimento do sujeito, independentemente do que seja. Neste contexto, os autores apoiaram suas definições e discussões na abordagem de privacidade determinada por "*The right to be let alone*", o direito de ficar sozinho ou deixado em paz, cunhado pelo juiz norte americano Judge Cooley. Nessa abordagem, a privacidade é entendida como solidão e não como intrusão. O direito de "ser deixado só" foi uma necessidade em relação à coleta e divulgação de informações referentes a uma pessoa, especificamente por meio de publicações e circulações não autorizadas de fotografias.

> Nenhum outro tem o direito de publicar suas produções sob qualquer forma, sem o seu consentimento. Este direito é totalmente independente do material sobre o qual, ou os meios pelos quais, o pensamento, o sentimento ou a emoção são expressos (WARREN; BRANDEIS, 1890, p. 99, tradução nossa) [34].

Muitas vezes, os termos privacidade, intimidade e vida privada emergem indistintamente. Assim, para delimitar conceitos envolvidos com vida privada, foi criada por Heinrich Hubmann[35] a Teoria dos Círculos Concêntricos da Esfera da Vida Privada, na qual Hubmann busca exemplificar os graus de privacidade (SZANIAWSKI, 1993).

Segundo a teoria dos círculos concêntricos, a esfera de menor raio (interna), a *Intimsphare*, ou seja, intimidade é onde o indivíduo mantém segredo supremo perante a coletividade, caracterizando maior grau de privacidade (SZANIAWSKI, 1993). Para Pereira (2003, p. 111) "[...] a intimidade é o mais interior da pessoa, seus pensamentos, ideias, emoções" e está vinculado ao 'direito de ficar só' pelo juiz norte americano Judge Cooley, como citado anteriormente.

O segundo círculo, o intermediário, consiste na esfera secreta, denominado de *Geheimnisphare*, é mais ampla que a esfera *Intimsphare*, nela os segredos são compartilhados com poucas pessoas, como parentes e amigos mais próximos. A última esfera é onde desenvolve a personalidade da pessoa que é a esfera privacidade (externa), a *Privatsphare*, onde não se tem

---

e que exigências análogas àquelas que a burguesia fez valer ou não foram reconhecidas em qualquer media à classe operária ou foram somente mais tarde [...]" (RODOTÀ, 2008, p. 26-27).

[34] "*No other has the right to publish his productions in any form, without his consent. This right is wholly independent of the material on which, or the means by which, the thought, sentiment, or emotion is expressed*".

[35] Autor da obra *Persönlichkeitsrecht* de 1953. 'Esta teoria foi posteriormente utilizada pelo Tribunal Constitucional Federal Alemão, no célebre acórdão de 1983 que autonomizou o direito à autodeterminação informativa' (CORREIA; JESUS, 2013, p. 147)

o conhecimento dos fatos da vida das pessoas, o acesso público é restrito, caracterizando a vida privada (SZANIAWSKI, 1993).

No mesmo contexto, Westin (1967), afirma que o indivíduo pode passar por vários estágios proporcionados pela privacidade, e enfatiza a abordagem da privacidade como o direito de ficar só. Para o autor, quando o indivíduo tem necessidade de ficar sozinho e realiza o diálogo consigo mesmo, mantendo-se afastado de qualquer observação e convívio com outras pessoas, ele entra em estado de solidão, caracterizando como o estado mais completo de privacidade, o direito de ficar só. No entanto, em vários momentos da vida, o indivíduo se mantém mais próximos de algumas pessoas, criando uma relação mais íntima, como a relação marido-esposa, ou um convívio mais próximo com entes familiares. Nesses casos, a privacidade se caracteriza como intimidade (WESTIN, 1967).

A necessidade de limitar a comunicação para aqueles que estão à sua volta, guardando seus segredos e evitando falar sobre si, faz com que o indivíduo entre em estado de reserva (WESTIN, 1967). E por último, há situações em que a identidade do indivíduo não pode ser conhecida num conjunto de fatos, como na divulgação de dados da saúde, onde é preciso garantir a privacidade dos referenciados no conjunto de dados e, ao mesmo tempo, disponibilizar dados de interesse da sociedade. Nesse cenário, a privacidade atua como anonimato para o indivíduo (WESTIN, 1967). Para Wallace (2008) o anonimato busca proteger alguém pela responsabilidade da ação, evitar a discriminação, evitar represálias, pois o anonimato e a privacidade estão intrinsicamente relacionados, sendo o anonimato um meio de garantir a privacidade.

Embora o indivíduo possa perpassar por esses estágios, ele não fica necessariamente e permanentemente em um estágio. Westin (1967) afirma que, em determinado momento, o indivíduo deseja estar recluso com sua família ou amigos íntimos; em outro, deseja o anonimato; em algumas situações deseja estar totalmente sozinho e não observado; ainda, em outras ocasiões, pode desejar conviver em grupos.

Nesse contexto, Westin (1967) define que a privacidade é basicamente um meio para o indivíduo atingir metas individuais e ajustar seus mecanismos emocionais aos sociais que ele encontra na vida diária, não se caracterizando como estado autossuficiente, nem um fim em si. Assim, a privacidade se torna adaptável de acordo com o contexto, o que pode impactar no modo que visualiza as ameaças que pode sofrer devido a sua exposição ou divulgação de seus dados.

Para explicitar o motivo pelo qual o indivíduo busca por privacidade, Westin (1967) indica quatro funções específicas: autonomia pessoal, liberdade pessoal, auto avaliação,

comunicação limitada e protegida. Desta forma, quando o indivíduo entra em estado de privacidade (solidão, intimidade, reserva e anonimato), ele busca por uma das seguintes funções:

- ✓ **Autonomia pessoal**: está vinculada ao desejo de evitar ser manipulado, dominado ou exposto aos outros. A ameaça mais séria à autonomia de um indivíduo é a possibilidade de permitir que o invasor conheça seus segredos extremos, seja por meio físico ou psicológico. Quando acontece essa invasão, o indivíduo fica vulnerável a situações constrangedoras, e pode ficar sob controle daqueles que conheceram seus segredos. A capacidade do indivíduo de decidir quando revelar seus segredos ao público é um aspecto crucial para o sentimento de autonomia.
- ✓ **Liberdade emocional**: a privacidade, nesse aspecto, proporciona ao indivíduo a possibilidade de estar livre, retirar a máscara, viver momentos de anonimato nas ruas, ficar despercebido perante um grupo, permitindo que os indivíduos se desviem, temporariamente, da etiqueta social, podendo realizar ações permitidas quando se está sozinho, tais como colocar os pés na mesa, xingar, entre outros. A privacidade se torna importante na vida do indivíduo quando ele passa por momentos de perda, choque ou tristeza. Nesses momentos, a sociedade proporciona conforto, tanto por meio de apoio quanto pelo respeito à privacidade do indivíduo e de seus íntimos.
- ✓ **Auto avaliação**: a privacidade é essencial para que o indivíduo exerça a auto avaliação, visto que cada indivíduo precisa de um momento sozinho para assimilar as informações que recebe durante suas atividades. Assim, a privacidade proporciona um tempo para analisar, reformular e originar novas ideias, visto que estudos de criatividade mostram que é na reflexão durante um momento de solidão que um pensamento é verbalizado.
- ✓ **Comunicação limitada e protegida**: a maior ameaça à vida social seria se cada indivíduo fosse totalmente sincero por meio de sua comunicação com os outros, dizendo exatamente o que sabe e o que sente em todos os momentos. Essa função envolve dois aspectos: oferecer ao indivíduo a oportunidade de compartilhar informações confidenciais e intimidades com aqueles que ele confia, no caso, as pessoas próximas, como seus pais, filhos, marido, esposa, e colegas próximos de trabalho; estabelecer limites entre a esfera pública e a privada.

Os estudos de Westin (1967) vinculam a essência da privacidade com a noção de autonomia e controle. Assim, o autor define privacidade "[...] como o direito de indivíduos, grupos, instituições determinar por si mesmo, quando, como e em que medida as informações sobre eles são comunicadas aos outros" (WESTIN, 1967, p. 5). Observa-se, nesse sentido, que

Westin (1967) foca as suas preocupações de privacidade no compartilhamento de informações do indivíduo com terceiros, no âmbito do controle e da disponibilização, e não na coleta de dados propriamente.

A definição de Westin cria uma nova visão ao direito a privacidade, não ficando limitado apenas no direito à exclusão (WARREN; BRANDEIS, 1890), mas apoiando-se no direito ao controle. Para Pereira (2003, p. 127) "[...] o direito à intimidade passa a ter, também, um caráter dinâmico pelo qual o indivíduo pode exercer um controle sobre o que deve ou não ser conhecido, por parte dos demais, sobre determinados aspectos de sua personalidade".

Embasado também na abordagem de controle ou autodeterminação informativa[36], Rodotà (1995) afirma que o "direito de ser deixado só", embora ainda envolva a essência do problema da privacidade, já não traz tanta representatividade, concedendo lugar ao poder de controle. Nesse cenário, Rodotà (1995, p. 122, tradução nossa) [37] define a privacidade como "[...] o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada". O autor, ainda, ressalta que o direito à privacidade não está mais embasado na tríade "pessoa-informação-segredo", mas sim nos elementos "pessoa-informação-circulação-controle". Dessa forma, o titular dos dados passa a exigir seu direito de controlar os diversos aspectos envolvidos no controle de seus dados.

Moore (2008) também defende a definição de privacidade baseada no controle, sendo direito do indivíduo controlar o acesso a lugares e às informações pessoais, juntamente com o direito de uso e de controle para esses elementos. Assim, o autor define que o direito à privacidade "[...] é um direito de controle de acesso e uso de lugares, corpos e informações pessoais" (MOORE, 2008, p. 27, tradução nossa) [38], limitando o acesso público a si mesmo e as informações sobre si mesmo.

> A privacidade é o controle sobre quando e por quem as várias partes de nós podem ser percebidas por outras. Por percebido, significa simplesmente ver, ouvir, tocar, cheirar ou provar. Por "partes de nós" também inclui objetos muito intimamente associados a nós. Por "intimamente associado" entende-se principalmente o que é espacialmente associado. Os objetos que são "partes de nós" são objetos que nós geralmente mantemos conosco ou trancados em

[36] A sentença de 15 de dezembro de 1983, do Tribunal Constitucional Federal alemão, consolidou a existência de um "direito à autodeterminação informativa" (*informationelle selbstestimmung*), que consistia no direito de um indivíduo controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa (DONEDA, 2011, p. 95).

[37] "*Diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera private*".

[38] "*A right to privacy is a right to control access to and uses of places, bodies, and personal information*".

> um lugar acessível apenas para nós (PARKER, 1974, p. 281, tradução nossa) [39].

No cenário de não ter as informações conhecidas por terceiros, caracterizando a não intercepção de informação, Wang (2011, p. 8, tradução nossa) [40] afirma que a privacidade é "[...] um direito, que consiste em um número de interesses individuais, e que indivíduos querem manter seus negócios e informações pessoais livre de interferências de outros".

No domínio da doutrina jurídica e jurisprudência, Pereira (2003) ressalta que ambos atribuíram o direito a privacidade ao status de defesa contra as intromissões que poderiam acontecer à vida privada do indivíduo tanto pelos poderes públicos quanto por particulares.

Tavani (2008) também aborda as questões de intercepção e de controle ao distinguir quatro tipos de privacidade: (1) privacidade física ou de acessibilidade, que considera a privacidade como não intrusão no espaço físico; (2) privacidade de decisão, que determina a não interferência nas escolhas pessoais; (3) privacidade psicológica e mental, que consideram que o pensamento e a identidade pessoal não devem ser invadidos; e (4) a privacidade informacional, que possibilita ter o controle sobre o acesso à informação pessoal.

O conhecimento de informações pessoais por terceiros também é abordado por Parent (1983b). O autor afirma que "[...] a privacidade deve ser definida como a condição de não ter informações pessoais indocumentadas[41] sobre si mesmo conhecidas por outras" (PARENT, 1983b, p. 306, tradução nossa) [42], visto que o conhecimento das pessoas sobre o indivíduo faz a sua privacidade ser diminuída. Decew (1986) critica a abordagem dada por Parent (1983b), pois não considera que a privacidade esteja apenas vinculada a não ter posse e aquisição do conhecimento pessoal indocumentado, pois deve se proteger tanto a privacidade da informação civil quanto a privacidade da informação constitucional.

Como pode ser observado, o conceito de privacidade é plurifacetado e pode apresentar várias definições, dependendo do contexto, do ambiente e da necessidade do indivíduo, tanto no âmbito jurídico como em questões de ética, tornando-se, assim, um tema que atende uma

---

[39] "*Privacy is control over when and by whom the various parts of us can be sensed by others. By 'sensed' is meant simply seen, heard, touched, smelled, or tasted. By 'parts of us' is meant the part of our bodies, our voices, and the products of our bodies. 'Parts of us' also includes objects very closely associated with us. By 'closely associated' is meant primarily what is spatially associated. The objects which are 'parts of us' are objects we usually keep with us or locked up in a place accessible only to us*".

[40] "[...] *is a right, which consists of a number of individual interests that individuals have in keeping their personal information and personal affairs free from interference from others*".

[41] Para o autor, informações indocumentadas é o oposto de informações documentadas, esta última definida por Parent (1983b) como informações encontradas em registro público ou que estão disponíveis publicamente, por exemplo, informações encontradas em jornais, processos judiciais e outros documentos oficiais abertos ao público.

[42] "[...] *privacy be defined as the condition of not having undocumented personal information about oneself known by others*".

variedade de interesses (WESTIN, 1967; GAVISON, 1980; POST, 2001; SOLOVE, 2006; DECEW, 1986; WANG, 2011).

Para Gavison (1980), embora elementos como segredo, anonimato e solidão sejam distintos e independentes, eles se mantêm inter-relacionados com o conceito de privacidade. De acordo com Gavison (1980, p. 421) "[...] o indivíduo tem privacidade perfeita quando ele está inacessível para outros" [43], e a privacidade pode ser caracterizada por meio de algumas questões como: a quantidade de informações conhecida sobre um indivíduo e os problemas da relação entre o indivíduo e a correlação com trechos de informações; a atenção sobre um determinado indivíduo; o acesso físico a um indivíduo; e a relação entre os elementos segredo, anonimato e solidão (GAVISON, 1980).

Ao abordar sobre os problemas da correlação do indivíduo com fragmentos de informação, Gavison (1980) realiza a seguinte comparação metafórica: durante uma festa, ao responder a uma pergunta sobre situações que acontecem no confessionário, o sacerdote revela que a situação mais estranha que lhe aconteceu foi a revelação de um crime por um confessionário durante a sua primeira confissão como sacerdote. No mesmo instante, chega à roda um senhor bem aparentado e cumprimenta o sacerdote, quando perguntaram de onde eles se conheciam, o senhor disse: fui o primeiro que se confessou com ele. Essa situação é muito representativa nos dias atuais, em que todos os rastros deixados nos ambientes digitais se caracterizam como pedaços de informação que, quando correlacionados, podem revelar muito sobre o indivíduo, causando brechas de privacidade.

Essa situação pode ser representada ao que Westin (1967) cunhou como *data shadow* (sombra de dados), um meio figurativo para representar o rastreamento de indivíduos por meio de dados, pois, a partir da persistência de dados que contém opiniões e fatos da vida particular, esses dados passam a acompanhar esse indivíduo nos mais diversos lugares, sem que ele perceba, contribuindo para o conhecimento sobre a sua vida pessoal. Assim, observa-se que, a "sombra de dados" prevalece nos diversos ambientes digitais e serviços tecnológicos utilizados pelos indivíduos, revelando cada vez mais dados que, de certa forma, deveriam estar apenas na esfera privada do indivíduo.

Westin (1967) leva em consideração que o direito à privacidade não se trata de um direito absoluto, pois muitas vezes ele é baseado em outros direitos coletivos ou individuais:

[43] "*An individual enjoys perfect privacy when he is completely inaccessible to others*".

> O desejo do indivíduo por privacidade nunca é absoluto, uma vez que a participação em sociedade é igualmente importante. Assim, cada indivíduo está continuamente envolvido em um processo pessoal de equilíbrio entre o desejo de privacidade e o desejo de exposição e comunicação com os outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive. O indivíduo o faz em face das pressões da curiosidade dos outros e dos processos de vigilância que toda sociedade necessita para a implementação de normas sociais (WESTIN, 1967, p. 7).

Solove (2002) também corrobora que a privacidade pode ser discutida sob diferentes vertentes e, ainda, considera que cada uma tem um ponto de vista diferente sobre privacidade, e os conceitos podem sobrepor-se. Assim, o autor destaca seis aspectos que são pilares para a definição de privacidade: o direito de ser deixado só; o acesso limitado ao eu; o segredo; o controle de informações pessoais; a personalidade e a intimidade. Nesse sentido,

> [...] a privacidade é um conceito abrangente, englobando (entre outras coisas) a liberdade de pensamento, o controle sobre o corpo, a solidão na casa, o controle sobre informações pessoais, a liberdade da vigilância, a proteção da reputação e a proteção contra buscas e interrogatórios (SOLOVE, 2002, p. 1088, tradução nosssa) [44].

Wang (2011) ressalta que a maioria das definições de privacidade tentou distinguir conceitos relacionados à forma de privacidade, como a intimidade, a autonomia, o controle aos acessos, e não a um conceito específico.

A privacidade é, em si, um conjunto de direitos, derivada de outros direitos, como a vida, a liberdade e os direitos de propriedade. Não se trata, portanto, de um grupo específico de direitos, mas do entrelaçamento de grupos de direitos: "[...] o direito à privacidade está em todo lugar, sobreposto por outros direitos" [45] (THOMSON, 1975, p. 310). A autora ressalta que ao se torturar um indivíduo, a fim de descobrir informações pessoais, acontece a violação do direito (o direito de não ser torturado para obter informações pessoais), que tanto é um direito à privacidade, por causa das informações pessoais, quanto é um direito de não ser ferido e prejudicado. Assim, mais de um direito é infringido.

No entanto, Nissenbaum (2011) crítica o conceito de privacidade estar atrelado a outros direitos. Para a autora, a privacidade não é apenas o direito ao segredo, estar sozinho ou ao controle, mas está vinculada ao fluxo apropriado de informação pessoal nos diversos contextos. Para verificar as possíveis brechas de privacidade, é preciso analisar o contexto, os atores, o

---

[44] "[...] *privacy is a sweeping concept, encompassing (among others things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogation*".
[45] "*I suspect there aren't any, and that the right to privacy is everywhere overlapped by other rights*".

tipo de informação e os princípios de transmissão, tais como a confidencialidade, a reciprocidade e a necessidade.

Doneda (2006) ressalta que, embora a privacidade seja definida sob várias perspectivas, é difícil defini-la em um único conceito. Para Leonardi (2011) a falta de clareza sobre as definições de privacidade dificulta a definição de políticas públicas e resolução de julgados práticos, pois se torna difícil enunciar os danos vinculados a privacidade em situação jurídica, dificultando ou inviabilizando sua tutela.

Contudo, Doneda (2006) argumenta ainda que é perceptível que a privacidade está sempre envolvida com as tecnologias, independentemente da época e sociedade: "[...] o advento de estruturas jurídicas e sociais que tratem do problema da privacidade são respostas diretas a uma nova condição da informação, determinada pela tecnologia" (DONEDA, 2006, p. 37). Moor (2006, p. 114) argumenta que a privacidade é "[...] um conceito em evolução e que seu conteúdo é frequentemente influenciado pelas características políticas e tecnológicas do ambiente da sociedade". A justificativa aos conceitos de privacidade estarem envolvidos com as tecnologias fica evidente na fala de Fairfield (2005). Para o autor,

> [...] mais transações tenderão a ser registradas; os registros tendem a ser mantidos por mais tempo; A informação tende a serem dadas a mais pessoas; mais dados tendem a ser transmitidos através de canais de comunicação públicos; **Menos pessoas saberão o que está acontecendo com os dados**; os dados tendem a ser mais facilmente acessíveis; e os dados podem ser manipulados, combinados, correlacionados, associados e analisados para produzir informações que não poderiam ter sido obtidas sem o uso de computadores (FAIRFIELD, 2005, p. 38, tradução nossa, grifo nosso) [46].

Ao explanar sobre o direito à privacidade em uma sociedade *orwelliana*, Correia e Jesus (2013) argumentam que, no contexto das tecnologias da informação, há uma associação entre a proteção da privacidade e a proteção de dados pessoais, no entanto, caracterizam-se como direitos distintos e autônomos. Assim, os autores concluem que o direito à privacidade está envolvido com elementos que garantam a permanência do indivíduo em sua esfera privada, como o estado de solidão, a guarda de seus segredos ou o seu anonimato, mantendo-se protegido contra qualquer intrusão. Já o direito à proteção de dados pessoais delimita essa proteção aos dados que passam por tratamento automatizado, em que a abordagem está relacionada ao poder de controlar a utilização de dados pessoais, caracterizando a autodeterminação informativa.

[46] "[...] *the records will tend to be kept longer; information will tend to be given to more people; more data will tend to be transmitted over public communication channels; fewer people will know what is happening to the data; the data will tend to be more easily accessible; and data can be manipulated, combined, correlated, associated and analyzed to yield information which could not have been obtained without the use of computers*".

Pereira (2003, p. 123), afirma que a "doutrina que se ocupa do estudo do Direito Informático[47] costuma vincular a ideia de privacidade com a da proteção de dados pessoais tratados eletronicamente".

A privacidade também está atrelada às questões de consciência, Pötzsch (2008, p. 228, tradução nossa) [48], ao abordar sobre ferramentas que apoiam consciência nos ambientes digitais, define que "[...] a consciência é baseada na atenção, percepção e cognição física e não física de um objeto pelo sujeito", e ainda, que o estado de estar ciente prevalece enquanto há estímulos, por meio de informações do ambiente ou de outras pessoas.

Patil e Kobsa (2009) argumentam que os conceitos de consciência e de privacidade são ambos relacionados à divulgação da informação, isso pode ser observado na presença das políticas de privacidade nos ambientes digitais, cujo objetivo é disponibilizar informações para que o usuário tenha consciência da coleta e do uso dos dados.

No contexto das diversas definições de privacidade, Pötzsch (2008) ressalta dois conceitos vinculados a tecnologias da informação e à consciência sobre privacidade:

- ✓ Privacidade da esfera pessoal: baseada na definição de Warren e Brandeis (1890), como o "direito de ser deixado sozinho". Nesse conceito, a privacidade é entendida como solidão e não intrusão;
- ✓ Privacidade de dados pessoais, muitas vezes mencionada pelos pesquisadores da ciência da computação como o direito de o usuário selecionar quais dados pessoais sobre ele podem ser conhecidos por outros, essa definição enfatiza o aspecto de controle sobre a informação dos indivíduos, suas conversas e suas ações.

Para Pötzsch (2008), a privacidade da esfera pessoal considera especialmente os aspectos sociais da privacidade, enquanto a privacidade de dados pessoais está mais focada nos dados e, portanto, muito mais orientado para a técnica. No entanto, não se pode negar que os dois conceitos estão relacionados, pois a coleta de dados realizada pelos dispositivos tecnológicos contribui exacerbadamente para que ocorram várias brechas de privacidade, o que por si só influencia os aspectos sociais do indivíduo. De acordo com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, "[...] o direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na

[47] "Conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador – como meio e como fim- que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do software; o comércio eletrônico, e as relações humanas realizadas de maneira sui generis nas redes, em redes ou via internet" (PAIVA, 2003).

[48] "*Awareness is based on an individual's attention, perception and cognition of physical as well as non-physical objects*".

sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade" (UNIÃO EUROPEIA, 2016).

Considerando os dois conceitos de privacidade, Pötzsch (2008) afirma que ter consciência sobre privacidade deve envolver atenção, percepção e cognição em relação a:

- ✓ Quais dados pessoais são coletados?
- ✓ Como esses dados são ou podem ser processados e usados?
- ✓ Qual a quantidade de dados sobre as atividades do indivíduo pode ser obtida?

A consciência sobre a privacidade permite que indivíduos tomem decisões informadas. Consequentemente, pode-se supor que pessoas conscientes das questões de privacidade declaram a intenção de proteger seus dados pessoais e a esfera pessoal (PÖTZSCH, 2008).

Devido à privacidade apresentar várias definições e estar envolvida com outros conceitos, Patil e Kobsa (2009) descrevem três perspectivas para contextualizar a privacidade, incluindo as questões tecnológicas:

- ✓ Normativa: em que a privacidade é um conceito ético, visto como um "direito" do indivíduo e, portanto, uma questão de liberdade. Nessa perspectiva, a privacidade do indivíduo precisa ser protegida por meios legais e, cada vez mais, a legislação é ampliada para proteger a sua esfera privada.
- ✓ Social: em que a privacidade é construída com base no comportamento e nas interações de indivíduos. A consciência sobre privacidade evolui à medida que as mudanças externas provocam alterações nas expectativas e nos comportamentos, ou à medida que a tecnologia introduz novas formas ou meio de interação.
- ✓ Técnica: em que a privacidade é vista no contexto do uso de sistemas de informação. Nesse sentido, a privacidade é tratada considerando o controle adequado sobre dados e informações, incluindo mecanismos e técnicas para garantir a privacidade na coleta, armazenamento e propriedade no uso e acesso a dados pessoais.

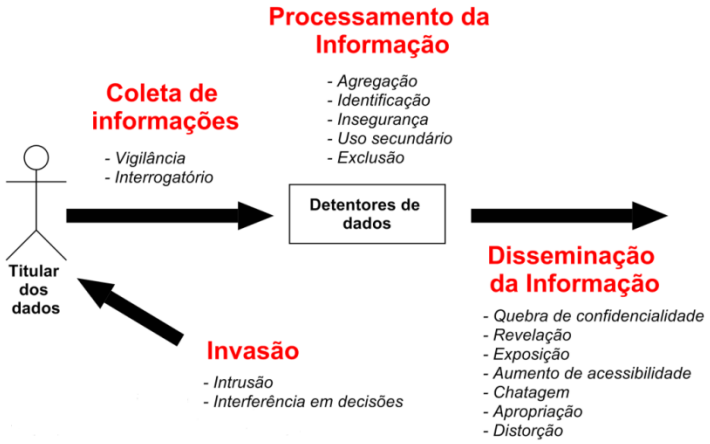
Para Patil e Kobsa (2009), as três perspectivas não atuam isoladas. Ao contrário, elas são correlatas e podem contribuir umas com as outras, pois as leis de privacidade podem ser promulgadas com base em considerações técnicas ou sociais, enquanto as interações sociais podem ser alteradas devido às mudanças de leis e de tecnologias.

Observa-se que a privacidade pode estar envolvida a muitos conceitos, ora no âmbito do controle e do consentimento, ora representada em um conjunto de direitos. Devido a essa diversidade de conceitos, Solove (2006) argumenta que o termo se torna vago, e que muitos a define como um conceito unitário. No entanto, para o autor, quando se trata em proteger a

privacidade, isso não está claro, pois os danos à privacidade não estão explícitos; se existe essa obscuridade, o desenvolvimento de leis e medidas para proteger a privacidade é afetado.

Baseado nesse cenário, Solove (2006) desenvolveu uma taxonomia que se concentra nos diferentes tipos de atividades que influenciam a privacidade, ressaltando: “Eu me esforço para mudar o foco do vago termo ‘privacidade’” (SOLOVE, 2006, p. 481) [49]. O Framework proposto por Solove (2006) consiste em uma taxonomia por meio dos grupos e subgrupos para evidenciar as ameaças à privacidade nas fases de coleta, processamento, disseminação da informação e invasão (Figura 7).

Figura 7 - Elementos da taxonomia de privacidade



Fonte: Solove (2006, p. 490, tradução nossa)

O primeiro grupo é a coleta de informações, representado pelas atividades que ameaçam e violam a privacidade do indivíduo no momento da coleta. Esse grupo possui duas formas de coletar informação do usuário, a vigilância e o interrogatório (SOLOVE, 2006).

Devido à coleta de dados ocorrer durante a permanência do usuário no ambiente, emerge a vigilância como a atividade que possibilita descobrir novas informações, além do que se procurava inicialmente, contribuindo para que o detentor de dados tenha um maior conhecimento sobre o titular dos dados (SOLOVE, 2006).

Na coleta de dados por interrogatório acontece a sondagem do indivíduo, com a finalidade de coletar informações. Essa atividade, muitas vezes, exerce uma pressão no indivíduo para que ele divulgue suas informações (SOLOVE, 2006).

No segundo grupo, Solove (2006) discute cinco formas de processamento da informação: agregação, identificação, insegurança, uso secundário e exclusão.

[49] *“I endeavor to shift focus away from the vague term ‘privacy’.*

Na agregação acontece a combinação de vários dados do indivíduo, coletados nos mais diversos contextos. Quando correlacionados e analisados esses dados, resultam na construção do perfil do usuário, revelando novos fatos sobre uma pessoa, que antes não eram conhecidos quando os dados estavam isolados (originais) (SOLOVE, 2006).

A atividade de agregação se sobressai, atualmente, devido aos avanços nas tecnologias da informação e comunicação. Embora ela possa resultar em benefícios para o usuário, em termos de recuperação da informação, implica a construção de perfil sobre a vida do indivíduo. Quando o titular deixa seus dados nas mais diversas atividades, acredita que seus dados estão sendo coletados apenas naquele momento, não fica claro que esses dados ao serem agregados vão permitir um conhecimento muito maior sobre sua vida (SOLOVE, 2006).

A identificação é a fase que referencia um indivíduo no conjunto de dados que alguém teve o acesso. Para Solove (2006), o problema da identificação se dá com a vinculação dos dados a um único sujeito, pois ao correlacionar identidade ao contexto, promove-se o aprendizado sobre o titular dos dados em várias transações e atividades. A identificação é uma fase vinculada à vigilância e à agregação, pois facilita a detecção e a monitoração, além de vincular o usuário diretamente ao seu contexto real.

A insegurança é causada pelas falhas na identificação do usuário, roubo de identificação de identidade e perfis, e como os dados coletados ficam sob tutela de terceiros, no caso o detentor de dados, resta ao usuário confiar nas ações que esses promovem para proteger a privacidade (SOLOVE, 2006).

A insegurança é causada devido os dados coletados estarem sob tutela de terceiros, assim, às medidas de segurança em relação às falhas na identificação do usuário, o roubo de identidade e perfis, ficam sob responsabilidade do detentor de dados, restando ao usuário confiar nessas ações para proteção da privacidade (SOLOVE, 2006).

O uso secundário é a utilização dos dados que foram coletados para fins diferentes daqueles que o titular de dados consentiu ou que teve consciência no momento da coleta. Assim, o titular de dados poderia não permitir a coleta, se ele não soubesse para qual propósito seria o uso dos seus dados. Logo, o uso secundário dos dados assemelha-se ao dano causado pela insegurança, pois o indivíduo perde o controle sobre as atividades que serão realizadas com seus dados, gerando incertezas sobre como a informação será utilizada no futuro (SOLOVE, 2006).

A atividade de exclusão envolve a consciência do usuário em relação às questões relacionadas à coleta dos seus dados, dentre elas: o conhecimento sobre quais dados serão coletados; o processo de tratamento que será realizado com os dados pessoais; a alteração dos

seus registros de dados. Assim, a exclusão acontece quando o indivíduo é ignorado sobre o uso de seus dados, por não ser informado sobre a coleta e o tratamento dos seus dados. A exclusão também cria uma sensação de vulnerabilidade em relação à informação pessoal, pois a falta de controle sobre seus dados pode levar a sentimentos de impotência e de frustação (SOLOVE, 2006).

O terceiro grupo de atividades envolve a disseminação de informação. Consiste na revelação ou ameaça de divulgação de informações pessoais. Nesse grupo estão presentes as seguintes atividades: violação de confidencialidade, revelação, exposição, aumento da acessibilidade, chantagem, apropriação e distorção (SOLOVE, 2006).

A violação da confidencialidade envolve a revelação de segredos sobre uma pessoa, principalmente os vinculados a dados pessoais. Quando as pessoas utilizam serviços de bancos, provedores de serviços de Internet ou empresas de telefonia acreditam que suas informações estão sob sigilo, e que essas empresas garantem que informações não serão divulgadas para terceiros (SOLOVE, 2006).

A revelação (divulgação) está vinculada ao uso secundário da informação compartilhada, ocorre quando a informação sobre o indivíduo é divulgada publicamente, implicando na exposição das informações para terceiros (SOLOVE, 2006).

O subgrupo exposição caracteriza-se por mostrar a terceiros informações sobre condições físicas e emocionais de indivíduos, atributos que, quando expostos, podem criar constrangimento, humilhação em todos os aspectos da vida privada (SOLOVE, 2006).

Ainda, há situações que as consequências da coleta de dados podem levar ao que Solove (2006) denomina de chantagem, que consiste em coagir um indivíduo à exposição de seus segredos pessoais, caso não atenda às exigências do chantageador.

A fase de disseminação da informação é influenciada pelo aumento de acesso da informação, pois a informação sobre o indivíduo pode ser compartilhada com terceiros e ser utilizada para outros fins, diferentes daqueles que o usuário teve ciência de como seriam utilizados quando fez o uso do serviço (SOLOVE, 2006).

A manipulação da forma como um indivíduo é percebido e julgado pelos outros, podendo resultar em constrangimento, humilhação e danos à reputação, devido à divulgação de uma informação que não é verdadeira, é caracterizada pela ameaça de distorção (SOLOVE, 2006).

O quarto e último grupo envolve a invasão em assuntos privados das pessoas, representada pelas atividades de intromissão e de interferência em decisões.

A intromissão refere-se aos atos invasivos em assuntos privados do indivíduo, que perturbam a sua tranquilidade ou solidão, muitas vezes alterando suas rotinas e causando situações desconfortáveis (SOLOVE, 2006).

Quando acontece interferência governamental nas decisões dos indivíduos, sobre certos assuntos de suas vidas, caracteriza-se a ameaça à interferência decisional, que permeia áreas que são tradicionalmente consideradas privadas, tais como o lar, a família e o corpo.

2.1 Resultados

Com base nas abordagens sobre privacidade explanadas neste capítulo, o Quadro 1 apresenta uma síntese das definições de privacidade no contexto da informação pessoal e o foco presente em cada definição. Esses conceitos impactaram muito no domínio da privacidade, e é alicerce para as questões de proteção de dados pessoais em vários contextos, desde o amparo aos julgados jurídicos até o desenvolvimento de modelos e técnicas na ciência da computação.

Quadro 1 - Síntese das definições de privacidade no contexto da informação pessoal

Autor (es)	Definição	Abordagem
Warren e Brandeis (1890, p. 99)	"Nenhum outro tem o direito de publicar suas produções sob qualquer forma, sem o seu consentimento".	Consentimento
Westin (1967, p. 5)	"Direito de indivíduos, grupos, instituições determinar por si mesmo, quando, como e em que medida as informações sobre eles são comunicadas aos outros".	Controle
Parker (1974, p. 281)	"A privacidade é o controle sobre quando e por quem as várias partes de nós podem ser percebidas por outras [...]".	
Rodotà (1995, p. 122)	"[...] o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada".	
Tavani (2008)	"[...] a privacidade informacional, que possibilita ter o controle sobre o acesso à informação pessoal".	
Pötzsch (2008)	A privacidade de dados é enfatiza pelo aspecto de controle sobre as informações do indivíduo, suas conversas e suas ações.	
Moore (2010, p. 27)	"[...] é um direito de controle de acesso e uso de lugares, corpos e informações pessoais".	
Wang (2011, p. 8)	"[...] um direito, que consiste em um número de interesses individuais, e que indivíduos querem manter seus negócios e informações pessoais livre de interferências de outros".	Intercepção
Parent (1983b, p. 306)	"[...] a privacidade deve ser definida como a condição de não ter informações pessoais indocumentadas".	Conhecimento
Gavison (1980, p. 421)	Caracteriza a privacidade em relação à quantidade de informação conhecida sobre o indivíduo e os problemas da correlação de informação.	
Thomson (1975, p.310)	"[...] o direito à privacidade está em todo lugar, sobreposto por outros direitos".	Conjunto de direitos a privacidade

Solove (2006, p. 1088)	"A privacidade é um conceito abrangente, abrangendo (entre outras coisas) a liberdade de pensamento, o controle sobre o corpo, a solidão na casa, o controle sobre informações pessoais, a liberdade da vigilância, a proteção da reputação e a proteção contra buscas e interrogatórios".	
Nissenbaum (2011)	A privacidade não é apenas o direito ao segredo, estar sozinho ou ao controle, mas está vinculada ao fluxo apropriado de informação pessoal nos diversos contextos.	Análise do Contexto

Fonte: Elaborado pela autora

Observa-se no Quadro 1 que muitos dos conceitos vinculados à proteção da informação estão relacionados à situação de controle, na qual o titular teria a possibilidade de decidir sobre a coleta, o uso e a divulgação de fatos referentes à sua pessoa.

Interessante ressaltar a abordagem dada por Pötzsch (2008), o autor enfatiza que a privacidade no domínio da divulgação e uso de dados pessoais está vinculada ao destinatário, assim, o indivíduo enquanto proprietário dos dados deve ter a possibilidade de guardar dados confidenciais e a opção de divulgar seus dados para detentores de acordo com seu interesse.

Neste trabalho, cujo foco é a proteção de dados pessoais na fase de coleta, adotou-se o conceito de privacidade baseado em Westin (1967), Parent (1983a) e Solove (2006). Logo, a privacidade no contexto de proteção de dados é o direito do titular dos dados ter consciência sobre as atividades e danos envolvidos na coleta de seus dados, de forma que esses dados não sejam apoderados por terceiros sem que haja o consentimento do titular, fomentando, assim, a autonomia e controle do indivíduo sobre os seus dados.

2.2 Considerações Finais

Neste capítulo foram resgatadas definições e dimensões de privacidade, a fim de explanar as diferentes nuances sobre a temática. Desta forma, foi exposto desde o posicionamento do jurista Judge Cooley com "o direito de ser deixado só", perpassando pelo conceito de privacidade como estado de solidão, intimidade, reserva, anonimato, até questões de consciência, direito ao controle da informação e as ameaças que permeiam as fases de coleta, processamento, disseminação da informação e invasão.

Observa-se que os conceitos e dimensões da privacidade estão atrelados ao controle sobre a informação pessoal, caracterizado como a possibilidade do indivíduo decidir sobre as atividades que serão realizadas com suas informações. Neste trabalho o controle é a possibilidade do usuário interferir na coleta de seus dados pessoais, destaca-se que, para que

esse controle seja efetuado, é necessário que o usuário tenha consciência sobre essa coleta durante a interação com o ambiente digital.

O próximo capítulo explana sobre os elementos envolvidos com a proteção de dados pessoais, tais como: tipos de dados que impactam na identificação do indivíduo presente em um conjunto de dados, e os modelos e técnicas de anonimização para proteção de dados pessoais.

3 ASPECTOS TÉCNICOS ENVOLVIDOS NA PROTEÇÃO DE DADOS PESSOAIS

O modo invisível NÃO oculta seus dados de navegação. Seu empregador, seu provedor de Internet e os websites visitados continuam tendo acesso a essas informações.
(GOOGLE CHROME)

Parte da informação que circula nos ambientes digitais é a informação pessoal, definida por Parent (1983a) como fatos que a maioria das pessoas não gostaria de revelar para outras pessoas, com exceção de pessoas próximas ou familiares, ou situações que são extremamente sensíveis, as quais o sujeito decide não revelar sobre si mesmo.

A informação pessoal, aqui tratada como dados pessoais, representa elemento principal nas questões de privacidade no âmbito das tecnologias da informação. Para garantir e mitigar as ameaças à privacidade dos indivíduos e referenciados em conjunto de dados, busca-se a proteção de dados pessoais, definida pela ISO (2017) como um regime técnico e social para gerenciar e garantir a privacidade informacional e a segurança. O Regulamento (UE) 2016/679 define dado pessoal como:

> [...] qualquer informação relativa a um indivíduo identificado ou identificável [...] que pode ser identificado, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador on-line ou um ou mais fatores específicos de sua identidade física, fisiológica, genética, mental, econômica, cultural ou social desse indivíduo (UNIÃO EUROPEIA, 2016, p. 33) [50].

No Art. 5º do Projeto de Lei 5.276/2016 para a Proteção de Dados Pessoais, o conceito de dado pessoal é relacionado "[...] à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016a).

Lioudakis et al. (2007), ao desenvolver um *framework* que utiliza dados pessoais, define três categorias diferentes de dados pessoais:

- ✓ Dados ativos: aqueles que são controlados pelo usuário. Cabe a ele divulgar, de acordo com o seu interesse, dados como a sua identidade e o número de cartão de crédito. Nesses dados, o usuário tem total ciência da transmissão para um terceiro.

[50] "[...] *means any information relating to an identified or identifiable natural person […] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

- ✓ Dados semiativos: dados originados por sensores e dispositivos *Radio-Frequency IDentification* (RFID). O usuário tem controle parcial sobre esses dados.
- ✓ Dados passivos: dados pessoais que são produzidos e divulgados sem qualquer ação do usuário, tais como vídeo de vigilância e dados coletados por sensores, o usuário aceita passivamente a coleta desses dados, e na maioria das vezes não tem consciência sobre essa atividade.

Vários modelos e técnicas para proteção de dados têm sido estudadas e propostas para minimizar os impactos nas questões vinculadas a quebras de privacidade. No entanto, Sweeney (2002) ressalta que, antes de compreender os modelos de proteção de privacidade, é preciso distinguir a proteção de privacidade e anonimização da área de segurança da informação. Enquanto a segurança da informação visa restringir o acesso à informação, o estudo da proteção da privacidade e anonimização buscam meios para evitar a divulgação da identidade de um indivíduo, sem permitir sua identificação na amostra de dados (SWEENEY, 2002).

Anonimização é o conjunto de métodos e técnicas para proteger os dados de indivíduos referenciados em um conjunto de dados antes de liberá-los para publicação, tornando o referenciado não identificável dentro de um conjunto de assuntos. Por meio desse procedimento, o dado anonimizado perde a possibilidade de associação, direta ou indiretamente, a um indivíduo específico (BREKNE; ÅRNES; ØSLEBØ, 2005; JÄNDEL, 2014; BRASIL, 2016a). A proteção da privacidade baseada em anonimização garante que os dados publicados não possam ser vinculados de volta a um indivíduo (NERGIZ; GÖK, 2014).

A busca pela anonimização visa impedir o processo de reidentificação (ou de desanonimização), definido por Rubinstein e Hartzog (2015) como o processo de tentar descobrir a identidade do indivíduo, cujos identificadores foram removidos do conjunto de dados. A reidentificação é o processo de associação de dados pessoais sem qualquer tipo de identificador com a identidade de seu proprietário, utilizando para isso informações auxiliares (BUCHMANN et al., 2013).

A gênese da anonimização foi determinada em dados estruturados por meio das tabelas relacionais que estruturam o conjunto de dados. Posteriormente, devido à expansão das tecnologias, o conceito ampliou-se também para dados não estruturados.

Uma tabela de dados relacional armazena os dados a serem anonimizados, em que cada registro contém um conjunto de atributos. Esse conjunto de dados é normalmente estruturado em uma única relação R, definido em um esquema relacional R (a1, a2, a3,... an), sendo a1 um atributo no domínio Di, com i=1,... n. Esse conjunto de dados possui atributos com informações

sobre indivíduos, que podem ser classificados em identificadores (I), semi-identificadores (SI) e atributos sensíveis (S) (CAMENISCH et al., 2011; SAMARATI, 2001).

Os dados denominados Identificadores (I) caracterizam-se por identificar univocamente o indivíduo no conjunto de dados (nome, número de matrícula, número de registro no plano de saúde, CPF - Cadastro de Pessoa Física, carteira de identidade (Registro Geral), identificadores biométricos, impressões digitais, retina). Esses dados são os primeiros a serem excluídos e protegidos quando o objetivo é garantir a privacidade dos referenciados (SAMARATI, 2001).

No entanto, devido à presença de atributos semi-identificadores, esses conjuntos de dados, que aparentemente foram anonimizados, podem ser combinados com outras bases de dados, ameaçando a privacidade do indivíduo (RUN et al., 2012; SAMARATI; SWEENEY, 1998). Affonso e Sant'Ana (2015) reforçam que a quantidade de semi-identificadores presente em uma base de dados contribui para a descaracterização do anonimato, pois amplia as possibilidades de correlação com outros conjuntos de dados.

Assim, os dados Semi-Identificadores (SI) são aqueles que não identificam univocamente o sujeito referenciado no conjunto de dados, mas quando combinados com uma base de dados externa, podem identificar o indivíduo e descobrir seus dados confidenciais. São classificados como dados semi-identificadores: IP, CEP, data de consultas médicas, data de nascimento, entre outros. Para Clarke (1994), a identificação humana é a associação de dados ou informações a uma determinada pessoa, de modo que seja possível identificar uma pessoa de várias formas, não apenas pelos atributos identificadores, mas também pela associação de dados referentes:

- ✓ Aparência – ou o visual da pessoa;
- ✓ Comportamento social – ou como a pessoa interage com outras;
- ✓ Nomes – ou pelo que a pessoa é chamada por outras pessoas;
- ✓ Códigos – ou como a pessoa é identificada por uma organização;
- ✓ Conhecimento – ou o que uma pessoa sabe;
- ✓ Posses – ou o que a pessoa tem;
- ✓ Biodinâmica – aquilo que a pessoa faz;
- ✓ Fisiologia natural – ou aquilo que a pessoa é;
- ✓ Características físicas impostas – aquilo que a pessoa é agora.

Portanto, por meio dessa combinação de dados e informações, é possível a identificação do indivíduo e, embora o dado seja um elemento bruto, quando combinado com outros dados contribui para a formação de uma nova informação, tornando esse dado significante no contexto das tecnologias da informação.

> Decisivos são sua utilidade e possibilidade de uso. Estas dependem, por um lado, da finalidade a que serve a estatística e, por outro lado, das possibilidades de ligação e processamento próprias da tecnologia de informação. Com isso, um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados "insignificantes" no contexto do processamento eletrônico de dados (SCHWABE, 2005, p. 239).

Formalmente, os semi-identificadores podem ser representados como um conjunto de elementos em uma entidade U na entidade-especificada T (A_1,..., A_n), f_c: U→T e f_g: T→U', onde U⊆U'. O semi-identificador de T, escrito Q_T, é o conjunto de atributos {A_1,..., A_j} ⊆ {A_1,..., A_n} onde ∃*pi* ∈ U ambos que $f_g(f_c(p_i)\ [Q_T]) = p_{i..}$ (SWEENEY, 2002).

A merecida atenção aos SI foi dada por Sweeney (2002), quem descobriu que 87% da população nos Estados Unidos pode ser identificada exclusivamente por meio de três atributos: gênero, data de nascimento e código postal de 5 dígitos (considerados dados semi-identificadores). Esses dados, quando combinados com registros de eleitores, podem identificar o sujeito referenciado, pois ao disponibilizar um conjunto de dados os identificadores são normalmente removidos, por serem explicitamente reconhecidos como atributos que ameaçam a privacidade. No entanto, Sweeney (2002) explicita em seu trabalho que, por meio dos SI, é possível vincular dados confidenciais aos referenciados, ocasionando brechas de privacidade.

Wallace (1999) também ressalta a importância da atenção nos SI para a proteção da privacidade, e exemplifica que com apenas dados referentes ao nascer e ao pôr do sol, vinculados ao horário e a data, é possível fornecer informações sobre a localização de uma viagem, pois a diferença entre o nascer e pôr do sol pode ser usado para determinar latitude, enquanto o valor absoluto do nascer do sol pode ser usado para determinar a altitude. Os dados meteorológicos também podem ser usados para identificar a região de um motorista e serem utilizados para compor um conjunto de dados sobre o indivíduo (WALLACE, 1999).

Outra classificação para os dados são os Atributos Sensíveis (SE). Segundo De Capitani di Vimercati et al. (2012), esses são dados que, quando vinculados a um indivíduo, podem colocá-lo em situação de constrangimento, pois representam dados confidenciais, o que, indubitavelmente, invade a privacidade do referenciado (ex.: notas de alunos, doenças, salário, exames médicos, lançamentos do cartão de crédito).

> Dados que revelam informações sobre uma pessoa que podem potencialmente dar origem à discriminação caso sejam conhecidos por terceiros - além de levar aos seus limites o nível de proteção concedido aos dados pessoais, constitui um ponto de análise valioso por possibilitar identificar a sensibilidade de um ordenamento aos problemas mais graves que envolvem a informação pessoal e as garantias fundamentais da pessoa, como a sua própria liberdade (DONEDA, 2010, p. 189).

No Art. 5º do Projeto de Lei 5.276/2016 para a Proteção de Dados Pessoais é definido que dados sensíveis são:

> Dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos (BRASIL, 2016a).

A invasão de privacidade ocorre quando os valores dos atributos sensíveis publicados podem ser associados a indivíduos específicos (ou empresas) (HAJIAN; DOMINGO-FERRER, 2012).

Quando os dados não se enquadram nas três categorias explicitadas e o uso ou a divulgação não causam nenhuma ameaça à privacidade e à exposição do indivíduo, esses são denominados de atributos não sensíveis (NS) (FUNG et al., 2010; DE CAPITANI DI VIMERCATI et al., 2012).

Doneda (2006) afirma que, embora os dados sejam qualificados como não sensíveis, quando submetidos a um determinado tratamento, eles podem revelar aspectos sobre a personalidade do sujeito, podendo levar a práticas discriminatórias. O Quadro 2 ilustra exemplos de atributos identificadores, semi-identificadores, sensíveis e não sensíveis de um conjunto de dados, representando dados de consulta médica.

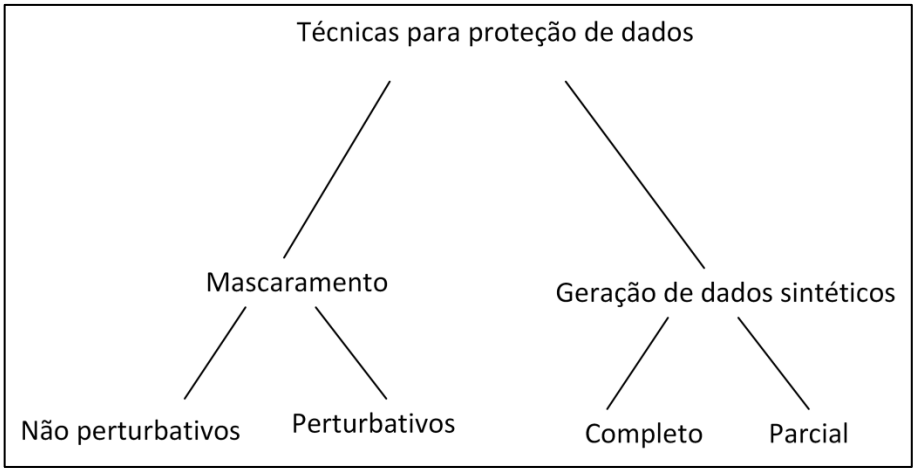
Quadro 2 - Exemplo de atributos identificadores, semi-identificadores, sensíveis e não sensíveis

Atributo	**Tipo de atributo**
Número de identificação da guia	Identificador
Número da carteira plano de saúde	Identificador
Nome do beneficiário	Identificador
Validade da carteira	Semi-identificador
Nome do profissional	Semi-identificador
Tipo de Consulta	Sensível
Tipo de identificador de acidente	Sensível
Código de procedimento	Sensível
Conselho profissional	Não sensível
Atendimento ao recém-nascido	Não sensível

Fonte: Adaptado de Affonso e Sant'Ana (2017)

Para compreender os aspectos vinculados à proteção de dados pessoais, faz-se necessário a discussão de modelos e de técnicas no domínio da anonimização de dados. Segundo Sánchez e Batet (2015), a busca pela proteção da privacidade visa diminuir as possibilidades de identificação de um sujeito em um conjunto de dados. As principais técnicas de proteção de dados podem ser classificadas em duas categorias: técnicas de mascaramento e técnicas de geração de dados sintéticos (CIRIANI et al., 2007a), conforme Figura 8.

Figura 8 - Classificação das técnicas para proteção de dados



Fonte: Ciriani et al. (2007a, tradução nossa)

Para Ciriani et al. (2007a), as técnicas de mascaramento transformam dados originais com a finalidade de produzir novos dados, tornando possíveis as análises estatísticas e protegendo a privacidade dos sujeitos referenciados no conjunto de dados. Lane (2012) também define as técnicas de mascaramento como o meio de substituir dados por valores semelhantes, de forma a prover resultados que se parecem com os originais, mas que não apresentam possibilidades de brechas de privacidade com a sua exposição.

Para Lane (2012), mascarar é um termo genérico que pode estar envolvido na coleta de dados, no armazenamento de dados e na disponibilização dos dados. O termo é usado como uma referência para mudar dados originais em outros valores. Lane (2012) expõe os seguintes termos utilizados no âmbito da técnica de mascaramento:

- ✓ Máscara: método de ocultação, uma máscara de dados é uma função que transforma os dados em algo novo, mas similar ao original. As máscaras devem ocultar os dados originais e não devem ser reversíveis;
- ✓ Mascaramento: conversão de dados em forma mascarada – dados sensíveis convertidos em não sensíveis, mantendo o mesmo formato;
- ✓ Ofuscação: ocultação do valor original.

Ciriani et al. (2007a) definem que o mascaramento pode ser realizado por meio de métodos:

- ✓ Não perturbativos: os dados originais não são modificados, eles são suprimidos ou removidos detalhes dos dados com a finalidade de diminuir ameaças à privacidade;
- ✓ Perturbativos: os dados são modificados.

Considerando a proposta de tornar os dados anônimos por técnicas não perturbativas e perturbativas, seguem, nos próximos tópicos, as mais populares técnicas de mascaramento.

3.1 Mascaramento (métodos não perturbativos)

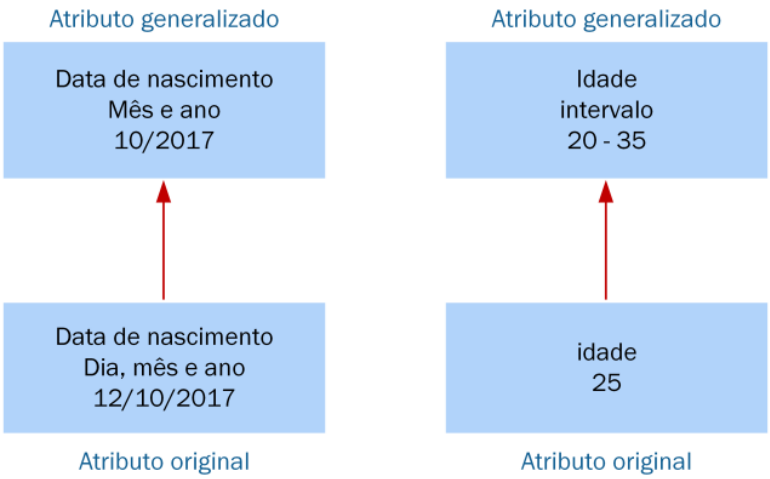
3.1.1 Generalização

De acordo com Sweeney (2002), generalizar um atributo é captar seu valor e substituí-lo por um valor menor específico, mais geral que o original, de maneira que esse valor não seja único em um conjunto de dados anonimizados. A generalização permite evidenciar as semelhanças entre tipos de entidades de nível superior e esconder as diferenças, em que a entidade nível inferior fornece mais detalhes do que a entidade de nível superior (KORTH; SILBERSCHATZ, 1993; WONG et al., 2006).

A Figura 9 demonstra o uso de generalização aplicada a um atributo. Os atributos data de nascimento e idade foram substituídos por valores menos específicos; ao invés de liberar o atributo data de nascimento estruturado em dia-mês-ano, generaliza-se para mês-dia e, dependendo da necessidade, pode-se generalizar apenas para ano. No atributo idade, após a generalização, o valor passa a estar presente no intervalo de dados que representa a idade de um indivíduo.

Por meio da generalização, é possível manter a representação semântica dos dados e preservar a veracidade, resultando em mais registros com resultados semelhantes em uma tabela (SAMARATI, 2001; CIRIANI et al., 2007a; NERGIZ; GÖK, 2014).

Figura 9 - Exemplo de generalização



Fonte: Elaborado pela autora

No trabalho de Affonso, Oliveira e Sant'Ana (2017), foi utilizada generalização para tornar menos específico os valores data de atendimento de consultas médicas e validade da carteirinha do plano de saúde, conforme ilustrado na Figura 10. Observa-se que, ao aplicar a generalização, os valores dos atributos generalizados se repetem no conjunto de dados. Essa semelhança contribui para a proteção da privacidade, minimizando as possibilidades de identificar o indivíduo no conjunto de dados.

Figura 10 - Uso de generalização para anonimização de um conjunto de dados

RegANS	ValCart	RN	CodOp	NomeContr	CNES	NomeProf	Cprof	NumCons	UF	CBO	IndAc	DtAtend
373357	out/18	sim	1000	Hosp. X	2080516	AAA	6	10723	SP	225250	1	jun/15
227326	fev/16	não	2000	Hosp. Y	2053462	BBB	6	17634	SP	225121	9	jan/15
373357	fev/16	não	1000	Hosp. X	2080516	CCC	6	15432	SP	225175	9	jun/15
227326	out/18	não	2000	Hosp. Y	2053462	DDD	6	19573	SP	578934	9	jan/15

Fonte: Adaptado de Affonso, Oliveira e Sant'Ana (2017)

Para Ciriani et al. (2007a), a generalização pode ser aplicada nos seguintes elementos:

- ✓ Atributo: a generalização ocorre nos valores da coluna;
- ✓ Células: a generalização acontece em cada célula. Como resultado, a tabela pode conter, em uma coluna específica, valores distintos nos atributos,

No exemplo da Figura 10, a generalização foi aplicada a nível de atributo, pois a transformação ocorreu em todos os valores dos atributos "ValCart" e "DtAtend".

3.1.2 Supressão

A técnica de supressão refere-se a um processo não perturbativo, que consiste em suprimir dados identificadores ou dados que podem comprometer a privacidade do referenciado. Esse processo se torna fundamental para promover a proteção de dados pessoais. De acordo com Sweeney (2002), a supressão consiste em remover o valor do atributo que revela ameaças à privacidade do referenciado. Para isso, o valor do atributo é substituído por "*" (indicando que houve supressão do valor original), assim é possível ampliar a privacidade e, ainda, reduzir o conteúdo do banco de dados. A supressão em um conjunto de dados pode ocorrer de três formas (CIRIANI et al., 2007a):

- ✓ No registro: onde é removido todo o registro da tabela, assim a supressão é efetuada na linha;
- ✓ No atributo: todos os valores de um atributo (coluna) são suprimidos;
- ✓ Em células individuais: apenas células específicas de um determinado registro são suprimidas.

3.1.3 Anatomização

A anatomização requer dividir o conjunto de dados em subconjuntos, de modo que cada tupla[51] da tabela de dados pertença a um subconjunto, denominado de QI-*groups*, que seja *l-diverse* (apresenta diversidade). Dada a partição *l-diverse* com os subgrupos, a anatomia produz uma tabela com semi-identificadores e uma tabela com dados sensíveis. Ambas as tabelas têm um atributo comum chamado de ID do grupo, valores presentes no mesmo grupo serão vinculados e, logo, podem ser utilizados (XIAO; TAO, 2006). Ao contrário da generalização e da supressão, a anatomização não modifica o semi-identificador ou o atributo sensível, mas desassocia a relação entre os dois (FUNG et al., 2010). Nessa técnica, geralmente, os semi-identificadores e os atributos sensíveis são publicados separadamente (XU et al., 2014).

3.1.4 Permutação

Zhang et al. (2007) propõem a permutação para romper o vínculo entre semi-identificadores e atributos numéricos sensíveis. Ao dividir um conjunto de registros de dados em grupos, mistura-se os valores sensíveis dentro de cada grupo; assim, dado um conjunto de tuplas de uma tabela de dados de-identificada, permuta-se, aleatoriamente, a associação entre semi-identificadores e dados sensíveis. Mesmo que um invasor possa vincular o indivíduo ao semi-identificador (por meio de conhecimento prévio), ainda ele não será capaz de saber exatamente o valor do atributo sensível do referenciado. Essa técnica é parecida com a anatomização, e a ideia é desassociar a relação entre um semi-identificador e um atributo numérico sensível ao particionar um conjunto de registros em grupos, embaralhando seus valores sensíveis dentro de cada grupo (FUNG et al., 2010). A permutação não modifica os dados originais, eles ainda podem necessitar de apoio de técnicas de generalização.

3.1.5 Amostragem

A tabela de dados protegida é obtida como uma amostra do conjunto de dados originais, uma vez que, o conjunto contém apenas as tuplas de uma amostra de toda a população. Como há a incerteza se um indivíduo específico está presente ou não na amostra, o risco de reidentificação do conjunto de dados liberado é minimizado. Essa técnica opera apenas em atributos categóricos (CIRIANI et al., 2007a).

3.1.6 Recodificação global (ou recodificação em intervalos)

[51] Cada linha da tabela de dados (KORTH; SILBERSCHATZ, 1993).

O domínio de um atributo é divido em intervalos, e cada intervalo é associado a um rótulo. A proteção dos dados é obtida substituindo os valores do atributo pelo rótulo associado ao intervalo correspondente. A recodificação global diminui os detalhes do conjunto de dados e, portanto, diminui o risco de reidentificação. Por exemplo, os valores de um atributo denominado temperatura serão alterados de acordo com os intervalos: sem febre (sf) [35 – 39.9], com febre (f) [37 – 38.9] e com febre alta (fa) [39 – 40.9], assim, o valor da tupla é substituído pelo rótulo de acordo com o intervalo proposto (CIRIANI et al., 2007a).

3.1.7 *Shuffling*

Nesta técnica, os valores das variáveis confidenciais são "embaralhados" entre as observações. A técnica randomiza valores existentes verticalmente num conjunto de dados, por exemplo, embaralhando uma coluna que possui salários de funcionários. Embora o conjunto de dados torna-se inútil para aprender sobre o salário de determinado funcionário, valores médios da coluna são mantidos. Os dados *shuffling* fornecem um alto nível de utilidade de dados e minimizam riscos de divulgação, desassociando o relacionamento de dados sensíveis, preservando os valores agregados (MURALIDHAR; SARATHY, 2006; LANE, 2012). Para Muralidhar, Sarathy e Dandekar (2006), ao aplicar data *suffling* em dados originais, a técnica não modifica os valores dos dados originais.

3.2 Mascaramento (método perturbativo)

3.2.1 Perturbação de dados por valor aleatório (randomização)

O método de perturbação por valor aleatório (randomização) (AGRAWAL; SRIKANT, 2000) busca proteger a privacidade dos dados, modificando os atributos de valores sensíveis, utilizando processo de randomização, principalmente pela distorção de valor. Nessa abordagem, o detentor de um conjunto de dados utiliza um valor aleatório obtido normalmente pela distribuição Gaussiana (com média 0 e desvio padrão 1) para ser acrescentado aos dados originais a serem perturbados (KARGUPTA et al., 2005). Encontra-se nessa abordagem a técnica de adição de ruído, ruído multiplicativo e ruído logarítmico.

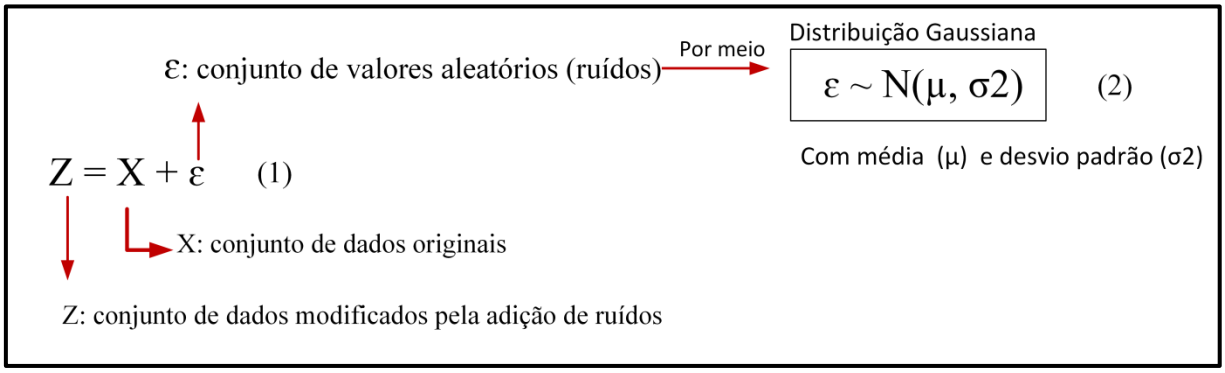
a) Adição de ruído

A técnica de adição de ruído consiste em substituir os valores dos atributos de um conjunto de dados por valores aleatórios, denominados de ruídos. Dessa forma, os dados que serão disponibilizados são perturbados (disfarçados) aleatoriamente por meio de uma distribuição. No entanto, ainda se mantém as características estatísticas do conjunto de dados

(DOMINGO-FERRER; SEBÉ; CASTELLÀ-ROCA, 2004; KARGUPTA et al., 2005; CIRIANI, 2007b). A adição de ruído é considerada uma técnica eficiente no contexto da proteção de dados pessoais. No entanto, ela é aplicada apenas em atributos que possuem valores numéricos.

A adição aleatória de ruídos em um conjunto de dados é realizada por meio da expressão (1) definida por Kim (1986), utilizando a distribuição Gaussiana (2) para compor os valores aleatórios, conforme Figura 11:

Figura 11 - Adição de ruído



Fonte: Baseado em Kim (1986).

Os valores obtidos da distribuição Gaussiana são adicionados a X, compondo o valor de Z, que representa o conjunto de dados modificados por meio da adição de ruídos (KARGUPTA et al., 2005; MIVULE, 2012).

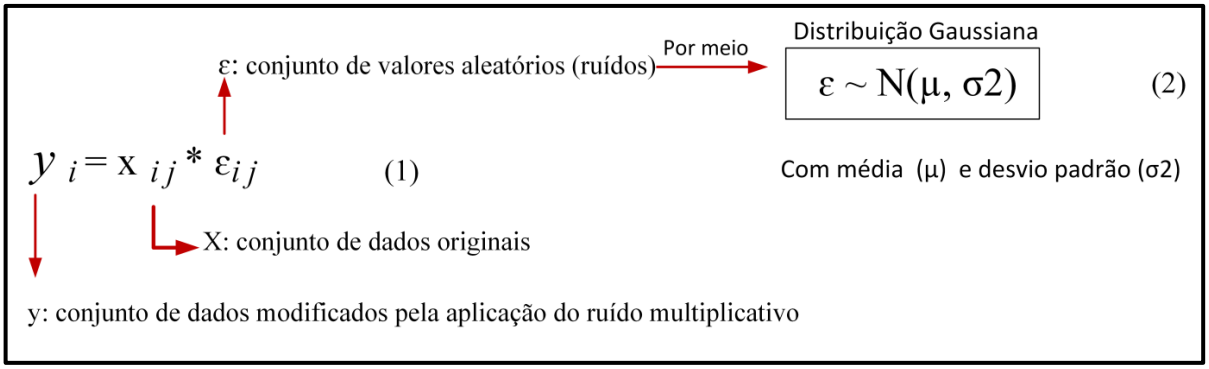
Além da adição de ruídos na abordagem de perturbação de dados, Mivule (2012) cita a técnica de ruído multiplicativo, utilizando também valores aleatórios.

b) Ruído multiplicativo

Para Kim e Winkler (2003), existem duas formas de ruído multiplicativo: a primeira abordagem é a geração de números aleatórios para multiplicá-los aos dados originais, resultando em novos dados com ruído; a segunda abordagem é o ruído multiplicativo logarítmico.

A aplicação do ruído multiplicativo em um conjunto de dados é realizada por meio da expressão (1) definida por Kim e Winkler (2003), com a expressão (2), representando a distribuição Gaussiana, conforme Figura 12:

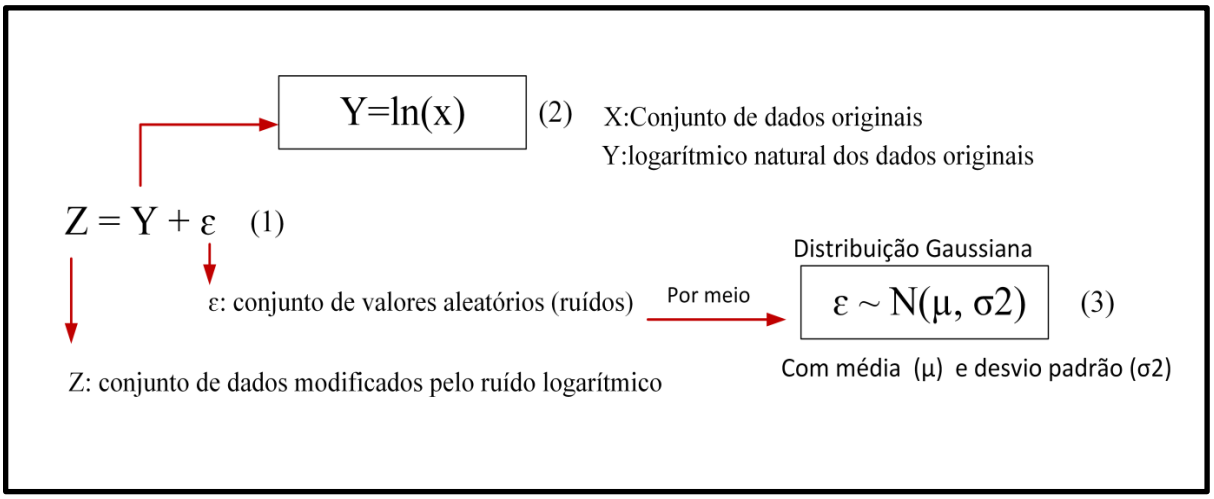
Figura 12 - Ruído multiplicativo



Fonte: Baseado em Kim e Winkler (2003)

Kim e Winkler (2003) descrevem o ruído multiplicativo logarítmico por meio das expressões (1), que adiciona o cálculo do logarítmico Y (2) a variável de distribuição aleatória ε (3) (Figura 13).

Figura 13 - Ruído multiplicativo logarítimo



Fonte: Baseado em Kim e Winkler (2003)

A adição de ruído aleatório, ruído multiplicativo e ruído multiplicativo logaritmo utilizam da distribuição aleatória gaussiana e tornam os dados modificados, alterando a semântica do dado.

3.2.2 *Micro-aggregation* (ou *Blurring*)

Consiste em agrupar tuplas individuais em pequenos agregados de k dimensão fixa, publicando a média do agregado ao invés de valores individuais. Os grupos são formados usando critérios de similaridade máxima (CIRIANI et al., 2007a). Essa técnica é aplicada em atributos numéricos ou tipo data (LANE, 2012).

3.2.3 *Resampling*

Essa técnica consiste em substituir os valores de um atributo sensível por um valor médio, calculado sobre um determinado número de amostras coletadas dos dados originais (CIRIANI et al., 2007b).

3.2.4 *Data swapping*

Data swapping foi inicialmente proposta por Dalenius e Reiss (1982) para o mascaramento de variáveis categóricas, em vez de variáveis numéricas. Para Ciriani et al. (2007a), esta técnica consiste em modificar um subconjunto de tuplas em uma tabela de dados, trocando os valores de um conjunto de atributos sensíveis, denominados de atributos trocados, entre pares de tuplas selecionados, de acordo com um critério bem definido. Essa técnica reduz o risco de reidentificação, pois proporciona incerteza sobre o verdadeiro valor dos dados de um indivíduo. A ideia geral é anonimizar uma tabela de dados trocando valores de atributos sensíveis entre os registros dos indivíduos, mantendo algumas características estatísticas dos dados, como a contagem e frequência de atributos (FUNG et al., 2010).

3.2.5 Anulação

Substitui os dados sensíveis por um valor genérico, como “X”. Esta é a forma mais simples de mascarar, entretanto, a saída não fornece nenhum tipo de utilidade (LANE, 2012).

3.3 Geração de dados sintéticos

Muitos métodos de controle de divulgação estatística utilizam geração de dados sintéticos para proteger a privacidade dos titulares de dados e manter as características estatísticas. Essa técnica tem a finalidade de construir um modelo estatístico a partir dos dados originais e, em seguida, gerar um conjunto de dados sintéticos a partir do modelo construído. Esses dados sintéticos representam os dados que serão publicados, em vez dos originais (FUNG et al., 2010).

Como a tabela de dados disponibilizada contém dados sintéticos, o risco de reidentificação é minimizado, sendo que a divulgação pode ser inteiramente sintética ou parcialmente sintética (CIRIANI et al., 2007a). Um requisito importante para geração de dados sintéticos é que os dados sintéticos e originais devem apresentar a mesma qualidade de análise estatística. Essa técnica coloca mais atenção na qualidade dos dados divulgados do que nos problemas de reidentificação (CIRIANI et al., 2007a).

A geração de dados sintéticos pode ser dividida em duas categorias: totalmente sintética e parcialmente sintética. Na técnica totalmente sintética é gerado um conjunto novo de dados, enquanto na segunda categoria os dados originais são mesclados com os dados sintéticos (CIRIANI et al., 2007a).

3.4 Criptografia

Loukil et al. (2017), ao abordar técnicas para proteger a privacidade de dados, inclui a criptografia como um meio de restringir o acesso a dados, pois essa técnica visa limitar o uso dos dados por meio de bloqueios ao acesso ou codificação de entradas, sendo eficaz no compartilhamento de dados, evitando a intercepção dos dados por terceiros.

A criptografia consiste em transformar dados em estado ilegível. Ao contrário de outros métodos, o valor original pode ser determinado a partir do valor criptografado, mas só pode ser revertido a partir do conhecimento da chave. No entanto, a criptografia mantém o formato original dos valores (LANE, 2012).

O mascaramento está presente no gerenciamento de todo o ciclo de vida dos dados – da coleta até a recuperação, enquanto a criptografia é aplicada de forma centralizada, muitas vezes independente em vários pontos diferentes, para minimizar riscos específicos de privacidade (LANE, 2012). Tecnicamente, a criptografia viola a determinação de tornar os dados irreversíveis após o processo de mascaramento de dados (LANE, 2012); assim, podem ser denominadas de pseudoanonimização[52], pois pode permitir a reversão de dados (BREKNE; ÅRNES; ØSLEBØ, 2005).

Para Schuster et al. (2017), um campo de pesquisa que tem recebido atenção, após as revelações de Snowden, é a área da *Privacy-Enhancing Technologies* (PETs), que se refere às tecnologias que permitem aos usuários proteger sua privacidade de dados enquanto usam serviços ou aplicativos. Uma das opções propostas a curto prazo é adoção de criptografia de ponta a ponta (*end-to-end encryption* - E2EE).

A E2EE é a técnica mais segura para proteger a privacidade e segurança da informação em comunicações eletrônicas. Quando as mensagens E2EE são criptografadas no dispositivo do remetente e descriptografadas no dispositivo do destinatário, as operadoras de telecomunicações e provedores de Internet só veem as informações criptografas. A E2EE oferece um nível aprimorado de confidencialidade das informações e, portanto, da privacidade,

[52] Tipo particular de-identificação que remove a associação com um titular de dados, acrescentando uma associação entre um determinado conjunto de características relativas à pessoa em causa em um ou mais pseudônimos (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2017).

protegendo os usuários contra a censura, a repressão e intercepções injustificadas pelas agências de aplicação de lei e inteligência (SCHUSTER et al., 2017).

Uma alternativa para a autenticação de usuários é a utilização de protocolos de prova *zero-knowledge*, denominado de protocolos de conhecimento de zero, cuja finalidade é permitir que uma parte comprove para a outra que uma situação é verdadeira, sem que para isso seja preciso revelar qualquer informação adicional além do fato que foi transmitido (QUISQUATER et al., 1989).

O protocolo *Zero-knowledge* permite que se prove o conhecimento de uma afirmação, sem revelar qualquer informação sobre ela. Esse tipo de protocolo não revela segredos durante as operações, uma vez que os segredos não são transferidos para outra parte. Assim, é possível manter a comunicação, provando a identidade, sem revelar informações (GIANI, 2001).

A criptografia tem sido utilizada na proteção de dados como um meio para tornar os dados ininteligíveis, enquanto explora a fragmentação como forma de quebrar associações sensíveis entre as informações (CIRIANI et al., 2007b).

3.5 Modelos de proteção de privacidade

Para a proteção dos dados pessoais, muitas técnicas apresentadas são utilizadas em combinação com modelos, tais como k-anonimato, *l-diversity* e privacidade diferencial, que serão explanadas a seguir.

3.5.1 k-anonimato

Sweeney (2002) ressalta que a sobrevivência dos bancos de dados depende da capacidade do detentor em produzir dados anônimos, pois não permitir a divulgação diminui a utilidade para a sociedade (tais como dados genômicos para pesquisa), enquanto que a falta de proteção adequada pode prejudicar os indivíduos referenciados nos conjuntos de dados.

No entanto, segundo Samarati e Sweeney (1998), há um mito em relação à anonimização: muitos detentores de dados removem dados identificadores acreditando que a identidade do indivíduo não possa ser revelada. Contudo, a informação divulgada pode conter dados semi-identificadores que, quando combinados com outras bases de dados, podem reidentificar o indivíduo, caracterizando quebra de privacidade.

A Figura 14 demonstra essa situação, ilustrando como os atributos semi-identificadores como CEP, Data de Nascimento e Sexo podem ser utilizados na correlação de dados para a reidentificação do indivíduo.

Figura 14 - Correlação por meio de semi-identificadores

Fonte: Sweeney (2002, p. 2, tradução nossa)

Sweeney (2002) demonstra a vulnerabilidade dos atributos semi-identificadores representados na Figura 14 por meio do seguinte exemplo:

> Por vinte dólares eu comprei a lista de registro de eleitores de Cambridge, Massachusetts, e recebi as informações em dois disquetes. O círculo mais à direita na figura mostra que esses dados incluem o nome, endereço, código postal, data de nascimento e sexo de cada eleitor. Esta informação pode ser correlacionada utilizando código postal, data de nascimento e sexo com as informações médicas de um hospital do círculo à esquerda. Por exemplo, William Weld era governador de Massachusetts, e seus registros médicos estão na base de dados do GIC. Governador Weld vive em Cambridge Massachusetts. De acordo com a lista de eleitores de Cambridge, seis pessoas possuem a data de nascimento como a de Weld; apenas três deles eram homens. E, ele era apenas o que tinha código postal de 5 dígitos (SWEENEY, 2002, p. 3, tradução nossa) [53].

É possível observar que a divulgação de dados semi-identificadores e o conhecimento prévio do atacante sobre um indivíduo, como o seu código postal, torna possível descobrir a identidade do sujeito no conjunto de dados disponibilizados.

O modelo k-anonimato emerge da necessidade de liberar um conjunto de dados com todos os atributos e valores, de modo que a identidade do indivíduo fique protegida (anônima). Para tanto, o modelo determina a utilização das técnicas de generalização e supressão para que seja possível divulgar um conjunto de dados e manter protegida a identidade dos indivíduos referenciados no conjunto de dados, levando em consideração as possíveis correlações dos

[53] "*For twenty dollars I purchased the voter registration list for Cambridge Massachusetts and received the information on two diskettes [4]. The rightmost circle in Figure 1 shows that these data included the name, address, ZIP code, birth date, and gender of each voter. This information can be linked using ZIP code, birth date and gender to the medical information, thereby, linking diagnosis, procedures, and medications to particularly named individuals. For example, William Weld was governor of Massachusetts at that time and his medical records were in the GIC data. Governor Weld lived in Cambridge Massachusetts. According to the Cambridge Voter list, six people had his particular birth date; only three of them were men; and, he was the only one in his 5-digit ZIP code*".

atributos semi-identificadores com tabelas externas publicadas (SAMARATI; SWNEEY, 1998).

No momento que um atacante procura por um registro na tabela, este deve estar vinculado a pelo menos k possíveis registros correspondentes; assim, o conjunto de dados anônimos deverá ser indistinguível de pelo menos k-1 registros, sendo que o valor de k é definido pelo detentor de dados e deve ser representado por um número inteiro positivo (SWEENEY, 2002; BETTINI; RIBONI, 2015).

> A anonimização dos dados deve atender as exigências para atingir a preservação da privacidade, para isso, utiliza-se da remoção dos atributos identificadores, generalização dos dados para um nível de menor detalhe e supressão dos registros que não atendem ao k-anonimato, de forma a gerir os dados do sujeito e suas ações, preservando a privacidade e garantindo o anonimato (AFFONSO; SANT'ANA, 2017, p. 39).

O Quadro 3 apresenta exemplo de uma tabela que adere ao k-anonimato. Durante o processo de anonimização foram suprimidos os atributos identificadores, generalizando os atributos data de nascimento e código postal. Também foi aplicado o modelo k-anonimato de forma que o conjunto de dados preparado para disponibilização apresente k registros correspondentes. Assim, dado o conjunto de semi-identificadores SI = {Raça, nascimento, sexo, código postal} e k = 2, observa-se que, para cada uma das tuplas contidas na tabela, os valores das tuplas que compreendem o semi-identificador aparecem pelo menos duas vezes no conjunto de dados (SWEENEY, 2002).

Quadro 3 - Conjunto de dados que adere ao k-anonimato

Raça	Data de Nascimento	Sexo	Código Postal	Problema
Negro	1965	M	0214*	Respiração curta
Negro	1965	M	0214*	Dor no peito
Negro	1965	F	0213*	Hipertensão
Negro	1965	F	0213*	Hipertensão
Negro	1964	F	0213*	Obesidade
Negro	1964	F	0213*	Dor no peito
Branca	1964	M	0213*	Dor no peito
Branca	1964	M	0213*	Obesidade
Branca	1964	M	0213*	Respiração curta
Branca	1967	M	0213*	Dor no peito
Branca	1967	M	0213*	Dor no peito

Fonte: Sweeney (2002, tradução nossa)

Ainda que o modelo k-anonimato proporcione meios para proteger a privacidade, ele apresenta a deficiência de permitir que um atacante vincule os atributos sensíveis a um indivíduo, quando não há diversidade nesse conjunto de dados, denominado de ataque de homogeneidade (CIRIANI et al., 2007a; FRIEDMAN; WOLFF; SCHUSTER, 2008).

3.5.2 l-*diversity*

Esse modelo foi desenvolvido por Machanavajjhala et al. (2006), com a finalidade de suprir as limitações do modelo k-anonimato. A proposta do *l-diversity* é permitir maior diversidade de registros semi-identificadores. Portanto, um conjunto é considerado *l-diversity* se possuir pelo menos 1 (um) valor distinto para os atributos sensíveis. O Quadro 4 demonstra uma estrutura de dados com atributos sensíveis e não sensíveis, simulando dados coletados em um hospital. Observa-se que os identificadores únicos já foram suprimidos do conjunto de dados.

Quadro 4 - Exemplo de conjunto de dados de hospital

	Dados não sensíveis			**Dados Sensíveis**
	Código Postal	**Idade**	**Nacionalidade**	**Condição**
1	13053	28	Russo	Doença Cardíaca
2	13068	29	Americano	Doença Cardíaca
3	13068	21	Japonês	Infecção Viral
4	13053	23	Americano	Infecção Viral
5	14853	50	Indiano	Câncer
6	14853	55	Russo	Doença Cardíaca
7	14850	47	Americano	Infecção Viral
8	14850	49	Americano	Infecção Viral
9	13053	31	Americano	Câncer
10	13053	37	Indiano	Câncer
11	13068	36	Japonês	Câncer
12	13068	35	Americano	Câncer

Fonte: Machanavajjhala et al. (2006, p. 3, tradução nossa)

No Quadro 5 é demonstrado o conjunto de dados que passou pelas operações determinadas pelo k-anonimato, os atributos código postal e idade foram generalizados, e suprimiu-se o atributo nacionalidade. Ao verificar a aderência do modelo k-anonimato, considerando o conjunto de semi-identificadores SI {Código Postal e Idade} e k=3, nota-se que, para cada SI procurado na tabela, existe pelo menos 2 (duas) tuplas no conjunto de dados, atendendo ao princípio de k registros anônimos.

Quadro 5 - Conjunto de dados anonimizado pelo k-anonimato (4-anônimos)

	Dados não sensíveis			Dados Sensíveis
	Código Postal	**Idade**	**Nacionalidade**	**Condição**
1	130**	< 30	*	Doença Cardíaca
2	130**	< 30	*	Doença Cardíaca
3	130**	< 30	*	Infecção Viral
4	130**	< 30	*	Infecção Viral
5	1485*	>= 40	*	Câncer
6	1485*	>= 40	*	Doença Cardíaca
7	1485*	>= 40	*	Infecção Viral
8	1485*	>= 40	*	Infecção Viral
9	130**	3*	*	Câncer
10	130**	3*	*	Câncer
11	130**	3*	*	Câncer
12	130**	3*	*	Câncer

Fonte: Machanavajjhala et al. (2006, p. 3, tradução nossa)

Machanavajjhala et al. (2006) ressaltam que, mesmo que o conjunto de dados tenha aderido ao k-anonimato, não é possível garantir a privacidade dos indivíduos referenciados nesse conjunto de dados. Para os autores, ao realizar um ataque de homogeneidade e ter conhecimento prévio sobre o indivíduo, é possível relacionar o indivíduo ao seu atributo sensível. Para ilustrar o possível ataque de homogeneidade, os autores relatam a seguinte situação:

> Alice e Bob são vizinhos. Um dia Bob adoece e é levado de ambulância para o hospital. Tendo visto a ambulância, Alice decide descobrir qual doença Bob está sofrendo. Alice tem acesso aos registros hospitalares de individuos anônimos, publicados pelo hospital [..], e por isso ela sabe que um dos registros nesta tabela contém os dados de Bob. Desde que Alice é vizinha de Bob, ela sabe que Bob é um homem americano, de 31 anos, e que vive no código postal 13053. Portanto, Alice sabe que o código de Bob nos registros é 9, 10, 11 ou 12. Todos esses pacientes têm a mesma condição médica (câncer), e assim Alice conclui que tem Bob câncer (MACHANAVAJJHALA et al., 2006, p. 3-4, tradução nossa) [54].

Por meio desse exemplo, observa-se que o modelo k-anonimato não é totalmente eficiente na proteção da privacidade quando o conjunto de semi-identificadores não apresenta diversidade no conjunto de dados sensíveis. Desta forma, Machanavajjhala et al. (2007)

[54] "*Alice and Bob are antagonistic neighbors. One day Bob falls ill and is taken by ambulance to the hospital. Having seen the ambulance, Alice sets out to discover what disease Bob is suffering from. Alice discovers the 4-anonymous table of current inpatient records published by the hospital [...], and so she knows that one of the records in this table contains Bob's data. Since Alice is Bob's neighbor,she knowsthat Bob is a 31-year-old American male who lives in the zip code 13053. Therefore, Alice knows that Bob's record number is 9,10,11, or 12. Now, all of those patients have the same medical condition (cancer), and so Alice concludes that Bob has cancer*".

sugerem que, além da aplicação do modelo k-anonimato, a tabela anonimizada também deve garantir a "diversidade", onde todas as tuplas que serão disponibilizadas devem ter nos seus semi-identificadores valores diversos para os atributos sensíveis.

Em relação ao ataque de conhecimento prévio, Machanavajjhala et al. (2007, p. 4, tradução nossa) [55], relatam a seguinte situação:

> Alice tem um amigo que se chama Umeko que esteve presente no mesmo hospital de Bob, e cujos registros de paciente também aparecem no conjunto de dados ilustrado no Quadro. Alice sabe que Umeko tem 21 anos, é japonês e que vive atualmente no código postal 13068. Com base nessa informação, Alice aprende que a informação de Umeko está contida nos registros 1, 2, 3, ou 4. Sem informações adicionais, Alice não tem certeza se Umeko está com infecção viral ou teve doença cardíaca. No entanto, sabe-se que os japoneses têm incidência extremamente baixa em relação a doenças cardíacas. Portanto, Alice conclui com certeza que Umeko teve uma infecção viral.

Os autores demonstram que, ao realizar ataques de conhecimento prévio, um conjunto de dados que estava em aderência com o k-anonimato pode divulgar informações confidencias e permitir quebra de privacidades. No Quadro 6, apresenta-se uma nova versão do conjunto de dados em aderência com o modelo *l-diversity*, considerando 3-diversos dados sensíveis.

Quadro 6 - Microdata dos pacientes do hospital anonimizada pelo *l-diversity* com 3-diversos

	Dados não sensíveis			**Dados Sensíveis**
	Código Postal	**Idade**	**Nacionalidade**	**Condição**
1	1305*	<=40	*	Doença Cardíaca
4	1305*	<= 40	*	Infeção Viral
9	1305*	<= 40	*	Câncer
10	1305*	<= 40	*	Câncer
10	1485*	> 40	*	Câncer
6	1485*	> 40	*	Doença Cardíaca
7	1485*	> 40	*	Infecção Viral
8	1485*	> 40	*	Infecção Viral
2	1306*	<= 40	*	Doença Cardíaca
3	1306*	<= 40	*	Infecção Viral
11	1306*	<= 40	*	Câncer
12	1306*	<= 40	*	Câncer

Fonte: Machanavajjhala et al. (2006, p. 17, tradução nossa)

[55] "*Alice has a penfriend named Umeko who is admitted to the same hospital as Bob, and whose patient records also appear in the table shown in Figure 2. Alice knows that Umeko is a 21 yearold Japanese female who currently lives in zip code 13068. Based on this information, Alice learns that Umeko's information is contained in record number 1,2,3, or 4. Without additional information, Alice is not sure whether Umeko caught a virus or has heart disease. However, it is wellknown that Japanese have an extremely low incidence of heart disease. Therefore Alice concludes with near certainty that Umeko has a viral infection*".

Ao realizar novamente os ataques, Alice não consegue afirmar que Bob possui câncer. Mesmo que ela tenha conhecimento do seu código postal, ela encontrará 4 (quatro) registros na tabela e, embora ela saiba que Bob tem 31 anos, o atributo idade para o código postal de Bob apresenta-se generalizado, sendo assim torna-se complicado distinguir Bob no conjunto de dados. Para garantir o anonimato, o *l-diversity* utiliza-se das técnicas de supressão de dados e registros (MACHANAVAJJHALA et al., 2006).

3.5.3 *t-closeness*

Este modelo foi proposto por Li, Li e Venkatasubramanian (2007) com a finalidade de suprir as limitações do modelo *l-diversity* em relação ao ataque de conhecimento prévio do k-anonimato na divulgação de atributos sensíveis. O modelo define que uma classe de equivalência satisfaz *t-closeness* quando a distância entre a distribuição de um atributo sensível nesta classe e a distribuição do atributo em toda a tabela não é mais do que um limite t. A mensuração entre distância máxima entre as classes e a distribuição global é realizada por meio da *Earth Mover Distance* (EMD), a qual considera que quanto maior o valor da distância, maiores são as ameaças à privacidade. Isso efetivamente limita a quantidade de informações individuais específicas que um observador pode aprender. O modelo *t-closeness* resolve claramente a vulnerabilidade de divulgação de atributo.

3.5.4 Privacidade diferencial

A privacidade diferencial foi proposta Dwork (2008) como um modelo estatístico para proteção de privacidade que limita o atacante de ganho de conhecimento entre os conjuntos de dados e disponibiliza informações estatísticas sobre ele, sem ameaçar a privacidade dos sujeitos referenciados.

A essência do modelo é o usuário enviar uma consulta para um detentor de dados, e esse realiza a anonimização de dados por meio de adição de ruído. Para isso, normalmente, utiliza-se da distribuição de *Laplace* para geração de variável aleatória. A privacidade diferencial aborda o paradoxo de não aprender nada sobre um único referenciado enquanto aprende informações úteis sobre uma população. Por exemplo, um banco de dados médico pode ensinar que o tabagismo causa câncer; no entanto, o tabagista não é prejudicado pela análise. O que pode acontecer é a visão que uma companhia de seguros terá sobre fumantes e os custos médicos a longo prazo. Assim, os preços dos seguros para fumantes podem aumentar. Com a divulgação do conjunto de dados chega-se à conclusão sobre determinado assunto, que até pode

influenciar a vida do indivíduo, no entanto, não é identificada a presença do fumante no conjunto de dados, minimizando as quebras de privacidade (DWORK; ROTH, 2014).

Privacidade diferencial é uma das melhores técnicas para garantir privacidade, porque é muito difícil para o adversário inferir a presença ou ausência de qualquer indivíduo no conjunto de dados, mesmo que o adversário conheça informações exatas de todos os indivíduos envolvidos (SHRIVASTVA; RIZVI; SINGH, 2014).

As técnicas e exemplos relatados foram desenvolvidos na sua gênese para dados presentes em conjunto estruturados (tabelas relacionais e microdados). No entanto, devido ao aumento exponencial de coleta de dados pelos diversos dispositivos, emerge outros contextos em que essas técnicas e modelos têm sido abarcados, tal como as preocupações em relação às ameaças à privacidade no âmbito de dados de localização. Assim, quando a proteção de dados pessoais está relacionada a dados de localização, principalmente nos serviços baseados em localização (*Location Basead Servisse*- LBS), resgatam-se muitas dessas técnicas e modelos, como também emergem novas.

No contexto da proteção da privacidade de dados de localização, Chow, Mokbel e Liu (2006) afirmam que as técnicas de proteção da privacidade se baseiam nos seguintes conceitos:

- ✓ Locais falsos: quando o usuário protege sua localização enviando locais falsos;
- ✓ Locais exatos: esses dados são enviados junto com um conjunto de locais falsos (*dummies*), para um LBS;
- ✓ Transformação espacial: as informações e dados de localização do usuário são transformados em outro espaço, em que suas relações espaciais exatas ou aproximadas são mantidas para responder serviços baseados em localização.
- ✓ *Spatial cloaking*: tem a finalidade de desfocar a localização exata de um usuário de modo que atenda ao k-anonimato.

A técnica de *spatial cloaking* é uma técnica que desfoca a localização exata de um usuário pertencente a uma região espacial, com a finalidade de proteger a privacidade de sua localização. A ideia básica da técnica de *spatial cloaking* é desfocar a área utilizada, de forma que satisfaça os requisitos de privacidade especificados pelo usuário. Os requisitos de privacidade mais populares para a *spatial cloaking* é o k-anonimato, ou seja, a área coberta deve conter pelo menos k usuários (CHOW; MOKBEL; LIU, 2006).

No contexto da privacidade para dados de localização, a técnica de *spatial cloaking* é a mais popular e apresenta a vantagem de suportar vários ambientes, por exemplo, centralizado, distribuído, *Peer-to-Peer* (P2P), redes sem fio, e atende a vários tipos de problemas, consulta instantânea, consulta contínua e trajetórias (CHOW; MOKBEL; LIU, 2006).

Em termos de modelos de arquitetura, as técnicas para *spatial cloaking* e outras técnicas voltadas para anonimização de dados de localização podem ser categorizadas em três modelos (CHOW; MOKBEL; LIU, 2006):

- ✓ **Centralizado:** existe a presença de um terceiro confiável, denominado de anonimizador local, que é colocado entre o usuário e um provedor LBS. O anonimizador é o responsável por desfocar os locais exatos dos usuários que pertencem à área de *cloaked* (coberta), de modo a satisfazer os requisitos de privacidade, e ainda realizar a comunicação com o fornecedor do serviço, no caso o LBS. Esse modelo apresenta o problema de escalabilidade, pois exige que todos os usuários enviem, periodicamente, suas localizações exatas ao anonimizador de localização e, além disso, aumenta a vulnerabilidade de ataques, visto que todas as localizações ficam armazenadas em um único local, tornando-se um único ponto de ataque, no caso, o anonimizador local.
- ✓ **Distribuído:** utiliza uma infraestrutura de comunicação fixa, ou seja, estações base para anonimizar estrutura de dados complexas;
- ✓ ***Peer-to-Peer* (P2P)*:*** permitem que usuários móveis possam trabalhar juntos para desfocar seus locais e área, sem usar qualquer infraestrutura de comunicação fixa ou centralizada. Como o processador de consulta não conhece a localização exata da consulta, ele determina um conjunto de respostas que atenda à consulta e envia a resposta para o usuário, que verifica a resposta exata em um conjunto de resposta ou a melhor resposta no conjunto disponibilizado pelo servidor.

Nesse cenário, De Capitani di Vimercati et al. (2012) consideram que as definições de privacidade e as principais técnicas para anonimizar dados e promover a proteção da privacidade podem ser classificadas em duas categorias: Privacidade Sintática e Privacidade Semântica.

A privacidade sintática é determinada pelo uso de técnicas e métodos não perturbativos (DE CAPITANI DI VIMERCATI et al., 2012) que têm a finalidade de não modificar os valores originais dos dados durante o processo de anonimização. Para Affonso, Oliveira e Sant'Ana (2017, p. 84) a privacidade sintática pode ser definida como:

> Conjunto de técnicas que tem como foco aspectos estruturais e de composição dos dados, visando impacto mínimo na semântica do conteúdo dos atributos, na busca por uma redução do potencial de identificação dos envolvidos no conjunto de dados alvo.

Encontra-se nessa definição as técnicas de generalização e de supressão, e os modelos k-anonimato, *l-diversity*, *t-closeness* (DE CAPITANI DI VIMERCATI et al., 2012; MIVULE, 2014).

A privacidade semântica considera as técnicas perturbativas (DE CAPITANI DI VIMERCATI et al. (2012), as quais, segundo Mivule (2015), têm o objetivo de transformar ou perturbar dados originais por meio da adição de ruídos, ruído multiplicativo, ruído multiplicativo logaritmo, como também pelo uso do modelo privacidade diferencial. Affonso, Oliveira e Sant'Ana (2017, p. 84) definem privacidade semântica como o "[...] conjunto de técnicas utilizadas na modificação do conteúdo dos atributos (significado), [...] e, por meio destas técnicas pode-se gerar um conjunto de dados modificados".

3.6 Considerações Finais

Neste capítulo, foram explanados os principais conceitos vinculados à proteção de dados, incluindo técnicas e modelos que abarcam os aspectos de privacidade no contexto da anonimização de dados, processo que busca minimizar quebras de privacidade.

Observa-se que a essência das definições de privacidade explanadas no Capítulo 2 está pautada na ideia de controle que o indivíduo deveria ter sobre os dados. Atualmente, esse controle e consciência sobre a coleta devem ser muito mais precisos, pois a quantidade expressiva de dados que é coletada pelos diversos dispositivos não gera apenas preocupações por conter valores identificadores e sensíveis, mas pela presença de dados semi-identificadores que pode causar diversas ameaças à privacidade. No entanto, a atividade de correlação desses dados pode passar imperceptível para o usuário, tornando-o insciente sobre o processo que envolve os seus dados.

Diante do problema de exposição de dados e da correlação dos semi-identificadores emergem técnicas e modelos com o propósito de garantir a privacidade dos titulares ou referenciados no conjunto de dados, nota-se que novos modelos são desenvolvidos a fim de aprimorar as deficiências de um modelo existente.

Porém, a finalidade das técnicas e modelos está voltada principalmente a proporcionar um conjunto de dados disponíveis para a sociedade, de modo que não seja possível a identificação do indivíduo. Isso fica explícito na justificativa de Samarati e Swenney (1998, p.1), ao propor o objetivo do artigo que apresenta o principal modelo de proteção da privacidade, o k-anonimato: "Neste artigo abordamos o problema de **liberar** dados específicos de pessoas e, ao mesmo tempo garantindo o anonimato dos indivíduos referenciados nos dados"

(SAMARATI; SWEENEY, 1998, p.1, tradução nossa, grifo nosso) [56]. Esse relato demonstra a preocupação com a liberação de dados, portanto, anonimização sendo realizada na fase de recuperação e não na fase de coleta de dados.

Visto que a anonimização é um meio de proteger dados pessoais, busca-se no próximo capítulo verificar como a anonimização tem sido tratada por pesquisadores na fase de coleta de dados. Assim, por meio de revisão sistemática da literatura são elucidados o escopo e as principais características abarcadas em cada trabalho recuperado, como também os dados resultantes da coleta e análise dos documentos, tais como: os dados de frequência dos países das instituições dos autores, as técnicas e modelos utilizados e os contextos nos quais a anonimização foi aplicada.

[56] "In this paper we address the problem of releasing person-specific data while, at the same time, safeguarding the anonymity of the individuals to whom the data refer".

4 PROTEÇÃO DE DADOS PESSOAIS: ANONIMIZAÇÃO NA FASE DE COLETA

> *Quanto à "morte do anonimato" por cortesia da Internet, ... submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca. Ou talvez, ainda, a pressão no sentido de levar nossa autonomia pessoal para o matadouro seja tão poderosa, tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e resolutos estejam preparados para a tentativa séria de resistir. [...] (BAUMAN, 2014, p. 20).*

Em razão de a anonimização de dados possibilitar o amparo à proteção de dados mediante suas técnicas e modelos, evidencia-se nesta seção como a proteção de dados tem se efetivado na fase de coleta de dados por meio de anonimização. Para tanto, apresenta-se o resultado da revisão sistemática da literatura, conduzida com base no protocolo de Kitchenham (2004).

O objetivo principal dessa revisão foi verificar como a proteção de dados pessoais, especificamente por meio de anonimização, tem sido abordada na fase de coleta de dados pela comunidade acadêmica, buscando identificar modelos, técnicas e informações relevantes que possam contribuir para o estudo dessa temática. Neste capítulo, estão descritas as atividades realizadas nessa revisão, que envolve: identificação da pesquisa; seleção de estudos; verificação da qualidade; extração dos dados; síntese dos dados e as discussões.

4.1 Resultados e Discussões

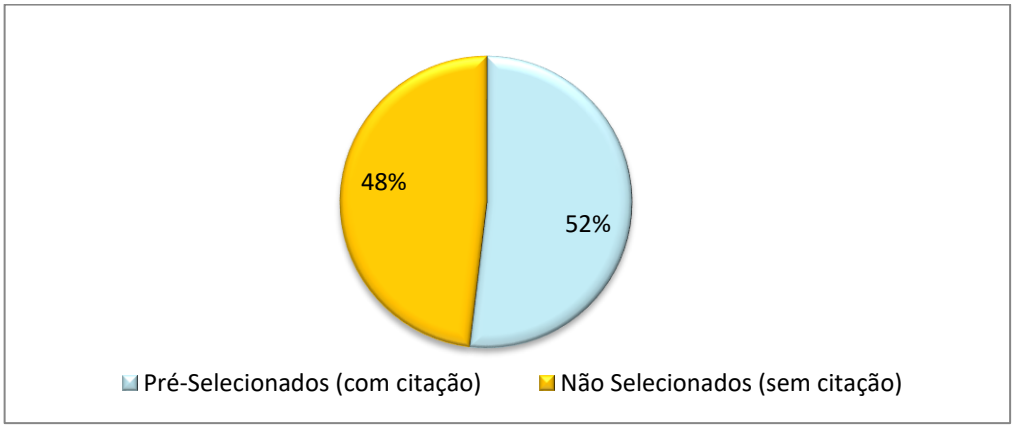
Realizou-se uma busca, por meio dos termos descritores "*anonymization", "anonimización" e* "anonimização" na base de dados *Web of Science*. A coleta foi realizada no mês de abril de 2017, e obteve-se como resultado 1.212 documentos recuperados que trouxeram, ao longo do texto e no título, o termo *"anonymization*". A busca com os termos "anonimização*" e "anonimización"* não retornou nenhum resultado.

Após a realização da busca de documentos na *Web of Science*, as informações de cada documento foram armazenadas em planilhas; assim, foram armazenados os 1.212 documentos, para que fosse possível o processo de seleção de acordo com os critérios de inclusão e exclusão estabelecidos na metodologia.

Para delimitar a amostra, foram considerados apenas artigos que obtiveram citação. Assim, obteve-se um *corpus* de 629 documentos, que fizeram parte da seleção preliminar dos

documentos. Esta amostra representa 52% dos documentos recuperados na base de dados *Web of Science*, resultado da busca por trabalhos que apresentaram no seu contexto o termo *anonymization* (Figura 15).

Figura 15 - Seleção preliminar de documentos



Fonte: Elaborado pela autora

A Figura 15 apresenta o total de trabalhos recuperados da base de dados, totalizando 1.212 documentos que tiveram, no seu contexto, o termo *"anonymization*". Os documentos pré-selecionados (que tiveram pelo menos uma citação) totalizam 629 documentos (52% do resultado da coleta), e os que não foram selecionados, pois não apresentaram no momento da coleta citações, representam 583 documentos (48% do resultado da coleta).

Após a leitura dos resumos, introduções e conclusões dos 629 documentos, seguindo os critérios de inclusão e exclusão definidos na metodologia deste trabalho, considerou-se como resultado para análise apenas o *corpus* de trabalhos com anonimização realizada na fase de coleta de dados.

Obteve-se como resultado 57 documentos que abarcaram anonimização na fase de coleta do ciclo de vida dos dados, e 508 documentos em que o foco foi a anonimização de dados na fase de recuperação.

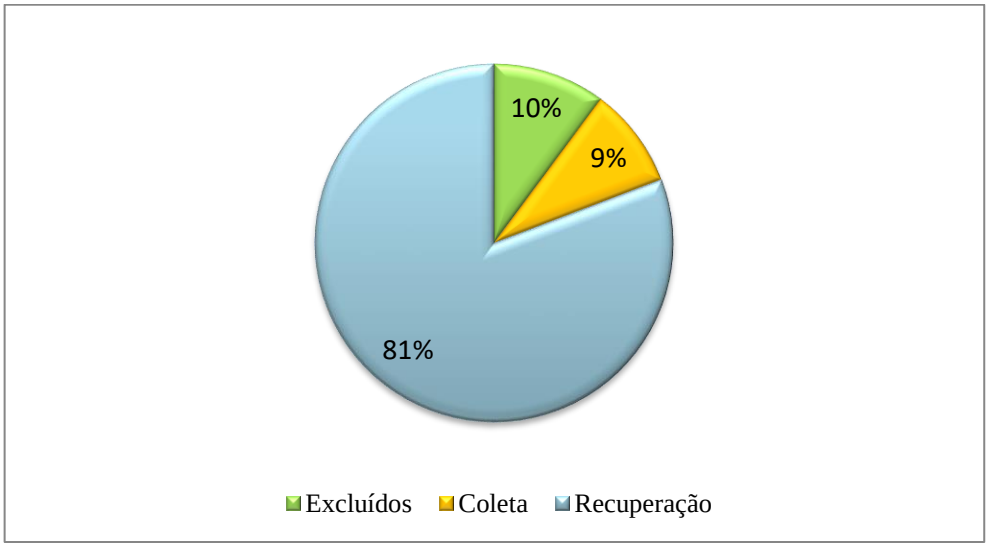
Do conjunto de trabalhos obtidos que tiveram citação, 64 foram excluídos, pois não estavam em aderência com o propósito deste estudo. A exclusão dos documentos se deu pelas seguintes justificativas:

- ✓ O termo anonimização foi apenas citado. Por exemplo, o termo surgia quando o autor relatava que a base de dados do hospital tinha passado por anonimização, mas, no decorrer do texto, não houve descrição do processo ou detalhes que justificasse a seleção do trabalho para análise;

- ✓ A temática foi abordada no contexto de ataques por terceiros durante o processo de comunicação entre duas entidades. Nesses casos, o foco é a segurança da informação, buscando garantir a confidencialidade dos dados, de modo que durante a comunicação do usuário com o destino não há intercepção de terceiros. Foram também recusados para compor a amostra os trabalhos em que a anonimização era resultado do uso de *software* como Tor.

A Figura 16 demonstra que os estudos em relação à proteção de dados pessoais, utilizando anonimização, têm se sobressaído na fase de recuperação de dados (81%). Logo, essa amostra revela que as pesquisas apresentam um foco expressivo no contexto de proteger a privacidade para disponibilização de dados, e não na fase de coleta (9%). A atenção das pesquisas na fase de recuperação deve-se às possíveis ameaças ao divulgar um conjunto de dados para a sociedade e à possibilidade de reidentificação dos indivíduos referenciados nesses dados.

Figura 16 - Seleção e exclusão de documentos



Fonte: Elaborado pela autora

Muitas pesquisas têm sido realizadas nesse contexto, como as de Sweeney (2002), Domingo-Ferrer e Torra (2005), Machanavajjhala et al. (2006), Ciriani et al. (2007b), Li, Li e Venkatasubramanian (2007); Affonso, Oliveira e Sant'Ana (2017). Nelas, buscam-se minimizar a reidentificação por meio de supressão de identificadores e a aplicar técnicas que minimizam a possível correlação de semi-identificadores com outras bases de dados públicas, ou a partir do conhecimento prévio do atacante.

Esse cenário pode contribuir para a falta de consciência sobre as ameaças presentes no processo de coleta usuário-detentor de dados. Dessa forma, constrói-se uma percepção de que as ameaças à privacidade são maiores quando um conjunto de dados é disponibilizado para sociedade, ignorando o fato de que a brecha da privacidade já se inicia a partir do momento em que o detentor de dados tem conhecimento dos dados pessoais do indivíduo. No entanto, cabe ao detentor toda a decisão e uso desses dados, salvo que eles seguem (ou deveriam seguir) legislações impostas para esse cenário.

Baseou-se nos critérios definidos por Dyba, Dingsoyr e Hanssen (2007) para demonstrar, após a leitura dos 57 documentos, a qualidade de cada um deles. Os critérios de inclusão e exclusão, juntamente com esses critérios de qualidade, corroboraram para a inclusão dos trabalhos na seleção final. O Quadro 7 apresenta, na primeira coluna, o atributo "Art.", que representa a identificação de cada trabalho selecionado para análise; a coluna dois apresenta o título dos trabalhos; e as colunas seguintes apresentam os critérios de avaliação de qualidade. A validação de cada trabalho em relação aos critérios foi realizada por meio da dicotomia "sim" e "não", em que S representa "sim" (atende ao critério), e N representa "não" (não atende ao critério). Os critérios utilizados para verificação da qualidade dos trabalhos foram os seguintes:

[1] O documento é baseado em pesquisas ou é apenas um relatório de "lições aprendidas" com base na opinião de especialista?

[2] Os objetivos da pesquisa foram definidos de forma clara?

[3] Existe uma descrição adequada do contexto em que a pesquisa foi realizada?

[4] O projeto de pesquisa é apropriado para resolver os objetivos da pesquisa?

[5] Existe uma descrição clara de resultados?

[6] O estudo representa valor para pesquisa ou prática?

Quadro 7 - Avaliação dos documentos selecionados

Art.	Documentos que abordam anonimização na fase de coleta	[1]	[2]	[3]	[4]	[5]	[6]
1	*Protecting location privacy with personalized k-anonymity: Architecture and algorithms* (GEDIK; LIU, 2008)	S	S	S	S	S	S
2	*Location privacy in mobile systems: A personalized anonymization model* (GEDIK; LIU, 2005)	S	S	S	S	S	S
3	*Smart grid privacy via anonymization of smart metering data* (EFTHYMIOU; KALOGRIDIS, 2010)	S	S	S	S	S	S
4	*Engineering privacy* (SPIEKERMANN; CRANOR, 2009)	S	S	S	S	S	S
5	*Casper: query processing for location services without compromising privacy* (CHOW; MOKBEL; AREF, 2009)	S	S	S	S	S	S
6	*Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments* (CHOW; MOKBEL; LIU, 2011)	S	S	S	S	S	S
7	*MobiMix: Protecting Location Privacy with Mix-zones over Road Networks* (PALANISAMY; LIU, 2011)	S	S	S	S	S	S

8	*A privacy-preserving location monitoring system for wireless sensor networks* (CHOW; MOKBEL; HE, 2010)	S	S	S	S	S	S
9	*CAM: cloud-assisted privacy preserving mobile health monitoring* (LIN et al., 2013)	S	S	S	S	S	S
10	*Microaggregation for database and location privacy* (DOMINGO-FERRER, 2006)	S	S	S	S	S	S
11	*Protection of query privacy for continuous location based services* (PINGLEY et al., 2011)	S	S	S	S	S	S
12	*A reciprocal framework for spatial K-anonymity* (GHINITA et al., 2010)	S	S	S	S	S	S
13	*k-Anonymous data collection* (ZHONG; YANG; CHEN, 2009)	S	S	S	S	S	S
14	*Regulating the Internet of things: first steps toward managing discrimination, privacy, security, and consent* (PEPPET, 2014)	S	S	S	S	S	S
15	*Query-aware location anonymization for road networks* (CHOW et al., 2011)	S	S	S	S	S	S
16	*An algorithm for k-anonymous microaggregation and clustering inspired by the design of distortion-optimized quantizers* (REBOLLO-MONEDERO; FORNÉ; SORIANO, 2011)	S	S	S	S	S	S
17	*Cloaking locations for anonymous location based services: a hybrid approach* (ZHANG; HUANG, 2009)	S	S	S	S	S	S
18	*Camouflage: automated anonymization of field data* (CLAUSE; ORSO, 2011)	S	S	S	S	S	S
19	*Privacy, quality of information, and energy consumption in participatory sensing systems* (VERGARA-LAURENS; MENDEZ; LABRADOR, 2014)	S	S	S	S	S	S
20	*A privacy-preserving reputation system for participatory sensing (*HUANG; KANHERE; HU, 2012)	S	S	S	S	S	S
21	*Anonymous user tracking for location-based community services.* (RUPPEL et al., 2006)	S	S	S	S	S	S
22	*Analysis of seam-carving-based anonymization of images against PRNU noise pattern-based source attribution* (DIRIK; SENCAR; MEMON, 2014)	S	S	S	S	S	S
23	*CoinShuffle: practical decentralized coin mixing for bitcoin* (RUFFING; MORENO-SANCHEZ; KATE, 2014).	S	S	S	S	S	S
24	*Privacy protection through k-anonymity in location.based services* (ZUBERI; LALL; AHMAD, 2012)	S	S	S	S	S	S
25	*Dummy-based schemes for protecting movement trajectories* (LEI et al., 2012)	S	S	S	S	S	S
26	*Anonymization models for directional location based service environments* (SHIN; VAIDYA; ATLURI, 2010)	S	S	S	S	S	S
27	*Composition and generalization of context data for privacy preservation* (PARESCHI et al., 2008)	S	S	S	S	S	S
28	*A fast privacy-preserving framework for continuous location-based queries in road networks* (WANG; KOBSA, 2013)	S	S	S	S	S	S
29	*Road network mix-zones for anonymous location based services* (PALANISAMY et al., 2013)	S	S	S	S	S	S
30	*Query processing in private data outsourcing using anonymization* (NERGIZ; CLIFTON, 2011)	S	S	S	S	S	S
31	*k-anonymity based framework for privacy preserving data collection in wireless sensor networks* (BAHŞI; LEVI, 2010)	S	S	S	S	S	S
32	*Adaptive photo-response non-uniformity noise removal against image source attribution* (KARAKÜÇÜK; DIRIK, 2015)	S	S	S	S	S	S
33	*Preserving privacy while reducing power consumption and information loss in LBS and participatory sensing applications* (VERGARA-LAURENS; LABRADOR, 2011)	S	S	S	S	S	S
34	*How to protect privacy in floating car data systems* (RASS et al., 2008)	S	S	S	S	S	S
35	*Distributed privacy preserving data collection* (XUE et al., 2011)	S	S	S	S	S	S
36	*Ad hoc privacy management in ubiquitous computing environments* (BUNNIG; CAP, 2009)	S	S	S	S	S	S

37	*METoe"P: revisiting Privacy-Preserving Data Publishing using secure devices* (ALLARD; NGUYEN; PUCHERAL, 2014)	S	S	S	S	S	S
38	*Anonymizing continuous queries with delay-tolerant mix-zones over road networks* (PALANISAMY et al., 2014)	S	S	S	S	S	S
39	*Balancing trajectory privacy and data utility using a personalized anonymization model* (GAO et al., 2014)	S	S	S	S	S	S
40	*A PLA-based privacy-enhancing user modeling framework and its evaluation* (WANG; KOBSA, 2013)	S	S	S	S	S	S
41	*Hilbert-order based spatial cloaking algorithm in road network* (KIM et al., 2013)	S	S	S	S	S	S
42	*Protecting location privacy in mobile geoservices using fuzzy inference systems* (HASHEMI; MALEK; MR, 2012)	S	S	S	S	S	S
43	*RSSI-based user centric anonymization for location privacy in vehicular networks* (WEI; CHEN; SHAN, 2009)	S	S	S	S	S	S
44	*Privacy preserving social networking through decentralization* (CUTILLO; MOLVA; STRUFE, 2009)	S	S	S	S	S	S
45	*Privacy-preserving loyalty programs* (BLANCO-JUSTICIA; DOMINGO-FERRER, 2015)	S	S	S	S	S	S
46	*A privacy-preserving continuous location monitoring system for location-based services* (SONG et al., 2015)	S	S	S	S	S	S
47	*CLOPRO: A framework for Context Cloaking Privacy Protection* (PANDIT; POLINA; KUMAR, 2014)	S	S	S	S	S	S
48	*CAPPA: Context Aware Privacy Protecting Advertising - an extension to CLOPRO framework* (PANDIT et al., 2014)	S	S	S	S	S	S
49	*Collusion-resistant query anonymization for location-based services* (ZHANG; LAZOS, 2014)	S	S	S	S	S	S
50	*Efficient time-stamped event sequence anonymization* (SHERKAT; LI; MAMOULIS, 2013)	S	S	S	S	S	S
51	*Velocity similarity anonymization for continuous query location based services* (GUSTAV et al., 2013)	S	S	S	S	S	S
52	*Engineering privacy for big data apps with the unified modeling language* (JUTLA; BODORIK; ALI, 2013)	S	S	S	S	S	S
53	*Protecting location privacy with k-confusing paths based on dinamyc pseudonyms* (MANO; MINAMI; MARUYAMA, 2013)	S	S	S	S	S	S
54	*MultiPathPrivacy: enhanced privacy in fault replication* (LOURO; GARCIA; ROMANO, 2012)	S	S	S	S	S	S
55	*Private data analytics on biomedical sensing data via distributed computation* (GONG; FANG; GUO, 2016)	S	S	S	S	S	S
56	*Privacy for location based system in mobile P2P environment* (PRIYA; MANI, 2012)	S	S	S	S	S	S
57	*Leveraging social links for trust and privacy in networks* (CUTILLO; MOLVA; STRUFE, 2009)	S	S	S	S	S	S

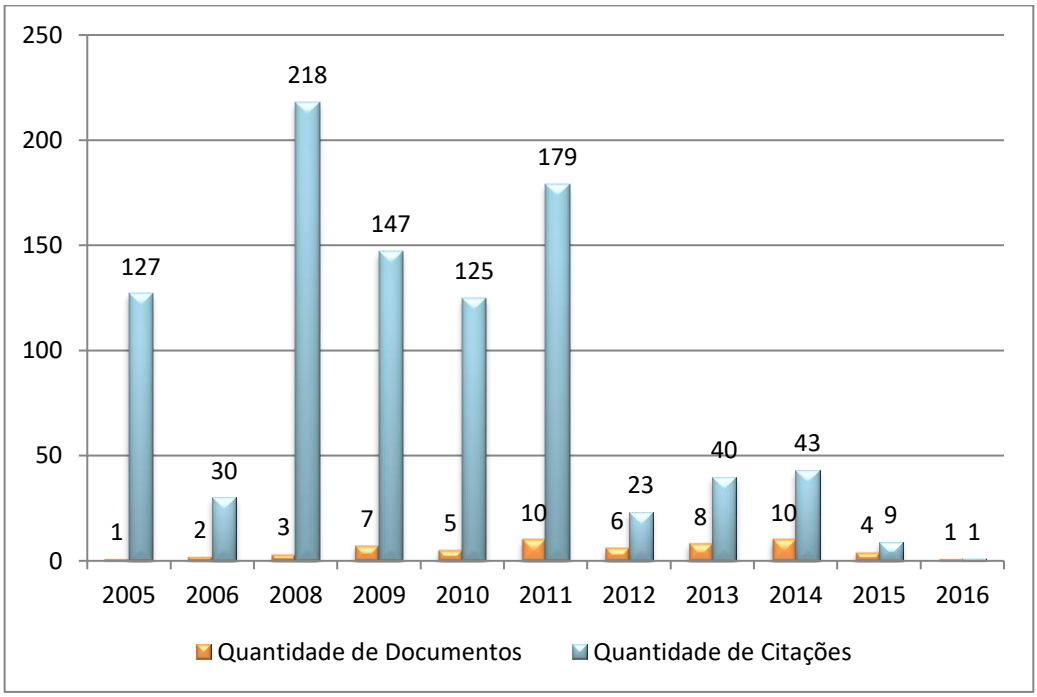
Fonte: Elaborado pela autora

Os critérios verificados no Quadro 7 contribuem para justificar a inclusão dos trabalhos na amostra para ser analisada. Observou-se que os objetivos dos trabalhos foram definidos de forma clara e concisa, facilitando o atendimento às questões de pesquisa dessa revisão. O contexto em que a anonimização foi aplicada está explicita em 100% dos trabalhos, o que permite identificar cenários que carecem de atenção à proteção da privacidade.

4.1.1 Quantidade de documentos, citação e ano de publicação

A Figura 17 ilustra o ano de publicação dos trabalhos, a quantidade de artigos publicados e de citações. Por meio das informações presente na Figura 17, observa-se uma média de 5.18 documentos por ano, e um desvio padrão de 2.7, com maior concentração de trabalhos nos anos 2005, 2008, 2009, 2010 e 2011. Em relação à citação, há uma média de 86,63 citações por ano, e um desvio padrão de 75,64. No ano de 2008, destaca-se a quantidade de citações e a visibilidade do artigo intitulado *Protecting location privacy with personalized k-anonymity: Architecture and algorithms* dos autores Gedik e Liu (2008), constando 210 citações. Esse trabalho foi publicado pela IEEE *Transactions on Mobile Computing*.

Figura 17 - Produção e citação *versus* ano da publicação



Fonte: Elaborado pela autora

Para destacar o escopo e a característica de cada trabalho, realizou-se a leitura dos documentos que compuseram o *corpus* da literatura selecionada, a fim de encontrar elementos conceituais vinculados às questões de proteção de dados pessoais por meio de anonimização.

A sumarização dos trabalhos (Apêndice A) inclusos na revisão sistemática foi caracterizada por meio dos seguintes atributos: Art. (número que identifica o trabalho, de acordo com a descrição no Quadro 7), autores, ano, número de citações, escopo e característica principal de cada trabalho.

A partir da sumarização apresentada, nota-se que o foco das pesquisas está no contexto de dados coletados a partir de dispositivos móveis, e que a maioria dos trabalhos buscam

mecanismos e técnicas, ou desenvolvem modelos, com a finalidade de esconder a identidade do titular dos dados presente em conjunto de dados que possuem dados de localização, ou durante a solicitação de um serviço LBS. Assim, é nítida a carência de estudos e pesquisas na fase de coleta de dados por outros contextos, tais como redes sociais, mecanismos de busca e na área médica.

Para corroborar com a interpretação realizada pela leitura dos documentos, utilizou-se da contagem de palavras para verificar a frequência de termos ou expressões nos resumos dos 57 documentos recuperados. O Quadro 8 mostra os resultados obtidos com a utilização da ferramenta *Textalyser.net*. Nele, é possível observar que os termos "privacidade" e "localização" ocupam posição de destaque, resultados que confirmam a interpretação da leitura dos trabalhos e a síntese discursiva (Apêndice A).

Esse conjunto de palavras fornecidas pela ferramenta *Textalyser.net*, teve a função de descobrir os assuntos relevantes e de comprovar os resultados encontrados por meio da leitura dos documentos, processos denominados de função heurística e administração da prova (BARDIN, 2009). Desta forma, esses resultados favoreceram a definição dos atributos (modelos, técnicas, contexto em que a anonimização foi aplicada e a arquitetura de redes utilizadas) presentes no Quadro 8 e a elaboração dos seus respectivos gráficos.

Quadro 8 - Frequência e palavras principais

Palavra	**Ocorrência**	**Frequência**	**Rank**
Privacy	205	3.1%	1
Location	155	2.3%	2
Data	93	1.4%	3
Users	84	1.3%	4
Based	83	1.2%	5
Information	69	1%	6
User	61	0.9%	7
Anonymization	61	0.9%	8
Anonymity	55	0.8%	9
Query	48	0.7%	10

Fonte: Elaborado pela autora

Utilizou-se, também, o recurso proeminência do *Textalyse.net*, cuja finalidade é indicar o nível de visibilidade ou o destaque de uma palavra dentro do texto. A medição foi realizada com expressões compostas entre duas e quatro palavras. O Quadro 9 apresenta a frequência e proeminência de palavras, por meio dos seguintes atributos: expressão, contagem de expressão, frequência e proeminência. Apenas as combinações de maior relevância por posição e

proeminência foram consideradas para exibição no Quadro 9, que exibe os dados na ordem decrescente por contagem de expressão.

Quadro 9 - Proeminência e frequência de palavras por meio do *Textalyser* V1.05

Expressão	Contagem Expressão	Freq.	Proeminência	Expressão	Contagem Expressão	Freq.	Proeminência
Frequência de duas palavras							
location Privacy	35	0.3%	60.9	*data obfuscation*	3	0%	42.3
k anonymity	28	0.3%	60.4	*anonymization model*	3	0%	49.1
spatial cloaking	13	0.1%	67.4	*k anonymization*	3	0%	74.6
location information	13	0.1%	89.4	*cloaked área*	3	0%	82.7
mix zones	10	0.1%	43.7	*private location*	3	0%	91.1
privacy protection	10	0.1%	46.3	*perturbation engine*	3	0%	97.6
data collection	10	0.1%	47.9	*personalized location*	3	0%	97.7
location anonymization	9	0.1%	78.3	*be encrypted*	2	0%	41.5
user's location	8	0.1%	45.9	*location kanonymity*	2	0%	48.7
privacy aware	7	0.1%	92.7	*obfuscation techniques*	2	0%	54.2
spatio temporal	6	0.1%	61	*encryption techniques*	2	0%	61.2
location k	6	0.1%	77.8	*trusted third*	2	0%	80.2
mobile clientes	6	0.1%	82.8	*lbs server*	2	0%	80.4
the lbs	5	0%	44	*anonymization algorithms*	2	0%	88.4
temporal cloaking	4	0%	80.4	*p2p environments*	2	0%	88.6
cloaking algorithms	4	0%	82.3	*message perturbation*	2	0%	97.5
lbs provider	4	0%	82.7	*anonymity model*	2	0%	97.5
the p2p	3	0%	29	*location perturbation*	2	0%	98.4
Frequência de três palavras							
location privacy of	8	0.1%	63.8	*data collection paradigma*	2	0%	51.2
location k anonymity	6	0.1%	77.8	*encryption techniques to*	2	0%	61.2
privacy aware query	5	0%	91.7	*k anonymity in*	2	0%	80.3
on road networks	4	0%	55	*cloaking algorithm is*	2	0%	87.8
protect the privacy	4	0%	55.3	*peer location information*	2	0%	88.1
mobile users to	4	0%	55.5	*location anonymization algorithms*	2	0%	88.5
privacy preserving mechanisms	4	0%	61.8	*mobile p2p environments*	2	0%	88.6
user location privacy	4	0%	64.3	*an lbs provider*	2	0%	90
mix zone framework	3	0%	54.7	*lbs request messages*	2	0%	97.3

peer to peer	3	0%	58.2	*location anonymization on*	2	0%	97.3
mix zone construction	3	0%	58.2	*message perturbation engine*	2	0%	97.5
preserving data collection	3	0%	63.3	*efficient message perturbation*	2	0%	97.5
spatial cloaking based	3	0%	66.3	*k anonymity model*	2	0%	97.6
location privacy protection	3	0%	73.3	*personalization framework to*	2	0%	98.1
spatial cloaking algorithm	3	0%	88.1	*privacy personalization framework*	2	0%	98.1
				protecting location Privacy	2	0%	98.4
Frequência de quatro palavras							
location based services lbs	7	0.1%	53.5	*a trusted third party*	2	0%	80.2
location privacy of mobile	6	0.1%	61	*spatial cloaking algorithm is*	2	0%	87.8
privacy of mobile users	5	0%	53.3	*peer location information to*	2	0%	88.1
the location privacy of	4	0%	54.4	*the user's location Privacy*	2	0%	89.5
protect the privacy of	4	0%	55.3	*to an lbs provider*	2	0%	90.1
new data collection paradigma	2	0%	51.2	*personalized location k anonymity*	2	0%	96.9
network mix zone construction	2	0%	65	*cloaking of location information*	2	0%	97.2
based location privacy protection	2	0%	66.2	*identity removal and spatio*	2	0%	97.2
spatial cloaking based location	2	0%	66.2	*efficient message perturbation engine*	2	0%	97.5
mix zone framework to	2	0%	66.4	*k anonymity for a*	2	0%	98
privacy enhancing k anonymization	2	0%	76.7	*location k anonymity for*	2	0%	98
anonymity preserving data collection	2	0%	76.9	*for protecting location privacy*	2	0%	98.4

Fonte: Elaborado pela autora

Por meio da contagem de termos nos documentos, é possível ter a percepção dos contextos em que a anonimização de dados foi aplicada. Assim, a análise mostra a ocorrência do termo "*Location Privacy*" representando as questões de privacidade no contexto da localização. O termo "*Location Perturbation*" (proeminência 98,4) caracteriza as técnicas de perturbação que foram aplicadas em dados de localização para anonimização dos dados; e os

termos *Location Anonymization* (proeminência 78) e *Location Anonymization Algorithms* (proeminência de 88,5) comprovando a anonimização de dados no âmbito da localização.

Destacam-se também os termos "*Data Collection*" e "*Preservation Data Collection*", que representam o foco desta pesquisa, indicando a fase do ciclo de vida a que os trabalhos se referem, confirmando que a amostra realmente aborda questões de privacidade voltadas para a fase de coleta de dados.

O modelo k-anonimato surge na análise pelos seguintes termos: "*k-anonymit model"* (proeminência 97,6); *"k-anonymization*" (proeminência 74,6); "*k-anonymity*" (proeminência 60.4), e com destaque também o termo "*location k anonymit"* (proeminência 60,4), indicando o k-anonimato no contexto da localização.

Esses termos representam a influência do modelo k-anonimato nas questões de proteção de dados. Embora esse modelo tenha sido desenvolvido com a finalidade de evitar a reidentificação de indivíduos em um conjunto de dados publicados, sua filosofia tem sido utilizada nos mais variados contextos e aplicações, inclusive sendo utilizado como base para outros diversos modelos e como meio de proteger dados pessoais na fase de coleta.

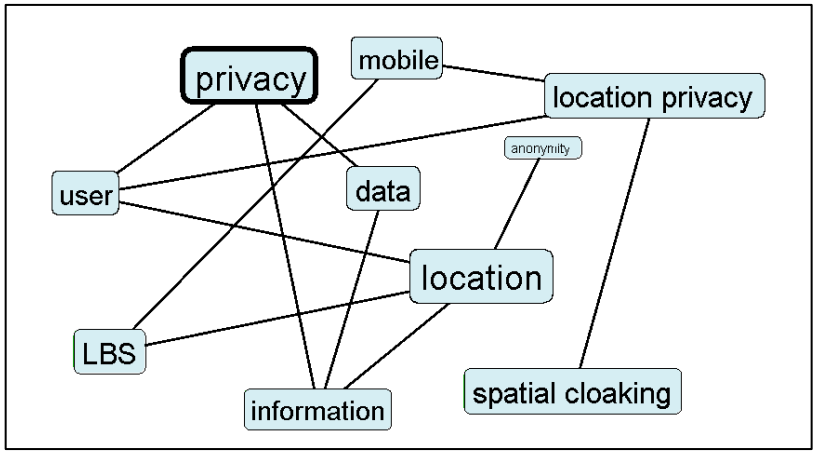
Outro resultado que chama atenção são os termos: "*Spatial Cloaking Algorithm"* (proeminência 88,1); "*Cloaking Algorithm"* (proeminência 82,3); "*Spatial Cloaking*" (proeminência 67,4); "*Spatial Cloaking based location*" (proeminência 66,2), que são técnicas e algoritmos voltados para as questões de proteção da privacidade no contexto da localização.

Em relação às técnicas para garantir a confidencialidade durante a troca de dados, os termos "*encryption techniques"* (proeminência 62,2) e "*be encrypted"* (proeminência 41,5) se destacam representando o uso de criptografia na comunicação de dados, e as técnicas de perturbação estão presentes por meio dos termos "*Perturbation Engine*" (proeminência 97,6), "*Message Perturbation*" (proeminência 97,5) e, "*data obfuscation"* (proeminência 42,3).

Em relação às arquiteturas de redes de computadores, emergem os termos "P2P *Environments"* (proeminência 88,6) e "Peer to Peer" (proeminência 58,2) referindo-se à arquitetura distribuída para a proteção de dados, sem a necessidade de um terceiro confiável. O termo "*A trusted third party"* (proeminência 80,2), por sua vez, determina à presença de um terceiro confiável, normalmente denominado de servidor anonimizador, cuja finalidade é ser o elo entre o usuário e o servidor LBS, que também surge por meio das ocorrências das expressões como "*LBS provider*" (proeminência 82,7) e "*LBS Server*" (proeminência 80,4).

Com a ferramenta Sobek, extraíram-se os termos frequentes dos resumos dos documentos, encontrando os relacionamentos entre eles (Figura 18).

Figura 18 - Principais termos envolvidos nos trabalhos



Fonte: Elaborado pela autora

Por meio dos termos que foram frequentes no texto, verifica-se que a predominância de conteúdo abordado na amostra selecionada na *Web of Science* é relacionada à proteção da privacidade no contexto da localização, especificamente quando o usuário utiliza serviços LBS e compartilha dados de localização, destacando-se o modelo k-anonimato e as técnicas *cloaking spatial* como meios para garantir a privacidade dos dados.

A partir dos termos evidenciados nas análises realizadas, tanto pela ferramenta *Textalyser* quanto pela *Sobek*, foi possível determinar as unidades semânticas para a caracterização dos trabalhos na síntese dos resultados (Quadro 10). Dessa forma, a estrutura é composta com os seguintes atributos: contextos, modelos, técnicas e arquitetura de rede, conjuntamente com as categorias já identificadas anteriormente durante a coleta dos trabalhos (origem, fonte, tipo de documento, área de pesquisa).

Quadro 10 - Sistematização dos trabalhos recuperados – Anonimização de dados na fase de coleta

Art.	País	Fonte	Tipo de Documento	Área de Pesquisa	Contexto	Modelo	Técnica	Arquitetura
1	Estados Unidos	*IEEE Transactions on Mobile Computing*	Artigo em evento	Ciência da Computação	Localização	k-anonimato	Supressão, *Spatial Cloaking* criptografia, generalização	Centralizada (Terceiro Confiável)
2	Estados Unidos e Inglaterra	*25th IEEE International Conference on Distributed Computing Systems, Proceedings*	Artigo em evento	Ciência da computação	Localização	k-anonimato	Supressão, *Spatial Cloaking*, criptografia	Centralizada (Terceiro Confiável)
3	Inglaterra	*2010 IEEE 1st International Conference on Smart Grid Communications (Smartgridcomm)*	Artigo em evento	Ciência da Computação Engenharia e Telecomunicação	Internet das Coisas	Não explícito	Criptografia	Centralizada (Terceiro Confiável)
4	Alemanha	*IEEE Transactions on Software Engineering*	*Revisão*	Ciência da Computação e Engenharia	*Privacy Design*	k-anonimato, l-diversity	Não explícito	Não explícito
5	Estados Unidos	*ACM Transactions on Database Systems*	Artigo em evento	Ciência da Computação	Localização	k-anonimato	*Spatial Cloaking*, supressão	Centralizada Terceiro Confiável
6	Estados Unidos	*Geoinformatica*	Artigo	Ciência da Computação e Geografia Física	Localização	k-anonimato	*Spatial Cloaking*, *pseudônimo*	P2P
7	Estados Unidos	*IEEE 27th International Conference on Data Engineering (Icde 2011)*	Artigo em evento	Ciência da Computação e Engenharia	Localização	k-anonimato e Mix zones	Pseudônimo	P2P
8	Estados Unidos	*IEEE Transactions on Mobile Computing*	Artigo	Ciência da Computação e Telecomunicação	Localização	k-anonimato	*Spatial Cloaking e Micro agregação*	Hibrida (Terceiro Confiável e P2P*)*
9	Estados Unidos	*IEEE Transactions on Information Forensics And Security*	Revisão	Ciência da Computação e Engenharia	Medicina	Não explícito	Criptografia, Permutação e randomização	Centralizada (Terceiro Confiável)
10	Espanha	*Next Generation Information Technologies And Systems, Proceedings*	Artigo em evento	Ciência da Computação	Localização	k-anonimato	Micro agregação e randomização	Centralizada (Terceiro Confiável)
11	Estados Unidos e Portugal	*2011 Proceedings IEEE Infocom*	Artigo em evento	Ciência da Computação Engenharia e Telecomunicação	Localização	Não explícito	*randomização*	Não explícito
12	Estados Unidos e China	*Information Systems*	Artigo em evento	Ciência da Computação	Localização	k-anonimato	*Spatial Cloaking*, *supressão*	Centralizada (Terceiro Confiável)

13	Estados Unidos	*Information Sciences*	Artigo	Ciência da Computação	Mineração de dados	k-anonimato	Randomização; Permutação*; zero- knowledge prot.* criptografia Supressão	Não explícito
14	Estados Unidos	*Texas Law Review*	Artigo	Governo e Leis	Internet das Coisas	Não explícito	Não explícito	Não explícito
15	Estados Unidos e China	*Geoinformatica*	Artigo	Ciência da Computação e Geografia Física	Localização	k-anonimato	*Spatial Cloaking*; *supressão*	Centralizada (Terceiro confiável)
16	Espanha	*Data & Knowledge Engineering*	Artigo	Ciência da Computação	Localização	k-anonimato	Rand. supressão e micro agregação	Centralizada (Terceiro Confiável)
17	Estados Unidos	*Geoinformatica*	Artigo	Ciência da Computação e Geografia Física	Localização	k-anonimato	*Spatial Cloaking* e Randomização	Hibrida (Terceiro Confiável e P2P)
18	Estados Unidos	*33rd International Conference on Software Engineering (Icse)*	Artigo em evento	Ciência da Computação	Localização	Não explícito	Supressão	Não explícito
19	Estados Unidos e Colômbia	*2014 IEEE International Conference on Pervasive Computing And Communications (Percom)*	Artigo em evento	Ciência da Computação e Engenharia	Localização	Não explícito	Criptografia; randomização	Centralizada (Terceiro Confiável)
20	Austrália	*37th Annual IEEE Conference on Local Computer Networks (Lcn 2012)*	Artigo em evento	Ciência da Computação e Engenharia	Localização	k-anonimato	randomização e pseudônimo	Centralizada (Terceiro Confiável)
21	Alemanha	*Location- And Context-Awareness, Proceedings*	Artigo em evento	Ciência da Computação Inteligência Artificial; Sistemas de Informação Teoria e Métodos	Localização	k-anonimato	Randomização, Transformada de distância	Hibrida (Terceiro Confiável e P2P)
22	Turquia	*IEEE Transactions on Information Forensics And Security*	Artigo	Ciência da Computação	Imagem	Não explícito	*randomização*	Não explícito
23	Alemanha	*Computer Security - Esorics 2014, Pt Ii*	Artigo em evento	Ciência da Computação	*Bitcon*	Não explícito	Criptografia e *shuffling*	P2P
24	Índia	*Iete Technical Review*	Artigo	Engenharia e Telecomunicações	Localização	k-anonimato	*Spatial cloaking*	Hibrida (Terceiro Confiável P2P)

25	Taiwan	*Journal of Information Science And Engineering*	Artigo	Ciência da Computação	Localização	*Não explícito*	*Randomização transformada de distância*	P2P
26	Estados Unidos	*Computers & Security*	Artigo	Ciência da Computação	Localização	k-anonimato	Generalização Randomização	Centralizada (Terceiro Confiável)
27	Itália	*2008 IEEE International Conference on Pervasive Computing and Communications*	Artigo em evento	Ciência da Computação	Localização	k-anonimato	Generalização, supressão, pseudônimo	Centralizada (Terceiro Confiável)
28	China	*Journal of Network And Computer Applications*	Artigo	Ciência da Computação	*Localização*	*k-anonimato; l-diversity*	*Spatial Cloaking*	Centralizada (Terceiro Confiável)
29	Estados Unidos	*2013 IEEE 29th International Conference on Data Engineering (ICDE)*	Artigo em evento	Ciência da Computação	*Localização*	*k-anonimato Mix-zone*[57]*s*	*Pseudônimo*	P2P
30	Estados Unidos	*Data and Applications Security And Privacy XXY*	Artigo em evento	Ciência da Computação	*Dados relacionais*	*l-diversity*	*Criptografia e anatomização generalização*	Centralizada (Terceiro Confiável)
31	Turquia	*Turkish Journal of Electrical Engineering And Computer Sciences*	Artigo	Ciência da Computação	*Sensores de redes wireless*	*k-anonimato*	*Generalização; Criptografia*	Centralizada (Terceiro Confiável)
32	Turquia	*Digital Investigation*	Artigo	Ciência da Computação e Engenharia	*Imagem*	Não explícito	*Filtro wavelet, supressão*	Não explícito
33	Estados Unidos	*2011 IEEE Globecom Workshops (GC WKSHPS)*	Artigo em evento	Ciência da Computação; Engenharia e Telecomunicações	*Localização*	*l-diversity*	*randomização e Criptografia*	Centralizada (Terceiro Confiável)
34	Áustria	*Vanet'08: Proceedings of the Fifth ACM International Workshop on Vehicular Inter-Networking*	Artigo em evento	Ciência da Computação Telecomunicações e Transporte	*Localização*	Não explícito	*Criptografia e randomização, pseudônimo*	Centralizada (Terceiro Confiável)
35	Singapura; EUA; França e Arábia Saudita	*Database Systems for Advanced Applications, PTI*	Artigo em evento	Ciência da Computação	*Medicina*	*k-anonimato e L-diversity*	*Generalização; criptografia*	Cliente-Servidor
36	Alemanha	*2009 Second International Conference on Advances In Human-Oriented And Personalized*	Artigo em evento	Ciência da Computação	*Internet das Coisas*	Não explícito	Não explícito	Não explícito

[57] Mix zones quebra a continuidade da exposição da localização dos usuários, de modo que nenhum aplicativo rastreia o movimento do usuário.

		Mechanism, Technologies, and Services						
37	Espanha e França	*Distributed and Parallel Databases*	Artigo	Ciência da Computação	*Genérico*	*K-anonimato; L-diversity; Privacidade diferencial e t-closeness*	*Criptografia e os algoritmos αβ-algorithm; Bucketization e Mondrian*	P2P
38	Estados Unidos	*Distributed and Parallel Databases*	Artigo	Ciência da Computação	*Localização*	*k-anonimato; Mix Zone*	*Randomização; Pseudônimo e Spatial Cloaking*	P2P
39	China	Journal of Network and Computer Applications	Artigo	Ciência da Computação	Localização	k-anonimato	Generalização, randomização	Distribuída
40	Estados Unidos	*User Modeling and User-Adapted Interaction*	Artigo	Ciência da Computação	Ambiente Web	Não explícito	Randomização	Não explícito
41	Coreia do Sul	*Concurrency and Computation-Practice & Experience*	Artigo	Ciência da Computação	Localização	k-anonimato	*Spatial Cloaking*	Centralizada (Terceiro Confiável)
42	Iran	*Computers Environment and Urban Systems*	Artigo	Ciência da Computação; Engenharia; Ciências Ambientais e Ecologia; Geografia; Pesquisa e Gestão de operações	Localização	Não explícito	Não explícito	Centralizada (Terceiro Confiável)
43	Taiwan	*Security in Emerging Wireless Communication and Networking Systems*	Artigo	Ciência da Computação; Engenharia e Telecomunicações	Localização	Não explícito	Medidas de distância, randomização	P2P
44	França	*Wons 2009: Sixth International Conference on Wireless on-Demand Network Systems Services*	Artigo em evento	Ciência da Computação	Redes Sociais	Não explícito	Criptografia, pseudônimo	P2P
45	Espanha	*Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*	Artigo em evento	Ciência da Computação	Ambiente Web	Não explícito	Generalização e Criptografia, *; zero- knowledge protocol*	Distribuída
46	Coreia do Sul	*International Journal of Distributed Sensor Networks*	Artigo	Ciência da Computação e Telecomunicações	Localização	k-anonimato	*Spatial Cloaking*	Centralizada (Terceiro Confiável)

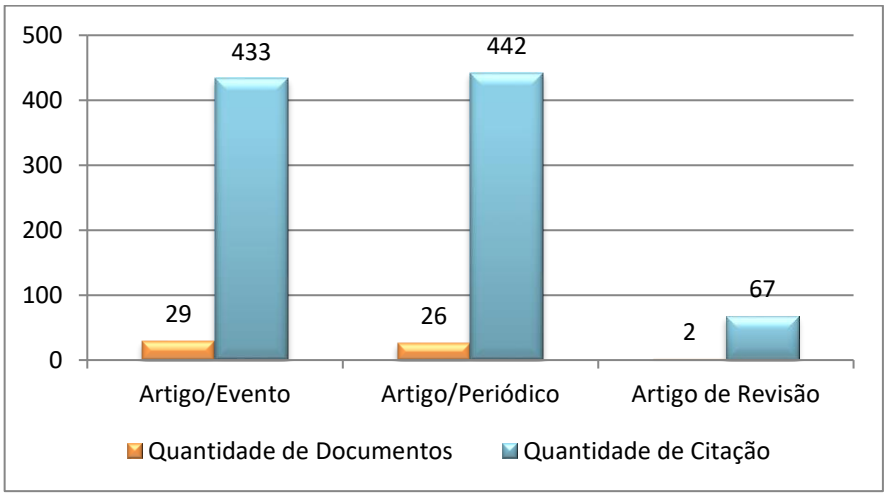
47	Estados Unidos	*2014 Fourth International Conference on Communication Systems and Network Technologies*	Artigo	Ciência da Computação Engenharia e Telecomunicações	Localização	k-anonimato	Generalização; *randomização* e Criptografia	Centralizada (Terceiro Confiável)
48	Estados Unidos	*2014 IEEE International Conference on Services Computing (SCC 2014)*	Artigo em evento	Ciência da Computação e Engenharia	Localização	K-anonimato	Generalização; criptografia	Centralizada (Terceiro Confiável)
49	Estados Unidos	*2014 IEEE International Conference on Communications (Icc)*	Artigo em evento	Telecomunicações	Localização	k-anonimato	Criptografia; Permutação e S*huffling*	P2P
50	China	*ACM Transactions on the Web*	Artigo	Ciência da Computação	Dados de interação e timestamped	k-anonimato e l-diversity	Supressão; Generalização	Não explícito
51	China	*2013 International Conference on Computational Problem-Solving (ICCP)*	Artigo em evento	Ciência da Computação	Localização	k-anonimato	*Spatial Cloaking, supressão e micro agregação*	Centralizada (Terceiro Confiável)
52	Canadá	*2013 IEEE International Congress on Big Data*	Artigo em evento	Ciência da Computação e Engenharia	*Privacy* Design	Não explícito	Não explícito	Não explícito
53	Japão	*2013 IEEE International Conference on Pervasive Computing and Communications Workshops (Percom Workshops)*	Artigo em evento	Ciência da Computação Engenharia e Computação	Localização	Não explícito	Pseudônimos	Centralizada (Terceiro Confiável)
54	Portugal	*2012 Ninth European Dependable Computing Conference (EDCC 2012)*	Artigo em evento	Ciência da Computação	Dados de relatório	Não explícito	Randomização	Cliente-servidor
55	Alemanha	*IEEE-ACM Transactions On Computational Biology And Bioinformatics*	Artigo	Bioquímica e Biologia Molecular; Ciência da Computação e Matemática	Medicina	Não explícito	Criptografia, randomização	P2P
56	Índia	*International Conference On Modeling Optimization And Computing*	Artigo em evento	Ciência da Computação; Engenharia; Pesquisa e Gestão de Operações	Localização	k-anonimato	*Spatial Cloaking*	P2P
57	Alemanha	*Inetsec 2009 - Open Research Problems In Network Security*	Artigo	Ciência da Computação	Redes Sociais	Não explícito	Pseudônimo	P2P

Fonte: Elaborado pela autora

A partir dos dados recuperados dos documentos e demonstrados no Quadro 10, realizou-se as representações gráficas e a análise dos resultados.

Primeiramente, verificou-se os tipos de formatos de publicação que mais prevaleceram no *corpus* de documento e a quantidade de citações por formato de publicação. Em sua maioria, os documentos foram frutos de trabalhos de eventos (*proceedings paper)*, totalizando 50,9% dos documentos. Em seguida estão os trabalhos publicados em periódicos, resultando em 45,6% dos documentos. Por fim, 3,5% são de trabalhos de revisão (Figura 19).

Figura 19 - Tipo de produção e citação



Fonte: Elaborado pela autora

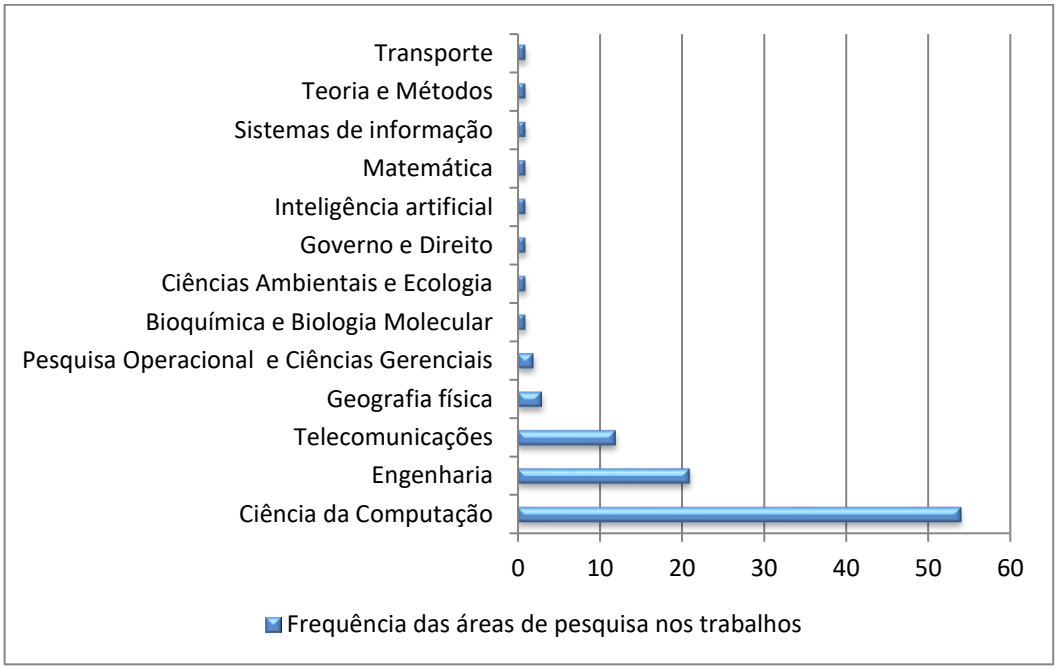
A Figura 24 destaca a visibilidade dos trabalhos publicados em periódicos, sendo que mais citado foi o trabalho intitulado "*Spatial Cloaking for anonymous location-based services in mobile peer-to-peer environments*", dos autores Chow, Mokbel e Liu (2011), com 42 citações, publicado no periódico GeoInformatica. Nos artigos de revisão o trabalho com mais citação foi o "*Engineering Privacy*", dos autores Spiekermann e Cranor (2009), com 67 citações, publicado em 2011 pela *IEEE Transaction on Software Engineering.* E em artigos de eventos, o trabalho *Protecting location privacy with personalized k-anonymity: Architecture and algorithms*, dos autores Gedik e Liu (2008), constando 210 citações. Esse trabalho foi publicado pela IEEE *Transactions on Mobile Computing,* como citado anteriormente.

4.1.2 Áreas de pesquisa

A análise foi baseada nas áreas de pesquisas disponibilizada pela *Web of Science* para classificar os documentos. Os trabalhos pertencem a várias áreas de pesquisa, uma vez que cada trabalho pode estar vinculado a mais de uma área. A Ciência da Computação aparece em 54

trabalhos, seguidos da Engenharia, presente em 21 documentos, e das Telecomunicações, em 12 pesquisas. Outras áreas também são representadas, mas com menores ocorrências, tais como a Geografia Física, Governos e Leis, e a Matemática (Figura 20).

Figura 20 - Frequência das áreas de pesquisa nas quais os documentos estão vinculados



Fonte: Elaborado pela autora

Esses resultados (Figura 20) indicam que as questões de privacidade estão centradas nos modelos e técnicas computacionais, portanto, possuem características mais tecnológicas, o que justifica a predominância da Ciência da Computação, da Engenharia e das Telecomunicações. Observa-se uma pequena participação de outras áreas de pesquisa em relação à privacidade no âmbito da coleta de dados, tais como, Governos e Leis, Ciência Ambientais e Ecologia, inclusive da ausência da Ciência da Informação.

A justificativa para a carência de estudos na área da Ciência da Informação sobre essa temática na amostra coletada poderia ser devido ao termo descritor "Anonimização" estar intrinsecamente vinculado à computação. No entanto, os autores Bembém, Sant'Ana e Santos (2015), ao verificarem como o tema privacidade tem sido abordado nas publicações do *Journal of the Association Science and Tecnology* (JASIST), utilizando o termo "*privacy*", obtiveram como resultado menos de 2% das publicações que trataram de privacidade. Além disso, a incidência da temática se deu no contexto da violação da privacidade, sendo predominantemente publicada no contexto internacional. Assim, observa-se que o uso do termo

"*anonymization"* não é um fator que justifica a ausência de trabalhos pertencentes à área de Ciência da Informação, pois mesmo com um termo mais genérico, como privacidade, também é evidente a carência de trabalhos nessa área.

Nesse cenário, portanto, a Ciência da Informação poderia contribuir para atender as necessidades da sociedade em relação à proteção de dados pessoais, fomentando pesquisas e métodos para minimizar a insciência sobre a fase de coleta de dados, tornando mais perceptível a identificação dos elementos que compõem esse cenário, a fim de minimizar quebras de privacidade.

4.1.3 Os países envolvidos nas pesquisas

A Figura 21 apresenta a distribuição geográfica das instituições dos autores dos trabalhos analisados. Dessa forma, é possível ter um panorama das regiões de interesse sobre a temática em estudo, incluindo os países que não tiveram representatividade no *corpus* de trabalhos recuperados.

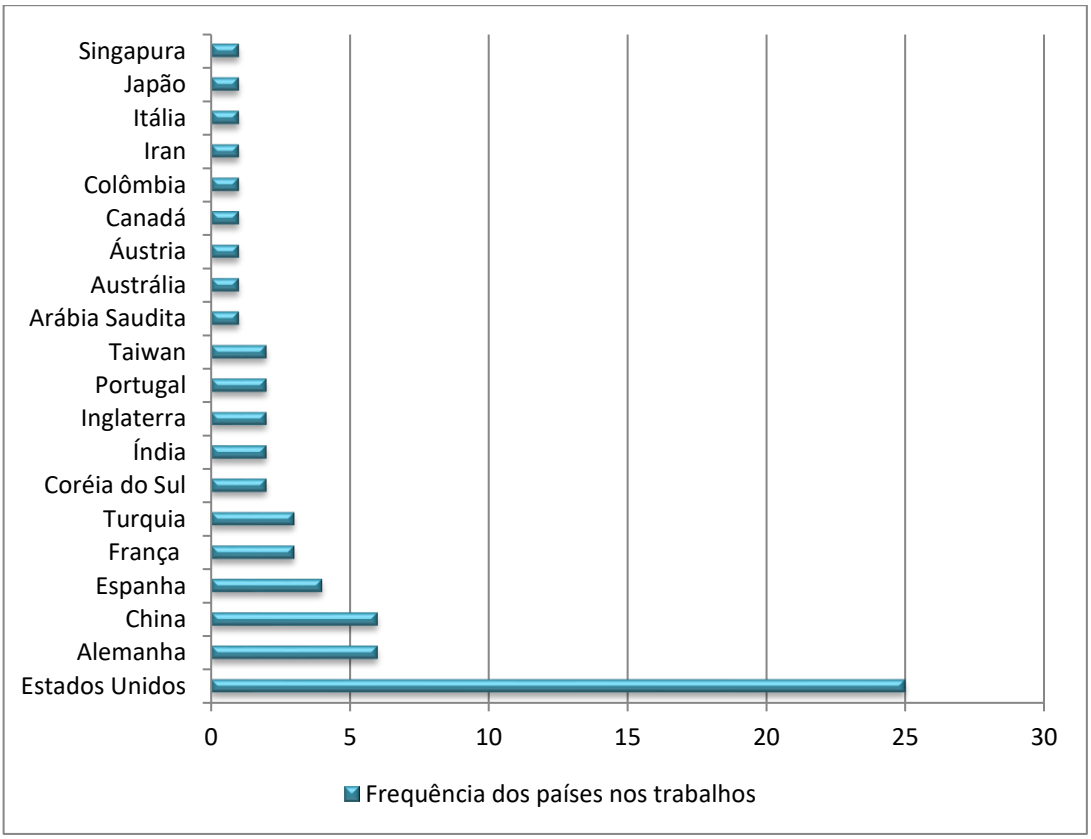
No universo dos trabalhos recuperados, foram identificados 20 países que representam a origem das instituições onde os autores são afiliados. Dos 20 países, observa-se uma maior frequência dos países da Ásia e da Europa representando 80% dos países. Em seguida a América com 15% e Oceania com 5%.

Figura 21 - Países representados nos documentos recuperados

Fonte: Elaborado pela autora

Entretanto, pode-se notar, na Figura 22, a expressiva presença dos Estados Unidos nas pesquisas que abordam anonimização na fase de coleta. O país está presente em 25 trabalhos. Posteriormente, emergem Alemanha, China, Espanha, França, Turquia, Coreia do Sul, Índia, Inglaterra, Portugal, Taiwan, Arábia Saudita, Austrália, Áustria, Canadá, Colômbia, Iran, Itália, Japão e Singapura com menor notabilidade.

Figura 22 - Frequência dos países nos trabalhos

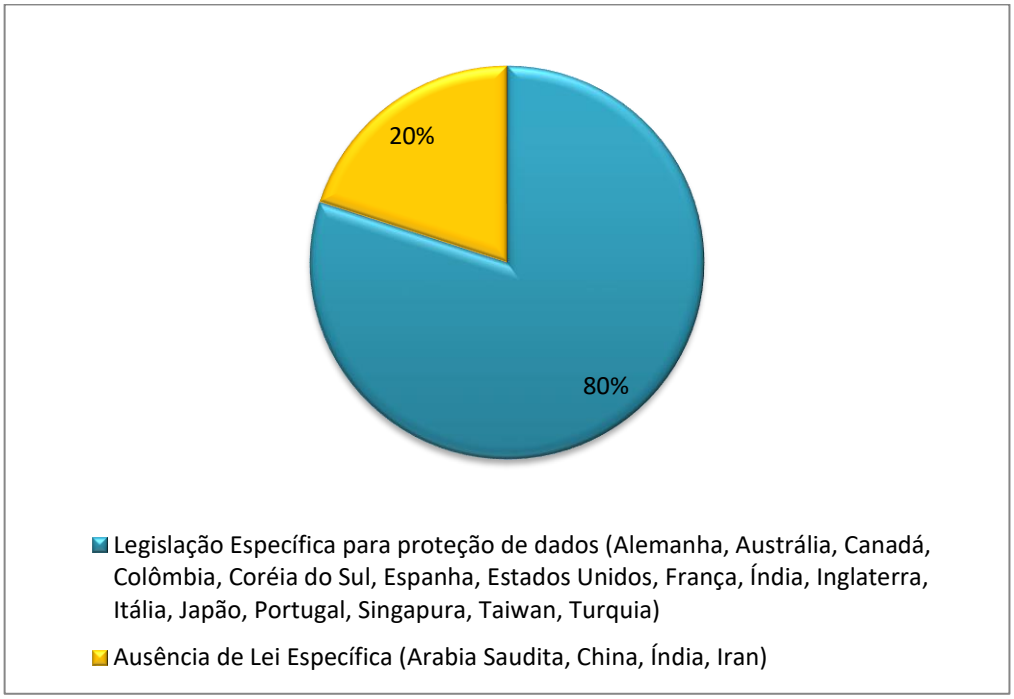


Fonte: Elaborado pela autora

O destaque dos Estados Unidos nos trabalhos recuperados pode ser reflexo da sua própria cultura, que expressa sinais de individualismo e necessidade de privacidade desde a época de sua colonização. Ao estabelecer as primeiras colônias, os colonos foram se estabelecendo sozinhos e costumavam tomar suas próprias decisões, seu trabalho era realizado para o enriquecimento próprio, estabelecendo, assim, o individualismo nas colônias americanas (DEPARTAMENTO DE ESTADO DOS ESTADOS UNIDOS, 2012; COLONIZAÇÃO DE POVOAMENTO, 2018), situação que pode ter acentuado a necessidade de manter a privacidade.

A existência de leis e decretos que amparam as questões de proteção de dados pessoais nos países de origem das instituições dos autores configura-se como um fator que pode contribuir ao interesse ou necessidade de pesquisas nessa temática. Dos países representados nos trabalhos recuperados, 80% apresentam leis específicas para proteção de dados pessoais, apenas a Arábia Saudita, China, Índia e o Iran, entre eles, não possuem legislação específica para proteção de dados (Figura 23).

Figura 23 - Países que possuem legislação específica para proteção de dados pessoais

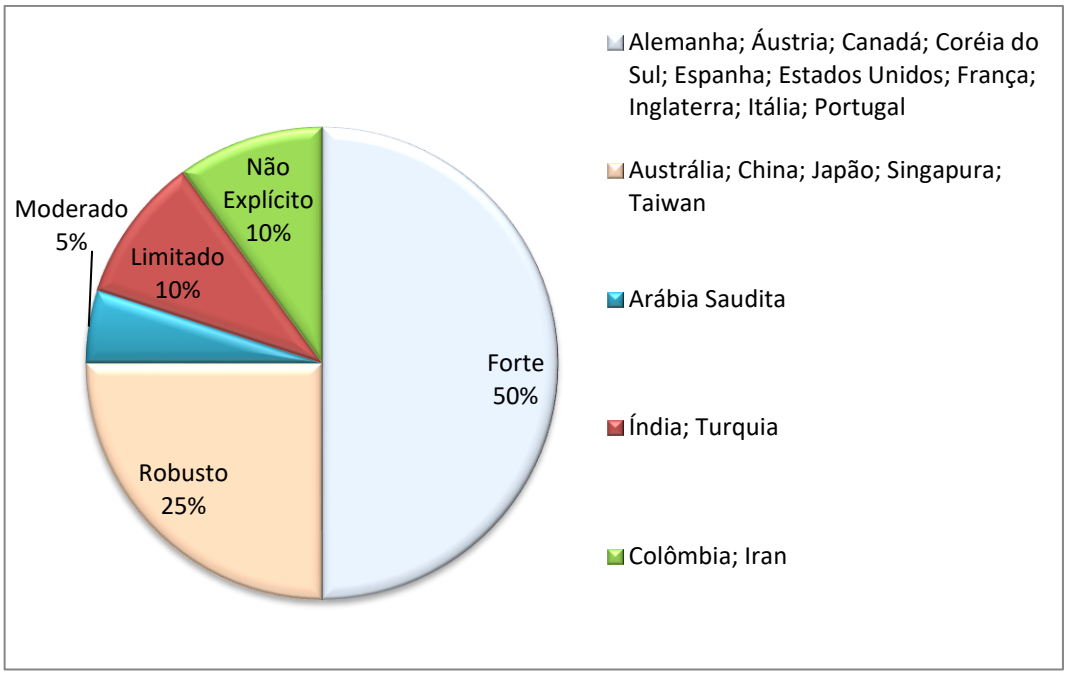


Fonte: Elaborado pela autora

Ainda, ao correlacionar os países presentes nos trabalhos publicados com a classificação disponibilizada pela DLA Piper (2017) [58], observa-se que 10 países (50%) estão enquadrados na categoria "Forte", e 5 países (25%) na categoria "Robusta". Ao somar essas duas categorias, obtém-se uma totalização de 15 países (75%) que buscam cumprir, severamente, os regulamentos e a execução das leis de proteção de dados pessoais (Figura 24).

[58] A associação classifica os países quanto aos regulamentos e à execução de leis de proteção de dados pessoais em: "forte"; "robusta"; "moderada"; "limitada".

Figura 24 - Países representados nos trabalhos e aderência a regulamentos e execução



Fonte: Elaborado pela autora

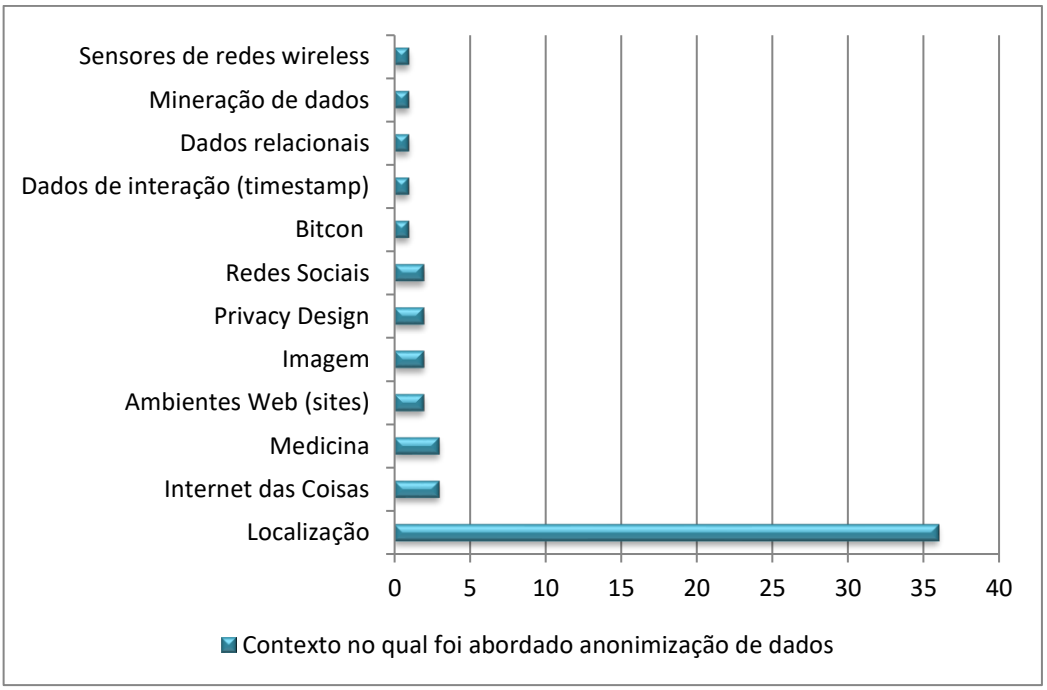
Esses dados levam a uma reflexão sobre a relevância do ordenamento jurídico para amparo à proteção de dados pessoais. A presença de legislações pode estimular pesquisadores a investigar novos modelos e técnicas para anonimizar dados, atitude que contribui com alternativas para que organizações públicas e privadas estejam em conformidade com os regulamentos para proteção de dados. Essa situação pode ampliar a consciência sobre os problemas envolvidos com quebras de privacidade e a necessidade de proteger dados pessoais devido à coleta de dados pelos diversos meios tecnológicos.

4.1.4 Domínio das pesquisas

Em relação ao contexto em que a anonimização de dados foi abordada, destaca-se o uso da anonimização em relação aos dados de localização do usuário. Desta forma, soluções que visam minimizar ameaças quando se utiliza serviços que coletam dados de localização, se efetuam em 65% dos trabalhos recuperados, tornando os outros contextos, tais como microdados, redes sociais, dados de interação, mineração de dados e medicina, com valores menos expressivos na fase de coleta de dados (Figura 25).

Esses resultados demonstram que as preocupações com a privacidade de dados dos indivíduos direcionam-se para aplicações e dispositivos que realizam a coleta de dados de localização, nesse caso, os serviços baseados em localização (LBS).

Figura 25 - Contexto em que a anonimização de dados foi abordada



Fonte: Elaborado pela autora

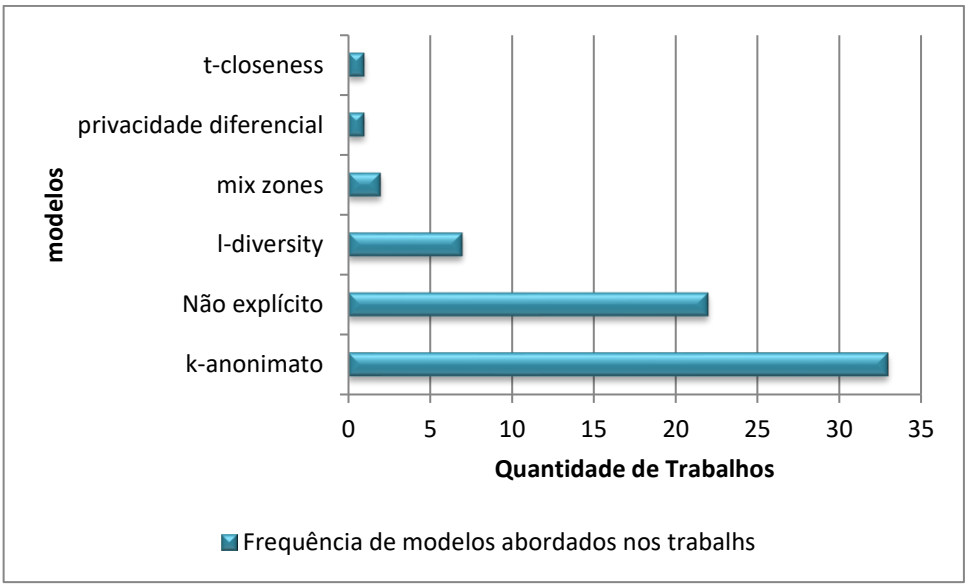
A ênfase nos dados de localização do usuário é fruto da ampliação do acesso a aplicativos e dispositivos móveis, visto que, na Figura 22, exibida anteriormente, o número de publicações se concentram em meados de 2011, período que apresenta um forte crescimento dessas tecnologias[59].

4.1.5 Modelos para proteção da privacidade

O modelo k-anonimato é destaque nos documentos recuperados como alternativa para a proteção de dados pessoais na fase de coleta de dados. Embora esse modelo tenha sido desenvolvido com a finalidade de permitir a disponibilidade de dados com garantias de privacidade, essa revisão revela que tal modelo tem sido ponto inicial para outros modelos abordados nos trabalhos, tornando-se uma referência para as questões de proteção de dados pessoais, com a intenção de impedir a reidentificação dos sujeitos. A Figura 26 ilustra a quantidade de documentos que abordaram modelos para anonimização dos dados, em que o modelo k-anonimato apresenta uma maior frequência nos trabalhos.

[59] O tráfego de dados móveis cresceu 18 vezes nos últimos cinco anos (CISCO, 2017).

Figura 26 - Frequência de modelos representados nos trabalhos



Fonte: Elaborado pela autora

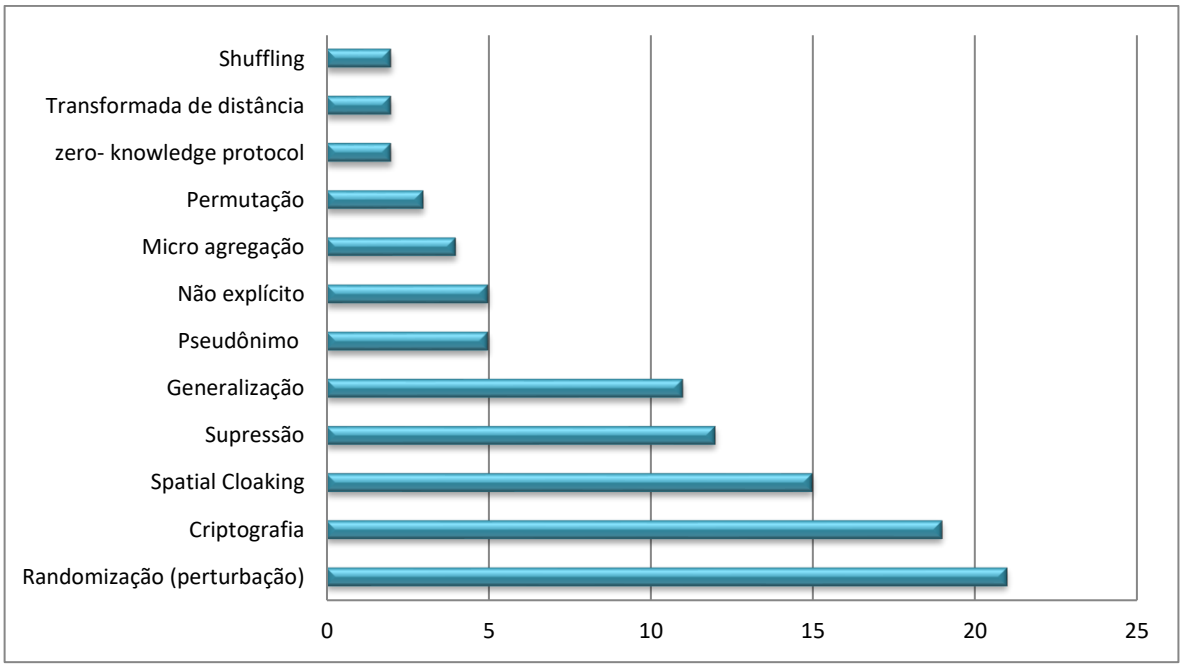
Ressalta-se que em alguns trabalhos, não ficaram explícitos os modelos de anonimização utilizado, apenas foram indicadas as técnicas para proteger dados pessoais, tais como generalização, criptografia e randomização.

4.1.6 Técnicas para proteção de dados

Muitas das técnicas empregadas para garantir a proteção de dados pessoais são herdadas das próprias diretrizes do k-anonimato, como a supressão de dados identificadores e a generalização de semi-identificadores.

Devido ao contexto de aplicação predominante ser a localização, as técnicas apresentam a finalidade de impedir a vinculação do usuário com a sua localização exata. A randomização e a criptografia se sobressaem em relação às outras técnicas. Esses meios de proteger os dados são, muitas vezes, combinados com outras técnicas, tais como: a generalização das coordenadas geográficas do usuário por uma área; *spatial cloacking*; supressão e as técnicas perturbativas que modificam os dados de origem por meio de adição de ruído, pseudônimos e permutação (Figura 27).

Figura 27 - Frequência das técnicas nos trabalhos recuperados



Fonte: Elaborado pela autora

Um ponto interessante é o uso da criptografia. Embora ela tenha sido amplamente utilizada como meio para proteção de dados, sua finalidade é voltada para permitir a confiabilidade entre as partes envolvidas no processo de comunicação, garantindo que, não haja a intercepção de terceiros ou de ataques. Deste ponto de vista, a criptografia protege os dados que circulam por meio das redes de computadores na comunicação usuário-detentor; no entanto, dependendo do algoritmo, os dados não se tornam anônimos para o detentor. Entretanto, a questão da privacidade, vista sobre o detentor de dados, continua sendo invadida, já que ele pode possuir acesso aos dados pessoais.

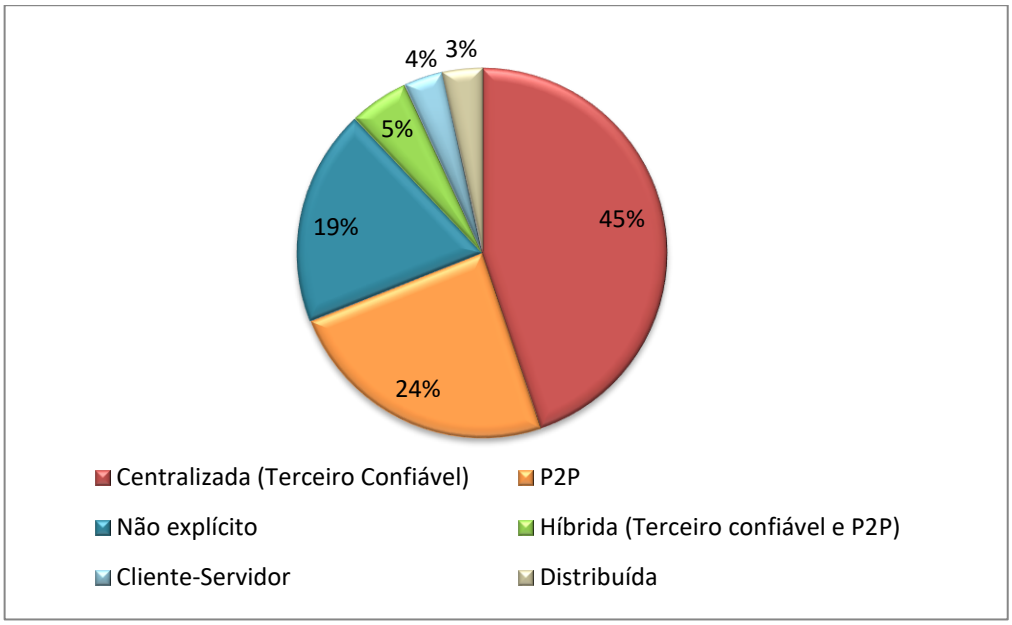
Portanto, mesmo que os ambientes prometam garantias de privacidade pela criptografia, usuários continuam apoderando os detentores com os seus dados. Esta pesquisa destaca a criptografia sendo combinada com outras técnicas de anonimização, tais como adição de ruído, perturbação, generalização e supressão, buscando, por meio dessas técnicas de mascaramento, impedir a descoberta de dados identificadores ou semi-identificadores.

4.1.7 Arquitetura de redes

Em relação à arquitetura de redes de computadores, os trabalhos analisados apresentam os seguintes termos: comunicação centralizada (terceiro confiável); arquitetura P2P e, híbrida (quando combinam as duas arquiteturas de redes), cliente-servidor e distribuída.

A necessidade de um terceiro confiável está presente em 26 trabalhos (45%), isso indica que um terceiro anonimizador terá acesso aos dados, e a abordagem da anonimização pode não estar sendo realizada diretamente na fonte. O problema nesse tipo de arquitetura é a possibilidade desse servidor ser invadido e resultar em ameaças e descobertas de dados dos indivíduos (Figura 28).

Figura 28 - Arquitetura de redes



Fonte: Elaborado pela autora

Em relação à arquitetura das redes, Domingo-Ferrer (2006) ressalta que o uso de um terceiro confiável é uma ameaça à privacidade, pois o anonimizador aprende a trajetória e a identidade de todos os usuários, causando, assim, uma falsa impressão de que os dados estão sob salvaguarda de privacidade.

4.2 Considerações Finais

Este capítulo realizou uma revisão sistemática que elucidou como a proteção de dados pessoais por meio de anonimização tem se efetuado na fase de coleta de dados. Assim, os trabalhos recuperados na *Web of Science* demonstraram que o foco das pesquisas em relação à anonimização está na recuperação de dados, e não na fase de coleta. Esse cenário ilustra que debates, pesquisas e estudos não concentram esforços para essas questões no âmbito da coleta de dados, visto que, é a coleta que impulsiona todo o ciclo de vida dos dados e promove ao

usuário consciência sobre o que essas empresas estão coletando, o motivo e o destino desses dados.

Essa carência de trabalhos faz com que as preocupações em relação à privacidade estejam na possibilidade de um atacante identificar o sujeito em um conjunto de dados, tornando a figura do detentor muitas vezes sem importância no domínio de quebras de privacidade. Ressalta-se que, a tarefa de proteger dados pessoais não deveria ser uma atividade deixada apenas para os detentores de dados.

Trabalhos de pesquisa têm a relevância de disseminar informações para criar e agregar conhecimentos para os indivíduos; se essa ciência apresenta déficit nessa temática, então há impacto no desenvolvimento de modelos, técnicas, desenvolvimento de políticas de informação e na construção de legislações que, consequentemente, contribui para a insciência sobre os aspectos vinculados à coleta dos dados e às ameaças à privacidade.

A representatividade da temática dá-se na coleta de dados de localização, principalmente pelos serviços LBS. Desta forma, as preocupações com os possíveis dados coletados pelas aplicações se caracterizam em dados que representam maior probabilidade de identificação do indivíduo, tal como, dados de localização, conforme foi revelado na revisão sistemática de literatura. No entanto, a coleta de dados, em outros contextos, também resulta em violações de privacidade e carecem de estudos e pesquisas.

A criptografia surge nos trabalhos combinada com técnicas de mascaramento, e é recorrente em vários trabalhos como medida para anonimizar dados, destaque também para as técnicas de *spatial cloaking*, supressão e generalização. Essas técnicas são combinadas com modelos de proteção de dados, destacando o modelo k-anonimato, que é referência quando se trata de anonimização de dados.

Interessante ressaltar a ciência da computação, telecomunicações e a engenharia, áreas de pesquisas nas quais a maioria dos trabalhos estão vinculados, situação que indica oportunidade para outras áreas pesquisarem nesse contexto, visto que, a privacidade está envolvida em vários domínios.

Essa revisão sistemática de literatura cumpre seu objetivo de evidenciar lacunas em pesquisas e de tirar conclusões gerais sobre algum fenômeno, que neste caso compreende a questão da anonimização de dados na fase de coleta.

Face ao exposto, observou-se que existe "***uma carência de pesquisas sobre proteção de dados pessoais na fase de coleta de dados",*** e esse elemento pode contribuir para o cenário que tende a levar a insciência do usuário, quando alvo de fases de coleta de dados.

Embora existam vários modelos e técnicas voltadas para a proteção de dados, as questões de privacidade devem estar amparadas pelo ordenamento jurídico. No próximo capítulo, são explanadas as principais legislações que abarcam questões de proteção de dados pessoais, buscando evidências para o amparo à privacidade do indivíduo especificamente na fase de coleta de dados.

5 PROTEÇÃO DE DADOS PESSOAIS: DOS PRINCÍPIOS ÀS LEGISLAÇÕES

> *Precisamos conversar sobre a vida do século XXI no ambiente digital, estão chegando os robôs e a Internet das coisas, existe a questão da privacidade, mas as consequências serão mais profundas; [...] é melhor começarmos a discutir isso agora, antes que todos os abusos e problemas éticos apareçam juntos. [...] Há uma esquizofrenia entre o mundo real e o digital, com coisas que são proibidas numa esfera e permitidas na outra (CAPURRO, 2014).*

A evolução das tecnologias da informação implica, cada vez mais, nas atividades que comprometem a privacidade do sujeito, que vão desde a expressiva quantidade de dados pessoais que são coletados diariamente por vários aparatos tecnológicos, até inovações, como as plataformas de compartilhamento e reuso de dados, destacando-se o banco de dados *Brazilian Initiative On Precision Medicine* (BIPMed) [60], o primeiro da América Latina a compartilhar dados genômicos e fenotípicos. Nesse cenário, a existência de uma regulamentação jurídica que seja facilitadora para vencer os desafios impostos pelos avanços tecnológicos vinculados à proteção de dados pessoais é imprescindível na sociedade hodierna.

No entanto, já houve momentos que a corrente doutrinária acreditava que não existia a necessidade de novas legislações para amparar o direito à privacidade no contexto das tecnologias da informação, conforme cita Pereira (2003, p. 148).

> [...] para uma parte da doutrina jurídica, não há necessidade de criação de um novo direito para a proteção da intimidade e, em especial, para a proteção dos dados pessoais, ante o uso das novas tecnologias, tendo em vista que o bem jurídico protegido segue o mesmo, qual seja, a intimidade.

Segundo o Comitê Gestor da Internet no Brasil (CGI) (2009), há casos em que a legislação não mantém o ritmo das aplicações oferecidas pelas tecnologias da informação e pela Internet, e nem sempre os *frameworks* abordam a capacidade de vigilância que as tecnologias modernas podem permitir. Ainda, em relação aos metadados, Kurbalija (2016) afirma que muitos países não possuem legislações que amparam a coleta, a divulgação e o uso desses dados, visto que deveriam existir medidas para a proteção da privacidade iguais as aplicadas ao acesso e ao conteúdo das comunicações de um indivíduo.

[60] Disponível em: <http://bipmed.iqm.unicamp.br/genes> e <http://bipmed.org/the-project>

> A Internet não exige apenas novas soluções jurídicas para os novos problemas; ela também afeta a maneira como os problemas e as soluções jurídicas devem ser analisados. Ao romper com os paradigmas jurídicos tradicionais e desafiar os mecanismos convencionais de tutela, a Rede representa um dos principais objetos de estudo dos doutrinadores preocupados com essa nova realidade social (LEONARDI, 2011, p. 39).

Para Solove (2008), há uma obscuridade sobre a privacidade quando as pessoas afirmam que a privacidade deve estar protegida, impactando na elaboração de políticas e na resolução de casos em que a privacidade foi invadida, visto que legisladores e juízes não conseguem estimar os danos das violações de privacidade. Para Solove (2006, p. 3), "[...] as novas leis surgem em resposta a mudanças tecnológicas que aumentam a coleta, disseminação e uso de informações pessoais".

Os direitos de privacidade necessitam de leis e indivíduos que estejam dispostos a ir aos tribunais em busca dos seus direitos de proteção de dados pessoais e ter atitudes contra os ataques e ameaças à privacidade. No entanto, o que se observa é que poucos indivíduos estão dispostos a fazer isso, resultando em direitos de privacidade sólidos em teoria, mas carentes na prática. Se a execução dos mecanismos para proteger a privacidade fosse simplificada, os indivíduos teriam maior consciência para controlar e proteger seus dados (MAYER-SCHÖNBERGER, 2011).

Garcia-Rivadulla (2016) atribui o motivo das leis não conseguirem acompanhar os últimos desenvolvimentos das tecnologias pelos seguintes fatores: a velocidade com o qual os dados estão sendo coletados; o avanço das análises de dados; e o modo como às tecnologias perpassam as fronteiras dos países, esquivando-se das regulamentações impostas pelas nações. Desta forma, a privacidade dependerá fortemente da capacidade de assegurar que os direitos dos indivíduos sejam respeitados.

Com o objetivo de orientar as decisões em relação à governança e uso da Internet no Brasil, a CGI determina no seu princípio – Liberdade, privacidade e direito humanos que: "[...] o uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática" (COMITÊ GESTOR DA INTERNET NO BRASIL, 2009).

Nas próximas seções, são descritos o ordenamento jurídico internacional, com destaque para o cenário nacional, buscando evidenciar como a legislação tem amparado às questões de proteção de dados pessoais, especificamente em relação à coleta de dados.

5.1 Cenário internacional de proteção de dados pessoais

O ordenamento jurídico que abarca questões de privacidade em diversos países apresenta variações em relação à terminologia utilizada para expressar o direito à privacidade. Nos Estados Unidos, o direito à privacidade emerge com a expressão "*right to privacy*" e "*right to be let alone*". Na França, encontram-se a expressão "*droit a la vie privée*" e "*droit a la intimité*". Na Itália, os termos utilizados são "*diritto alla riservatezza*", "*diritto alla segretezza*" e "*diritto alla rispetto della vita privatta*". A expressão "*derecho a la intimidad*" é usual na Espanha. Na Alemanha, é frequente o uso do termo *Recht auf informatiolelle Sebstbestimmung* (CARVALHO, 2003).

A proteção do direito à privacidade emerge no cenário internacional em 1948 mediante a Assembleia Geral das Nações Unidas que adotou e proclamou no dia 10 de dezembro de 1948 a Declaração Universal dos Direitos Humanos. Nessa Declaração ficou determinado em seu Art. 12 que "Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques" [61] (UNITED NATIONS, 1948, tradução nossa).

Posteriormente, em 1950 a Convenção Europeia para a proteção dos Direitos do Homem e das liberdades fundamentais convencionou no Art. 8º nº 1 sobre o Direito ao respeito à vida privada e familiar, que "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência" [62] (EUROPEAN COURT OF HUMAN RIGHTS, 2018?, p. 10, tradução nossa). Essa convenção foi baseada nos princípios da Declaração Universal dos Direitos Humanos.

Os direitos a privacidade também são determinados no Art. 17 do Pacto Internacional de Direitos Políticos, assinado em 16 de dezembro de 1966 e vigorado em 23 de março de 1976. Nesse artigo ficou regulamentado que "Ninguém poderá ser sujeito de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação", e que "Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas" [63] (UNITED NATIONS, 1966, tradução nossa).

---

[61] *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

[62] *Everyone has the right to respect for his private and family life, his home and his correspondence.*

[63] *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Em 1968, emerge a Recomendação nº 509 da 19ª Sessão Ordinária da Assembleia Consultiva do Conselho da Europa, que disserta sobre os perigos aos direitos dos indivíduos decorrentes ao desenvolvimento científico e tecnológico, que vão desde escutas telefónicas até o uso ilegítimo de pesquisas estatísticas. Essa recomendação foi devido à maioria dos Estados membros não oferecerem proteção adequada contra as ameaças à privacidade, necessitando de estudo detalhado dos problemas jurídicos decorrentes das violações da privacidade por dispositivos modernos (COUNCIL OF EUROPE, 1968).

Em 1969, na Conferência Especializada Interamericana sobre Direitos Humanos em San José, Costa Rica, estabeleceu a Convenção Americana sobre Direitos Humanos[64], a qual determinou no Art. 11, que discorre sobre Proteção da honra e da dignidade que "Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação" (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 2018).

Wacks (2015) ressalta que o alvorecer da tecnologia da informação, por volta de 1960, implicou em ameaças percebidas pela coleta, armazenamento e uso descontrolado de dados pessoais, o que fez vários países buscar regulamentações para essas atividades potencialmente intrusivas. A primeira lei de proteção de dados pessoais no mundo foi promulgada no estado alemão de Hesse[65], em 1970. Posteriormente, surgiu a legislação nacional da Suécia (1973), Estados Unidos (1974), Alemanha (1977) e da França (1978).

Em 1973, o comitê consultivo do governo dos Estados Unidos propôs um conjunto de princípios para proteção de dados pessoais, a denominada *Fair Information Practice Principles* (FIPPs). Esse foi o primeiro documento dos Estados Unidos que deu suporte às leis e à criação de *frameworks* de diversos países, tais como: *Privacy Act* dos Estados Unidos; Princípios de Privacidade da *Organization for Economic Co-operation and Development* (OECD); *Personal Information Protection and Electronic Documents Act* (PIPEDA) do Canadá; e APEC (*Asian Pacific Economic Cooperation*) *Privacy Framework* (GELLMAN, 2017).

As FIPPs são fruto do estudo ao longo dos anos de várias agências governamentais dos Estados Unidos, Canadá e Europa para investigar como entidades coletam e usam informações pessoais, denominadas de "Práticas de informação", e as salvaguardas para assegurar que essas práticas sejam justas e garantam privacidade. O resultado foi uma série de relatórios e diretrizes que representam princípios amplamente aceitos em relação às práticas justas de informação.

[64] Também conhecida como Pacto de San José da Costa Rica

[65] A lei do estado alemão Hesse, de 1970, limitava-se a regulamentar o tratamento autorizado dos dados pessoais (BENNETT, 1992, p. 77).

São comuns nesses documentos cinco princípios fundamentais para proteção da privacidade: Aviso/Consciência; Escolha/Consentimento; Acesso/Participação; Integridade/Segurança e; Execução/Reparação (FEDERAL TRADE COMMISSION, 1998b).

- ✓ **Princípio 1 – Aviso e Consciência**: Os indivíduos devem ser avisados sobre as atividades realizadas com os dados antes de eles serem coletados. É fundamental o indivíduo ter consciência antes da divulgação de dados pessoais, pois, os outros princípios só são válidos quando o indivíduo possui conhecimento das políticas e de seus direitos sobre privacidade. Assim, é preciso identificar as seguintes questões:
  a) Quem é a organização que coleta os dados;
  b) Qual será o uso dos dados pelas organizações;
  c) Para quem os dados serão enviados;
  d) Natureza dos dados coletados e o como serão coletados;
  e) Verificar se a permissão para a coleta é voluntária ou exigida; e, quando recusada, quais são as consequências para o titular dos dados;
  f) Quais são as medidas adotadas pelo detentor de dados para garantir confidencialidade, integridade e qualidade dos dados.
- ✓ **Princípio 2 - Escolha e Consentimento:** A escolha representa prover ao indivíduo opções quanto à forma como seus dados pessoais coletados podem ser usados, referindo-se também ao uso secundário dos dados. Os regimes de escolha e consentimento utilizados tem sido: *opt-in* ou *opt-out.* O regime *opt-in* requer que o usuário confirme a permissão da coleta e/ou uso dos dados, enquanto que o regime *opt-out* requer afirmações para impedir a coleta ou uso desses dados.
- ✓ **Princípio 3 - Acesso e Participação:** refere-se à capacidade do indivíduo referenciado no conjunto de dados em acessar seus dados e contestar questões de qualidade dos dados, tais como a precisão e a integridade.
- ✓ **Princípio 4 - Precisos e Seguros:** Para garantir a integridade dos dados, detentores devem realizar as seguintes medidas: apenas o uso de fontes confiáveis; destruir dados que não serão mais utilizados ou realizar anonimização de dados. Em relação à segurança, deve haver medidas e técnicas para proteger-se contra a perda, a exclusão, a divulgação e acesso não autorizado dos dados. As medidas de gestão dos dados nas questões de segurança incluem limitação no acesso, uso de criptografia, limites de acesso por meio de senhas e armazenamento de dados em servidor seguros.
- ✓ **Princípio 5 - Execução e Recurso:** Deve haver mecanismo de execução e de reparação para que os princípios sejam eficazes e garantam o seu cumprimento.

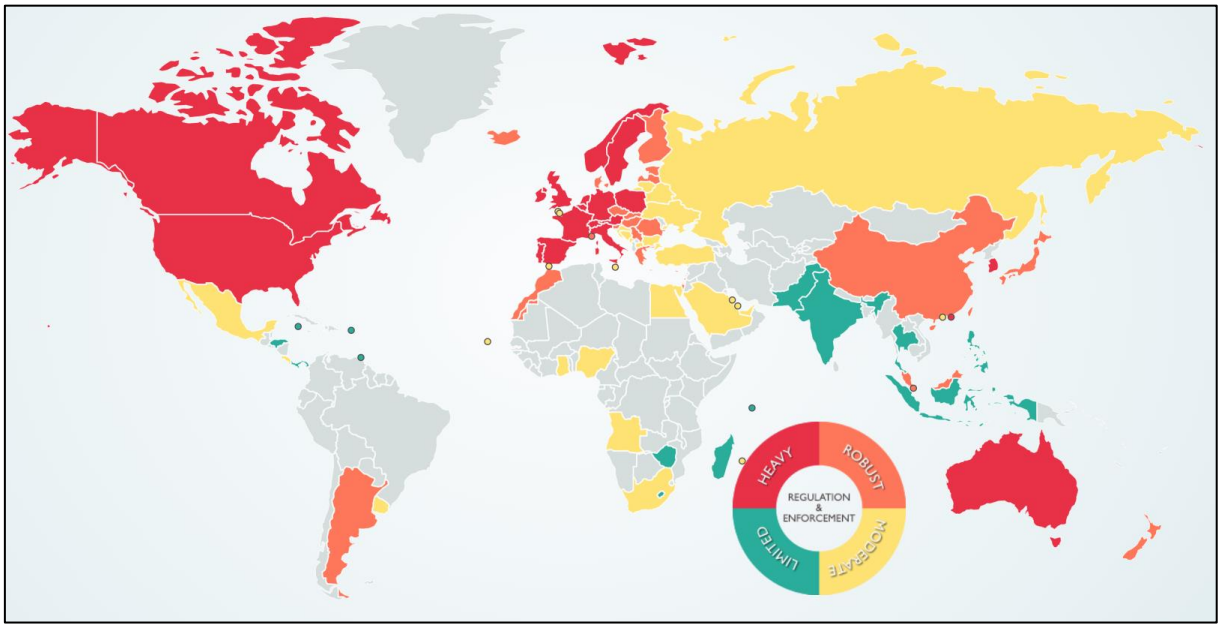
A OECD, desde meados da década de 1970, tem se envolvido em questões para garantir o respeito à privacidade de indivíduos, e para isso apresenta um *framework* de diretrizes sobre privacidade e fluxos transfronteiriços de dados pessoais, denominado de Princípios Básicos de Aplicação Nacional, que estabelece a seguintes diretrizes (ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2017):

- ✓ **Princípios de limitação de coleta:** as organizações e detentores de dados devem considerar limites para coleta de dados pessoais, e quando coletados devem ser obtidos por meios legais e justos. Quando for o caso, o titular deve ter consciência e disponibilizar o consentimento sobre a coleta;
- ✓ **Princípio da Qualidade**: Os dados pessoais devem ser precisos, completos e atualizados;
- ✓ **Princípio da especificação do objetivo**: Os motivos pelos quais os dados pessoais são coletados devem ser especificados no momento coleta de dados, e seu uso de acordo com o propósito especificado;
- ✓ **Princípio da limitação de uso:** Os dados pessoais não devem ser divulgados ou utilizados de forma diferente do motivo especificado, de acordo com o princípio anterior, exceto:
  a) Se o titular ou referenciado nos dados der o consentimento;
  b) Se solicitado por autoridades jurídicas;
- ✓ **Princípio da salvaguarda de segurança:** Os dados pessoais devem ser protegidos por garantias de segurança, tais como, contra riscos de perda, acesso e divulgação não autorizada, destruição, uso ou modificação;
- ✓ **Princípio de abertura:** Deve haver regras para disponibilizar informações e os mecanismos devem ser facilmente acessíveis para estabelecer a natureza dos dados pessoais e os principais fins de seu uso, bem como a identidade e a residência atual do detentor de dados;
- ✓ **Princípio da participação individual:** Os indivíduos devem ter o direito de:
  a) Obter de um detentor de dados a confirmação;
  b) Receber comunicação em relação aos dados:
     - Dentro de um prazo razoável;
     - A uma taxa, quando houver, e que essa, não seja excessiva;
     - De forma razoável, e que seja facilmente inteligível para eles.
  c) Indicar as razões se um pedido realizado nos parágrafos (a) e (b) for negado;
  d) Contestar dados relacionados a eles, possibilitando a exclusão e a alteração.

- ✓ **Princípio da responsabilidade:** um detentor de dados deve ser responsável pelo cumprimento das medidas que concretizam os princípios acima mencionados.

Para amparar às questões vinculadas a privacidade do indivíduo quanto à proteção de seus dados pessoais, o estabelecimento de leis se torna extremamente necessário. A Figura 29 ilustra o panorama dos países que possuem, em seu ordenamento jurídico, regulamentações e leis que buscam atender questões relacionadas à privacidade, especificamente vinculadas à proteção de dados pessoais.

Figura 29 - Panorama mundial em relação a leis específicas para proteção de dados pessoais



Fonte: DLA Piper (2017)

Na Figura 29, as cores diferenciadas em cada país representam a aderência dos países à regulação e à execução de leis e decretos no âmbito da proteção de dados pessoais. Observa-se que os países Europeus (Alemanha, Áustria, Bélgica, Espanha, França, Holanda, Irlanda, Itália, Noruega, Polônia, Portugal, Reino Unido, Suécia e Suíça), os Estados Unidos, o Canadá, a Austrália, Hong Kong e a Coreia do Sul seguem bem determinados nas questões de privacidade, devido à presença de legislações específicas para proteção de dados. O Brasil apresenta-se na Figura 29 em uma posição limitada no tocante a regulação de leis ao amparo à proteção de dados pessoais, fator que pode ser atribuído à ausência de uma legislação específica para esse domínio.

A fim de determinar diretrizes para as mais diversas situações que causam ameaças à proteção de dados pessoais, é necessária que as questões de privacidade sejam amparadas por

uma legislação específica. Indubitavelmente, as tecnologias da informação têm sido elemento determinante nas mudanças de leis em inúmeros países, causando novas nuances na legislação ao abordar aspectos derivados do uso constantes dos aparatos tecnológicos pelos indivíduos, que cada vez mais promovem uma progressiva coleta de dados.

Nos próximos itens, são mencionadas legislações internacionais e nacionais, a fim de identificar como leis e regulamentos versam sobre questões de privacidade do sujeito que tem seus dados envolvidos nas diversas atividades que coletam dados.

5.2 Leis de privacidade internacionais

Para a identificação das principais legislações internacionais, adotou-se, neste trabalho, apenas os países que estão representados pela DLA Piper (2017) na categoria "fortes" em questões de privacidade, tais como a Austrália, Canadá, Estados Unidos, determinados países da Europa, Hong Kong e Coreia do Sul (Figura 29).

5.2.1 Austrália

A proteção de dados pessoais na Austrália é amparada por uma combinação de legislações federais e estaduais, tais como: Lei de Telecomunicações de 1997; Lei Nacional de Saúde de 1953; Lei de Registros de Saúde e informações sobre privacidade de 2002; e a Lei de Vigilância no trabalho de 2005 (JONES, 2018). Nesta pesquisa, apresentam-se, especificamente, a *Privacy Act* 1998 e os Princípios de Privacidade da Austrália.

A Lei Federal de Privacidade (*Privacy Act* 1988) e os Princípios de Privacidade da Austrália (*Australian Privacy Principles* - APPs) se aplicam às entidades do setor privado com faturamento anual de, pelo menos, 3 milhões de dólares e a todas as agências governamentais da *Commonwealth Government* e do *Australian Capital Territory Government.* A *Privacy Act* 1988 é o amparo jurídico para a coleta de dados vinculados com *cookies*, dados de tráfego ou qualquer tecnologia semelhante (JONES, 2018).

5.2.1.1 *Privacy Act* 1988

A *Privacy Act* 1988 regula a forma como as informações pessoais são tratadas e conceitua informação pessoal como: "[...] informação ou opinião que é razoavelmente identificável, seja a informação ou opinião verdadeira ou não, e seja armazenada em forma material ou não, sobre um indivíduo identificado ou um indivíduo que seja razoavelmente

identificável” [66] (AUSTRÁLIA, 2018, tradução nossa). Informações identificáveis sobre um indivíduo são: nome ou apelido; data de nascimento; sexo; endereço atual ou último endereço conhecido; nome do empregador atual ou último conhecido do indivíduo; número da carteira de motorista. Classifica-se como informação pessoal: informações de saúde sobre um indivíduo; informações genéticas; informações biométricas e modelos biométricos (AUSTRÁLIA, 2018).

A *Privacy Act* 1988 inclui 13 Princípios Australianos de Privacidade que descrevem como organizações privadas, organizações sem fins lucrativos, agências governamental da Austrália e da ilha de Norfolk, devem tratar, usar e gerenciar dados pessoais, esses princípios estão contidos na *Privacy Act* de 1988 (AUSTRÁLIA, 2018). A *Privacy Act* 1988 apresenta os seguintes princípios (AUSTRÁLIA, 2018):

- ✓ Proporcionar aos indivíduos a proteção da privacidade;
- ✓ Reconhecer que a proteção da privacidade deve ser equilibrada com as necessidades das organizações nos exercícios de suas funções ou atividades;
- ✓ Fornecer base para uma regulamentação nacionalmente consistente no âmbito da proteção de dados pessoais;
- ✓ Propiciar o gerenciamento responsável e transparente das informações pessoais por entidades;
- ✓ Garantir um sistema eficiente de relatórios de crédito, assegurando simultaneamente que a privacidade dos indivíduos seja respeitada;
- ✓ Facilitar o livre fluxo de informações por meio das fronteiras nacionais, de forma a garantir a privacidade do titular dos dados;
- ✓ Fornecer meios para que os indivíduos questionem as interferências em relação às ameaças à privacidade;
- ✓ Garantir a obrigação internacional da Austrália em relação à privacidade.

O Quadro 11 relata os princípios da *Privacy Act* 1988. A primeira coluna indica as partes (descreve as regras), e a segunda coluna determina os princípios para a proteção de dados pessoais referentes a cada parte.

[66] *Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.*

Quadro 11 - Síntese dos Princípios Australianos de Privacidade

Partes	Princípios
Parte 1: Estabelece princípios que garantem que as entidades da APP gerem informações pessoais de forma aberta e transparente.	Gerenciamento aberto e transparente informações pessoais.
	Anonimato e pseudoanonimato.
Parte 2: Estabelece princípios que tratam da coleta de informações pessoais, incluindo informações pessoais não solicitadas.	Coleta de informações pessoais solicitadas.
	Lidar com informações pessoais não solicitadas.
	Notificação da coleta de informação pessoal.
Parte 3: Estabelece princípios sobre como as entidades da APP lidam com informações pessoais e identificadores relacionados ao governo. Esta parte incluir princípios sobre o uso e divulgação de informações e esses identificadores.	Uso ou divulgação de informação de informações pessoais.
	Marketing direto.
	Divulgação de informações pessoais que ultrapassam os limites da fronteira do país.
	Adoção, uso ou divulgação de identificadores relacionados ao governo.
Parte 4: Estabelece princípios sobre integridade das informações pessoais.	Qualidade da informação pessoal.
	Segurança de informações pessoais.
Parte 5: Estabelece princípios que lidam com pedidos de acesso e correção de informações pessoais.	Acesso a informações pessoais.
	Correção de informações pessoais.

Fonte: Baseado em Austrália (2018).

A Austrália não possui leis ou regulamentos especificamente relacionados às questões de privacidade *online*, tais como coleta de dados de localização, dados de tráfego ou uso de *cookies*. Caso tenha a coleta de dados pessoais por meio de *cookies* ou tecnologias semelhantes, incluindo dados coletados por aplicativos, devem ser cumpridas as determinações da *Privacy Act* em relação à coleta, uso, divulgação e armazenamento de informações pessoais (JONES, 2018).

5.2.2 Canadá

A proteção de dados pessoais nos setores privados, públicos e da saúde são regidos por 28 estatutos federais, provinciais e territoriais de privacidade. Embora cada um apresente seus objetivos e alcance diferenciados, todos estabelecem um regime abrangente para coleta, uso e divulgação de dados pessoais (FRIEDMAN; HUNTER, 2017).

A Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos (*Personal Information Protection and Electronic Documents Act* – PIPEDA) e a Lei de Privacidade (*Privacy Act*) são duas leis federais do Canadá que garantem as questões relacionadas à coleta, armazenamento e tratamento de dados pessoais (CANADÁ, 2018).

Algumas províncias possuem legislação de privacidade similar à PIPEDA para o setor privado. As cidades de Alberta, British Columbia e Québec têm legislações consideradas

similares e se aplicam às empresas do setor privado que coletam, usam e divulgam dados pessoais enquanto realizam negócios dentro dessas províncias (CANADÁ, 2018).

5.2.2.1 Lei de Privacidade (*Privacy Act*)

Essa lei tem o objetivo de estender as leis atuais do Canadá sobre o armazenamento de informações pessoais por instituição governamental e de proporcionar aos indivíduos o direito de acesso a essas informações (CANADÁ, 1985). A lei determina questões sobre: coleta, armazenamento e descarte de informações pessoais; proteção da informação pessoal; bancos de informação pessoal; índices de informação pessoal e direito ao acesso. Além disso, institui o *Office of the Privacy Commissioner* como órgão responsável em garantir o cumprimento das normas e dirimir conflitos (CANADÁ, 1985).

A *Privacy Act* aplica-se somente às instituições do governo federal listadas na *Privacy Act Schedule of Institutions* e ampara questões vinculadas as informações pessoais que o governo federal cobra, usa e divulga, seja sobre indivíduos ou funcionários (CANADÁ, 2018).

5.2.2.2 Personal Information Protection and Electronic Documents Act (PIPEDA)

A PIPEDA é uma lei federal do Canadá que estabelece regras para a coleta, uso e divulgação de informações pessoais pelo setor privado quando envolvidos em atividades comerciais, incluindo o apoio ao comércio eletrônico. Essa lei foi sancionada em 2000 e alterada, pela última vez, em fevereiro de 2017 (CANADÁ, 2018).

No anexo 1 da PIPEDA, são determinados os princípios para proteção de dados pessoais destinados às organizações que estão sob essa lei. Os dez princípios são sintetizados a seguir (CANADÁ, 2000):

I. **Responsabilidade**: As organizações são responsáveis pelas informações pessoais que estão sob seu controle e devem designar um encarregado para adequar as organizações a esses princípios;
II. **Identificação dos objetivos da coleta da informação**: o motivo da coleta das informações pessoais deve ser identificado antes da informação ser coletada;
III. **Consentimento**: todo indivíduo deve ter o conhecimento e dar consentimento para a realização da coleta, uso ou divulgação de informações pessoais, exceto quando não for apropriado;
IV. **Limitação da Coleta:** A coleta de informações pessoais deve ser limitada ao propósito que foi definido pela organização, sendo realizada de modo justo e legal;

V. **Limitação do uso, divulgação e retenção**: Deve haver limite na coleta e compartilhamento da informação, estando de acordo com os motivos que foram estipulados no momento da coleta, salvo com o consentimento do titular de dados ou conforme exigências regulatórias. A informação pessoal só deve ser armazenada enquanto for necessária para o cumprimento dos propósitos pelo qual foi coletada;
VI. **Precisão:** as informações pessoais devem ser precisas, completas e atualizadas, a fim de atingir os objetivos;
VII. **Salvaguardas:** As informações pessoais devem ser protegidas por medidas de segurança de acordo com o grau de sensibilidade que possui;
VIII. **Transparência:** Organizações devem disponibilizar prontamente para os indivíduos informações sobre suas políticas e práticas relacionadas à gestão de informações pessoais;
IX. **Acesso à informação pessoal:** O titular dos dados deve ser informado sobre a existência, o uso e a divulgação de suas informações pessoais, podendo contestar a exatidão e a completude da informação e alterá-la conforme apropriado;
X. **Questionamento do cumprimento da lei**: O indivíduo tem o direito de questionar sob o descumprimento dos princípios determinados na lei ao responsável pela conformidade dos princípios.

Em relação à privacidade *online*, os dados armazenados por meio de *cookies* são consideradas dados pessoais, e, portanto, sujeito as determinações da PIPEDA. Os dados de localização também são considerados dados pessoais, e como tal, qualquer atividade de coleta, uso ou divulgação de dados de localização, requer, aviso e consentimento prévio do titular dos dados (FRIEDMAN; HUNTER, 2017).

5.2.3 Coreia do Sul

As questões de proteção de dados pessoais são determinadas pela Lei de Proteção de Informações Pessoais - *Personal Information Protection Act* (PIPA), que foi promulgada e entrou em vigor em 30 de setembro de 2011. A PIPA determina os seguintes objetivos:

> Promover o tratamento das informações pessoais com a finalidade de reforçar o direito e o interesse dos cidadãos, concretizando a dignidade e o valor dos indivíduos, a fim de proteger sua privacidade em relação à coleta não

> autorizada, vazamento, abuso e uso indevido de informações pessoais[67] (COREIA DO SUL, 2011, tradução nossa).

Na PIPA o termo processamento se refere ao conjunto de atividades com dados pessoais, tais como coleta de dados, geração, registro, armazenamento, alteração, recuperação, divulgação, no entanto, existe menção a coleta de dados no decorrer da lei (COREIA DO SUL, 2011).

A Coreia do Sul também possui legislações específicas para questões de privacidade vinculadas às tecnologias da informação, como a *Act on Promotion of Information and Communication Network Utilization* (*IT Network Act)* (LEE, 2017).

A *Act on Promotion of Information and Communication Network Utilization and Information Protection* tem finalidade de "promover o uso de informações e redes de comunicação, protegendo as informações do usuário quando estiverem utilizando serviços de informação e comunicação [...]" [68] (COREIA DO SUL, 2001). Essa lei apresenta um capítulo específico sobre proteção de informação pessoal, no qual as questões de coleta de informações pessoais são regulamentadas no Art. 23 da seção 1 – denominada de Coleta de Informações Pessoais. Nessa seção fica determinado que o usuário deve ser notificado sobre a coleta de dados e ter a oportunidade de dar seu consentimento para essa atividade. Os provedores de serviços são obrigados a informar o objetivo da coleta e uso de informações pessoais e, ainda, fica regulamentado no Art. 23 que esses provedores devem coletar o mínimo de informações pessoais, apenas o necessário para a realização do serviço (COREIA DO SUL, 2001).

Outras leis amparam as questões de coleta de dados na Coreia do Sul, tais como a Lei de Uso e Proteção de Informações de Crédito - *Use and Protection of Credit Information Act* (UPCIA) que regula o uso e divulgação de dados pessoais de crédito e; a Lei sobre Transações Financeiras de Nome Real e Garantia de Sigilo - *Act on Real Name Financial Transactions and Garante of Secrecy* (ARNFTGS) (LEE, 2017).

O uso de *cookies*, log, informações de IP são regulamentados pela *IT Network Act*, que os consideram dados pessoais, pois quando combinados com outros dados podem permitir a identificação de um indivíduo, para tanto, determina o consentimento do titular de dados

---

[67] *The purpose of this Act is to provide for the processing of the personal information for the purpose of enhancing the right and interest of citizens, and further realizing the dignity and value of the individuals by protecting their privacy from the unauthorized collection, leak, abuse or misuse of personal information.*

[68] *This Act's purpose is to promote the use of information and communications networks, to protect the user's personal information when they are in use of information and communications services.*

mediante *opt-out* e políticas de privacidade para informações sobre coleta de dados (LEE, 2017).

Os dados de localização são regidos pela *Law on the protection and use of location information* estabelecida em 27 de janeiro de 2005, cujo propósito é "proteger a privacidade contra vazamento, abuso e uso indevido de informações de localização e promover um ambiente para uso de informações de localização [...]" [69] (COREIA DO SUL, 2005, tradução nossa). Essa lei determina o consentimento prévio do titular dos dados para coleta de dados de localização, salvo se tiver alguma situação de emergência (COREIA DO SUL, 2005). É determinado no Art. 18, que trata da coleta de dados de localização pessoal, que essa atividade deve coletar a menor quantidade possível de dados, apenas para atingir o objetivo da coleta.

Em relação os direitos dos titulares dos dados, a *Law on the protection and use of location information* determina no Art. 24 que o titular dos dados pode solicitar a qualquer momento a suspensão temporariamente da coleta, uso ou fornecimento de seus dados de localização (COREIA DO SUL, 2005).

5.2.4 Estados Unidos

Os Estados Unidos não possuem uma legislação única para proteção de dados pessoais, uma vez que, utilizam uma abordagem setorial que depende da combinação entre legislação, regulamentação e auto regulação. Possuem certa de 20 leis nacionais específicas de privacidade ou de segurança de dados, e centenas de leis entre seus 50 estados e territórios (HALPERT; KASHATUS; LUCENTE, 2017). A gênese das leis de privacidade nos Estados Unidos foi a *Fair Credit Reporting Act*, de 1970, e a *Privacy Act*, de 1974.

A *Fair Credit Reporting Act* tem o objetivo de garantir a privacidade de indivíduos que possuem informações em arquivos de relatórios de consumidor. Entre os direitos oferecidos nessa lei estão à garantia ao consumidor para obter informações que estão no seu arquivo, acessar às suas informações e o direito ao consentimento quando seus relatórios forem fornecidos a empregadores (ELECTRONIC PRIVACY INFORMATION CENTER, 2018a).

A *Privacy Act* 1974 se configurou como uma das mais influentes legislações no âmbito da proteção de dados pessoais. Essa lei emergiu devido às preocupações com o desenvolvimento de banco de dados informatizados e suas implicações nos direitos de privacidade, pois o avanço nas tecnologias tornou a combinação de dados mais rápida e fácil. Desta forma, a lei determina um conjunto de códigos para reagir à coleta, à manutenção, ao uso

[69] *The purpose of this law is to protect privacy against the leak, abuse and misuse of location information, promote a safe environment for using location information* [...].

e à disseminação de informações sobre indivíduos que estão armazenados nos arquivos de agências federais (ESTADOS UNIDOS, 2015; ELECTRONIC PRIVACY INFORMATION CENTER, 2018b).

A *Privacy Act* 1974 determina a proteção da privacidade mediante quatro direitos: (1) ordena que agências governamentais disponibilizem ao indivíduo informações armazenadas por ele; (2) exige que as agências, quando armazenam e manipulam dados pessoais, estejam alinhadas a certos princípios, denominados de "práticas justas de informação"; (3) determina restrições no âmbito do compartilhamento de dados de indivíduo com outras pessoas e agências; (4) permite que indivíduos processem o governo por não atenderem às disposições da lei (ELECTRONIC PRIVACY INFORMATION CENTER, 2018b).

Na *Privacy Act* 1974 a coleta de dados surge como o termo manter, que incluir manter, coletar, usar ou disseminar. Utiliza-se também do termo "registro" que significa qualquer item, coleta ou agrupamento de informação sobre um indivíduo (ESTADOS UNIDOS, 1974).

Cada uma das leis supracitadas são voltas para setores específicos, enquanto a *Fair Credit Reporting Act* tem a finalidade de proteção de dados no setor privado, a *Privacy Act* é voltada para o setor público. Essa situação caracteriza a legislação dos Estados Unidos como um conjunto de leis setoriais, buscando a atender objetivos específicos, não apresentando uma lei unificada para as questões de proteção de dados pessoais, destacando-se nesse cenário a FERPA (*Family Educational Rights and Privacy Act*) e HIPPA (*Health Insurance Portability and Accountabilit Act).*

5.2.4.1 FERPA

Essa lei tem o objetivo de proteger a privacidade dos registros escolares de alunos que estudam em escolas que recebem verbas do departamento de educação dos EUA. A FERPA estabelece, aos pais de alunos, direitos em relação às informações relacionadas à vivência de seus filhos na escola. O aluno, quando tiver 18 anos ou se frequenta um curso superior, passa a ter esse direito, se torna-se "estudantes elegíveis". Os pais ou estudantes elegíveis têm o direito de verificar e revisar informações escolares do aluno mantidos pela escola; e tem o direito de solicitar que a escola corrija os registros quando esses estiverem errados. Os pais ou alunos elegíveis devem dar consentimento por escrito para a escola para que essa disponibilize quaisquer informações do registro escolar de um aluno (ELECTRONIC CODE OF FEDERAL REGULATIONS, 2017).

De acordo com a FERPA às escolas podem divulgar esses registros, sem consentimento, nas seguintes condições (ELECTRONIC CODE OF FEDERAL REGULATIONS, 2017).

- ✓ Funcionários da escola com interesse especificamente educacional;
- ✓ Para outras escolas às quais um estudante está sendo transferido;
- ✓ Funcionários que foram determinados para fins de auditoria ou avaliação;
- ✓ Partes apropriadas que concedem ajuda financeira ao aluno;
- ✓ Entidades que realizam pesquisas para ou em nome da escola;
- ✓ Organizações de credenciamento;
- ✓ Cumprir uma ordem judicial;
- ✓ Funcionários que foram determinados em casos de emergência de saúde ou segurança;
- ✓ Autoridades estaduais e locais, de acordo com a legislação estatal específica.

Existem informações que podem ser divulgadas sem o consentimento do titular dos dados, essas são denominadas de informações de diretório[70], incluem: o nome do aluno, o endereço, a lista telefônica, o e-mail, a fotografia, a data e o local de nascimento, a principal área de estudo; o nível de ensino, o status de inscrição (exemplo: graduação, pós-graduação, a tempo integral ou parcial), a frequência, a participação em atividades e esportes oficialmente reconhecidos, o peso e altura dos membros das equipes atléticas, as honras e prêmios recebidos. As informações de diretório do aluno não incluem o número de segurança social e o número de identificação do estudante (ID) (ELECTRONIC CODE OF FEDERAL REGULATIONS, 2017).

Os pais e estudantes elegíveis devem receber informações sobre os direitos concedidos pela FERPA (ELECTRONIC CODE OF FEDERAL REGULATIONS, 2017).

5.2.4.2 HIPAA

Uma das mais importantes reformas na área da saúde é a HIPAA, uma lei aprovada pelo Congresso dos Estados Unidos e promulgada pelo presidente Bill Clinton, em 1996, que apresenta diretrizes para a privacidade e a proteção de dados de saúde.

A regra de privacidade da HIPAA exige garantias adequadas para proteger a privacidade das informações pessoais de saúde de indivíduos, estabelecendo limites e condições sobre uso e divulgações de dados que podem ser realizadas sem o consentimento do paciente. A regra também provê aos pacientes o direito sobre suas informações de saúde, incluindo direitos para examinar, obter cópia de seus registros de saúde e solicitar alterações em registros (HEALTH & HUMAN SERVICES, 2012). A HIPAA também abarca regulamentações para transações

[70] A informação do diretório significa informação contida em um registro educacional de um aluno que geralmente não seria considerado prejudicial ou uma invasão de privacidade caso seja divulgado (ELECTRONIC CODE OF FEDERAL REGULATIONS, 2017).

eletrônicas de dados para provedores, planos de saúde e empregados, incluindo a segurança e a privacidade desses dados (HEALTH & HUMAN SERVICES, 2012).

O Departamento de Saúde e Serviços Humanos (*Department of Health and Human Services* - DHHS) dos EUA desenvolve e publica as regras relativas à implementação da HIPAA e os padrões a serem utilizados. Dessa forma, todas as organizações de saúde que são impactadas pela HIPAA são obrigadas a cumprir os padrões (HEALTH & HUMAN SERVICES, 2012).

A HIPPA determina uma lista de 18 identificadores que devem ser removidos para evitar a reidentificação do indivíduo em um conjunto de dados: (1) nome; (2) todas as subdivisões geográficas menores que um Estado, incluindo o endereço, cidade, código postal (exceto os três dígitos iniciais); (3) os atributos de datas (exceto ano) quando relacionadas diretamente a um indivíduo, todas as idades com mais de 89 anos (4) Número de telefone; (5) número de fax; (6) e-mail; (7) número de segurança social; (8) número de registro médico; (9) número de beneficiário de planos de saúde; (10) número de conta; (11) número de licença; (12) identificadores de veículos; (13) identificadores do dispositivo e números de série; (14) URL; (15) IP; (16) Identificadores biométricos, incluindo impressões digitais e voz; (17) imagens fotográficas completas e imagens comparáveis; (18) Qualquer outro número, característica ou código de identificação exclusivo (HEALTH & HUMAN SERVICES, 2012).

Em relação à privacidade *online*, os Estados da Califórnia e Delaware obrigam que *sites* comerciais e aplicativos móveis disponibilizem políticas de privacidade para informar a respeito de atividades envolvidas com dados pessoais. Essa exigência vale para o uso de *cookies* ou mecanismos de rastreamento, visto que não existe uma lei federal específica que regule a coleta de dados por essa atividade. Entretanto, a *Children's Online Privacy Protection Act* (COPPA) regula dados que são coletados automaticamente (HALPERT; KASHATUS; LUCENTE, 2017).

A COPPA, estabelecida em 1998, exige no seu regulamento que o operador de *sites* ou qualquer serviço *online* que seja destinado para crianças e que realiza a coleta de dados, informe no próprio *site* os dados que serão coletados de crianças pelo detentor de dados, e como este utiliza essas informações e as suas práticas de divulgação, incluindo a descrição dos tipos específicos de informações pessoais coletadas. Nessa situação, o *site* deverá ter estratégias para obter consentimento dos pais para a coleta, uso ou divulgação de dados pessoais de crianças (FEDERAL TRADE COMMISSION, 1998a).

A *Federal Communications Commission* regulamenta a coleta e a divulgação de dados de localização por operadoras, sendo que serviços de localização que tenha alvo crianças

menores de 13 anos deve cumprir os regulamentos da COPPA, incluindo o consentimento dos pais. A Procuradoria Geral da República da Califórnia e a *Federal Trade Commission* (FTC) indicam a disponibilização de políticas de privacidade para conscientizar a respeito da coleta desse tipo de dado (HALPERT; KASHATUS; LUCENTE, 2017).

5.2.5 Europa

5.2.5.1 União Europeia: Diretiva 95/46/CE do Parlamento Europeu e o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho

Na União Europeia (UE), os direitos à proteção de dados pessoais eram assegurados pela Diretiva 95/46/CE de 24 de outubro de 1995, "relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre-circulação desses dados" (UNIÃO EUROPEIA, 1995, p. 32). Por essa diretiva abarcar todos os Estados-Membros, ela garante padronização em relação à proteção de dados.

A Diretiva 95/46/CE foi um marco histórico no âmbito de proteção de dados pessoais na Europa e se manteve em vigor praticamente por vinte anos, garantindo a proteção efetiva dos direitos e das liberdades dos indivíduos. No entanto, devido ao intenso uso das tecnologias, a Diretiva 95/46/CE não conseguia garantir aos problemas vinculados às ameaças de privacidade, não garantindo com eficiência a proteção de dados pessoais, nem mantendo a padronização exigida pela EU (EU GENERAL DATA PROTECTION REGULATION, 201-a).

A Diretiva 95/46/CE foi substituída pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, também denominado de *General Data Protection Regulation* (GDPR). Essa diretiva de proteção de dados entrou em vigor no dia 25 de maio de 2018 para todos os estados membros. A partir dessa data, as organizações que não estiverem em aderência com esse regulamento sofrerão sanções significativas (EU GENERAL DATA PROTECTION REGULATION, 201-a).

Regulamento (UE) 2016/679 foi desenvolvido para conformizar leis de privacidade de dados em toda a Europa, a fim de proteger a privacidade de dados e remodelar a forma como as organizações da UE abordam as questões de privacidade (EU GENERAL DATA PROTECTION REGULATION, 201-a). A finalidade do Regulamento (UE) 2016/679 é proteger todos os indivíduos da UE das violações de dados pessoais, considerando as ameaças à privacidade que emergiram com as tecnologias da informação (EU GENERAL DATA PROTECTION REGULATION, 201-a).

> Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudoanonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável [...] Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anônimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável, nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado [...] (UNIÃO EUROPEIA, 2016, p. 5).

Regulamento (UE) 2016/679 define conceitos essenciais em relação à proteção de dados pessoais, tais como: violação de dados pessoais; dados genéticos; dados biométricos; dados relativos à saúde e, dados pessoais, definido como:

> [...] qualquer informação relativa a uma pessoa singular identificada ou identificável ("titular de dados"); Uma pessoa singular identificável é aquela que pode ser identificada, diretamente ou indiretamente, em particular por referência a um identificador, como nome, um número de identificação, dados de localização, identificador on-line ou mais fatores específicos para a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural (UNIÃO EUROPEIA, 2016, p. 106).

O Quadro 12 explicita os princípios relativos ao tratamento de dados pessoais, presente no Art. 5 do Regulamento (UE) 2016/679. Nele, observa-se que a maioria dos princípios estão relacionados aos princípios determinados pela *Fair Information Practice Principles.*

Quadro 12 - Princípios relativos ao tratamento de dados pessoais do GDPR

Princípios relativos ao tratamento de dados pessoais	
Tratados de modo justo e transparente	Licitude do tratamento
Coletados para finalidades determinadas, explícita e leal.	Limitação da finalidade
Adequados, pertinentes e limitados ao mínimo necessário, relativo às finalidades para as quais são tratados.	Minimização de dados
Exatos e Atualizados sempre que necessário	Precisão
Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.	Preservação de dados
Tratados de forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizacionais adequadas.	Segurança de dados (Integridade e confidencialidade)
O responsável pelo tratamento é responsável pelo cumprimento das atividades e deve poder comprovar esse cumprimento	Responsabilidade

Fonte: Baseado em União Europeia (2016, p. 35-36)

O Regulamento (UE) 2016/679 aplica-se ao tratamento de dados pessoais das pessoas singulares, independentes da sua nacionalidade ou do seu local de residência. Os principais pontos abordados são (EU GENERAL DATA PROTECTION REGULATION, 201-b):

- ✓ O aumento do alcance territorial: A Diretiva se aplica a todas as empresas que processam dados pessoais de indivíduos que residem na UE, independentemente da localização da empresa;
- ✓ Emergem questões sobre *Privacy design*[71] e *Privacy default*[72]. Fica explícito no Art. 25 que o responsável deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, somente os dados pessoais necessários devem ser processados. Essa obrigação aplica-se à quantidade de dados pessoais coletados, à extensão do processamento, ao período de armazenamento e à sua acessibilidade;
- ✓ Penalidades: Organizações que violam Regulamento (UE) 2016/679 podem receber sanções até 4% do volume de negócios global anual ou 20 milhões de euros (o que for maior). Caracteriza-se, nesse contexto, como infração grave a falta de consentimento do cliente para processar dados ou violar os conceitos de *Privacy by design*;
- ✓ Consentimento: Os pedidos de consentimento devem ser disponibilizados de forma acessível e clara, não utilizando mais termos longos e ilegíveis que dificultam a compreensão pelo usuário;
- ✓ Avaliações de impacto sobre proteção de dados;
- ✓ Surge a figura do encarregado de proteção de dados;
- ✓ Em relação à segurança dos dados pessoais, fica explícito que o responsável e o encarregado devem implementar medidas técnicas e organizacionais adequadas para garantir o nível de segurança, incluindo: pseudoanonimização e criptografia de dados pessoais;
- ✓ Com a finalidade de demonstrar o cumprimento do Regulamento (UE) 2016/679, é determinado que os estados-membros, as autoridades de supervisão, o conselho e a comissão estabeleçam mecanismo de certificação de proteção de dados e selos, assim as organizações que estão em aderência com o regulamento serão certificadas;
- ✓ Merece destaque no regulamento as considerações em relação aos dados pessoais de crianças, que também estão amparados pela legislação.

> As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais.

[71] A privacidade por design exige inclusão de proteção de dados desde o início da concepção dos sistemas, tais como medidas de minimização dados e limite de acesso aos dados pessoais (EU GENERAL DATA PROTECTION REGULATION, 2017a).

[72] O controlador deve implementar medidas técnicas e organizacionais adequadas para garantir que somente os dados pessoais que são necessários para cada finalidade específica sejam processados (EU GENERAL DATA PROTECTION REGULATION, 2017a).

> Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como a recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança (UNIÃO EUROPEIA, 2016, p. 7).

Dentre os artigos que compõe o Regulamento (UE) 2016/679, os direitos do titular dos dados são determinados no Capítulo III desse regulamento, explicitados no Quadro 13.

Quadro 13 - Direitos do titular dos dados

Seção	Artigos
Direito a Transparência	Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados.
Direito a informação e acesso aos dados	Informações sobre a coleta de dados pessoais junto ao titular.
	Informações sobre a coleta de dados pessoais quando não foram obtidos junto ao titular.
	Direito de acesso do titular dos dados
Direito a exclusão e alteração	Direito a alteração.
	Direito a exclusão dos dados (direito ao esquecimento).
	Direito à restrição de tratamento.
	Obrigação de notificação da alteração ou exclusão de dados pessoais ou restrição de tratamento.
	Direito de portabilidade dos dados (O GDPR introduz esse conceito), o sujeito recebe os dados pessoais relativos a ele e, têm o direito de transmitir esses para outro detentor.
Direito a oposição (discordância)	Direito de oposição.
	Direito a tomar decisões individuais automatizadas
Direito a limitação do tratamento	Limitações.

Fonte: Baseado em União Europeia (2016).

Assim, de acordo com Araújo (2017, p. 206), "[...] neste novo quadro jurídico da proteção de dados, os princípios e objetivos da Diretiva 95/46/CE são mantidos. O regulamento, contudo, pretende adaptá-los aos desafios apresentados pela rápida evolução tecnológica e globalização".

5.2.5.2 Diretiva 2002/58/EC do Parlamento Europeu e do Conselho de 12 de julho de 2002 (Diretiva e-*Privacy*)

Essa diretiva é relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas, também denominada de Diretiva de Privacidade e Comunicações Eletrônicas (Diretiva e-*Privacy*), que emerge devido à necessidade de regulamentos específicos no que se refere à proteção de dados pessoais do usuário (UNIÃO EUROPEIA, 2002).

A Diretiva de Privacidade considerou para suas diretrizes a Diretiva 95/46/CE do Parlamento Europeu; respeita os direitos fundamentais pelas determinações da Carta dos Direitos Fundamentais da União Europeia e pela Convenção Europeia para Proteção dos Direitos do Homem e das Liberdades Fundamentais, e as constituições dos Estados-Membros; e a Diretiva 97/66/CE do Parlamento Europeu e do Conselho relativa ao tratamento da privacidade no setor das telecomunicações (UNIÃO EUROPEIA, 2002).

Essa Diretiva foi alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de novembro de 2009 (UNIÃO EUROPEIA, 2009). A Diretiva 2009/136/CE também ficou conhecida como EU-*Cookies*.

Em relação aos dados de tráfego, esses devem ser apagados ou anonimizados quando não forem mais necessários para a transmissão de uma comunicação. Os dados de tráfego podem ser processados para fins de faturamento e pagamentos de contas de usuários. Para efeitos de comercialização de serviços de comunicação eletrônica ou prestação de serviços de valor agregado o processamento dependerá do consentimento do usuário, que poderá a qualquer momento retirar seu consentimento. Antes de o usuário conceder o consentimento, os prestadores de serviços informarão ao usuário os tipos de dados de tráfego que serão processados (UNIÃO EUROPEIA, 2009).

Quanto aos dados de localização, desde que não sejam dados de tráfego, esses somente poderão ser tratados se houver anonimização ou consentimento dos usuários durante o período de prestação de serviço. O usuário deverá ter informação sobre os dados de localização que serão tratados, os motivos e a duração do tratamento, e se os dados são transmitidos para terceiros, podendo o usuário retirar o seu consentimento para o processamento de dados de localização (UNIÃO EUROPEIA, 2009).

Na Diretiva 2009/136/CE emerge diretrizes para as questões de armazenamento ou acesso a informações no equipamento do usuário, enfatizando que essas informações podem ser utilizadas para vários fins, desde *cookies* até *softwares* espião ou vírus. Enfatiza que são necessárias informações claras e exaustivas para o usuário sobre essas questões, devendo proporcionar o direito de recusar essas atividades, e que a forma de consentimento seja a mais clara e simples possível (UNIÃO EUROPEIA, 2009).

O uso de *cookies* é mencionado na Diretiva 2009/136/CE, a qual abordou nas considerações, especificamente no item 25, que o uso de *cookies* deve ser permitido apenas se os detentores de dados disponibilizarem informações claras e precisas sobre os propósitos do uso de *cookies* ou dispositivos semelhantes, a fim de garantir que o usuário seja informado sobre essa atividade. O usuário deve ter a oportunidade de recusar ou consentir armazenamento

de um *cookie* em seu equipamento e, deve ter os métodos mais amigáveis para realizar essas atividades (UNIÃO EUROPEIA, 2009).

Embora a Diretiva 2009/136/CE do Parlamento Europeu e do Conselho seja adequada, ela não acompanhou plenamente a evolução das tecnologias e do mercado, o que resultou em uma proteção de dados pessoais insuficiente. O Parlamento Europeu e o Conselho da União Europeia consideram uma nova proposta que revoga a Diretiva 2009/136/CE, o Regulamento do Parlamento Europeu e do Conselho 2017/0003 (COD), que era para ser aplicável a partir de 25 de maio de 2018, acompanhando também o novo Regulamento (UE) 2016/679 (UNIÃO EUROPEIA, 2017). No entanto, o Regulamento do Parlamento Europeu e do Conselho 2017/0003 (COD) não foi finalizado para cumprir o prazo de 25 de maio de 2018. Dentre as considerações abarcadas, ressalta sobre a importância e impacto dos metadados de comunicação nas questões de privacidade.

> O conteúdo das comunicações eletrônicas pode revelar informações altamente sensíveis acerca das pessoas singulares envolvidas na comunicação, desde experiências e emoções pessoais a condições de saúde, preferências sexuais e opiniões políticas, cuja divulgação poderia resultar em danos pessoais e sociais, prejuízos econômicos ou constrangimento. De igual modo, os metadados derivados de comunicações eletrônicas podem também revelar informações muito sensíveis e pessoais. Estes metadados incluem os números ligados, os sítios web visitados, a localização geográfica, a hora, a data e duração da chamada, etc., permitindo tirar conclusões precisas relativas à vida privada das pessoas envolvidas na comunicação eletrônica, tais como as suas relações sociais, os seus hábitos e atividades da vida quotidiana, os seus interesses, gostos, etc. (UNIÃO EUROPEIA, 2017, p. 12-13).

Ainda, o Regulamento 2017/0003 (COD), os dados das comunicações eletrônicas devem ser tratados como dados confidenciais, sendo proibida qualquer interferência com a transmissão de dados de comunicações eletrônicas, sendo por intervenção humana ou por tratamento automatizado, sem que haja consentimento dos titulares. O presente regulamento deve exigir que os prestadores de serviços de comunicações eletrônicas obtenha o consentimento dos usuários para procederem ao tratamento dos metadados de comunicações eletrônicas (UNIÃO EUROPEIA, 2017).

O Regulamento 2017/0003 (COD), define dados de comunicação eletrônica como o “conteúdo das comunicações eletrônicas”; conteúdo das comunicações eletrônicas como “o conteúdo trocado através de serviços de comunicações eletrônicas, sob a forma de texto, voz, imagem e som”; e metadados de comunicações eletrônicas que inclui os “dados utilizados para detectar uma comunicação e identificar a sua fonte e destino, a localização do dispositivo no

contexto da comunicação e data, hora, duração e tipo de comunicação" (UNIÃO EUROPEIA, 2017, p. 28).

O Regulamento 2017/0003 (COD) abarca também sobre programas espiões, pixels espiões, identificadores ocultos que podem rastrear o equipamento do usuário, sem o seu conhecimento, a fim de aceder a informações, armazenar informações ocultas ou rastrear atividades. Essas atividades caracterizam-se como uma grave intrusão na privacidade de usuários, e só podem ser permitidas com o consentimento, para fins específicos e transparentes. Aborda também sobre uso de dados de IMEI e *Media Access Control* (MAC), esses tipos de dados quando utilizados para algumas funcionalidades não implicam em riscos de privacidade elevados, no entanto, outras atividades com esses dados únicos podem caracterizar quebras de privacidade, tal como rastreio de usuários por um determinado período e o conhecimento sobre seus atos (UNIÃO EUROPEIA, 2017).

Explanados os principais regulamentos da Europa que versam sobre proteção de dados pessoais, nos próximos tópicos são descritas as principais leis referentes à proteção de dados, de acordo com as delimitações determinadas na metodologia deste trabalho.

a) Alemanha

A Lei Federal de Proteção de Dados Pessoais (*Federal Data Protection Act of 30 June 2017*) é a principal determinação legal para proteção de dados na Alemanha que visa proteger dados pessoais do processamento e uso pelas autoridades federais e órgãos públicos. A Alemanha alterou sua lei de proteção de dados em junho de 2017, que alinha com os requisitos do Regulamento (UE) 2016/679, sendo o primeiro estado-membro da UE que realizou as adequações de acordo com o novo regulamento (LIBRARY OF CONGRESS, 2018).

A *Federal Data Protection Act* traz dentre suas seções: processamento de dados em órgãos públicos; videovigilância de espaços públicos; responsável pela proteção de dados em órgão públicos; processamento de categorias especiais de dados pessoais; transferência de dados por órgãos públicos; notificação quando são coletados dados do titular; direito ao esquecimento. Ressalta-se que devido à aderência ao Regulamento (UE) 2016/679, a *Federal Data Protection Act* determina o termo tratamento de dados para designar várias atividades, dentre elas a coleta, armazenamento, registro, utilização, divulgação, combinação, exclusão, consulta e alteração.

Em relação aos dados de localização e *cookies*, esses são considerados como dados pessoais, e só podem ser processados se forem necessários para a execução dos serviços solicitados pelo usuário, mediante informações prévias e consentimento do usuário (essas

determinações são baseadas na *German Telemedia Act* (TMG). O consentimento deve ser registrado corretamente, podendo o usuário ter acesso ao conteúdo. Os ambientes Web devem disponibilizar para o usuário um link para configurar o navegador em relação ao uso de *cookies* (GRENTZENBERG; MEENTS; POHLE, 2017).

b) Áustria

A *Federal Act concerning the Protection of Personal Data (DSG 2000)* implementou Regulamento (UE) 2016/679 em 25 de maio de 2018, apresenta na sua lei como direito fundamental ao indivíduo que:

> Toda pessoa terá o direito ao sigilo dos seus dados pessoais, especialmente no que diz respeito à sua vida familiar, na medida em que essa pessoa tem interesse que mereça proteção. Tal interesse é excluído se os dados não puderem estar sujeitos ao direito de sigilo devido à disponibilidade geral dos dados ou porque não podem ser vinculados ao titular dos dados[73] (ÁUSTRIA, 1999, p. 5, tradução nossa).

Define o termo tratamento como qualquer operação com dados pessoais, automatizados ou não, como coleta, armazenamento, registro, exclusão e divulgação. A *Federal Act concerning the Protection of Personal Data* aborda sobre processamento automatizado, incluindo a criação de perfis de indivíduos (ÁUSTRIA, 1999).

As atividades com dados de tráfego são regulamentadas pela *Austrian Telecommunications Act* (*Telekommunikationsgesetz* 2003, - TKG), na qual os dados de tráfego devem ser excluídos ou anonimizados pelos prestadores de serviços. Em relação aos dados de localização, esses só podem ser processados com o consentimento do usuário e devem ser anonimizados, podendo o usuário retirar o consentimento a qualquer momento e recusar temporariamente o processamento dos dados de localização em cada transmissão (ÁUSTRIA, 2003).

> Pessoas que não sejam usuário não poderão escutar, tocar, gravar, interceptar ou de outra forma monitorar comunicações e os dados de tráfego ou de localização, bem como transmitir informações sem o consentimento de todos os usuários envolvidos[74] (ÁUSTRIA, 2003, p.74).

---

[73] *Every person shall have the right to secrecy of the personal data concerning that person, especially with regard to the respect for his or her private and family life, insofar as that person has an interest which deserves such protection. Such an interest is precluded if data cannot be subject to the right to secrecy due to the data's general availability or because they cannot be traced back to the data subject.*

[74] *Persons other than a user shall not be permitted to listen, tap, record, intercept or otherwise monitor communications and the related traffic and location data as well as pass on related information without the consent of all users concerned.*

Em relação ao uso de *cookies*, as organizações devem proporcionar ao usuário ciência sobre o armazenamento ou processamento de seus dados pessoais quando envolvidas com essa atividade (FEHRINGER; PANIC, 2017).

Na *Austrian Telecommunications Act* o termo dados de tráfego é definido como "Quaisquer dados tratados para fins de transmissão de comunicação em rede de comunicações [...]" [75] (ÁUSTRIA, 2003, p. 73) e dados de conteúdo como "conteúdo das comunicações transmitidas" [76] (ÁUSTRIA, 2003, p. 73). Na lei é determinada que os dados de conteúdo, dados de tráfego e dados de localização estão sujeitos à confidencialidade das comunicações e só podem ser coletados para fins de prestação de serviços de comunicações (ÁUSTRIA, 2003).

c) Bélgica

O Regulamento (UE) 2016/679 foi implementado na *Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* em 10 de janeiro de 2018 e publicada em 25 de maio de 2018. A execução da lei é por meio da Autoridade de Proteção de Dados - *Data Protection Authority* (DPA) da Bélgica, definida em 3 de janeiro de 2017, antigamente denominada de Comissão para a Proteção da Privacidade, a DPA tem poder para implementar sanções para infrações em relação às questões de privacidade (EECKE, 2018; KURTH, 2018).

A Bélgica não possui uma abordagem setorial para regulamentação de privacidade, entretanto, possui uma série de leis e regulamentos específicos, tais como: instalação e uso de câmera de vigilância; monitoramento de comunicação *online* dos funcionários, lei das comunicações eletrônicas e lei dos direitos dos pacientes (D'HULST; KENGEN, 2017).

O escopo da Lei de Proteção de Dados da Bélgica é para controles de dados, seja de pessoa física ou autoridade pública, ou qualquer órgão que utiliza de processamento de dados pessoais, sendo que ele se aplica a processos automatizados ou não automatizados de dados pessoais. A Lei conceitua como processamento de dados pessoais o conjunto de atividade tais como: coleta, armazenamento, gravação, alteração, uso e consulta (D'HULST; KENGEN, 2017).

A Lei de Comunicação Eletrônica da Bélgica (*Loi relative aux communications électroniques*) recebeu as diretrizes do Art. 5 da *e-Privacy Directive* quanto ao uso, armazenamento e processamento de *cookies*, as quais regulamentam o fornecimento de

[75] *[...]means any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof*
[76] *means the contents of conveyed communications.*

informações claras e abrangentes e consentimento do usuário quando interage com ambientes Web e ocorrem a coleta e processamento de *cookies* (EECKE, 2018).

Quanto aos dados de localização o Art. 123 da Lei de Comunicação Eletrônica da Bélgica de determina que "[...] operadoras de rede móvel somente poderão processar dados de localização de um assinante ou usuário final quando esses dados tiverem sido anonimizados ou quando o processamento faz parte dos serviços de tráfego ou serviços de localização" [77] (BÉLGICA, 2005, p. 135, tradução nossa).

O processamento de dados de localização e de tráfego está sujeito a informações sobre essa atividade e a obtenção do consentimento do usuário. Dentre as informações que devem ser dadas aos titulares estão: tipo de dados a serem processados, objetivos específicos do tratamento; duração do tratamento; e, em relação aos dados de localização a disponibilização sobre os potenciais terceiros a quem estes dados serão transmitidos e a possibilidade de retirar o consentimento informado (BÉLGICA, 2005).

d) Espanha

A Espanha implementou a Diretiva de Proteção de dados da UE 95/46/EC em 13 de dezembro de 1999 com a *Ley Orgánica* 14/1999 *de Protección de Datos de Carácter Personal* – conhecida como LOPD. No entanto, a Espanha já tinha uma Lei de Proteção de dados, denominada de LORTAD – *Ley Orgánica* 5/1992, *de* 29 *de Octubre, de regulación del tratamiento automatizado de los datos de carácter personal*, que era compatível com a maior parte da Diretiva de Proteção de dados da UE 95/46/EC (RAMOS, 2017).

A *Ley Orgánica* 14/1999 *de Protección de Datos de Carácter Personal* tem o objetivo de "garantir e proteger, no que diz respeito ao tratamento de dados pessoais, a liberdade pública e os direitos fundamentais das pessoais naturais e, especialmente, em relação a sua honra e intimidade pessoa e familiar" [78] (ESPANHA, 1999, p. 4, tradução nossa).

Essa lei será aplicável aos dados pessoais que forem armazenados em suporte físico e que são passíveis de tratamento, considerando qualquer modalidade. Define o termo processamento como a toda operação, seja ela automatizada ou não, e que permite atividades

[77] *Les opérateurs de réseaux mobiles ne peuvent traiter de données de localisation se rapportant à un abonné ou un utilisateur final que lorsqu'elles ont été rendues anonymes ou que le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation.*

[78] *La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.*

com dados pessoais, tais como coleta, armazenamento, alteração e exclusão (ESPANHA, 1999).

Em relação à privacidade *online*, o uso de *cookies* é regulamentado pelas diretrizes da *Ley Orgánica* 14/1999 *de Protección de Datos de Carácter Personal* e pela Lei da Espanha sobre a Sociedade da Informação, Serviços e Comércios Eletrônico (*Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico*), alterado em março de 2012. A *Spanish Data Protection Commissioner's Office* também publicou orientações sobre o uso de *cookies*, mesmo que não sejam diretrizes legais, elas contribuem com melhores práticas para serem adotadas quanto ao uso de *cookies* (RAMOS, 2018).

A *Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico* determina que detentores de dados forneçam informações sobre o uso de *cookies* para os usuários, tais como sua existência, uso e como desativá-los Essa lei emergiu devido à necessidade de um marco legal apropriado para as questões envolvidas com a Internet e novas tecnologias, pois muitas vezes tem criado algumas incertezas jurídicas, assim, torna-se objetivo da *Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico:*

> [...] a regulamentação do regime jurídico dos serviços da sociedade da informação e contratação por meio eletrônicos, no que diz respeitos às obrigações dos prestadores de serviços, incluindo os que agem como intermediários a transmissão de conteúdo por meio das redes de comunicação [...] [79] (ESPANHA, 2002, p. 8).

Em relação à implementação do Regulamento (UE) 2016/679, a Espanha ainda não começou a trabalhar na legislação para aderência ao novo regulamento até o primeiro trimestre de 2018, desta forma, provavelmente a nova legislação não estará em vigor até o final de 2018 (RAMOS, 2018).

e) França

A principal lei que regula a proteção de dados na França é a Lei nº 78.17 de 6 de janeiro de 1978, dispõe sobre questões vinculadas a tecnologia da informação, Arquivos de Dados e Liberdade Civil. A França implementou o Regulamento (UE) 2016/679 em 25 de maio de 2018.

A França possui um órgão chamado *Commission Nationale de l'Informatique et des Libertés* (CNIL) que é responsável por garantir que o uso da tecnologia da informação nos serviços voltados para os cidadãos não comprometa os direitos humanos, a privacidade ou a

[79] […] *la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones* […]

liberdade pública ou individual (LEBEAU-MARIANNA, 2018). No Capítulo 1 Art. 1 da Lei 78.17 é determinado que:

> A informática deve estar a serviço de todo cidadão. Seu desenvolvimento deve ocorrer dentro da estrutura da cooperação internacional. Não deve interferir na identidade humana, nos direitos humanos, na privacidade ou nas liberdades individuais ou públicas. Todos têm o direito de decidir e controlar os usos que são feitos de dados pessoais que lhe dizem respeito, sobre as condições estabelecidas por esta lei (FRANÇA, 1978, tradução nossa) [80].

Esta lei se aplica tanto ao processamento automático de dados pessoais, tanto quanto ao processamento não automatizado de dados pessoais, e considera o termo tratamento para representar qualquer processo tais como coleta, armazenamento e exclusão (FRANÇA, 1978).

Em relação à privacidade *online*, a França é amparada pela Diretiva EU *Cookie*, a qual regula que os usuários de comunicações eletrônicas devem ser informados sobre a finalidade dos *cookies*, os meios de recusar *cookies* e a obtenção do consentimento mediante configurações no navegador (LEBEAU-MARIANNA, 2018).

Os dados de tráfego mantidos pelos prestadores de serviços de comunicação devem ser apagados ou anonimizados, exceto quando são utilizados em pagamento de serviços de comunicação eletrônica. Os dados de localização podem ser utilizados em circunstâncias muito limitados, por exemplo, para o encaminhamento adequado de comunicação e apenas quando o usuário tiver dado consentimento (LEBEAU-MARIANNA, 2018).

f) Irlanda

A principal lei de Proteção de dados da Irlanda é a Lei de Proteção de Dados de 1988 (*Data Protection Act 1988*), alterada pela Lei de Proteção de Dados de 2018 (*Data Protection Act 2018*), que implementou o Regulamento (UE) 2016/679 no dia 25 de maio de 2018.

A lei define o termo processamento de forma ampla, definido como qualquer operação relacionada aos dados, seja automaticamente ou não, incluindo, coleta, registro, armazenamento, alteração, consulta (CORBET et al., 2018).

Além da Lei de Proteção de dados, a Irlanda adere às diretrizes do *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications)* Regulations (2011) *(ePrivacy Regulations),* que *estabelecem* regras de

[80] *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.*

proteção de dados relacionadas com marketing direito, redes e serviços eletrônicos, incluindo questões com dados de localização e *cookies* (NOLAN, 2018).

O uso de *cookies* é mediante o consentimento informado, seguindo as diretrizes do *ePrivacy Regulations*, e o usuário deve receber informações claras, abrangentes e facilmente acessíveis sobre o uso de *cookies*. Quanto aos dados de localização, esses somente poderão ser processados se forem anonimizados ou com o consentimento do usuário (NOLAN, 2018).

g) Itália

Para as questões de proteção de dados pessoais a Itália possui o Decreto Legislativo nº 196 de 30 de junho de 2003, chamado de Código de Privacidade que seguiu a Diretiva Europeia 95/46 / CE (CORAGGIO, 2018). Fica expresso na seção 2 do presente decreto que: "[...] os dados pessoais são processados respeitando os direitos das pessoas em causa, as liberdades fundamentais e a dignidade, no que diz respeito à confidencialidade, à identidade pessoal e ao direito à proteção de dados pessoais" (ITÁLIA, 2003, p. 14). Até o presente momento a Lei italiana que integra o Regulamento (UE) 2016/679 não foi adotada (CORAGGIO, 2018).

Os princípios básicos envolvidos no Decreto Legislativo nº 196 são a simplificação, a harmonização e a eficácia, sendo esse código divido em três partes: A primeira define os princípios gerais de proteção de dados que se aplicam a todas as organizações. A segunda fornece medidas para os setores da saúde, telecomunicações, bancos, finanças ou recursos humanos e, a terceira parte define sanções e soluções. Os principais recursos do Decreto Legislativo nº 196 são a notificação, minimização de dados, direitos dos titulares, transferências de dados internacionais (GARANTE PRIVACY, 2014).

Embora o Decreto Legislativo nº 196 considere o termo processamento como qualquer operação relativo à coleta, armazenamento, modificação, seleção, recuperação, exclusão, a menção a coleta de dados ocorre durante todo o decreto, que considera tanto operações realizadas com ou sem ajuda de meios eletrônicos (ITÁLIA, 2003).

O Decreto Legislativo nº 196 apresenta um capítulo que apresenta diretrizes para o tratamento de dados pessoais no âmbito da prestação de serviços de comunicação eletrônica. Fica explícito na seção 123 sobre dados de tráfego que esses dados quando processados pelo provedor ou serviço de comunicação eletrônica deverá ser apagado ou anonimizado quando não forem mais necessários para a transmissão de informação eletrônica (ITÁLIA, 2003).

Em relação a dados de localização que não sejam dados de tráfego, fica determinado na Seção 126 que o prestador de serviço deve informar os usuários sobre as atividades realizadas

com os dados de localização, tais como finalidade e duração do processamento, antes de obter o consentimento do usuário (ITÁLIA, 2003).

No ano de 2012, foi emitido pelo governo italiano o Decreto Legislativo nº 69/2012, que emendou o Código Italiano de Proteção de Dados (Decreto Legislativo de 30 junho de 2003, nº 196) determinando diretrizes para provedores de serviços de comunicação eletrônica nas questões vinculadas ao uso de *cookies* e violações de privacidade (CORAGGIO, 2018).

Com a finalidade de esclarecer a aplicação do Decreto Legislativo nº 69/2012, a Autoridade de Proteção de Dados Pessoais ("Garante") desenvolveu um guia de orientações simplificadas para o uso de *cookies*, denominada S*implified information notice and cookie consent" ("Cookie Decision")*. No *Cookie Decision* são distinguidos *cookies* técnicos e *cookies* de criação perfil, e determina que para o uso de *cookies* técnicos não é necessário o consentimento do usuário, ao contrário dos *cookies* de perfil, que apresenta natureza altamente invasiva em relação à esfera privada do indivíduo. Deve haver informações estendidas sobre o motivo da instalação de *cookies* e permitir que o usuário selecione ou cancele os *cookies* individuais (GARANTE PRIVACY, 2014).

h) Polônia

A Polônia implementou a Diretiva de Proteção de Dados da EU 95/46/EC na Lei de Proteção de Dados Pessoais de 29 de agosto de 1997 (*Personal Data Protection Act* – PDPA), no texto consolidado *Journal of laws of 2016*, no item 922. Há também vários estatutos setoriais específicos no contexto de processamento de dados pessoais.

A PDPA considera o termo processamento de dados como qualquer operação que é realizada com dados pessoais como coleta, registro, armazenamento, alteração, divulgação (POLÔNIA, 1997).

Na Polônia, a coleta de dados de localização, dados de transmissão e uso de *cookies* são regulados pela Lei de Telecomunicações (*Telecommunications Act of* 16 *July* 2004). Em relação aos dados de transmissão, esses somente poderão ser processados mediante o consentimento do usuário. Para o processamento de dados de localização, o fornecedor de serviços deve obter o consentimento do usuário para processar dados ou anonimizá-los antes do processamento, salvo algumas restrições que concede o processamento de dados de localização, tal como para fins de fornecimento de serviços de valor agregado. O uso e o armazenamento de *cookies* só serão permitidos mediante o consentimento antecipado do usuário, sendo que o ambiente deve informar de modo claro e simples o propósito do armazenamento e como obter acesso a essas informações (KUROWSKA-TOBER; CZYNIENIK, 2018).

A Lei de Proteção de Dados Pessoais de 29 de agosto de 1997 determina no Art. 2 inciso 1 que "[...] os princípios do processamento de dados pessoais e os direitos das pessoas cujos dados pessoais são ou podem ser processados como parte de um sistema de arquivamento de dados" [81] (POLÔNIA, 1997, p. 1) e, no Art. 2 inciso 2 que "A lei é aplicável ao tratamento de dados pessoais em: arquivos, índices, livros, listas e outros registros, sistemas de computador [...]" [82] (POLÔNIA, 1997).

Estão tramitando no legislativo dois projetos de lei no âmbito da proteção de dados pessoais, sendo o primeiro um esboço emendado do PDPA, e o segundo abarca várias emendas setoriais, ambos os projetos buscam implementar o Regulamento (UE) 2016/679, desta forma, no dia 25 de maio de 2018, a Polônia não tinha publicado sua lei de acordo com Regulamento (UE) 2016/679, pois as atualizações ainda tramitam no legislativo (KUROWSKA-TOBER; CZYNIENIK, 2018).

i) Portugal

A Lei Portuguesa de Proteção de dados (Lei nº 67/98 de 26 de outubro) foi promulgada em conformidade com a Directiva 95/46/CE. Essa lei "Transpõe para a ordem jurídica portuguesa a directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados" (PORTUGAL, 1998, p. 5536).

A Lei nº 67/98 aplica-se as questões vinculadas ao tratamento de dados pessoais por meio total ou parcialmente automatizado, incluindo a videovigilância e outros meio de coleta de dados que permitam a identificação do indivíduo. O termo tratamento é utilizado para várias atividades vinculadas com dados, tais como coleta, processamento e armazenamento (PORTUGAL, 1998).

O projeto de lei de implementação do Regulamento (UE) 2016/679 ainda não foi aprovado no Parlamento Português, nesse cenário a Lei Lei nº 67/98 permanece em vigor após 25 de maio, ou seja, as disposições que não contradizem diretamente o Regulamento (UE) 2016/679 (QUINTA 2018).

Em relação ao uso de *cookies* a Lei nº 41/2004, de 18 de agosto (Proteção de Dados Pessoais e a Privacidade nas Telecomunicações) determina que o armazenamento de dados e

[81] *The Act shall determine the principles of personal data processing and the rights of natural persons whose personal data is or can be processed as a part of a data filing system*.
[82] *The Act shall apply to the processing of personal data in: computer systems, also in case where data are processed outside from a data filing system.*

acesso a dados é baseado no consentimento prévio do usuário, sendo que o consentimento deve ser claro e abrangente, evidenciando os fins de tratamento, salvo exceções quando o objetivo for para efetuar comunicação por meio de redes de computadores ou para a prestação do serviço. A Autoridade Reguladora Local não disponibilizou orientações específicas sobre a definição de "consentimento" (QUINTA, 2018).

Em relação aos dados de tráfego, quando não forem mais necessários para a transmissão da comunicação, eles devem ser excluídos ou anonimizados. O processamento de dados de tráfego é permitido quando requerido para faturamento de contas de assinantes, incluindo o consentimento do usuário. O usuário deve ter informações completas e precisas sobre o tipo de dados que irá ser processado, como também os propósitos, duração do processamento, e a possibilidade de divulgação a terceiros (PORTUGAL, 2004).

Para as questões que envolvem dados de localização, esses só podem ser processados quando realizada a anonimização, conforme explícito no Art. 7, inciso I:

> Nos casos em que sejam processados dados de localização, para além dos dados de tráfego, relativos a assinantes ou utilizadores das redes públicas de comunicações ou de serviços de comunicações eletrônicas acessíveis ao público, o tratamento destes dados é permitido apenas se os mesmos forem tornados anônimos (PORTUGAL, 2004).

No entanto, o tratamento de dados de localização é permitido para a prestação de serviço de valor agregado, sendo necessário o consentimento do titular dos dados, que deverá ter ciência sobre o tipo de dados de localização que será processado, a duração e os motivos do tratamento (PORTUGAL, 2004).

j) Suécia

A Suécia implementou a Diretiva de Proteção de Dados da EU 95/46/EC em 1998 com a Lei de Dados Pessoais - *Personal Data Act* (PDA) (*personuppgiftslagen*) (SUNDBERG; THÖRN, 2017), e atualizou em 25 de maio de 2018 pela Lei (2018:218) (*Data Protection Act* (2018:218)) com disposições adicionais ao Regulamento (UE) 2016/679.

Além da *Data Protection Act* (2018:218) foi proposta várias leis setoriais específicas na Suécia, incluindo o setor da saúde, financeiro, energia, meio ambiente, eleições, comunicação e leis trabalhistas. No dia 04 de abril de 2018 foi avaliada uma nova proposta para uma lei de dados científicos, no entanto foi criticada pelo governo, sugerindo a atualização da lei de ética, que seria o suficiente para acompanhar o Regulamento (UE) 2016/679 (SVENSSON; ADVOKATBYRÅ, 2018).

A *Data Protection Act* (2018:218) dispõe de sete capítulos, dentre eles a base jurídica para o processamento de dados pessoais; processamento de certas categorias de dados pessoais; restrições de uso; limitações de direitos e obrigações; decisão de autoridades de supervisão; danos e recursos.

Na seção 1 explicita que a lei complementa o regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e revoga a Diretiva 95/46/CE.

A lei determina que o termo processamento se refira a quaisquer atividades vinculadas a dados pessoais, como coletar, armazenar, processar, alterar e excluir dados pessoais. A lei aplica-se tanto em processamento de dados realizado por computadores ou em registros manuais, sendo que questões envolvidas com comunicação por correio eletrônico não estão no âmbito da Lei (SUÉCIA, 2018).

De acordo com a Lei das Comunicações Eletrônicas da Suécia (*Swedish Electronic Communications Act*), que foi alterada pela Diretiva e-*Privacy* 2009/12/EC, *cookies* podem ser armazenados no equipamento do usuário, somente se esse tiver informações claras sobre o propósito do processamento e deve dar seu consentimento prévio, salvo quando os *cookies* forem utilizados para a prestação do serviço solicitado pelo usuário ou para efetivar a transmissão da comunicação por meio das redes de computadores (SUNDBERG; THÖRN, 2017).

Para o uso de *cookies*, os provedores de serviços devem informar sobre a possibilidade de o usuário negar ou retirar o seu consentimento para essa atividade, enfatizando as possibilidades de alteração na configuração do navegador e a exclusão de *cookies*. Ressalta-se também a necessidade de especificar a finalidade do uso do *cookie*, de forma que o usuário tenha base para tomar decisão sobre o consentimento (MINA *COOKIES*, 2011) [83].

k) Holanda

A Lei de Proteção de Dados Pessoais da Holanda - *Dutch Personal Data Protection Act* (*Wet Bescherming Persoonsgegevens* - WBP) implementou a Diretiva de Proteção de Dados da EU 95/46/EC em 1 de setembro de 2001, aplicada por meio da Autoridade de Proteção de Dados da Holanda (SCHAIK; WIT, 2018).

Em 25 de maio de 2018 adotou o Regulamento (UE) 2016/679, a partir da denominada Lei de Implementação, que foi desenvolvida separada para tratar assuntos que se aplicam

[83] Mina Cookies é um site criado pela indústria de tecnologia sueca, com informações sobre cookies, tais como desativar cookies e recomendações da IAB (principal associação da indústria na Europa para o ecossistema de publicidade online) da Suécia sobre o uso de cookies.

especificamente à Holanda, como a Autoridade de Proteção de Dados, e dá uma interpretação mais específica às disposições do Regulamento (UE) 2016/679 sobre o tratamento de dados especiais. A Lei de Implementação revoga a WBP.

Em relação a dados de tráfego as diretrizes estão presentes no Art. 11.5 do *Tw. Traffic Data*, esses dados devem ser apagados ou anonimizados quando não forem mais necessários para o propósito de transmissão de uma comunicação. Os dados de localização só podem ser processados se esses estiverem anonimizados e com o consentimento informado do indivíduo (SCHAIK; WIT, 2018).

A Holanda implementou a *e-Privacy Directive* por meio da Lei de Telecomunicações Holandesa (*Dutch Telecommunications Act*), na qual determina que o *site* obtenha o consentimento prévio do usuário antes de usar *cookies*, informando de clara e inequívoca ao usuário sobre esses *cookies* (finalidade, tipo). O uso de *cookies* analíticos para fins de pagamentos será permitido sem o consentimento, desde que não sejam utilizados para criar perfis de usuários. A informação coletada mediante *cookies* deve ser considerada dados pessoais (SCHAIK; WIT, 2018).

l) Noruega

A Noruega, que é membro do Espaço Econômico Europeu, implementou a Diretiva de Proteção de Dados da EU 95/46/EC com a Lei de Dados Pessoais (LOV-2000-04-14-31) e o Regulamento de Dados Pessoais (*Personal Data Regulation*) de 15 de dezembro de 2000 (BJERKE, SANDTRØ, 2018). A LOV-2000-04-14-31 foi implementada de acordo com Regulamento (UE) 2016/679, denominada de *Lov om behandling av personopplysninger (personopplysningsloven)*. A Lei de Dados Pessoais descreve a seguinte aplicabilidade: aplica-se no todo ou em parte, ao tratamento de dados pessoais e também no processamento não automatizado de dados pessoais. Especifica na lei o tratamento para dados exclusivamente para fins jornalísticos ou para fins acadêmicos, artísticos ou literários.

A autoridade responsável pela legislação de proteção de dados pessoais é a *Datatilsynet* (Autoridade Norueguesa de Proteção de Dados), que colaborou, por exemplo, em questões de remoção dos resultados de pesquisa *online* no *Google* de cidadãos noruegueses (LIBRARY OF CONGRESS, 2018).

Na Lei de Proteção de Dados o termo processamento de dados pessoais é usado para definir qualquer atividade vinculada a dados pessoais, como a coleta, gravação, armazenamento ou a combinação dessas atividades. A lei se aplica quando esse processamento ocorre tanto de

forma total ou parcial por meios eletrônicos, incluindo a coleta realizada por câmeras de vigilância (NORUEGA, 2018).

Os dados de localização, tráfego e *cookies* são amparados pela Lei das Comunicações Eletrônicas (*Lov om elektronisk kommunikasjon (ekomloven))*. O consentimento explícito é necessário para o processamento desses dados, e em relação aos dados de localização e tráfego, eles devem ser excluídos ou anonimizados quando não forem mais necessários (NORUEGA, 2003).

Quanto aos *cookies* o armazenamento de dados no equipamento de comunicação do usuário, ou o acesso a ele, não é permitido sem que o usuário seja informado dos dados que estão sendo processados, a finalidade do processamento, o responsável pelo processamento, e o consentimento do usuário. Não é necessário obter o consentimento do usuário se o cookie tiver somente o propósito de transferir a comunicação na rede, quando houver processamento de dados pessoais, os prestadores de serviços terão de cumprir os requisitos da Lei de Proteção de Dados (NORUEGA, 2003).

m) Reino Unido

O Reino Unido implementou a Diretiva de Proteção de Dados da EU 95/46/EC em março de 2000 por meio da Lei de Proteção de Dados de 1998 (*Data Protection Act*), como o restante da União Europeia (DYSON; MCKEAN, 2018).

Devido o Regulamento (UE) 2016/679, o Reino Unido implanta a *Data Protection* Act 2018, com o objetivo de disponibilizar regulamentação de tratamento de informações relacionadas a indivíduos, prevendo um código de prática de marketing direto (REINO UNIDO, 2018). A *Data Protection Act* 2018 complementa o Regulamento (UE) 2016/679 e trata tipos de processamento ao qual esse regulamento não trata.

É definido na lei que o "processamento, em relação à informação, significa uma operação ou conjunto de operações que são realizadas com informações, tais como: coleta, registro, organização, estruturação ou armazenamento, alteração, recuperação, consulta [...] [84] (REINO UNIDO, 2018, p.2, tradução nossa).

Quanto aos dados de localização e dados de tráfego de comunicações eletrônicas o Reino Unido possui a *Privacy and Electronic Communication (EC Directive) Regulations 2003 (PEC Regulations)* que abarca questões vinculadas com esses tipos de dados. Os dados de

[84] "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as— (a) collection, recording, organization, structuring or storage, (b) adaptation or alteration, (c) retrieval, consultation […].

tráfego por um prestador de serviço devem ser excluídos e quando processados e armazenados necessitam de consentimento do titular de dados. Em relação ao processamento de dados de localização, a *PEC Regulations* determina que o processamento só ocorra quando titular dos dados não puder ser identificado a partir desses dados, e que se obtenha o consentimento do titular (REINO UNIDO, 2003).

n) Suíça

A Lei Federal de Proteção de Dados de 19 de junho de 1992 – *Federal Act on Data Protection* (FADP) é o ordenamento que regula o processamento de dados pessoais na Suíça, conjuntamente com suas portarias, a Portaria da Lei Federal de Proteção de dados – *Federal Act o Data Protection* (DPA) e a Portaria sobre Certificação de Proteção de Dados – *Ordinance on Data Protection Certification* (ODPC). Há ainda, outras leis para amparar questões de dados pessoais no setor público. O DPA passou por uma revisão em setembro de 2017 e espera-se que entre em vigor até o inicio de 2019, essa revisão teve a finalidade de fortalecer a proteção de dados e alinhar o DPA aos requisitos do Regulamento (UE) 2016/679 (MATHYS et al., 2018).

Na nova atualização da FADP publicada em 15 de setembro de 2017, é interessante ressaltar a definição do termo perfil, que demonstra o uso da análise de dados pelas tecnologias da informação.

> Avaliação de certas características de uma pessoa com base em dados processados de forma automatizada, a fim de analisar ou prever o desempenho de uma pessoa no trabalho, sua situação financeira, sua saúde, seu comportamento, suas preferências, sua localização ou sua mobilidade[85] (SUÍÇA, 2017, tradução nossa).

Na FADP o termo processamento equivale ao conjunto de operações com dados pessoais, independentemente dos meios aplicados, tais como a coleta, gravação, armazenamento, uso, alteração, divulgação e exclusão (SUÍÇA, 2017), no entanto, faz a menção à coleta de dados no decorrer da lei. A lei aborda sobre proteção de dados por *design* e por *default*, determinando que as medidas técnicas devem ser adequadas para a proteção de dados pessoais (SUÍÇA, 2017).

O tratamento de dados pessoais no contexto de serviços *online* está sujeito aos regulamentos da FADP, no entanto, o uso de *cookies* está regulamentado nas diretrizes da *Swiss Telecommunications Act* (TCA), que determina que o usuário deve ser informado sobre o

[85] *The evaluation of certain characteristics of a person on the basis of personal data processed in an automated manner; in particular in order to analyses or to predict a person's performance at work, his financial situation, his health, his behavior, his preferences, his location or his mobility.*

processamento de *cookies* e sua finalidade, bem como os meios para recusar. Quando *cookies* coletam dados sensíveis do usuário devem ser aplicadas regras mais estritas, como a informação sobre a identidade do detentor, a finalidade e os destinatários dos dados, caso sejam divulgados a terceiros (MATHYS et al., 2018).

o) *Privacy Shield*

O *framework* EU-U.S *Privacy Shield* e *Swiss-U.S. Privacy Shield* foram desenvolvidos pelo departamento de Comércio dos Estados Unidos, pela Comissão Europeia e governo da Suíça, com a finalidade de fornecer às empresas de ambos os lados do Atlântico um mecanismo que permita a transferência de dados pessoais da União Europeia e da Suíça para os Estados Unidos, de forma que cumpra os requisitos de proteção de dados pessoais durante o intercâmbio transatlântico de dados para fins comerciais (EUROPEAN COMMISSION, 2016; PRIVACY SHIELD, 201-a). A *Privacy Shield* substitui o *International Safe Harbor Privacy Principles*, que foram declarados inválidos pelo Tribunal de Justiça Europeu em outubro de 2015 (PRIVACY SHIELD, 201-a).

A justificativa para o *framework Privacy Shield* são os fortes laços comerciais entre a União Europeia e os Estados Unidos, visto que a transferência de dados pessoais constitui uma parte importante e necessária do relacionamento transatlântico. Essas transações envolvem a coleta e uso de dados pessoais, tais como: nome, número de telefone, data de nascimento, residência, endereço, número de cartão de crédito ou qualquer outro tipo de dado que permita identificar o titular dos dados. Desta forma, o *Privacy Shield* permite que os dados pessoais sejam transferidos da UE para empresas nos EUA, desde que o uso, armazenamento e transferências de dados pessoais por essas empresas estejam de acordo com o forte conjunto de regras e salvaguarda de proteção de dados (WIGAND; VOIN, 2016).

O governo suíço aprovou, em 11 de janeiro de 2017, o *framework Swiss-US Privacy Shield*, que substitui o acordo *Safe Habor* entre a Suíça e os Estados Unidos, esse *framework* busca garantir as questões de privacidade dos indivíduos na transferência de dados pessoais entre a Suíça e os Estados Unidos. A finalidade desse *framework* é determinar diretrizes para proteção de dados pessoais quando dados pessoais são transferidos da Suíça para uma empresa nos Estados Unidos. Com esse *framework*, a Suíça aplicará as mesmas regras que a União Europeia (por meio do EU-U.S *Privacy Shield)* para proteção de dados pessoais (SUÍÇA, 2016).

Segundo a *Privacy Shield* (201-b), para proteger o fluxo de dados entre a União Europeia e os Estados Unidos, o EU-US *Privacy Shield* e *Swiss*-U.S. *Privacy Shield* baseiam-se respectivamente nos seguintes princípios:

- ✓ **Aviso Prévio**: As organizações devem informar aos indivíduos sobre as questões envolvidas com dados pessoais, tais como: sua participação no *Privacy Shield*; os tipos de dados coletados; o motivo para a coleta e uso dos dados; como entrar em contado com a organização quando tiver dúvidas ou queixas a respeito dos seus dados; direito de acesso aos seus dados pessoais;
- ✓ **Escolha:** A organização deve oferecer aos indivíduos a opção de escolher se sua informação pessoal será divulgada a terceiros ou será utilizada para propósitos diferentes do motivo pelo qual foi coletada. Essa escolha deve ser amparada com informações claras, visíveis, e com mecanismos para permitir tal escolha. As mesmas considerações devem ser aplicadas quando se tratar de dados sensíveis, as organizações devem obter consentimento (*opt in*) de indivíduos se tais informações forem divulgadas a um terceiro ou se tiverem uso diferente do motivo da coleta;
- ✓ **Responsabilidade pela transferência:** As organizações devem estar alinhadas aos princípios de aviso e escolha quando realizar atividades de transferência de informações pessoais para um terceiro;
- ✓ **Segurança:** A organização deve tomar medidas apropriadas para proteger os dados em relação à perda, ao uso indevido, ao acesso não autorizado, à divulgação, à alteração e à exclusão, considerando os potenciais riscos envolvidos no processamento e a natureza dos dados pessoais;
- ✓ **Integridade dos dados e limitação do objetivo:** A organização não pode processar informações pessoais de modo que sejam incompatíveis pelo motivo que os dados foram coletados ou autorizados pelo indivíduo, tomando medidas para garantir que os dados sejam confiáveis para o uso pretendido, preciso, completo e atual;
- ✓ **Acesso:** As organizações devem disponibilizar aos indivíduos o acesso às informações pessoais que foram armazenadas. O titular de dados também deve poder corrigir, alterar ou excluir informação onde ocorreu imprecisão ou violação dos princípios;
- ✓ **Recurso, execução e responsabilidade:** a proteção efetiva contra ameaças à privacidade deve garantir meios para recursos aos indivíduos afetados por não conformidade aos princípios.

5.2.6 Hong Kong

A principal legislação sobre privacidade é a Portaria de Dados Pessoais, capítulo 486 das Leis de Hong Kong, promulgada em 1996 em respostas à Diretiva 95/46/CE (Diretiva de Proteção de Dados) (THIEL; BIGG, 2017). Em 2012 a Portaria de Dados Pessoais passou por

atualizações devido à necessidade de adicionar disposições e restrições ao uso e coleta de dados de marketing. Hong Kong não possui leis específicas para proteção de dados para os setores da indústria, no entanto, muitas associações implementam diretrizes com base na Portaria de Dados Pessoais (BLACKMORE, 2017).

A Portaria de Dados Pessoais engloba na definição de dados pessoais qualquer informação sobre comportamento, preferências, opiniões ou atividades que quando armazenadas podem ser correlacionadas com a identidade do titular dos dados. Dados imagéticos também são considerados dados pessoais (BLACKMORE, 2017), e também define Sistemas de Dados Pessoais "como qualquer sistema, automático ou não, que seja usado, no todo ou em parte, por um detentor de dados para a coleta, armazenamento, processamento ou uso de dados pessoais, e inclui qualquer documento ou equipamento que faça parte do sistema" [86] (HONG KONG, 1996). Interessante, ressaltar em termos de definição, que as questões de coleta de dados são tratadas especificamente e o termo processamento está vinculado ao tratamento ou exclusão dos dados, seja por meios automatizados ou não.

A coleta, uso e divulgação de dados de pessoais para fins de marketing são definidos também pela Portaria de Dados Pessoais, regulamentando questões como o armazenamento, tempo de retenção, precisão e segurança (acesso e alteração de dados). Não é determinada nessa portaria a transferência de dados pessoais para fora de Hong Kong e, questões vinculadas especificamente com dados confidenciais (sensíveis) (HONG KONG, 1996).

As diretrizes da Portaria de Dados Pessoais se aplicam também quando as atividades ocorrem no ambiente digital, tais como, questões como a obrigação de informar os titulares dos dados sobre os motivos da coleta e informações sobre uso de *cookies*, incluindo as implicações na funcionalidade do *site* quando não o titular dos dados não permite o uso de *cookies* (THIEL; BIGG, 2017).

5.3 Legislação para proteção de dados pessoais no cenário nacional

No Brasil ainda não há uma legislação que trate especificamente de questões vinculadas à proteção de dados pessoais. No que tange a terminologia, a doutrina brasileira emprega uma profusão de termos distintos para se referir à privacidade. Fala-se em "[...] vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e até mesmo 'privatividade' e 'privaticidade', entre outros" (DONEDA, 2006, p. 101).

---

[86] *Means any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system.*

> [...] no Brasil há escassez de estudos voltados para análise do direito à privacidade e à proteção dos dados em um contexto denominado como a era do culto do amador e do culto social, em que os próprios usuários são induzidos, ou seduzidos ao exibicionismo exacerbado, com a renúncia do direito humano fundamental da privacidade e com fornecimento de dados pessoais tão valiosos que compensam a oferta de serviços na Internet de forma gratuita (BOFF; FORTES, 2014, p. 11).

Ao realizar uma pesquisa exploratória nos sítios do governo federal, especificamente no portal da legislação, identificou-se 7 leis que apresentam menções fragmentadas à proteção de dados pessoais. Também foram encontrados 5 projetos de leis específicos para a proteção de dados pessoais: Projeto de Lei nº 4.060 de 2012; Projeto de Lei do Senado nº 330 de 2013; Projeto de Lei nº 131 de 2014; Projeto de Lei do Senado nº 181 de 2014, e o mais recente Projeto de Lei nº 5.276 de 2016, que está apensado ao PL 4.060/2012.

5.3.1 Legislação

A Constituição Federal de 1988 estabelece alguns princípios de privacidade e proteção de dados pessoais por meio do Art. 5, inciso X, no qual determina que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [...]", e no Art. 5, inciso XII, em que é designado "[...] o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas [...]" (BRASIL, 1988). No Art. 5, inciso LXXII, a Constituição Federal regula o direito ao *habeas data*, que possibilita o conhecimento das informações contidas em registros e bancos de dados pelo requerente e direito à retificação dos seus dados, que posteriormente se torna a Lei nº 9.507/1997 (BRASIL, 1988).

A Lei nº 7.232/1984 estabelece o Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação. Tem por finalidade a qualificação das atividades de informática. Em relação à proteção de dados pessoais, a Lei evidencia princípios que asseguram a proteção de dados armazenados e o direito ao acesso e a alterações dos seus dados, garantindo a proteção da privacidade de pessoas físicas, jurídicas, privadas e públicas (BRASIL, 1984).

Com a finalidade de estabelecer normas para a proteção dos dados pessoais do consumidor, a menção à proteção de dados pessoais na Lei nº 8.078/1990, estabelecida como o Código de Defesa do Consumidor, ocorre ao destacar banco de dados e cadastros de consumidores, garantindo a esses indivíduos o acesso à informação armazenada e a possibilidades de correção quando encontrar inconsistência nos dados (BRASIL, 1990).

A Lei Federal nº 9.507/1997 garante o direito ao *habeas data* ao requerente, permitindo obter conhecimento e a possibilidade de alterar dados presentes em registros ou banco de dados de instituições públicas (BRASIL, 1997a).

A Lei 9.472/1997, denominada de Lei Geral das Telecomunicações, dispõe, principalmente, sobre os elementos envolvidos nos serviços de telecomunicações. No que se refere à proteção de dados de pessoais, a lei ordena os direitos do usuário em relação ao uso de seus dados pessoais pelas operadoras, tais como a divulgação em documento de cobrança e a divulgação a terceiros (BRASIL, 1997b). A evidência em relação à proteção de dados fica explícita no Art. 3 inciso V, ao determinar que usuário tem direito "[...] à inviolabilidade e ao segredo de suas comunicações" (BRASIL, 1997b).

Conhecido como Lei do Cadastro Positivo, a Lei nº 12.414/2011 estabelece regulamento a respeito da criação e da consulta ao banco de dados com informações de inadimplência, provendo ao titular dos dados, denominado na lei de cadastrado, o direito a informações sobre o armazenamento dos seus dados e o propósito do tratamento (BRASIL, 2011a). Embora faça menção a tratamento de dados, a lei não explicita os aspectos que implicam nesta atividade, tais como técnicas de anonimização. Surge a figura do gestor e as suas responsabilidades referentes à proteção de dados do indivíduo referenciado na base de dados.

A Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011 - estabelece o direito fundamental de acesso à informação. Observa-se que a LAI aborda preocupação em relação à informação pessoal, ao conceituar os termos "informação pessoal" e "tratamento da informação", evidenciando que todo tratamento da informação deve estar claro para o titular dos dados (BRASIL, 2011b). Questões que envolvem o tratamento das informações pessoais são timidamente exploradas, não explicitando quais tratamentos deverão ser realizados para que se garanta a privacidade do indivíduo.

A Lei nº 12.737/2012, denominada Lei Carolina Dickemann (BRASIL, 2012), determina sobre a "tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências" (BRASIL, 2012). Essa lei emergiu devido à situação em que a atriz Carolina Dickemann teve seu computador pessoal invadido, resultando na cópia e na divulgação, sem autorização, de suas fotos íntimas e conversas na Internet. Surgiu, assim, a necessidade de providências para amparar esse tipo de situação.

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet (BRASIL, 2014c), foi resultado do Projeto de Lei 2.126/2001, elaborado por meio de debates e contribuições colaborativas entre vários atores da sociedade, com o objetivo de nortear os aspectos vinculados ao uso da Internet no Brasil. A proteção de dados pessoais é um dos princípios elencados pela lei, juntamente com a proteção da privacidade. Na lei são estabelecidos os direitos dos usuários quanto ao consentimento para coleta de seus dados, informações sobre as atividades de coleta,

uso, armazenamento, tratamento e proteção dos dados pessoais, incluindo o direito ao esquecimento. Emerge o termo dados sensíveis no contexto de proteção deste tipo de dado. Embora a Lei mencione a atividade de tratamento de dados, em nenhum momento o termo é conceituado.

5.3.2 Projetos de Leis

Como o Brasil não dispõe de leis específicas para proteção de dados pessoais, tramitam no congresso projetos de leis que abarcam esse cenário, tais como: Projeto de Lei nº 4.060 de 2012; Projeto de Lei do Senado nº 330 de 2013; Projeto de Lei nº 131 de 2014; Projeto de Lei do Senado nº 181 de 2014; Projeto de Lei 6.291/2016, e o Projeto de Lei nº 5.276 de 2016, que está apensado ao PL 4.060/2012.

O PL 4060/2012 "[...] dispõe sobre o tratamento de dados pessoais, e dá outras providências" (BRASIL, 2012b). São definidos nesse projeto de lei os termos: dado pessoal; tratamento de dados; banco de dados; dados sensíveis; responsáveis; interconexão; e bloqueio. Estão apensados nesse projeto o PL 5.276/2016 e o PL 6.291/2016.

O PL 6.291/2016 "[...] altera o Marco Civil da Internet, no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de Internet" (BRASIL, 2016b). Esse projeto de lei está apensado ao PL 5.276/2016. O projeto se justifica devido ao compartilhamento de dados por grandes empresas como *Google*, *Facebook* e *WhatsApp*, incluindo o próprio governo, que tem se tornado grandes detentores de dados. Assim, o projeto determina a proibição de compartilhamento de dados dos usuários, especialmente em relação aos dados sensíveis, e a necessidade de consentimento informado para tal atividade (BRASIL, 2016b).

O Projeto de Lei do Senado nº 330, de 2013, "[...] dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências" (BRASIL, 2013). Nesse projeto, são definidos os seguintes termos: dado pessoal; banco de dados; tratamento de dados pessoais; gestor de banco de dados; gestor aparente; proprietário do banco de dados; titular de dados pessoais; usuário de banco de dados; dados sensíveis; interconexão de dados e dissociação. No PLS 330, vale destacar a menção à dissociação de dados, medida utilizada para minimizar ameaças à privacidade, e a atenção à coleta de dados sensíveis.

O Projeto de Lei do Senado nº 131, de 2014, trata sobre as questões envolvidas com o fornecimento de dados de indivíduos ou de empresas brasileiras para autoridades ou tribunais estrangeiros. Assim, o Art. 1º determina que a presente lei "[...] dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiras a organismos estrangeiros" (BRASIL, 2014a).

O Projeto de Lei do Senado nº 181, de 2014, determina "[...] princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais" (BRASIL, 2014b). Ao fazer referência ao termo autodeterminação, aproxima-se da definição de privacidade cunhada por Westin (1967) e Rodotà (1995) no âmbito do indivíduo ter controle sobre as atividades realizadas com seus dados. Esse projeto de lei passa a tramitar em conjunto com os PLS 330/2013 e 131/2014 (BRASIL, 2014a).

Interessante ressaltar a característica brasileira de muitas regulamentações para tratar algo comum, como no caso dos projetos de leis supracitados para proteção de dados pessoais. Assim, devido à semelhança nos contextos dos projetos de lei, este trabalho focou-se no PL 5.276/2016, cujas diretrizes são sobre:

> [...] tratamento de dados pessoais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2016a).

A elaboração do PL 5.276/2016 ocorreu mediante debate público promovido pelo Ministério da Justiça, com a colaboração do Observatório Brasileiro de Políticas Digitais do Comitê Gestor da Internet no Brasil durante aproximadamente seis meses. A finalidade do projeto é estabelecer regulamentos, princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais. Destacam-se: o consentimento do usuário sobre atividades realizadas com seus dados pessoais; definição de regras para tratamento, compartilhamento, transferência internacional de dados, incluindo aspectos de segurança e sigilo de dados pessoais; e a estruturação de comitês para a construção de políticas públicas de informação (BRASIL, 2016a).

O PL 5.276/2016 apresenta conceitos vinculados ao processo de proteção da privacidade, tais como: dado pessoal, tratamento de dados, dados sensíveis, dados anonimizados, anonimização. Além disso, define os atores participantes do processo de proteção dos dados pessoais, como o titular, órgão competente, pode público, operador, responsável e administração pública. Ressalta-se que o conceito de "tratamento" emerge como um termo genérico que abarca:

> [...] toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2016a).

Em 20 de novembro de 2017 foi instituída pela Portaria Normativa PGJ nº 512 a Comissão de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal e Territórios (MPDFT), sendo a primeira iniciativa com a finalidade de proteger dados pessoais e a privacidade dos brasileiros.

A Comissão de Proteção dos Dados Pessoais do Ministério Púbico do Distrito Federal e Territórios (MPDFT) apresenta sete pilares básicos de atuação (MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS, 201-):

> Pilar Opinativo: sugerir diretrizes para uma Política Nacional de Proteção dos Dados Pessoais e Privacidade;
> Pilar Informativo: promover entre a população, empresas e órgãos públicos o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e privacidade, bem como medidas de segurança;
> Pilar de Estudos: promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
> Pilar de Cooperação: promover ações de cooperação com autoridade de proteção de dados pessoais de outros países, de natureza internacional ou transacional;
> Pilar de Notificação: receber comunicações sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares dos dados (*data breach notification*);
> Pilar Sancionador: propor ações judiciais visando à aplicação das sanções previstas no Art. 12, da Lei nº 12.965/14 - Marco Civil da Internet, em conjunto com o promotor natural;
> Pilar Investigativo: instaurar procedimento preparatório, inquérito civil público e procedimento administrativo, em conjunto com o promotor natural.

Os elementos envolvidos nas questões para proteger dados pessoais começam a emergir nas legislações, nos projetos de leis e nos regulamentos. Essas diretrizes buscam atender à necessidade de proteger dados pessoais durante todo o ciclo de vida dos dados, conforme o abarcado no termo “tratamento” no PL 5.276/2016.

5.4 Resultados e Discussões

5.4.1 Menção a proteção de dados pessoais no cenário nacional

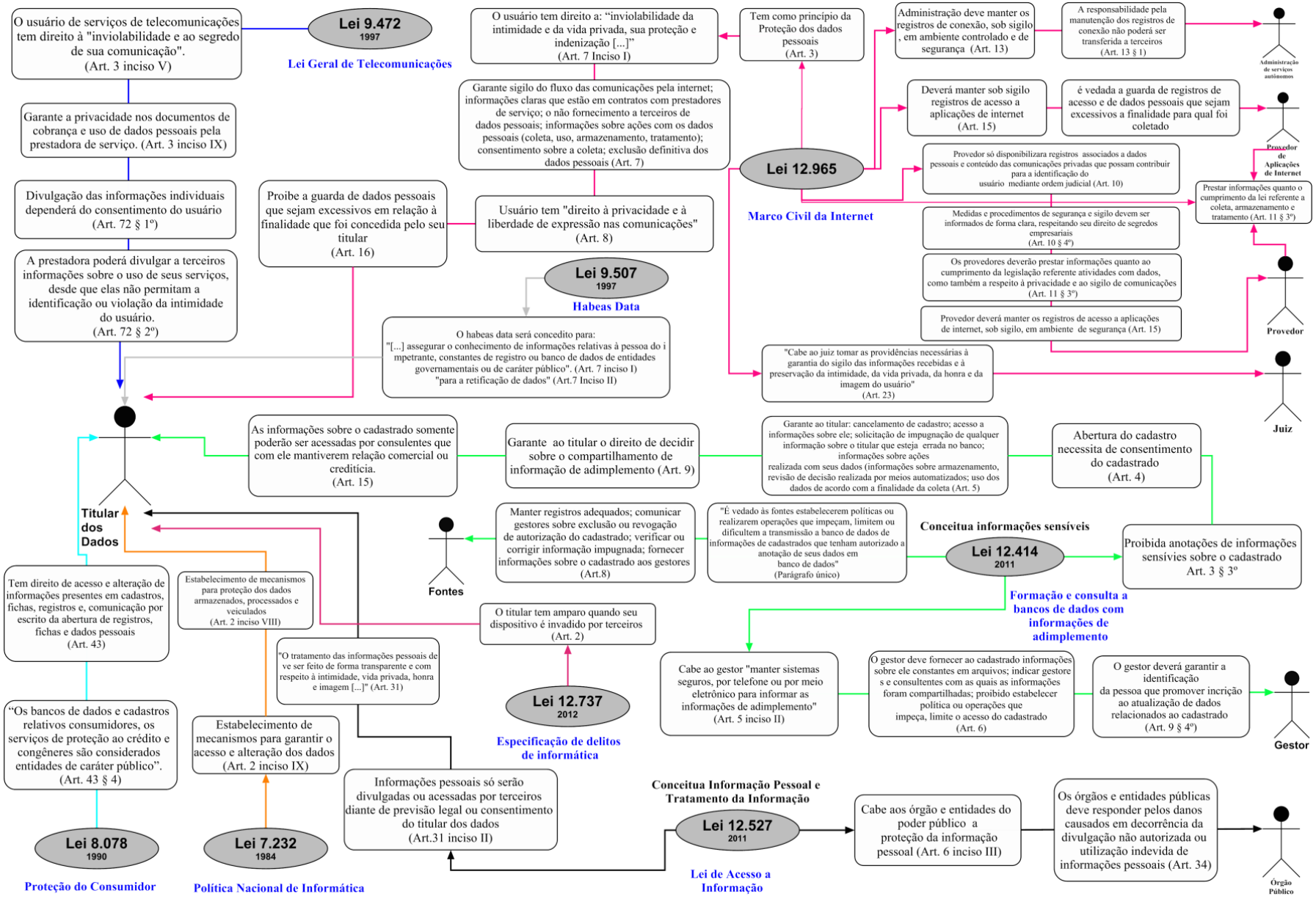
A partir do levantamento das leis e projetos de leis do Brasil, é possível identificar como a proteção de dados pessoais tem se efetuado nessas leis. A Figura 30 apresenta um panorama das leis brasileiras que mencionam proteção de dados pessoais, ilustrando o envolvimento com atores e regulamentos, incluindo as principais terminologias vinculadas à privacidade do sujeito. Também é apresentado um diagrama com o Projeto de Lei 5.276/2016, indicando seus principais atores e regulamentos (Figura 31). No Apêndice B é apresentada a categorização dos artigos presentes nas leis do Brasil, os atores envolvidos e os conceitos vinculados à proteção de dados pessoais.

No Brasil, a abordagem relacionada à proteção de dados pessoais amplia-se no decorrer dos anos, visto que preocupação com questões de privacidade configuram-se com o aumento do uso das Tecnologias da Informação e Comunicação e com as atividades desenfreadas da coleta de dados nos ambientes digitais. Contudo, mesmo quando as leis recentes citam mecanismo para proteção dos dados pessoais, elas ainda não enfatizam anonimização de dados, apenas elencam tratamento da informação, termo utilizado para designar várias atividades referentes aos dados (Figura 30).

Encontram-se nessas leis os atores: titular dos dados, órgão público, gestor, fontes, o juiz, provedor e provedor de aplicação de Internet. Observa-se que em relação aos conceitos elencados nas leis sobre proteção de dados pessoais, emergem apenas a definição de informação pessoal, tratamento da informação e dados sensíveis (Figura 30).

Devido à legislação brasileira não possuir uma lei específica para proteção de dados pessoais, essas questões são amparadas pela necessidade de algum serviço, tais como serviços de telecomunicações, formação de banco de dados com consultas de adimplemento, ou em leis que determinam o acesso a informação.

Figura 30 – Síntese do conjunto de leis e fragmentos que mencionam proteção de dados pessoais



Fonte: Elaborado pela autora

Tramitam no Congresso Nacional projetos de leis para o amparo à proteção de dados. Na Figura 31, apresenta-se a sistematização dos principais atores, determinações e os conceitos envolvidos no PL 5.276/2016, que "[...] dispõe sobre o tratamento de dados pessoais para garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural" (BRASIL, 2016a, p.1). No Apêndice C são descritos as determinações, os atores envolvidos e as principais definições.

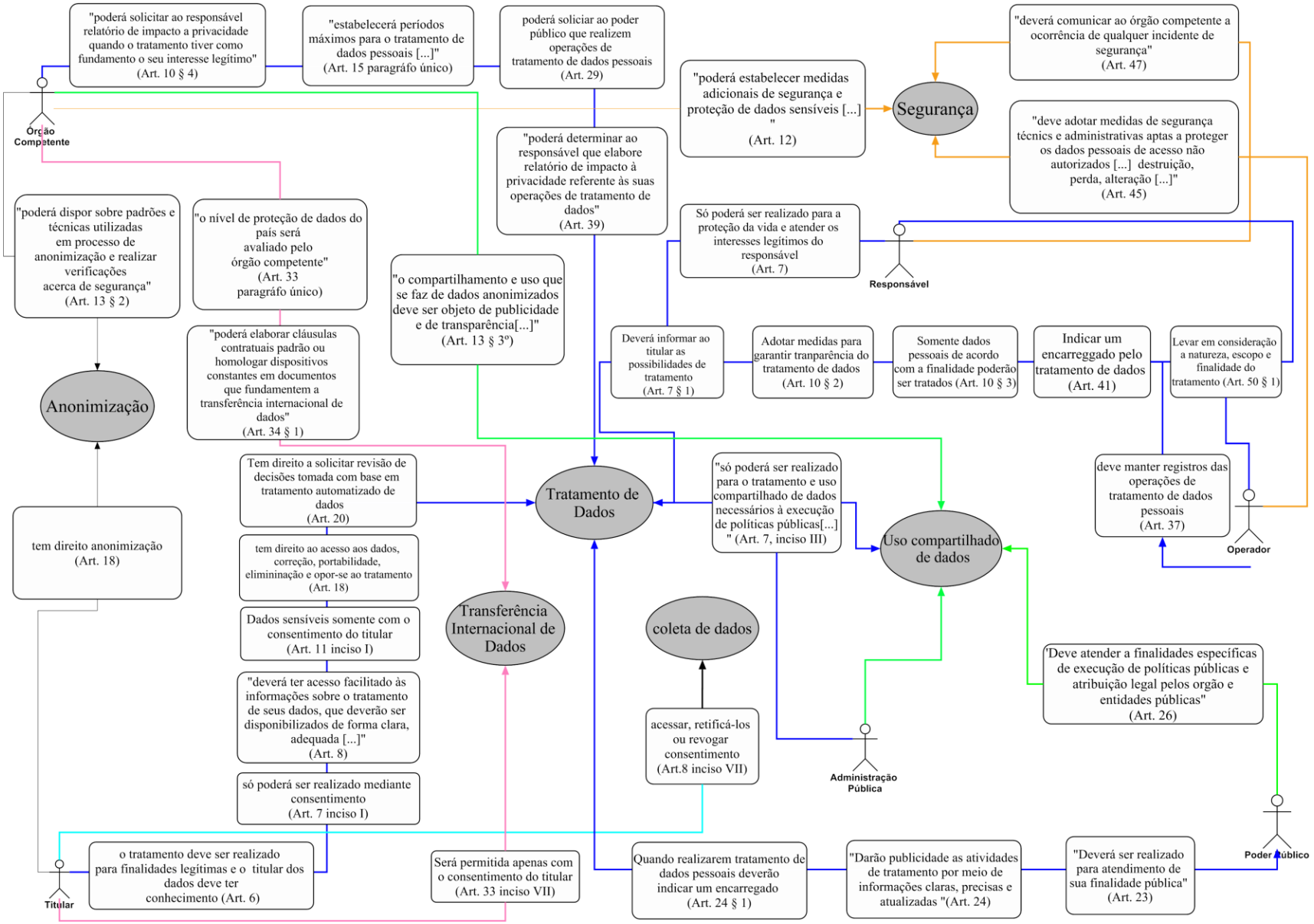
Observa-se no PL 5.276/2016 a diversidade de atores, princípios e garantias envolvidas no âmbito da proteção de dados pessoais, especificamente com um maior enfoque nas ações voltadas aos direitos do titular de dados e à necessidade de manter esses sujeitos informados sobre as atividades que permeiam seus dados. Visto que a díade coletar dados e privacidade estarão sempre em conflito, exigem-se, assim, cada vez mais mecanismos, leis e políticas que respondam a essas vertentes de forma equilibrada.

Anonimização de dados no PL 5.276/2016 é definida como uma atividade necessária para proteger indivíduos referenciados num conjunto de dados. Contudo, não é especificada em qual fase do ciclo de vida essa proteção (anonimização) irá se efetuar. Os dados semi-identificadores não evidenciados em uma categoria especial, uma vez que esse tipo de dado, quando combinado com outras fontes de dados externas podem permitir a identificação do indivíduo, devendo assim ser foco de maiores análises e estudos.

A elaboração de lei específica para a proteção de dados pessoais é recente no Brasil, e a concretização desse projeto poderá fornecer elementos para o desenvolvimento de políticas públicas de informação ou políticas públicas destinadas a outros contextos, visto que no PL 5.276/2016 é determinado, no Art. 53, inciso II, que o órgão competente terá a atribuição de "[...] elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade" (BRASIL, 2016a).

Ressalta-se, ainda, a relevância da aprovação desse projeto de lei, pois, por meio da consolidação da lei, diversos interesses passam a ser atendidos e ter legalidade. Quando há leis, consequentemente há a obrigação de a sociedade, os órgãos públicos e privados estarem em aderência com essas legislações, o que pode minimizar a insciência do usuário sobre o processo de coleta.

Figura 31 - Síntese do Projeto de Lei 5.276/2016



Fonte: Elaborado pela autora

5.4.2 Menção a coleta de dados nas legislações

Com o objetivo de averiguar como as legislações têm mencionado questões envolvidas especificamente com coleta de dados pessoais, o Quadro 14 apresenta as principais leis e regulamentos levantados neste trabalho e, especificamente a abordagem em relação à coleta de dados sujeito-detentor.

Quadro 14 - Menção a coleta de dados nas leis e regulamentos[87]

País	leis	Data	Principal abordagem a coleta de dados
Austrália	*Privacy Act* *Australian Privacy Principles* – APPs	1988	Possui uma seção para coleta de dados. Explicita situações nas quais os APPS não se aplicam em relação à coleta de dados; situações de saúde que permitem a coleta; determina a proibição de coleta de informações de crédito; autorização de coleta de dados em situação de emergência. Tipo de informações pessoais que a entidade coleta; Meios como a entidade coleta informações pessoais; Notificação da coleta; Fins para os quais a entidade coleta, detém, usa e divulga informações pessoais; Agências e Organizações só podem coletar informações pessoais (além de confidenciais) se estiver relacionada à atividade da entidade; Informações sensíveis só podem ser coletadas se o indivíduo consentir a coleta. Aborda anonimização na coleta. Não são evidentes os termos dados de localização, tráfego e cookies (AUSTRÁLIA, 1998).
Brasil	Lei nº 7.232	1984	Apenas cita o termo coleta como uma atividade realizada por meio de dispositivos (BRASIL, 1984).
	Lei nº 8.078	1990	Não explícito. (BRASIL, 1990).
	Lei nº 9.507	1997	Não explícito. (BRASIL, 1997).
	Lei nº 9.472	1997	Não explícito (BRASIL, 1997).
	Lei nº 12.527	2011	Não explícito. O foco da lei é a questão da invasão de dispositivos. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 1997).
	Lei nº 12.414	2011	Uso dos dados de acordo com a coleta. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 2011).
	Lei nº 12.737	2012	Não é explícita a coleta usuário-detentor. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 2012).
	Lei nº 12.965	2014	Usuário tem direito a informações claras sobre a coleta, motivo da coleta; consentimento sobre a coleta. Não são evidentes os termos dados de *cookies* e localização. Não menciona anonimização. Menciona dados de tráfego (BRASIL, 2014).
	PL nº 4060	2012	Informações sobre a utilização dos dados coletados; direito a autodeterminação informativa sobre os dados coletados. Consentimento informado quando a coleta é de dados de criança. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 2012).
	PLS nº 330	2013	Possui uma seção para coleta de dados. Define motivos pelos quais dados sensíveis poderão ser coletados; usuário tem o direito ao consentimento

[87] * Atualizado pelo novo GDPR; ** até o momento não atualizado pelo novo GDPR.

			prévio como requisito a coleta; proteção aos dados coletados. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 2013).
	PLS nº 131	2014	Não explícito. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 2014).
	PLS nº 181	2014	Meio de coleta; motivo da coleta; uso de acordo com a coleta; recebimento de informações claras sobre a coleta; consentimento sobre a coleta; vedada a coleta de dados pessoais obtidos por meio de ato ilícito; limitação da coleta. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 2014).
	PL nº 6.291	2016	Não explícito. Não são evidentes os termos dados de *cookies*, localização e tráfego. Não menciona anonimização (BRASIL, 2016).
	PL nº 5.276	2016	A coleta é mencionada como tratamento de dados. Quando acontecer coleta continuada de dados o titular dever ter informações sobre o tratamento. Motivo do tratamento. O tratamento deverá ser realizado para fins específicos e informado ao titular; tratamento deve se limitar ao mínimo necessário para realizar suas finalidades; titular deve ter direito as modalidades de tratamento; informações claras sobre o tratamento; tratamento não pode ser realizado para fins discriminatórios; consentimento do usuário para tratamento de dados pessoais; finalidade específica do tratamento; forma e duração; identificação do responsável; informação do responsável; tratamento de dados é vedado quando o consentimento foi dado mediante erro, dolo, coação; transparência no tratamento; acesso as informações sobre coleta (finalidade forma, duração, informação de contato do responsável); mecanismo para o indivíduo se opor a coleta; vedado tratamento de dados sensíveis, salvo com consentimento do usuário; tratamento de dados de criança e incapaz mediante consentimento dos responsáveis. Proíbe a coleta de dados sensíveis, com ressalvas determinadas no Art. 11. Não são evidentes os termos dados de *cookies*, localização e tráfego. Menciona anonimização na coleta (BRASIL, 2016).
Canadá	PIPEDA	2000	Possui uma seção para coleta de dados. Informações a respeito da coleta; princípio da transparência; limitação da coleta; motivo da coleta (antes ou no momento); consentimento antes da coleta; coleta de endereços eletrônicos; coleta de dados em sistemas de informação; coleta de dados por meio de telecomunicações; especifica quando a coleta pode acontecer sem o consentimento do usuário. Aborda anonimização. Não é evidente os termos dados de localização, tráfego e *cookies* (CANADÁ, 2000).
	Privacy Act	1985	Possui uma seção para coleta de dados. Nenhuma informação pessoal deverá ser coleta por instituição governamental, sobre ressalva se estiver vinculada a alguma atividade. Não aborda anonimização na coleta. Não são evidentes os termos dados de localização, tráfego e *cookies* (CANADA, 1985).
Coréia do Sul	*Personal Information Protection Act* (PIPA)	2011	Possui uma seção para coleta de dados. A coleta deve ser mínima e de forma a justificar seus fins. Coleta é tratada como processamento. O processador de informações deve se esforçar para processar informações pessoais no anonimato, se possível. Consentimento para a coleta de dados. Informações sobre a coleta. O processador de informações pessoais não processará informações sensíveis, salvo

			exceções determinadas na lei. Limitação na instalação de dispositivos visuais de processamento de dados. Estabelecimento e Divulgação de Políticas de Privacidade para indicar as atividades com os dados. Proibido coletar dados de forma fraudenta, imprópria ou injusta. Titular de dados tem o direito de confirmar o processamento de dados; o direito de suspender o processamento de dados pessoais. Limitação no processamento de dados sensíveis. Não são evidentes os termos dados de localização, tráfego e *cookies*. Realizar anonimização quando possível (COREIA DO SUL, 2011).
	Act on promotion of information and communications network utilization and information protection, etc	2001	Possui uma seção para coleta de dados. Finalidade da coleta; restrições à coleta de dados sensíveis, propósito da coleta; consentimento sobre a coleta; pode revogar o consentimento dado a coleta de dados; Quando a coleta é de dados de criança o consentimento será dado pelo responsável; aborda proibições em relação à coleta de dados, como a coleta por meios fraudulentos. Coleta de dados por meio de instalação de programas no computador dos usuários (ex: *cookies*) deve ser por meio do consentimento informado. Não são evidentes os termos dados de localização e tráfego. Não é evidente anonimização na coleta (COREIA DO SUL, 2001).
	Law on the protection and use of location information	2005	Possui uma seção para coleta de dados. Provedor de informação de localização ou LBS deverá determinar taxas e condições relativas à coleta. Não pode coletar informação pessoal sem o consentimento do usuário, salvo exceções, tais como urgência de saúde. Aqueles que alugam dispositivos capazes de coletar dados devem notificar o usuário que o dispositivo coleta dados de localização. Se o provedor for coletar dados de localização, deverá especificar dados do provedor e obter o conhecimento informado; Propósito da coleta; O titular dos dados de localização pode pedir a qualquer momento o acesso para suspender a coleta de dados de localização. Não aborda anonimização. Não é evidente os termos dados tráfego e *cookies* (COREIA DO SUL, 2005).
Estados Unidos	*Privacy Act* de 1974	1974	Deve haver informação sobre a coleta que relate o propósito da coleta da informação pessoal; obtendo do indivíduo o consentimento informado sobre essa atividade, minimização da coleta. Não são evidentes os termos dados de localização, tráfego e cookie. Não é mencionada anonimização de dados (ESTADOS UNIDOS, 1974).
	Fair Credit Reporting Act	1974	Consentimento do consumidor de forma oral ou escrita, antes da coleta de qualquer informação. Não são evidentes os termos dados de localização, tráfego e cookie. Não menciona anonimização na coleta (FEDERAL TRADE COMMISSION, 2016).
	FERPA	1974	Dados coletados devem ser protegidos de modo a não permitir a identificação pessoal do indivíduo, não apresenta foco em relação à coleta. Diretrizes para a proteção em relação ao acesso por terceiros e para a exclusão de dados quando não forem mais necessários. Não são evidentes os termos dados de localização, tráfego e cookie. Não aborda anonimização (ELECTRONIC CODE OF FEDERAL REGULATIONS, 2018).
	HIPAA	1996	Não explícito. O foco principal da HIPAA é a definição de medidas para a disponibilização de dados de saúde. Não são evidentes os termos dados

			de localização, tráfego e cookie. Anonimização de dados (HEALTH & HUMAN SERVICES, 2012).
	COPPA	1998	Possui uma seção para coleta de dados. Proibido coletar dados de criança sem o consentimento dos pais; coleta está vinculada ao consentimento dos pais; informações sobre os tipos de dados coletados. Não aborda anonimização na coleta de dados. Não são evidentes os termos dados de localização, tráfego e *cookies* (FEDERAL TRADE COMMISSION, 1998a).
Hong Kong	*Chapter 486 Personal Data (PRIVACY) Ordinance*	1996	Possui uma seção para coleta de dados. A coleta de dados pessoais deve ser lícita, justa e não excessiva. Detentor de dados deve fornecer ao titular de dados informações sobre a coleta de dados pessoais. O consentimento do titular se faz necessário se a utilização não estiver de acordo com o propósito inicial especificado. Consentimento pode ser escrito ou on-line, aborda atividade para menores e pessoas incapacitadas. Não são evidentes os termos dados de tráfego e cookie. Menciona coleta de dados de localização e não menciona anonimização (HONG KONG, 1996).
Noruega	*Lov om behandling av personopplysninger (personopplysningsloven)*	2018*	Coleta por videovigilância, trata a coleta como processamento de dados. Aborda sobre processamento de dados sensíveis; processamento de informações de saúde; Não é explícito dados de *cookies*, localização, tráfego e anonimização de dados (NORUEGA, 2018).
	Lov om elektronisk kommunikasjon	2003	Aborda a coleta de *cookies*, dados de localização e dados de tráfego. Em relação à coleta de *cookies*, regula a necessidade de consentimento informado. Menciona dados de cookie, tráfego e localização. Anonimização na recuperação (NORUEGA, 2003).
Reino Unido	*Data Protection Act 2018*	2018	A coleta de dados pessoais deve ser especifica explícita e legítima, e os dados pessoais devem ser coletados de forma que não seja incompatível com o propósito para o qual foi coletado; dados pessoais coletados para fins de aplicação da lei podem ser processados desde que o detentor esteja autorizado por lei e o tratamento é necessário; controlador pode criar logs de coleta; deve ser especificada a finalidade da coleta. Consentimento emerge em todas as situações no contexto de processamento (coleta) de dados. Não são evidentes os termos dados de tráfego e cookie. Menciona coleta de dados de localização. Aborda anonimização, tratada como *de-identification* (REINO UNIDO, 2018).
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	2003	Notificação sobre a coleta de dados; consentimento para a coleta de dados. Aborda diretrizes em relação a dados de localização e tráfego, no entanto, menciona atividade de processamento para esses. Não aborda anonimização e não é evidente o termo dados de cookie dados (REINO UNIDO, 2003).
Suíça	*Federal Act on Data Protection* (FADP)	2017	Possui uma seção para coleta de dados. A coleta de dados pessoais deve ser evidente; controlador de dados deve informar a coleta de dados pessoais. Obter informação como identidade do controlador e informação de contato; A coleta de dados também é mencionada como processamento. O consentimento para processamento de dados sensíveis (coleta). Informações para o titular sobre a coleta de dados sensíveis. Se os dados coletados não forem da pessoa em causa, o titular deve ser informado. Não são evidentes os termos dados de localização, tráfego e cookie. Aborda anonimização (SUÍÇA, 2017).
Alemanha	*Federal Data Protection Act 2017*	2017*	Notificação sobre a coleta; dados devem ser coletados para um fim específico, de forma legal e

				justa; Coleta reduzida com mínimo de dados pessoais. Dados pessoais podem ser processados para fins de científicos de acordo com as garantias para o usuário. Aborda sobre processamento de dados de empregado. Titular deve ser informado a respeito do processamento. Se processar dados sensíveis deve obter o consentimento do usuário. Garantir que a coleta de dados pessoais para diferentes propósitos seja processada separadamente; Aborda sobre coleta por meios de videovigilância. Não são evidentes os termos dados de localização, tráfego e cookie. Aborda anonimização para processamento (ALEMANHA, 2017).
		Telemedia Act TMA	2007	Prestador de serviço pode coletar dados pessoais somente para habilitar e faturar serviços. Não são evidentes os termos dados de localização e cookie. Menciona coleta de dados de tráfego e anonimização na recuperação (ALEMANHA, 2007).
Países União Europeia	**Áustria**	*Data Protection Act*	1999*	Coleta definida como tratamento. Dados devem ser coletados para fins específicos, explícitos e legítimos; titular deve estar na posse da informação. Não é permitido gravar imagem ou dados acústicos na esfera mais privada do titular dos dados sem o consentimento explícito do titular. Quando dados não são coletados do titular ele deve ter notificação da coleta no momento da coleta. Deve ser processados somente com o consentimento do usuário. Tratamento de dados sensíveis só quando necessário. Não são evidentes os termos dados de localização, tráfego e cookie. Aborda anonimização na fase de recuperação (ÁUSTRIA, 1999).
		Austrian Telecommunications Act	2003	Notificação da coleta; consentimento do usuário; Dados de localização e de tráfego não poderão ser interceptados ou monitorados ou transmitidos sem o consentimento do titular dos dados. Não é evidente o termo dado de cookie. Aborda anonimização (ÁUSTRIA, 2003).
	Bélgica	*Data Protection Authority (DPA)*	1992*	Os dados devem ser coletados para fins específicos, explícitos e legítimos, e não excessivos em relação aos fins para quais foram coletados. Dados de saúde só podem ser coletados da pessoa em causa. A coleta é mencionada também como processamento. Quando houver a coleta para fins de marketing direto o usuário pode opor-se ao tratamento; Os dados pessoais só podem ser processados quando o titular dos dados der consentimento, for necessário para cumprir uma obrigação, proteger interesses do titular ou interesse público. Proibido processamento de dados sensíveis, salvo as exceções expressas na lei. Se os dados pessoais não forem coletados do titular, o responsável deve disponibilizar nome e endereço do controlador, propósito do processamento, existência do direito de oposição e outras informações adicionais. Não são evidentes os termos dados de localização, tráfego e cookie. Não é evidente anonimização (BÉLGICA, 1992).
		Loi relative aux communications électroniques	2005	Não aborda coleta de dados, as questões vinculadas a dados de tráfego e localização são determinadas como tratamento, e neste caso, especifica que: o titular deve ter informação sobre os objetivos do tratamento, a possibilidade de retirar o consentimento para o tratamento de dados de localização e dados de tráfego. Não é evidente o termo dados de cookie. Aborda anonimização no tratamento (BÉLGICA, 2005).

	Espanha	*Ley Orgánica*	*1999***	Possui uma seção para coleta de dados. Os dados pessoais só podem ser coletados quando for apropriado, relevante e não excessivo quanto à finalidade. Proibida a coleta de dados por meios fraudulentos, injustos ou ilegais, sendo que são consideradas infrações muito sérias. Direito a informação sobre a coleta de dados; A coleta para fins de segurança é permitida sem o consentimento do titular. Não são evidentes os termos dados de localização, tráfego e cookie. Não aborda anonimização (ESPANHA, 1999).
		Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.	2002	Titular tem o direito de se opor ao tratamento no momento da coleta dos dados. Não são evidentes os termos dados de localização e cookie. Menciona o termo dados de tráfego. Não aborda anonimização (ESPANHA, 2002).
	França	*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*	1978*	Coleta é mencionada como atividade de tratamento. Dados pessoais são coletados para fins específicos e explícitos; a coleta de dados não deve ser excessiva. Dados devem ser coletados de maneira justa e lícita, para fins específicos, explícitos e legítimos. É proibido coletar ou processar dados pessoais considerados sensíveis. Notificação a respeito da coleta. Consentimento do usuário para a coleta de dados de serviços de certificação de assinaturas eletrônicas e para coleta de amostras biológicas identificáveis; dados devem ser coletados diretamente do titular. Não são evidentes os termos dados de localização, tráfego e cookie. Menciona anonimização, mas não fica explícito se é na coleta de dados (FRANÇA, 2018).
	Holanda	*Dutch Personal Data Protection Act (Wbp)* Lei de Implantação	2018*	Regulamento (UE) 2016/679
		Telecommunications Act	2012	Dados pessoais só poderão ser coletados para fins diferentes a menos que o titular tenha dado o consentimento. Não é evidente o termo dados de cookie. Menciona dados de localização e tráfego. Menciona anonimização, na fase de recuperação (HOLANDA, 2012).
	Irlanda	*Data Protection Act 2018*	2018*	Trata a coleta como tratamento de dados. O tratamento será permitido quando for diferente do motivo da coleta em situações de segurança nacional ou para fins de investigação. Os dados serão recolhidos para um ou mais dados especificados, explícitos e é incompatível com tais propósitos; Dados coletados pelo detentor para fins de arquivamento de interesse público, fins de investigação científica ou estatística desde que regras e ofereça garantias para o titular dos dados. Aborda proteção de dados por *design* e por *default*. Quando o detentor realiza processamento por meio automatizado, pode criar um registro de *log* quando na coleta de dados pessoais. Indica regulamento para o processamento de várias finalidades (saúde, fins de saúde, pesquisa, relativos a crimes). Consentimento do titular para processamento de seus dados pessoais. Não são evidentes os termos dados de localização, tráfego e *cookie*. Menciona anonimização, mas não fica explícito se é na coleta de dados (IRLANDA, 2018).
	Itália	Legislative Decree no. 196 of 30 June 2003. *Garante per la Protezione dei Dati Personale*	2003**	Possui uma seção para coleta de dados. Os dados deverão ser coletados para fins específicos, explícitos e legítimos, informando a coleta de dados. O titular dos dados deverá ter informação oral ou escrita sobre finalidades e modalidades de

				processamento; dados sensíveis e judiciais serão coletados da pessoa em causa. Entidades privadas incluídas no Sistema Estatístico Nacional devem coletar dados sensíveis para fins estatísticos em formato anônimo. Consentimento escrito para coleta de dados sensíveis. Não é evidente dados de *cookies*. Menciona dados localização e tráfego. Aborda anonimização (ITÁLIA, 2003).
	Portugal	Lei da Protecção de Dados Pessoais (Lei nº 67/68)	1998**	Coleta de dados é mencionada também como tratamento. Ter informações a respeito da coleta e finalidade da coleta. Os dados devem ser coletados e tratados para fins determinados; o tratamento de dados só poderá ser realizado mediante consentimento. Proibido o tratamento de dados sensíveis (ressalva quando houver interesse público; medicina preventiva, ou tiver consentimento do titular); Informação sobre a coleta de dados em redes abertas. A lei aplica-se a coleta por videovigilância. Não são evidentes os termos dados de tráfego e cookie. Não menciona anonimização e dados de localização (PORTUGAL, 1998).
		Lei n.º 41/2004, de 18 de Agosto. Protecção de dados pessoais e privacidade nas telecomunicações	2004	Proibida a escuta, instalação de dispositivo de escuta ou outros meios de vigilância dos dados de tráfego por terceiros sem consentimento prévio e expresso dos usuários. Acesso a dados no equipamento do usuário somente com o consentimento prévio e por meio de informações claras e completas, salvo para possibilitar a comunicação. Permitido o registro de dados de localização quando ocorrer necessidade de emergência Menciona dados de *cookies*, tráfego e localização. Aborda anonimização (PORTUGAL, 2004).
	Polônia	*ACT of August 29, 1997 on the Protection of Personal Data*	1997**	Quando coletado dados do titular, o responsável pelo tratamento é obrigado a fornecer ao titular: endereço de sua sede ou residência e seu nome completo; propósito da coleta. Essas medidas também são válidas no caso dos dados não terem sido obtidos do titular. Deve ser garantido que os dados sejam coletados para fins específicos e legítimos. O titular deve ter informações sobre as formas e meios de coleta de dados. A coleta é tratada também como processamento. O processamento só é permitido mediante consentimento do titular. Consentimento por escrito para dados sensíveis (não cita a palavra sensível), coloca dados de religião, políticos e raça. Não são evidentes os termos dados de localização, tráfego e cookie. Menciona anonimização. (POLÔNIA, 1997).
		Telecommunications Act of 16 July 2004	2004 (NT)	A coleta de dados confidenciais será realizada somente se for necessária para o oferecimento do serviço. Trata a coleta como processamento. Antes de dar o consentimento o usuário deverá ter informações sobre os dados que serão coletados, ouvida, interceptada ou objeto de vigilância. Não é evidente o termo dados de cookie. Menciona dados de localização e tráfego. Menciona anonimização, na fase de recuperação (POLONIA, 2004).
	Suécia	Lei (2018:218) com disposições adicionais à Portaria de dados da EU	2018*	Regulamento (UE) 2016/679 - Informações sobre a coleta, exigindo que as informações relacionadas à coleta sejam de fácil acesso e compreensão e formulada em uma linguagem simples; Finalidade da coleta; minimização da coleta; consentimento sobre a coleta; consentimento para coleta de dados de criança; alerta sobre os riscos da coleta; informações sobre o tratamento no momento da coleta; a lei não se aplica ao processamento de dados pessoais que ocorra para fins jornalísticos ou para fins

				acadêmicos, artísticos. Regulamenta o consentimento para o processamento de dados de criança quando ela tiver 13 anos, senão necessita do consentimento informado (SUÉCIA, 2018).
Europa		*e-Privacy*	2009	Aborda sobre a coleta de dados provenientes de equipamentos de usuários, sendo permitida para assegurar a transmissão de uma comunicação eletrônica, e quando o titular deu o consentimento necessário para execução do serviço. Aborda dados de localização, *cookies*, tráfego e anonimização de dados. Pseudoanonimização (EUROPA, 2009).
		Regulamento (UE) 2016/679	2016	Proteção específica à coleta de dados de criança; As finalidades do tratamento deverão ser explícitas e legítimas na coleta dos dados; Informações sobre a coleta de dados pessoais junto ao titular; O titular deverá ter o acesso a dados coletados sobre ele; Informações sobre a coleta de dados pessoais quando não foram obtidos junto ao titular; Dados deverão ser coletados para fins específicos, explícitos e legítimos. O controlador deverá implementar medidas técnicas para garantir que apenas serão coletados dados necessários (minimização de dados). Não traz diretrizes para dados de *cookies*, tráfego e localização. Menciona pseudoanonimização no tratamento dos dados.
Europa/EUA		EU-U.S *Privacy Shield*	2016	Aviso sobre coleta indicando os tipos de dados pessoais que será coletado, justificativa sobre uso e coleta dos dados. A coleta também é abordada como processamento. Consentimento informado para o processamento de dados sensíveis; limitação da coleta. Não é evidente o termo dados de cookie, dados de localização e tráfego. Menciona anonimização. (PRIVACY SHIELD, 201-a; PRIVACY SHIELD, 201-b).
Suíça /EUA		*Swiss-U.S. Privacy Shield*	2017	

Fonte: Elaborado pela autora

Mediante os dados relatados no Quadro 14, observa-se que as determinações para a coleta de dados não estão expressas na HIPPA dos Estados Unidos, cuja finalidade é a segurança dos dados armazenados, tais como o controle de acesso e as garantias quanto à proteção de dados sensíveis. Para tanto, a HIPPA indica os dados que devem ser removidos para que não ocorra a reidentificação dos sujeitos referenciados nos conjuntos de dados. Assim, o foco da HIPPA não são as questões vinculadas à coleta de dados, o que justifica a ausência de diretrizes relacionadas especificamente à coleta de dados.

Na Lei nº 7.232/1984 (Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação) não apresenta menção à coleta de dados pessoais, pois o foco são as questões em relação ao armazenamento, direitos ao acesso e à alteração de dados. A Lei 9.507/1997 (*Habeas data*) também não abarca a coleta de dados, a determinação é em relação ao conhecimento e à possibilidade de alterar dados armazenados. A Lei nº 8.078/1990 (Código de Defesa do Consumidor) não regulamenta questões vinculadas à coleta de dados de indivíduos, as diretrizes da lei estão relacionadas os dados de consumidores presente em bancos

de dados e sobre o acesso e a alteração de dados em cadastros e registros, a ênfase é no acesso realizado pelo titular.

Na Lei 12.737/2012 (Lei Carolina Dickemann), o cerne é a regulamentação para os aspectos envolvidos a invasão de dispositivos, que determina instruções legais para casos em que terceiros têm acesso, sem autorização, a dados confidenciais dos titulares desses dispositivos, não é evidente a menção sobre a coleta de dados na relação titular-detentor.

A Lei 12.527 (Lei de acesso à informação) também não relata a coleta de dados, pois sua finalidade é determinar diretrizes para o acesso à informação pela sociedade, desta forma, o objetivo não é a proteção em relação a dados que são coletados de indivíduos, porém, a efetuação da proteção de dados nos aspectos de disponibilização.

A coleta de dados também não é abordada na Lei nº 12.414/2011 (Cadastro Positivo) cujo objetivo é regular o acesso às informações de inadimplência pelo cadastrado, inclusive dados históricos. Do mesmo modo, a Lei 9.472/1997 (Lei das Telecomunicações) não versa a coleta de dados, uma vez que a proteção de dados pessoais é apontada em relação ao segredo e à inviolabilidade das comunicações, o cerne da lei é a intercepção por terceiros.

O PL 6.291/2016 (que altera o Marco Civil) não menciona a coleta de dados, suas diretrizes são para proibição do compartilhamento de dados pessoais em ambientes da Internet. O PLS 131/2013, por sua vez, dispõe a respeito do fluxo de dados de indivíduos para o governo ou o tribunal estrangeiro, não apresentando explicitamente regulamento referente à coleta de dados.

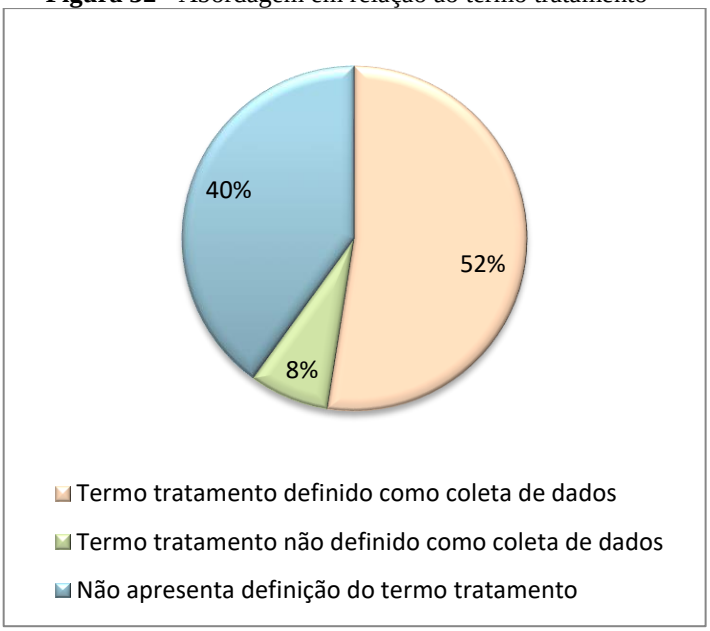
Ainda que questões vinculadas à coleta de dados não são mencionadas em algumas leis, essas representam a minoria. A menção à coleta de dados se efetua em muitas leis e regulamentos mediante determinações para prover informações claras sobre a coleta, motivo, e minimização da coleta de dados.

No entanto, mesmo que essas questões estejam presentes nas legislações, alguns pontos quando não especificados detalhadamente podem propiciar displicências em relação à proteção de dados pessoais no momento da coleta de dados, principalmente no que tange as questões tecnológicas, uma vez que, conforme citado por Sant'Ana (2016, p.124) "cada procedimento de coleta pode ter suas configurações próprias", assim, carecem ser especificadas exclusivamente e detalhadamente, pois, essa atividade na díade indivíduo-detentor é uma relação que é capaz de ocasionar diversas quebras de privacidade e impactar em outras fases do ciclo de vida dos dados.

Um dos pontos que merece destaque é a terminologia utilizada nas legislações, que muitas vezes utilizam de um conceito unitário para representar um conjunto de atividades ou

elementos, tal como o termo “tratamento”, que é utilizado como a referência a várias atividades envolvidas com dados, tais como coleta, armazenamento, consulta e divulgação, situação representada em 21 dos documentos jurídicos analisados (52%). Essa generalização do termo tratamento pode dificultar a identificação e execução de diretrizes específicas para a fase de coleta de dados. Ressalta-se que em 3 documentos (8%) o termo tratamento não é utilizado da forma supracitada (Figura 32).

Figura 32 - Abordagem em relação ao termo tratamento[88]



Fonte: Elaborada pela autora

O uso do termo tratamento como um conceito unitário ocorre principalmente nas leis específicas para proteção de dados pessoais dos países da União Europeia, devido à aderência a Diretiva 95/46/CE do Parlamento Europeu e recentemente ao Regulamento (UE) 2016/679 que define tratamento de dados pessoais como:

> Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a exclusão ou a destruição (UNIÃO EUROPEIA, 2016, p. 33).

[88] Para esses resultados foram consideradas apenas as leis e projetos de leis que mencionaram coleta de dados. Não foram considerados os regulamentos.

Embora o Regulamento (UE) 2016/679 trate a coleta inserida no termo tratamento, também realiza menções dispersas durante o texto, o que pode confundir as determinações específicas para a coleta.

O PL nº 4.060 do Brasil também define tratamento como "toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita o armazenamento, ordenamento, conservação, atualização, comparação, avaliação, organização, seleção, extração de dados pessoais" (BRASIL, 2012b, online), envolvendo várias atividades para o mesmo termo.

Em relação à menção a coleta de dados pelas leis, observou-se que 30%[89] dos documentos tratam às questões da coleta de dados pessoais em seções específicas, assim, as diretrizes relacionadas à coleta emergem em seções como: coleta de informação pessoal, limitação da coleta; coleta de dados em equipamentos de usuários finais e direito a informação sobre a coleta. Dentre os países representados nas leis estão: Austrália (*Privacy Act*/1998*)*, Canadá (*Privacy Act*/1995 *e a* PIPEDA/2000), Coreia do Sul (PIPA/2011; *Act on the Protection, use, etc. of Location Information*/2005 e; *Network Utilization and Information Protection*, etc/2001), Estados Unidos (COPPA/1998), Espanha (*Ley Orgánica* 15/1999), Itália (*ACT of the Protection of Personal Data/1997*), Suíça (*Federal Act on Data Protection/1992)* e Hong Kong (*Chapter 486 Personal Data (PRIVACY) Ordinance/1996)* e o Brasil (PLS nº 330/2013).

Ressalta-se que dentre os documentos que abarcam a coleta como uma atividade do tratamento, 23,8% dessas legislações também incluem uma seção específica para abordar os fatores envolvidos com a coleta de dados, assim, nas legislações aparecem tanto o termo tratamento quanto o termo coleta, tornando a distinção confusa e, consequentemente, podendo impactar na aplicação dessas leis pelos detentores de dados.

Por meio da análise dos documentos jurídicos foi possível identificar à presença de elementos vinculados as questões de proteção de dados pessoais com aderência às tecnologias, tais como o consentimento sobre as atividades vinculadas aos dados, anonimização, tipos de dados (localização, tráfego, *cookies*).

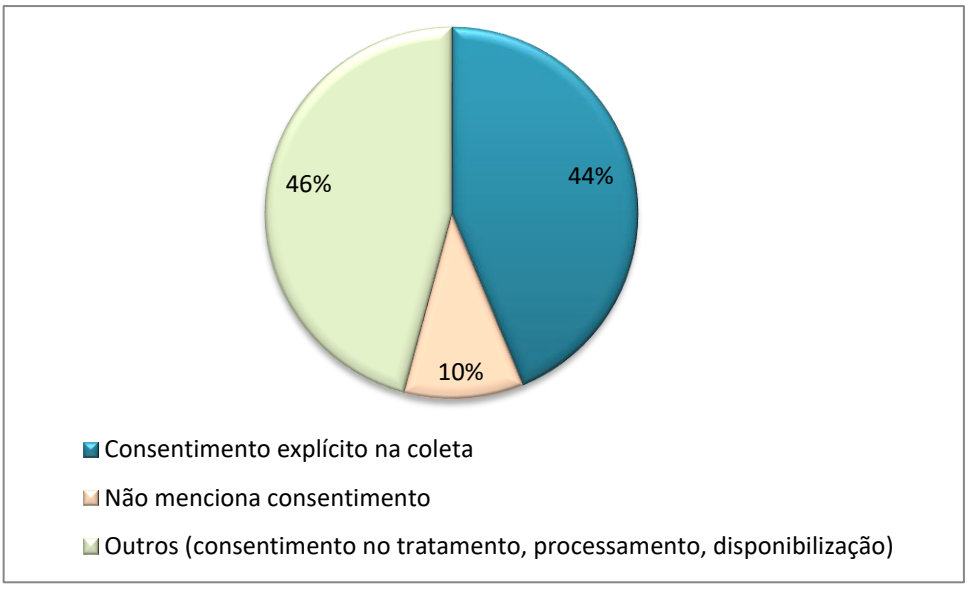
Nesse contexto, resgata-se a Lei nº 12.965/2014 (Marco Civil da Internet) que estabelece os direitos dos indivíduos referentes ao consentimento para coleta de seus dados e às informações sobre essa atividade. Desta forma, diretrizes em relação à coleta de dados e consentimento pelo titular ficam explícitas no Art. 7, inciso IX, que determina que o titular dos

[89] Para esses resultados foram consideradas apenas as leis e projetos de leis que mencionaram coleta de dados. Não foram considerados os regulamentos.

dados tenha o direito a estabelecer o "consentimento expresso sobre a coleta, uso, armazenamento e tratamento de dados pessoais [...]" (BRASIL, 2014c).

O consentimento informado pelo usuário é termo recorrente na maioria dos documentos jurídicos (Figura 33), uma vez que, esses dispõem sobre aspectos vinculados à proteção de dados pessoais. A menção ao consentimento especificamente na fase de coleta é explícita em 44% dos documentos (21 legislações), e o consentimento para a disponibilização e tratamento de dados, incluindo o consentimento do responsável para atividades com dados infantis, estão presentes em 22 legislações (46%). A Figura 33 demostra também que 5 documentos jurídicos analisados (10%) não mencionaram a necessidade do consentimento por parte do titular dos dados, ocorrências nas seguintes leis: Lei nº 7.232/1984 (Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação); 9.472/1997 (Lei Geral das Telecomunicações); Lei Nº 9.507/1997 (*Habeas Data*); Lei nº 8.078/1990 (Código de Defesa do Consumidor) e Lei 12.737/2012 (Lei Carolina Dickemann).

Figura 33 - Menção ao consentimento [90]



Fonte: Elaborado pela autora

Embora o termo consentimento seja recorrente na maioria das legislações, totalizando 90% dos documentos analisados, a abordagem tem se efetuado em muitas legislações de forma generalizada. Por exemplo, a Lei 12.965/2014 determina no Art. 7, inciso IX do Capítulo II (Direitos e Garantias dos usuários), que o "usuário tem o direito ao consentimento expresso

[90] Para esses resultados foram consideradas apenas as leis e projetos de leis. Não foram considerados os regulamentos.

sobre coleta, uso, armazenamento e tratamento de dados pessoais [...]" (BRASIL, 2014c), essa é a única menção ao consentimento em relação à coleta de dados do titular no decorrer da lei.

A generalização dos aspectos vinculados à coleta de dados também é perceptível no PL nº 4.060, no qual apresenta no Art. 17 à necessidade do consentimento no âmbito do tratamento de dados pessoais de crianças, e que essa atividade somente será possível mediante o consentimento dos pais ou responsáveis (BRASIL, 2012b). O consentimento mencionado no PL nº 4.060 é regulado para tratamento de dados infantis, no entanto, não é explícita a necessidade de consentimento na fase de coleta.

Caso semelhante pode ser observado na *Act of the Protection, Use, etc, of Location Information* da Coréia do Sul, que também aborda o consentimento modo genérico, apenas regulamentando que o titular deverá dar consentimento para a coleta de dados. A Ley 34/2002 da Espanha (*Servicios de la sociedade de la información y de comercio electrónico*) não abarca nas terminologias a coleta e o tratamento de dados, no entanto, discorre por toda a lei sobre tratamento e a necessidade do consentimento sobre essa atividade, podendo deixar dúvidas sobre a necessidade de execução dessa atividade na fase de coleta.

Sob outra perspectiva, existem leis que detalham o consentimento quando requerido na fase de coleta de dados, tais como a PIPEDA do Canadá. Esta lei dispõe na Cláusula 6.1 regulamentações sobre a validade do consentimento, determinando que seja necessário que o indivíduo entenda a natureza da coleta, assim como o motivo, as consequências e a possível divulgação desses dados, inclusive sobre a necessidade de as organizações identificarem quais são os dados sensíveis que irão compor o formulário de consentimento. Ainda, na Cláusula 7 da PIPEDA é indicado regulamentações para explicitar quando o consentimento não é necessário na fase de coleta, e, no Princípio 3, aborda como deverá ser o meio do consentimento (formulário de solicitação, caixa de verificação, oral por telefone, no uso do produto ou serviço).

O Regulamento (UE) 2016/679 determina que o consentimento deva ocorrer mediante declaração escrita, inclusive em formato eletrônico ou declaração oral. Ainda, detalha que o consentimento pode ser dado validando uma opção ao visitar um site ou por meio de conduta que indique claramente que o titular aceita o tratamento proposto com os dados pessoais. Nas diretrizes, o Regulamento (UE) 2016/679 também evidencia que caso o tratamento sirva a vários fins, deverá ser realizado um consentimento para cada serviço. Regula também na consideração 32 que quando o consentimento for solicitado durante um serviço eletrônico, ele deve ser claro e conciso, e não pode atrapalhar a utilização do serviço. No Art. 7. do presente regulamento é determinado as condições aplicáveis ao consentimento e, no Art. 8 as condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação.

No Regulamento (UE) 2016/679 ao abordar o consentimento na coleta de dados em sites Web, regulamenta que o silêncio, a pré-validação ou a omissão não deverão configurar-se como consentimento, delimitando nas suas regulamentações questões específicas sobre o consentimento. Ressalta-se que a menção ao consentimento na fase de coleta fica nítida apenas no contexto de interação com sites, durante o regulamento essa medida é mencionada em relação ao tratamento de dados.

Reflexo da implementação do Regulamento (UE) 2016/679 pode ser observado na *Federal Data Protection Act* 2017 da Alemanha, em conformidade com o novo regulamento, ao mencionar o consentimento para o tratamento de dados de funcionários, regula que essa atividade deverá ser realizada por escrito, inclusive com informações para o indivíduo retirar o seu consentimento quando julgar necessário.

A EU-U.S *Privacy Shield* e a *Swiss-U.S. Privacy Shield* descreve aspectos em relação à aplicação do aviso e consentimento (princípio de escolha) e estabelece que no aviso sobre a coleta de dados deve incluir explicação de como os dados podem ser utilizados em atividades de pesquisa médica ou farmacêutica, especificando nesse caso, a medida do consentimento para o setor da saúde.

Svensson e Advokatbyrå (2018, p. 6) relatam sobre essa carência de informações ao explanar sobre a Lei de Proteção de Dados da Suécia, principalmente em relação aos tipos de consentimento informado, assim, o autor afirma "não há exigência formal de consentimento. Como o ônus da prova, é aconselhável obter consentimento por escrito" [91].

A falta de especificidade nas leis pode ocasionar dificuldades durante a interpretação, por exemplo, a *Ley Orgânica* 15/1999 da Espanha determina que provedores de serviços, como os da Internet, podem usar meios de armazenamento e recuperação de dados no equipamento de usuários, desde que esses tenham dado consentimento, pois, os usuários devem receber informações claras e completas sobre o uso e propósito do tratamento. A presente determinação ao indicar o consentimento para recuperação dos dados no equipamento do usuário pode estar se referindo ao uso de *cookies* ou mecanismos similares, no entanto, não se torna explícito as possíveis tecnologias que estão envolvidas, fato que pode levar a insciência de quando esse consentimento deva ser aplicado.

Fato que ocorre também na *Telecommunications Act/2012* da Holanda, pois não define nas suas terminologias coleta e nenhum outro termo que faça referência a essa atividade, e no decorrer do texto, aborda questões em relação ao processamento de dados de localização e

[91] there is no formal requirement on how consent should be obtained. As the burden of proof for showing that valid consent has been obtained lies with the data controller, it is advisable to obtain consent in written form

dados de tráfego, tornando-se complexo distinguir quais são as regulamentações específicas para a coleta de dados e quais são para o processamento.

Observou-se que não há distinção de dados e de metadados de comunicação na maioria das leis de proteção de dados. Esses elementos deveriam ser evidenciados particularmente, pois cada um tem suas peculiaridades no âmbito da proteção de dados, como também a coleta de dados por *fingerprinting*, técnica que viola a privacidade de forma muito mais invasiva do que o próprio conteúdo semântico da interação com os ambientes digitais, no entanto, também não termos em destaque.

Nesse cenário, observou-se que a menção explícita aos dados de tráfego se efetua em 23% dos documentos analisados, tal como na Lei nº 12.965 do Brasil, que evidencia tanto a coleta de dados de tráfego quanto à proibição de fornecer a terceiros registros de conexão. No entanto, a presença desse tipo de dado prevalece nas leis de comunicação, dentre elas a *Telemedia Act TMA* da Alemanha; *Loi relative aux communications électroniques* da Bélgica e a *Austrian Telecommunications Act* da Áustria.

Os dados de localização, que podem identificar o indivíduo e ocasionar quebras de privacidade, aparecem em 25% das legislações, normalmente vinculados a ordenamentos específicos, tais como: *Act on the Protection, Use, etc. of Location Information* da Coréia do Sul; *Austrian Telecommunications Act* da Austrália, *Loi relative aux communications électroniques* da Bélgica, *Legislative Decree* no. 196 of 30 June 2003 da Itália; Lei n.º 41/2004 sobre Protecção de dados pessoais e a Lei da Protecção de Dados Pessoais (Lei nº 67/68) de Portugal; *Chapter 486 Personal Data (PRIVACY) Ordinance* de Kong Hong; e a The *Privacy and Electronic Communications* (EC Directive) *Regulations* 2003 e a *Data Protection Act* 2018 do Reino Unido.

O termo *cookies*, que está totalmente vinculado à coleta de dados e a quebras de privacidade, está presente em 6% das legislações, especificamente na *Act on Promotion of Information and Communications* da Coréia do Sul, na Lei n.º 41/2004 sobre Protecção de Dados Pessoais e Privacidade nas Telecomunicações de Portugal e a *Lov om elektronisk kommunikasjon* da Noruega. Ressalta-se que das leis que não mencionam o termo *cookies*, 31% são de leis/projetos do Brasil.

Medidas para promover a proteção de dados pessoais estão presentes similarmente nas legislações, que além do consentimento informado, exposto na maioria dos regulamentos e leis, surge a anonimização, pseudoanonimização ou de-identificação em 42% dos regulamentos analisados, tais como a *Privacy Act* 1988 da Austrália, na PIPEDA do Canadá, e no PL 5.276/2016 do Brasil.

A terminologia para anonimização é tratada de forma diferente nas leis e regulamentos, por exemplo, no Regulamento (UE) 2016/679 é mencionado a pseudoanonimização, já o PL 330 do Brasil utiliza o termo dissociação de dados[92], enquanto que na recente *Data Protection Act 2018 do* Reino Unido, o termo emerge como de-identificação.

Embora a anonimização como meio para proteger dados pessoais esteja presente em algumas leis, ela é mencionada timidamente, de modo genérico, pois, não é evidente na maioria das legislações que essa atividade deva se efetuar na fase de coleta, notou-se que a anonimização para a coleta de dados está explícita em 4% das legislações, sendo a *Privacy Act* da Austrália e o PL 5.276/2016 do Brasil. Assim, observa-se que as preocupações com a proteção de dados mediante a anonimização se acentuam na fase de recuperação de dados, conforme explicitado nos relatos a seguir:

No Art. 18 da Lei de Proteção de Dados da Polônia, o qual determina que caso haja violação a proteção de dados, o inspetor geral ordenará que se aplique medidas adicionais para proteger os dados coletados, no entanto, não se pronuncia sobre medidas para impedir a quebra de privacidade no momento da coleta. Ainda, o Art. 36 ordena que o responsável pelo tratamento seja obrigado a implementar medidas técnicas para proteger dados pessoais processados e, em especial a proteção contra a divulgação de dados não autorizada, o que torna evidente a ênfase na proteção de dados no âmbito da disponibilização e não na fase de coleta.

Da mesma forma, a *Federal Act o Data Protection* da Suíça ao abordar questões de segurança, menciona que os dados devem ser protegidos principalmente contra destruição não autorizada, perda acidental, falsificação, roubo, uso ilegal, alteração não autorizada, cópia, acesso ou outro processamento não autorizado, deixando evidente a carência de proteção dos dados nas questões de coleta usuário-detentor.

Ao tratar diretrizes de segurança, a Portaria de Dados Pessoais, capítulo 486 das Leis de Hong Kong determina que o detentor de dados deve tomar todas as medidas possíveis para garantir que os dados pessoais sejam protegidos contra acesso não autorizado ou acidental, processamento, exclusão, perda ou utilização, entretanto, não aborda medidas a serem realizadas para garantir a segurança no momento da coleta titular-detentor.

Ao abordar a anonimização, a EU-U.S *Privacy Shield e a Swiss-U.S. Privacy Shield* determinam que essa medida é voltada para que dados de pesquisa farmacêutica e de outros fins

[92] Procedimento destinado a impedir a identificação da pessoa a que se refere à informação coletada, armazenada ou transmitida (BRASIL, 2013).
Disponível em: <https://www12.senado.leg.br/ecidadania/visualizacaomateria?id=113947>. Acesso em 2 jan. 2017.

não fiquem vulneráveis a quebra de privacidade. Nota-se que a anonimização é evidenciada no contexto da recuperação dos dados, e não na fase de coleta.

O termo de-identificação é abordado pela HIPAA, incluindo os riscos da combinação de semi-identificadores com outros dados, e orientações sobre as consequências do compartilhamento de dados sem os devidos cuidados, observa-se que, novamente, a regulamentação é voltada para a recuperação de dados e não na fase de coleta.

Devido à implantação do Regulamento (UE) 2016/679 muitas empresas estão atualizando suas políticas de privacidade, como é o caso da Microsoft, que ao abordar sobre dados de *cookies* evidencia que: "**alguns** dos *cookies* que geralmente usamos estão listados abaixo. Essa lista não é **abrangente**, mas pretende ilustrar os principais objetivos pelos quais geralmente colocamos *cookies*" (MICROSOFT, 2018, grifo nosso). No entanto, a empresa não especifica todos os *cookies* utilizados e também não é possível identificar quais dados serão realmente coletados da máquina do usuário. Destaca-se que ao conectar-se no site do mecanismo de busca, em momento algum é solicitado o consentimento para o uso de *cookies*, ainda, essa coleta depende da consciência e habilidade do usuário para desativar o uso de tais ferramentas. Assim, observa-se que, mesmo tentando especificar sobre os *cookies*, há pontos falhos, essa falta de clareza na política de privacidade pode contribuir para insciência do usuario na fase de coleta.

Ciente das principais legislações e regulamentos que abarcam a proteção de dados pessoais e uma explanação como a essas questões tem se efetuado na fase de coleta, explora-se na próxima seção como os julgados envolvidos com proteção de dados pessoais e o uso das tecnologias da informação tem se caracterizado na jurisprudência brasileira.

5.4.3 Proteção de dados pessoais: Casos concretos no cenário nacional

A consolidação do Marco Civil da Internet (Lei nº 12.965/2014) deu amparo a muitas situações vinculadas a privacidade do indivíduo no domínio do uso das tecnologias da informação. Para relatar as principais questões vinculadas a proteção de dados pessoais na jurisprudência brasileira, utilizou-se das informações disponibilizadas no site Observatório do Marco Civil da Internet, realizando uma filtragem das jurisprudências por meio dos temas "Privacidade" e "Dados pessoais". Essa busca recuperou 59 casos que julgaram questões de privacidade vinculadas à tecnologia da informação e proteção de dados pessoais (Apêndice D). Ressalta-se que esses julgados ocorreram no período de 2014 a 2018.

Observou-se nos julgados que compôs o corpus dessa análise, que os casos nos quais o usuário é alvo de fases de coleta de dados, sobre ação dos detentores desses dados coletados, emergem em decisões isoladas, especificamente em três julgados, relatados a seguir.

Ação Civil Pública que versa sobre a coleta de dados realizada pela Microsoft por meio do sistema operacional Windows 10, julgada no dia 27/04/2018 pela 9ª Vara Cível Federal de São Paulo – SP, cuja relatora foi a juíza federal Cristiane Farias Rodrigues dos Santos. O autor da ação, no caso, o Ministério Público Federal, exige que a empresa adote medidas para garantir que quando o usuário não autorize o uso de seus dados pela Microsoft, a ferramenta utilizada para dar consentimento seja simples e fácil de utilizar.

> [...] Embora o autor sustente que tal ocorra, ou seja, a coleta de dados, com eventual partilha de informações, mesmo na hipótese de não concordância da coleta de dados pelo usuário, tal fato é contestado pela empresa, **não sendo** possível, igualmente, ao Juízo, em sede de cognição sumária, formular juízo acerca de fatos que necessitam de esclarecimentos técnicos e operacionais [...] Ante o exposto, considerado o que foi exposto, DEFIRO em parte, e, em menor extensão, a tutela antecipada requerida, para determinar que a Microsoft adote procedimentos específicos, no prazo de 30 (trinta) dias, de modo a permitir que o usuário do sistema operacional Windows 10, em caso de não autorizar o uso de seus dados, tenha ferramenta operacional e de interface que permita o exercício de tal opção de forma simples, fácil e direta, tanto quanto a interface operacional que permite a atualização do sistema com a autorização da coleta de dados do usuário (BRASIL, 2018c, p. 13).

O autor ainda relata que "durante a instalação e atualização do sistema operacional, a Microsoft apresenta como **opção padrão a ativação dessa coleta massiva de dados"** (BRASIL, 2018c, p. 2, grifo nosso), isso demonstra o problema de configurações padrões para o controle sobre a coleta de dados, que faz com que o usuário não tenha consciência dos dados coleta e das suas escolhas.

Outra situação envolvendo coleta de dados é o caso julgado pelo Tribunal Regional Federal da Primeira Região - 2ª Vara Federal – Teresina - PI no dia 29/01/2018, cuja autoria foi o Ministério Público Federal. O caso refere-se ao "escaneamento de e-mails e consentimento prévio". A ré contesta alegando que quando os usuários se cadastram no serviço do gmail eles concordam com os termos de uso dos dados.

> Trata-se de ação civil pública ajuizada pelo Ministério Público Federal, na qual se pretende provimento judicial no sentido de que seja suspensa, por parte da ré, a análise (escaneamento) do conteúdo dos e-mails dos usuários do Gmail, em todo o território nacional, enquanto não for colhido o consentimento prévio, expresso, e destacado do titular da conta de e-mail, inclusive para o envio de publicidade comportamental [...] (BRASIL, 2018a).

Nesse julgado foi determinado que a atividade de análise de e-mails não se caracterizava como invasão de privacidade pela ré, no caso o *Google*, pois não se tinha prova que tais fatos estariam ocorrendo e, ainda, que o usuário, quando se cadastra no serviço do *Google*, aceita os termos de uso dos dados, não havendo, portanto, ilegalidade, e que o usuário pode a qualquer momento excluir sua conta no serviço.

Outro caso referente à coleta de dados foi o caso julgado pelo Tribunal de Justiça do Distrito Federal e dos Territórios - 4ª Vara da Fazenda Pública – Brasília no dia 15/03/2018, no qual a requerente "99 Tecnologia Ltda" solicita que não haja a exigência de coletar e enviar dados de motoristas e informações de veículos para à Secretaria de Estado de Mobilidade do Distrito Federal (SEMOB/DF). A autor alega que os únicos dados de usuário obrigatórios para coleta são o IP, data e horário de uso da aplicação, devendo restringir a coleta de dados ao mínimo necessário, de acordo o motivo de uso dos dados.

> 99 TECNOLOGIA LTDA. pede tutela de urgência, de natureza antecipada, para que o DISTRITO FEDERAL: a) se abstenha de exigir da 99 o cumprimento das obrigações de coletar, fornecer ou permitir o acesso da SEMOB/DF ou de qualquer outro órgão ou agente do DF a dados pessoais dos motoristas parceiros, usuários do aplicativo da 99, mapas de calor das viagens realizadas pelos seus usuários, informações sobre quantidade de viagens, distância percorrida entre pares de origem e destino (Matriz Origem-Destino) e veículos cadastrados; e b) se abstenha de aplicar à 99 e aos motoristas parceiros quaisquer sanções ou empecilhos ao regular desenvolvimento das suas atividades, pelo não cumprimento das obrigações acima referidas e também em decorrência da não obtenção do Certificado Anual de Autorização (CAA). (...) (BRASIL, 2018b).

Essa tutela de urgência foi indeferida com as argumentações que as informações solicitadas são a respeito de dados de origem e destinos das corridas, mapas de calor sobre as viagens, quantidade de quilômetros percorridos e veículos cadastrados, com a finalidade de conhecer os serviços prestados e que não violam a privacidade dos usuários. Esses dados coletados colaboram com a Administração Pública para o controle e planejamento de questões de interesse coletivo, tais como planejamento de trânsito e transporte público (BRASIL, 2018b).

Uma questão bastante debatida nas jurisprudências foi em relação à divulgação de dados pessoais sem consentimento do titular dos dados, tal como o julgado pelo Tribunal de Justiça do Paraná de 16/06/2016 na seguinte ementa:

> Trata-se de ação de obrigação de fazer ajuizada em face de *Privacy* Protection Service Inc. em que os autores alegam, em síntese, a ilegalidade da exploração comercial e exposição não autorizada de seus dados pessoais e das sociedades que compõem junto ao "www.consultasocio.com" (ID: 2012741661_DOMAIN_COM-*site* VRSN). Aduziu que as informações fornecidas pelo *site* violam direito fundamental à intimidade, vida privada, honra e imagem (Art. 5º, X, CF), bem como à disciplina estabelecida nas Leis 12.965/2014, 12.414/2011, e 12.527/2011 quanto à utilização de informações cadastrais e restrição de acesso às informações relativas à vida privada sem consentimento (BRASIL, 2016d).

O caso descrito resultou no deferimento parcial da tutela provisória de urgência, dentre as determinações foi solicitado ao Estado da Austrália à interrupção de exibição dos dados pessoais do requerente no *site* www.consultasocio.com e o fornecimento de dados das pessoas físicas e jurídicas que criaram e mantém o respectivo *site*.

Boa parte dos casos julgados é referente à solicitação para que detentores forneçam dados cadastrais, registros de acesso e de IP, com a finalidade de identificação de responsáveis por publicações de conteúdo na Internet que ferem o direito à privacidade.

> Agravo de instrumento. Ação de obrigação de fazer. Decisão agravada que deferiu a antecipação dos efeitos da tutela para determinar o fornecimento dos registros de acessos e informações de usuários de banco de dados referente a endereço eletrônico de rede social. Recurso da ré. Acolhimento. Decurso de prazo superior a seis meses entre a divulgação do conteúdo e a citação da ré, pelo que não subsiste a obrigação de guarda dos registros de acesso a aplicações de Internet, nos termos do Art. 15 do Marco Civil da Internet. Ausência de obrigação de guarda de outros dados além dos registros de acesso a aplicações. Decisão revogada. RECURSO PROVIDO (BRASIL, 2017a).

No julgado supracitado a agravante alega que não possui os dados solicitados pela autora, visto que, no momento do processo, já decorria o prazo de seis meses para armazenamento de dados coletados exigidos pela legislação, e que não existe a obrigação legal de armazenamento de registros de acesso a aplicações de Internet após seis meses, conforme diretrizes previstas no Marco Civil de Internet.

Outro caso referente ao fornecimento de dados envolve o artista Danilo Gentili que entrou com ação contra o *Facebook*, solicitando ao Tribunal de Justiça do Estado de São Paulo que determinasse ao requerido o fornecimento de dados cadastrais de usuário que realizaram comentários ofensivos na sua *fanpage*, como também retirasse os respectivos comentários.

> Danilo Gentili Junior moveu a presente ação de requisição judicial de registros c/c pedido de exclusão de conteúdo publicado na rede social em face de Facebook serviços online do Brasil Ltda. alegando, em síntese, que em uma publicação do canal Comedy Central Brasil em seu perfil da rede social ré recebeu vários comentários lesivos a sua honra, nome e imagem. Requer, assim, a condenação a ré a fornecer os endereços de IP descritos na inicial, bem como os dados cadastrais e dados pessoais e a determinação para que os 16 comentários transcritos na inicial sejam indisponibilizados [...] (BRASIL, 2017b).

As solicitações do requerente foram negadas, a rede social não precisou informar os dados de usuários, pois justificou que era preciso a apresentação da URL de cada comentário, e que a plataforma não tem condições de fornecer outras informações, a não ser o IP, pois não detém tais dados. Em relação à retirada dos comentários, a magistrada justificou que a legislação brasileira protege tanto a proteção da intimidade e da honra quanto à liberdade de expressão, devido o fato de o autor ser uma pessoa pública, entendeu-se que esse está sujeito a críticas e que não houve ofensa ao patrimônio moral do autor, ressalva-se quando os comentários forem em relação a sua vida privada (BRASIL, 2017b).

Caso semelhante foi do atual governador do estado de São Paulo, Geraldo Alckmin, que após ser vítima de comentários supostamente ofensivos no *Twitter* recorreu ao Tribunal de Justiça do Estado de São Paulo para solicitar dados cadastrais e IP dos usuários. A decisão desse julgado determinou no dia 08/06/2017 que o Twitter disponibilizasse a identidade e os IPs de usuários que usaram a rede social para fazer agressões ao governador de São Paulo.

> Geraldo José Rodrigues Alckmin Filho forte na inviabilidade do anonimato ajuizou a presente tutela cautelar antecedente para exibição de documentos em face de *Twitter* Brasil rede de informação Ltda., qualificados nos autos, objetivando compelir a ré a apresentar os dados cadastrais e números de IP's dos perfis responsáveis pelas postagens para subsidiar as ações principais que (...) julgar necessárias (sic) [...] (BRASIL, 2017c).

Observa-se que solicitar informações de usuários de redes sociais, tais como dados cadastrais e IP são bem comum entre pessoas públicas e notórias.

Muitos dos julgados versam sobre disponibilização de dados por terceiros, solicitação a serviços de Internet para que forneçam dados de usuários, ou remoção de conteúdo (direito ao esquecimento). Como fica explicito no julgado abaixo, no qual o apelante solicitou a remoção do vídeo que foi disponibilizado no *Youtube*, pois o vídeo ocasionava ofensa à sua honra. O conteúdo do vídeo era referente ao diálogo entre o autor e o investigado Francisco Ramos da "grampos da operação influenza da Polícia Federal", apelação cível que teve preliminar rejeitado.

> Apelação cível. Obrigação de fazer. *Youtube*. Google. Exclusão vídeo. Conteúdo ofensivo. Mídia não juntada nos autos. Julgamento de mérito. Error in procedendo. Não configurado. Conteúdo indevido constatado por outros meios de prova. Remoção do conteúdo. Dano moral. Responsabilidade civil. Relação jurídica continuativa. Lei nova 12.965/14. Aplicabilidade. Dano decorrente de conteúdo gerado por terceiros. Provedor aplicações Internet. Responsabilidade não configurada. Art. 19 e Art. 21. 1 (BRASIL, 2014d).

O direito ao esquecimento se efetua também na ementa a seguir, na qual autor relata que ao realizar pesquisas em seu nome em *sites* de busca, encontrou diversos resultados relacionados à investigação que foi acusado em 1999, denominado de "Máfia dos Fiscais", e que, tais informações estariam lhe causando sérios constrangimentos. O autor solicita ao Tribunal de Justiça do Estado de São Paulo a desindexação dos seus dados dos *sites* de busca para que não seja possível vincular as notícias sobre investigação aos seus dados pessoais.

> Trata-se de ação de obrigação de fazer c/c danos morais e pedido liminar, alegando o autor que em 1999 fora investigado e denunciado em processo crime denominado pela mídia como "Máfia dos Fiscais", mas já teve extinta sua punibilidade em decorrência da prescrição da pretensão punitiva. Diz que através de pesquisas realizadas em seu nome nos *sites* de busca das rés "Google,", "Bing" e "Yahoo", existem diversos resultados vinculando-o às matérias jornalísticas publicadas na época e ao aludido fato pretérito, o que vem lhe causando sérios inconvenientes nos âmbitos pessoal, profissional e familiar. Afirma que apesar de notificadas, as rés se negaram a suspender a veiculação [...] (BRASIL, 2015b).

Neste caso, a decisão considerou o Art. 19 da Lei nº 12.965/2014 (Marco Civil da Internet) e determinou a remoção do material e a remoção definitiva das URLs, a fim de impedir o correlacionamento do nome do autor a quaisquer dados relatos a investigação "Máfia dos Fiscais".

Por outro lado, o recurso de Agravo de Instrumento julgado pelo Tribunal de Justiça de São Paulo teve o recurso desprovido em relação ao direito ao esquecimento, o autor solicita a ré, no caso *Google* Internet do Brasil que impeça a recuperação de resultados quando o usuário buscar pelo nome do autor, a fim de não vincular com matérias jornalísticas difamatórias, buscando o autor o direito ao esquecimento.

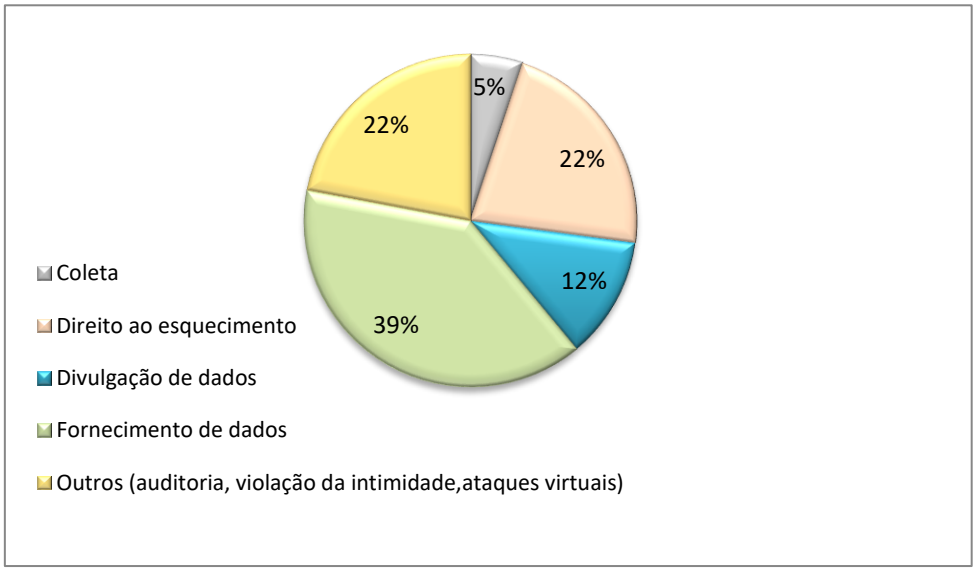
> AGRAVO DE INSTRUMENTO - Antecipação da Tutela - Referências ao autor em matéria jornalística – Pretensão que a Google crie mecanismos para quando se buscar seu nome, o mesmo não conste de seus mecanismos de busca, ou qualquer outro indexador de seu banco de dados - Decisão agravada que indeferiu liminar - Para concessão da antecipação da tutela não basta a relevância da fundamentação, mas há, ainda, que se demonstrar os requisitos legais e as condições da ação, pois na medida antecipada, conceder-se-á o exercício do próprio direito afirmado pelo autor, ainda que em caráter provisório É necessária a observância das garantias do contraditório e da

> ampla defesa para verificação de eventual ilicitude a ser coibida, não se justificando, nesta fase, a supressão das veiculações, sob pena de violação ao princípio constitucional da livre manifestação do pensamento, no que se inclui a divulgação de fatos de interesse público - Ausência dos requisitos legais - Recurso desprovido (BRASIL, 2015a).

Essa ação foi julgada como improcedente, tendo como umas das justificativas que a remoção do conteúdo, com natureza jornalística, afronta à determinação do Art. 220, parágrafo segundo da Constituição Federal, que veda de modo absoluto a censura ideológica. E ainda, que o mecanismo de busca presta o serviço de busca de conteúdos inseridos em provedores determinados, com personalidade jurídica própria, sendo os dois serviços autônomos (BRASIL, 2015a).

Por meio desses relatos observa-se que a maioria dos julgados, representados em 23 casos (39%), menciona o usuário solicitando o fornecimento de dados, tais como IP e dados de cadastro, a fim de identificar terceiros que por meio do uso de serviços de tecnologia levou o indivíduo algum constrangimento ou calúnias (Figura 34).

Figura 34 – Áreas temáticas dos julgados



Fonte: Elaborada pela autora

O direito ao esquecimento também emergem em vários casos, totalizando 13 julgados (22%), nos quais o indivíduo solicita a exclusão de vídeo ofensivo, retirada do nome do indivíduo de resultados em mecanismos de busca e exclusão de fotos íntimas. A categoria outros (violação da intimidade, ataques virtuais, auditoria) representa 13 julgados (22%). A categoria divulgação de dados efetua-se em 7 julgados (12%), mediante empresas que vendem dados de usuários ou disponibilizam dados sem consentimento do titular dos dados.

Observa-se que danos referentes à coleta de dados manifesta-se em poucos julgados, apenas em 3 casos (5%), o que demonstra a pouca relevância dada pelo titular a fase de coleta pelo detentor, reforçando que danos referentes ao direito ao esquecimento, disponibilização de dados sem o consentimento do titular e fornecimento de dados por terceiros são temáticas que se tornam muito mais perceptíveis para o usuário no domínio de ameaças a privacidade. Essa falta de percepção em relação à coleta, também foi revelada no Capítulo 4 ao abordar como a anonimização de dados tem se efetuado na fase de coleta de dados, e na falta de especificação dos aspectos de coleta nas legislações dos países. Os danos à recuperação de dados se tornam mais perceptíveis do que os relacionados com a coleta de dados.

5.5 Considerações Finais

Este capítulo teve o objetivo de identificar principais legislações internacionais e nacionais que tratam de questões vinculadas à proteção de dados pessoais, especificamente relatando como essas leis e regulamentos tem mencionado a fase de coleta de dados.

Observou-se que proteção de dados na fase de coleta se configura nas legislações internacionais e nacionais mediante os seguintes elementos: transparência que deve ser provida aos titulares sobre a coleta; ciência sobre os tipos de dados que serão coletados; motivo da coleta; direito ao consentimento sobre atividades vinculadas aos dados; e adoção de medidas para minimizar violações de privacidade.

Na maioria das leis a fase de coleta está inserida na definição do termo tratamento, que ao abarcar várias outras atividades relacionadas com dados, se torna um termo unitário dentro de vários contextos. A minoria das leis possui um tópico específico para a coleta, situação que pode acentuar a insciência do usuário no que tange a coleta de dados realizada pelos detentores.

> Apesar da profunda importância da privacidade e do crescimento de questões jurídicas a ela relacionadas, tentativas de definição desse direito fundamental pecam por tentar encontrar um conceito unitário, passível de ser aplicado a quaisquer situações (LEONARDI, 2012, p.48).

Essa generalização pode implicar na percepção que órgãos públicos ou privados têm a respeito da proteção de dados pessoais, principalmente na atual conjuntura da evolução tecnológica. A falta de percepção pode impactar na aplicabilidade dessas legislações, visto que, quando a lei regulamenta elementos técnicos de modo genérico, contribui para que detentores de dados promovam o mínimo para que o usuário tenha consciência sobre a coleta e uso de seus dados, situação que se torna muito conveniente para esses detentores. A generalização de

conceitos técnicos nas leis também pode impactar as decisões de julgados quando o tema das decisões está vinculado às questões de proteção de dados pessoais e privacidade.

Ressalta-se também termos técnicos que emergem nas leis de modo esparso, tais como anonimização, dados de *cookies* e dados de tráfego, na maioria das vezes o termo não está vinculado especificamente a coleta de dados.

Diante do exposto, observou-se que "***a generalização dos aspectos de coleta de dados em legislações***" pode contribuir para o cenário que tende a levar a insciência do usuário, quando alvo de fases de coleta de dados.

Como a coleta de dados está se intensificado nos ambientes digitais, este trabalho explana, no próximo capítulo, as questões envolvidas na coleta de dados, para tanto, realiza uma análise a partir da interpretação de políticas de privacidade, e mediante análise de pacotes de dados de tráfego, especificamente lançando luz aos possíveis dados coletados pelos ambientes dos mecanismos de busca.

6 COLETA DE DADOS E AS IMPLICAÇÕES NA PRIVACIDADE

> *[...] alimentavam com novos dados, ajustavam as perguntas de acordo com as necessidades do sistema e traduziam as respostas que lhes eram fornecidas [...] 'Ainda não há dados suficientes para uma resposta significativa' – o homem disse, 'Colete dados adicionais'. [...] A coleta de dados havia chegado ao seu fim. Não havia mais nada para aprender. No entanto, os dados obtidos ainda precisavam ser cruzados e correlacionados de todas as maneiras possíveis (ASIMOV, 1956).*

A sociedade hodierna convive com a coleta de dados realizada por diversos meios tecnológicos, o que torna isso tão natural que perpassa a esfera do privado ao público sem implicar em questionamentos ou preocupações. No entanto, ao coletar uma expressiva quantidade de dados, os ambientes digitais intensificam antigos problemas relacionados à privacidade de dados, resultado dos rastros de interação dos usuários com o ambiente digital (FLORIDI, 2005; BERGSTRÖM, 2015).

A falta de atenção à coleta de dados é reflexo dos benefícios proporcionados pelas diversas tecnologias. No entanto, a insciência sobre esse processo beneficia aqueles que se apoderam dos dados, cuja justificativa é prover melhores serviços ao usuário ou permitir que o usuário utilize o serviço.

Essa situação pode ser vista, por exemplo, durante o uso de aplicativos para dispositivos móveis, que solicitam permissão de acesso aos dados do usuário para que instalação seja concluída. Fica evidente, nessa situação, a troca de dados pelo benefício do uso do aplicativo, concretizando a ameaça à privacidade do sujeito. Para Mayer-Schönberger (2011), proporcionar melhores serviços e experiências personalizadas aos usuários torna-se a moeda de troca para a coleta de dados pessoais realizada pelos diversos serviços no ambiente Web.

Essa moeda de troca pode ser ilustrada em várias situações, como pelo uso do aplicativo *Meitu*, cuja finalidade é deixar a foto do usuário com aparência de *anime*. Para tanto, ele coleta, além da imagem do usuário, dados identificadores únicos, como IMEI *(International Mobile Equipment Identity*), ICCID *(Integrated Circuit Chip Card Identification)* e a localização do aparelho. A empresa justifica tais coletas para otimizar o desempenho do aplicativo e monitorar os melhores usuários; ainda, ressalta que não compartilha os dados de usuários com terceiros (FRANCESCHI-BICCHIERAI, 2017).

No mesmo cenário, a empresa Uber, em sua política de privacidade, informa que coleta, por meio do seu aplicativo, os seguintes dados quando o indivíduo se registra como usuário: nome, endereço eletrônico, país, idioma, senha, número de telefone celular, endereço de IP, endereço MAC, o número de cartão de crédito com data de validade e código de segurança, justificando oferecer melhores serviços e segurança a seus usuários (TELLES, 2017).

No momento da coleta, o usuário transfere para os detentores a tutela dos seus dados; assim, o uso desses dados não está mais sob controle do usuário. Na própria política de privacidade do Uber fica explícito: "Quando você usa o Uber, você nos confia suas informações" (TELLES, 2017). Ressalta-se que essas informações estão muito além do que o usuário tem consciência no momento que solicita o serviço, pois o conjunto de dados coletados também é formado por informações de log: "Quando você interage com nossos serviços, coletamos logs do servidor, que podem incluir informações como endereço IP do aparelho [...] *site* ou serviço de terceiros que **você estava usando antes de interagir com nosso serviço**" (TELLES, 2017, grifo nosso).

A coleta de dados mediante *Application Programming Interfaces* (APIs) em redes sociais também conduz a intangíveis quebras de privacidade, pois permite o conhecimento do usuário.

> Expomos cada dia mais e mais nossos dados pessoais em redes sociais e outros serviços, e parte destes dados são originários de informações da esfera privada: nossos gostos sobre uma fotografia, locais que frequentamos, nossas comidas favoritas, trabalhos que deram certo e que deram errado, as opiniões políticas, filosóficas, científicas e artísticas – e estas redes possuem *APIs* com acesso legalizado a agentes externos, que utilizam estes dados para – cada dia mais – nos conhecer melhor (RODRIGUES, 2017, p. 98).

Affonso, Monteiro e Camargo (2016) evidenciaram em seu trabalho os dados coletados durante a instalação de aplicativos em dispositivos móveis. Identificaram que, entre os aplicativos levantados, 98.75% solicitam acesso aos dados do usuário durante a instalação, tais como: dados de localização; informação de conexão Wi-Fi; acesso à câmera; identidade; dados de contato; entre outros. Muitos dos dados coletados são caracterizados como identificadores e semi-identificadores, permitindo a identificação do indivíduo ou a correlação com outros dados, o que torna possível a construção do perfil do usuário. Os autores enfatizam que a necessidade da coleta de dados não é justificável, pois a maioria dos aplicativos analisados na pesquisa é de natureza informativa e não faz uso dos dados para prover algum retorno para o usuário, tais como entrada de dados para cálculos ou comparações.

> A questão não é o medo do Big Brother porque, na verdade, a maior parte da vigilância não terá nenhuma consequência diretamente danosa para nós – ou, aliás, nenhuma consequência em absoluto. O aspecto mais atemorizante é, de fato a ausência de regras explícitas de comportamento, de previsibilidade das consequências de nosso comportamento exposto, segundo os contextos de interpretação, e de acordo com os critérios usados para julgar nosso comportamento por uma variedade de atores atrás da tela de nossa casa de vidro (CASTELLS, 2003, p. 149).

No entanto, não importa quão alto sejam os riscos, as pessoas estão geralmente dispostas a trocar suas informações por conveniência. Ainda que possam ter receios em relação às ameaças à privacidade, os indivíduos acabam apresentando um comportamento diferente quando estão em situações que envolvem coleta de dados e brechas de privacidade - paradoxo da privacidade, que neste caso se concretiza quando um aplicativo é baixado e o usuário aceita, antes da instalação, todas as suas condições, na maioria dos casos sem lê-las. Para Garcia-Rivadulla (2016), o indivíduo que utiliza de aplicações e ambientes digitais deveria estar preparado para renunciar qualquer tipo de privacidade digital em troca de conveniência, pois toda informação *online* se torna potencialmente público.

Nesse contexto também estão presentes os mecanismos de busca que fazem da coleta de dados a estratégia para proporcionar resultados de buscas relevantes aos seus usuários. Segundo Affonso et al. (2017), a opção por resultados relevantes, ao invés de se preocupar com ameaças de privacidade, é muito mais imediato e perceptível, determinando a troca de privacidade pelos benefícios na recuperação da busca.

6.1 A abstração na fase de coleta de dados

Além dos dados que estão perceptíveis para o usuário na fase de coleta dos dados, há uma abstração entre o momento de solicitação do serviço até a resposta pelo servidor, podendo envolver muitos outros dados. Essa abstração se dá em relação aos dados de tráfego que são coletados e aos valores semânticos que eles carregam, podendo resultar em algum tipo de brecha de privacidade aos sujeitos que interagem com ambientes Web.

> No que se refere ao aspecto público e ao privado no meio virtual, cabe destacar que a Internet é um ambiente que apresenta falsa sensação de privacidade, ou seja, o internauta, ao acessar a rede mundial de computadores, expõe-se sem preocupação quanto a suas comunicações e seus contatos, devido à intangibilidade do meio (GAMIZ, 2012, p. 64)

Para Lin e Lin (2012), é possível determinar dois tipos de informações que estão presentes nos dados de tráfego: as informações pessoais como senhas, históricos de navegação e endereços de e-mail; e as informações de sistemas ou aplicações utilizadas pelo usuário, como

a versão do sistema operacional ou o programa de servidor em um host. É notável que informações pessoais caracterizam-se como dados sensíveis. No entanto, os dados de aplicação também podem ameaçar a privacidade do indivíduo, pois um terceiro pode aproveitar de descobertas de *fingerprints* e encontrar alvos vulneráveis para descobrir informação privada (LIN; LIN, 2012).

Nos ambientes digitais, as redes de computadores são essenciais. Especificamente a Internet, que por meio da *Word Wide Web* (WWW), também conhecida como ambiente Web, que tem atraído miríades de novos usuários e tornou possível a configuração de diversas páginas de informações, contendo textos, figuras, sons e vídeo, com links incorporados para outras páginas (TANENBAUM, 2003).

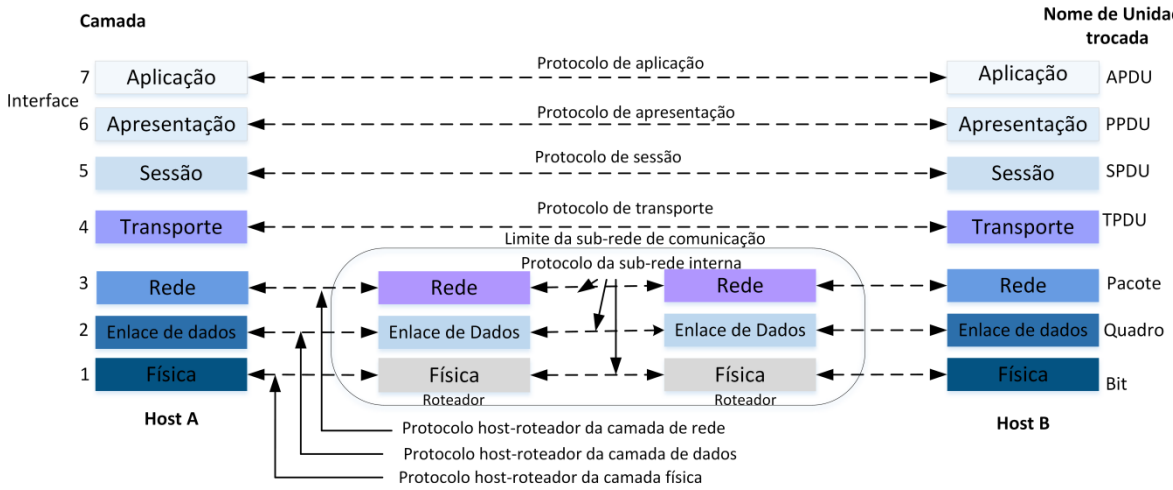
Para minimizar a complexidade que está envolvida no funcionamento dessas redes de comunicação, elas estão organizadas em camadas de abstração, cuja finalidade é prover serviços às camadas superiores, isolando essas camadas dos detalhes de implementação (TANENBAUM; WETHERALL, 2011). O conceito de abstração é comum na ciência da computação, recebendo diversos nomes, como ocultação de informação, tipos de dados abstratos e encapsulamento (TANENBAUM; WETHERALL, 2011).

Dessa forma, os meios digitais, ao realizarem coleta de dados utilizando redes de computadores, amparam-se em um modelo de camadas de abstração, com o objetivo de esconder do usuário detalhes técnicos das atividades e dos dados coletados. O princípio de abstração mais importante, no âmbito da comunicação em redes de computadores, é o modelo de referência OSI (*Open System Interconnection*).

6.2 Modelo de referência OSI

As redes de computadores, principalmente a Internet, por meio do ambiente Web, caracterizam-se como essenciais para a fase de coleta de dados. No entanto, para minimizar a complexidade envolvida no funcionamento dessas redes de computadores e prover uma interface mais amigável para o seu usuário, elas são organizadas em camadas de abstração, proposta pelo modelo de referência OSI (*Open System Interconnection*) (TANENBAUM; WETHERALL, 2011) (Figura 35).

Figura 35 - Camadas de abstração modelo de referência OSI



Fonte: Tanenbaum (2003, p. 41)

Para representar as funções presentes na estrutura do modelo OSI, o modelo conceitua serviços, interface e protocolos, desta forma, as camadas executam serviços para as camadas superiores a ela, determinando sua funcionalidade e semântica. A interface indica como os processos da camada superiores podem ser acessados, e os protocolos proporcionam o fornecimento do serviço (TANENBAUM; WETHERALL, 2011). Assim, cada camada oferece seu serviço, executando certas ações dentro da camada e utilizando os serviços da camada diretamente abaixo dela.

Por meio do modelo OSI é possível ter uma melhor compreensão das fases e elementos envolvidos na fase de coleta de dados. No entanto, os detalhes que não são operacionalmente importantes para o usuário são encapsulados pela abordagem em camadas proposta pelo modelo de referência OSI, tornando a visualização do processo de comunicação nas redes de computadores generalizado e com redução da complexidade (AFFONSO; SANT'ANA, 2018, no prelo).

Com a finalidade de transmitir o fluxo de bits brutos por um canal de comunicação, "[...] a camada física é o alicerce sobre o qual a rede é construída" (TANENBAUM; WETHERALL, 2011, p. 55), nela são especificados os aparatos de fiação e de conectores, como tensão e *bits* que transitam pela mídia cabeada ou sem fio, e ainda estão incluídos os repetidores, concentradores, *hubs* e cabos (OREBAUGH et al., 2004).

A camada de enlace de dados realiza o serviço orientado a conexão entre máquinas de origem e destino, cujo principal objetivo é transformar um canal de transmissão bruto em informação livre de erros que não foram detectadas pela camada de rede. Por meio da camada de enlace, cada transmissor divide os dados de entrada em quadro de dados, e a camada garante que

cada quadro será recebido uma única vez e na ordem correta, sendo o gerenciamento de quadros a principal atividade desta camada (TANENBAUM, 2003). A comunicação nessa camada é geralmente baseada em endereços MAC (*Media Access Control*) e podem estar presentes os protocolos *Ethernet, Token Ring, Point-to-Point* (PPP), operando nessa camada os dispositivos *bridges* e *switches* (OREBAUGH et al., 2004).

A camada de rede é a responsável em gerenciar o roteamento de pacotes de dados da origem ao destino, atividade que consiste em mover informações por meio de uma rede de comunicação. Isso inclui o controle do congestionamento de pacotes, a fim de garantir a qualidade do serviço e de possibilitar que redes heterogêneas se comuniquem (TANENBAUM, 2003). Podem estar presentes nessa camada os protocolos IP (*Internet Protocol*) e IPX (*Internetwork Exchange)*, e os dispositivos *switches* e roteadores. Além disso, essa camada retira os dados da camada de transporte e os envolve em um pacote ou *datagrama* para entregar os pacotes do computador de origem ao computador de destino (OREBAUGH et al., 2004).

A camada de transporte provê o envio de pacotes origem-destino, assegurando que os dados que trafegam na rede chegarão corretamente ao destino. A camada de transporte, nesse sentido, garante um nível de confiabilidade independentemente do tipo de rede física utilizado. Essa camada aceita os dados da camada superior e os divide em unidades menores, repassando-os à camada de rede. Nessa etapa, também é definido que tipo de serviço será oferecido para a camada de sessão (TANENBAUM, 2003).

Para Orebaugh et al. (2004), a camada de transporte também é responsável pela comunicação entre programas ou processos, utilizando números de porta ou *sockets* para identificar processos únicos. Dentre os protocolos que podem atuar nessa camada estão o TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*) e SPX (*Sequenced Packet Exchange)*.

Com o objetivo de permitir que usuários finais de diferentes máquinas estabeleçam conexão entre eles, a camada de sessão mantém o controle de diálogo, gerenciamento de *tokens* (impedem que duas partes realizem simultaneamente uma atividade crítica) e a sincronização da comunicação (TANENBAUM, 2003). Exemplos de protocolos na camada de sessão incluem NetBIOS e *Remote Procedures Call* (RPC) (OREBAUGH et al, 2004).

Relacionada à sintaxe e à semântica das informações que trafegam nas redes de computadores, a camada de apresentação é a responsável pela apresentação dos dados, possibilitando que computadores com diferentes representações de dados possam se comunicar (TANENBAUM, 2003). Essa camada também controla várias formas de

criptografia/descriptografia utilizadas para prover a segurança dos dados enviados ou recebidos (OREBAUGH et al., 2004; SANDERS, 2017).

A camada de aplicação possui diversos protocolos necessários para os usuários, tal como o HTTP, que constitui a base para a solicitação de uma página Web por um navegador. Inclui também: Protocolo para Transferência de Arquivos (*File Transfer Protocol* - FTP), Protocolo de Gerenciamento de Redes Simples (*Simple Network Management Protocol* - SNMP), Protocolo de Transferência de Correio Simples (*Simple Mail Transfer Protocol* - SMTP) e Telnet (TANENBAUM, 2003).

Conforme Orebaugh et al. (2004), essa camada é a responsável pelo gerenciamento de comunicações entre os aplicativos de rede, não sendo ela o próprio programa de aplicação. A título de ilustração, um navegador da Web é um aplicativo, mas é o protocolo HTTP que fornece a funcionalidade da camada de aplicação.

Essas camadas supracitadas presentes no modelo OSI permitem organizar e simplificar os conceitos envolvidos na comunicação de dados pelas redes de computadores, visto que, se esses conceitos não fossem abstraídos nessas camadas poderiam ser desnecessários e complexos (NIKKEL, 2005).

Um meio de compreender e monitorar o fluxo de dados que perpassa através das redes de computadores, e verificar a atuação dos protocolos nas camadas do modelo OSI é por meio de softwares analisadores de pacotes de redes de comunicação ou *sniffers.*

6.3 Ferramentas para análise de pacotes de redes de comunicação (*sniffers*)

A análise de rede, também conhecida como análise de tráfego, análise de protocolo, *sniffing*, análise de pacote ou espionagem, é o processo de captura do tráfego de dados da rede de computadores e de interpretação em tempo real do seu funcionamento, com a finalidade de decodificar ou de dissecar os pacotes de dados em um formato que seja compreensível por humanos (OREBAUGH et al., 2004).

Para realizar análise de pacotes, normalmente utiliza-se um *packet sniffer* (farejador de pacotes), ferramenta utilizada para capturar dados brutos que trafegam pelos fios de uma rede de computadores (SANDERS, 2017). Um *packet sniffers* é executado em um dispositivo conectado a rede, permitindo coletar passivamente todos os pacotes de dados que transitam nas redes de computadores. Os dados que foram coletados por meio do sniffers podem ser salvos para posterior análise (ASRODIA; PATEL, 2012).

Um analisador de tráfego de rede pode ser uma combinação de *hardware* e *software*, normalmente composto por cinco partes básicas (OREBAUGH et al., 2004):

- ✓ *Hardware*: Existem analisadores de *hardware* de rede, que oferecem benefícios, como análise de falhas de *hardware*, erros de verificação cíclica de redundância, problemas de tensão e de cabos, entre outros;
- ✓ *Driver* de captura: Responsável em capturar o tráfego de rede a partir do cabo e filtrar o fluxo de dados que deseja armazenar no *buffer*;
- ✓ *Buffer*: Armazena dados capturados pelo *driver* de captura;
- ✓ Análise em tempo real: Analisa os dados no momento que ele sai do cabo, assim é possível encontrar problemas de desempenho da rede ou verificar atividades suspeitas de intrusão;
- ✓ Decodificador: Exibe o conteúdo do tráfego de rede com descrições dos pacotes de dados, de forma que seja legível por humanos.

Os softwares *sniffers* podem ser utilizados para diversas finalidades, que vão desde a análise de desempenho de uma rede (monitoramento e análise de tráfego), detecção de intrusos e *spyware*, até a compreensão sobre a atuação dos protocolos nas camadas determinadas pelo modelo OSI (OREBAUGH et al., 2004). Todavia, devido à capacidade dos *sniffers* em capturar todo o tráfego das redes de comunicação, torna-se possível a potencial coleta de dados sensíveis do usuário, podendo ocasionar diversas quebras de privacidade (ASRODIA; PATEL, 2012).

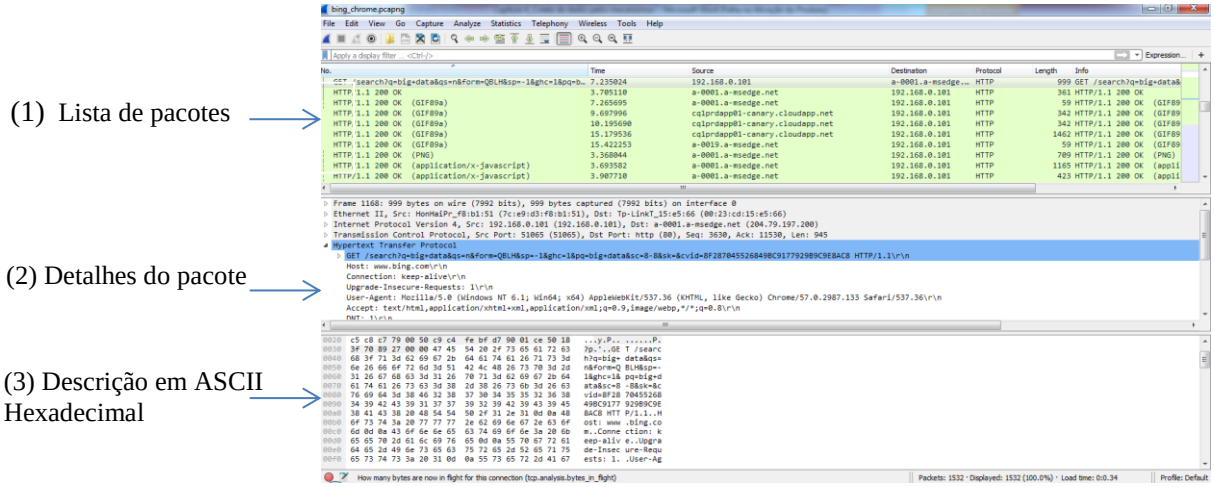
Para análise de pacotes de redes, existem diversas ferramentas *sniffers*, tais como: *Capsa Packet Sniffers*[93], *Microsoft Message Analyzer*[94], *PRTG Network*[95], *SmartSniff* [96], Tcpdump[97] e *Wireshark*[98], cada um com suas características e funcionalidades específicas.

Para verificar as questões vinculadas à coleta de dados e compreender as camadas de abstração do modelo OSI, utilizou-se neste trabalho a ferramenta *Wireshark*, um software livre baseado em licença GPL (*General Public Licence*) que captura e analisa pacotes de rede de computadores em tempo real. O *Wireshark* é utilizado principalmente para solucionar problemas de redes de computadores, questões de segurança, implementação de protocolos, incluindo a compreensão do fluxo de dados nas camadas OSI e a atuação dos protocolos (WIRESHARK, 2017).

[93] Disponível em:<http://www.colasoft.com/capsa-free/>. Acesso em: 5 mai. 2017.
[94] Disponível em:<https://www.microsoft.com/en-us/download/details.aspx?id=44226>. Acesso em: 5 mai. 2017.
[95] Disponível em:<https://www.br.paessler.com/prtg>. Acesso em: 5 mai. 2017.
[96] Disponível em:<http://www.nirsoft.net/utils/smsniff.html>. Acesso em: 5 mai. 2017.
[97] Disponível em: <http://www.tcpdump.org/>. Acesso em: 5 mai. 2017.
[98] Disponível em: <https://www.wireshark.org/>. Acesso em: 5 mai. 2017.

A Figura 36 ilustra a captura de pacotes realizada por meio do *software Wireshark*, onde se evidenciam os pacotes da interação do usuário com ambiente Web, ao realizar uma pesquisa com o termo "*big data*" no mecanismo de busca[99].

Figura 36 - Recorte da visualização de pacotes no *Wireshark*



Fonte: Elaborado pela autora

No painel (1), "lista de pacotes", são exibidos os pacotes e suas informações básicas, em que cada linha corresponde a um pacote que foi capturado durante a interação do usuário com o ambiente. Este painel é composto pelas seguintes colunas: **Nº**, que representa a numeração do pacote no arquivo de captura; ***Time***, *que se* refere ao tempo do início da captura ao momento em que o pacote foi capturado (em segundos); ***Source***, que ilustra o endereço IP da máquina de origem (exemplo: usuário); ***Destination***, que representa o endereço IP de destino (exemplo: página do mecanismo de busca); ***Protocol***, que traz a sigla do protocolo utilizado; ***Length*** do pacote, que informa o tamanho do pacote em *bytes*; e ***Info***, que corresponde à informação sobre o conteúdo do pacote. Ao selecionar uma linha nesse painel, mais detalhes serão apresentados no painel seguinte (2), "detalhes do pacote" (WIRESHARK, 201-).

O painel (2), "detalhes dos pacotes", mostra informações do pacote selecionado no painel (1) "lista de pacote". Nesse caso, está selecionado o pacote nº 1168, representado pelos seguintes campos: *frame, ethernet II, Internet protocol version 4, transmission control protocol, hypertext transfer protocol*. Cabe dizer que tais campos podem variar, de acordo com o pacote selecionado (WIRESHARK, 201-). Observa-se no campo *hypertext translater protocol* a presença do termo pesquisado no mecanismo de busca.

[99] Foi utilizado o mecanismo de busca Bing. Disponível em: <http://www.bing.com>. Acesso em: 30 mai. 2017.

Por último, o painel (3) é similar ao painel (2), “detalhes dos pacotes”. Porém, o painel (3) expõe a informação do tráfego de dados em sistema hexadecimal e sua correspondência no padrão ASCII (WIRESHARK, 201-).

No rodapé da página, é apresentada a barra de status que disponibiliza informações sobre o número de pacotes capturados (*packets*); o número de pacotes exibidos (*displayed*); e o número de pacotes que foram descartados (*dropped*) (WIRESHARK, 201-).

Por meio dessa ferramenta, é possível analisar cada pacote que o usuário recebeu e envio para o destino, verificando dados de IP de origem e destino, número de portas, data e horário de solicitação. E quando a página não possui criptografia, torna-se possível verificar os dados enviados do usuário para o ambiente.

6.4 A coleta de dados pelos mecanismos de busca

A gênese dos mecanismos de busca ocorreu em meados de 1990, a partir da ferramenta *Archie*, aplicação desenvolvida por um aluno da *McGill University*, cujo propósito era pesquisar arquivos baseados na Internet, formar um índice de cada arquivo e prover interface de busca. No entanto, somente técnicos e acadêmicos usavam o *Archie*, pois a usabilidade não era um elemento presente nesse sistema. O usuário pesquisava por meio de uma palavra-chave, que estaria no título do documento, e recuperava uma lista de locais onde esse documento poderia estar presente (BATTELLE, 2006).

A deficiência dessas ferramentas de busca, tais como as interfaces precárias ou as carências de linguagens para realizar consultas, juntamente com o crescimento da Web e o anseio por informações, desencadearam o surgimento do aplicativo de busca Alta Vista, idealizado pela DEC (*Digital Equipment Corporation*) por meio de Louis Monier. O Alta Vista previu muitas das inovações oferecidas pelos atuais mecanismos de busca, tais como *Yahoo* e o *Google* (BATTELLE, 2006).

Atualmente, a busca oferecida por essas ferramentas constrói a base de dados de intenção do usuário, “[...] constituída simplesmente pelos resultados agregados de todas as buscas já feitas, todas as listas de resultados já oferecidas e todos os caminhos tomados em consequência delas” (BATELLE, 2006, p. 5). Para Monteiro (2009, p. 35) “O resultado de busca, ou a própria busca, pode aparecer sob várias linguagens, imagens, textos, músicas, ilustrando a descentralização do verbalismo na organização do conhecimento no ciberespaço”.

Essa base de dados resultante das buscas realizadas representa toda a interação do usuário com ambiente do mecanismo de busca. Assim, por meio da coleta, do armazenamento

e da correlação, é possível construir histórias sobre o usuário, dado que, a busca, segundo Monteiro et al. (2011, p. 2550):

> É uma sintaxe em devir, de recursos variados, segundo as necessidades do usuário e os limites dos índices compilados pelos mecanismos, de tal modo que os operadores pragmáticos, envolvidos nesse processo, permitem construir um mapa de significados vigentes e atualizados, no momento da busca, no universo simbólico, virtual e movente que é o ciberespaço.

Cleland e Brodsky (2011) afirmam que o fluxo de informações não é somente do motor de busca para o usuário, mas com grande intensidade do usuário para o mecanismo. Cada vez que o usuário utiliza o mecanismo de busca, algo sobre ele é revelado, como suas carências, necessidades, desejos e medos, o que torna esses motores de busca muito próximo da onisciência (CLELAND; BRODSKY, 2011)

Para compreender os elementos envolvidos com os mecanismos de busca, Morville e Callender (2010) propõem a anatomia dos mecanismos, representada pelos elementos: criadores, conteúdo, motor, interface e usuários.

Os criadores são os que se preocupam com as questões de precisão e relevância dos resultados. O elemento conteúdo representa o que o usuário busca na Web, podendo ser uma página referente a um documento ou uma imagem, todos eles indexados e representados por metadados. Ressalta-se que esse cenário sempre está voltado a atender à necessidade do usuário.

O motor representa o próprio funcionamento da aplicação, que por meio dos seus algoritmos e tecnologias, procura prover resultados com maior relevância para o usuário, no entanto, esse contexto não é perceptível para o usuário durante a interação com o ambiente.

A interface é o elo entre o mecanismo e o usuário, local onde o usuário relata toda sua intenção de busca. Para que seja possível compreender essa interação, Morville e Callender (2010) relacionam o processo de busca com as técnicas de redação jornalísticas (*Who, Where, Why, What, When e How*), demonstrando **quem** representa o usuário no ambiente; o **local** do usuário no momento da busca; a **justificativa** da busca; **quando** o usuário realiza uma pesquisa; **como** o usuário realizada a busca. Ao conseguir respostas para essas perguntas, é possível obter informações sobre o usuário, que nem sempre ele tem consciência de tê-las enviado para o sistema, o que pode impactar em brechas de privacidade.

O elemento usuário é representado pelo conjunto de dados de comportamento obtidos a partir da coleta de dados de interação com o ambiente, situação que, pode ser tornar uma ameaça à privacidade do indivíduo.

As implicações dos mecanismos de busca, em relação à privacidade, é fruto da própria concepção de busca, definida por Battelle (2006, p. 5) como "[...] uma base de dados de desejos, necessidades, vontades e preferências que podem ser descobertas, citadas, arquivadas, seguidas e exploradas para todos os fins". Dessa forma, as representações do sujeito nesses ambientes podem resultar em diversas ameaças à sua privacidade.

> [...] os mecanismos necessitam resgatar os rastros do sujeito na ambiência da busca, coletando e apropriando-se dos mais diversos tipos de dados e, silenciosamente, essas atividades implicam no direito à privacidade. Cabe lembrar que a gênese desse processo emerge de uma necessidade e por consequência de um desejo de atendê-la, o que constitui uma intenção de busca. Esta intenção leva o usuário a interagir com recursos que possam responder a sua necessidade, interação esta que se compõe não só pela escolha de termos chave, mas antes pelo conjunto de ações realizadas durante a busca. Para ampliar a aderência do recurso escolhido em relação às especificidades de cada usuário, faz-se necessário considerar, ainda, o contexto do usuário, que permeando todo o processo, determina o cenário de funcionamento do mecanismo de busca junto a cada usuário-necessidade. Assim, os resultados disponibilizados pelos mecanismos de busca são a representação da valiosa combinação de dados de **intenção**, **interação** e **contexto** do usuário para uma necessidade de busca (AFFONSO et al., 2017, p. 429).

As ameaças à privacidade se ampliam à medida que essa combinação de dados de intenção, interação e contexto são utilizadas ou compartilhadas pelos detentores de dados dos mecanismos de buscas. Nissenbaum (2011) tece uma comparação entre as bibliotecas e os ambientes digitais e afirma que, embora a pesquisa realizada nos mecanismos de busca seja diferente da atividade realizada em uma biblioteca, há uma semelhança nas duas atividades, ambas podem permitir rastreio de pesquisa, conhecimento e enriquecimento intelectual. No entanto, assim, como nas bibliotecas, espera-se que os mesmos padrões prevaleçam no ambiente *online*, pois rastros *online* não deveriam ser registrados e, se armazenados, devem minimizar o risco de interferência, seja por humanos ou máquinas (NISSENBAUM, 2011).

Mayer-Schönberger (2011) aborda as implicações da coleta de dados pelos mecanismos de busca em relação ao aprendizado que esses ambientes têm sobre o usuário. O autor considera esses ambientes um exemplo poderoso de organizações que retém memória sobre cada usuário, com detalhes minuciosos da vida do indivíduo, tais como combinação de dados de *login*, *cookies* e endereço IP, compondo um histórico da vida do usuário que representa um grandioso poder informativo para essas organizações. A representatividade desse problema fica explícita no trabalho de Gibson (2010) em relação aos mecanismos de busca. Para o autor:

> O Google não é nosso. O que parece confuso, porque nós somos fornecedores de conteúdo não remunerados, de uma forma ou de outra. Nós geramos produtos para o Google, todas as nossas pesquisas são uma contribuição minúscula. O Google é feito de nós, uma espécie de recife de corais de mentes humanas e seus produtos[100] (GIBSON, 2010).

Os mecanismos de buscas, por meio de suas políticas de privacidade, justificam a coleta de dados realizada durante a interação do usuário com o serviço sempre com o argumento de proporcionar melhores resultados e serviços para o usuário. Assim, a interação de dados entre detentores-usuários é permeada pela política de troca e benefício.

Nesse contexto, fica explícito na política de privacidade do Bing que "A Microsoft usa os dados que coletamos para proporcionar experiências sofisticadas e interativas [...]" (MICROSOFT, 2017), ainda ressalta que, "combinamos dados que coletamos de contextos diferentes [...] ou obtemos de terceiros para proporcionar uma experiência melhor, mais consistente e personalizada" (MICROSOFT, 2017). Semelhantemente, a empresa Google relata na sua política de privacidade que: "Usamos as informações que coletamos em todos nossos serviços para fornecer, manter, proteger e melhorar esses serviços [...]" (GOOGLE, 201-).

Ao contrário dos mecanismos de busca *Google* e *Bing*, o *DuckDuckgo*[101] promete não coletar e nem compartilhar dados pessoais. De acordo com a política de privacidade do mecanismo, não são armazenados os valores de *user agent* ou o endereço IP. Assim, nenhuma pesquisa é armazenada de maneira identificável, pois a aplicação utiliza dados de pesquisa agrupados, e não pessoais, para tornar os serviços melhores e úteis para o usuário (DUCKDUCKGO, 201-).

Em relação aos dados presentes nos comentários enviados ao *DuckDuckgo*, a empresa afirma que esses dados podem ficar armazenados. No entanto, o mecanismo oferece a possibilidade de o usuário enviar seus comentários em modo anônimo. Ainda, quando o usuário clica em um link de resultados no ambiente *DuckDuckgo*, seus termos de pesquisas não são enviados para o *site* que o usuário clicou, essa configuração vem padrão no ambiente, mas o usuário pode desativar o recurso (DUCKDUCKGO, 201-).

No entanto, a obtenção da coleta de dados realizada por esses ambientes não se efetua apenas nos dados que o usuário envia no momento da busca e nos relatos da política das políticas de privacidade. As tecnologias envolvidas para proporcionar os resultados da busca, nesses ambientes, podem impactar muito na insciência que o usuário tem sobre esse processo.

---

[100] *Google is not ours. Which feels confusing, because we are its unpaid content-providers, in one way or another. We generate product for Google, our every search a minuscule contribution. Google is made of us, a sort of coral reef of human minds and their products.*

[101] Disponível em: <https://DuckDuckgo.com/?q=&bext=wcp&atb=v87-4__>. Acesso em: 02 jan. 2017.

> Além dos dados previstos nas políticas de privacidade, existe o potencial acesso e registro de dados não previstos nas políticas de privacidade, que podem ainda ter seu uso potencializado pela interação com outros dados à disposição daqueles que detêm o controle sobre os aplicativos de busca (AFFONSO et al., 2017, p. 439).

Na próxima seção, evidencia-se a abstração existente na fase de coleta por meio dos possíveis dados coletados pelos mecanismos de busca e as ameaças à privacidade do usuário enquanto alvo de coleta por detentores de dados.

6.5 Resultados e Discussões

Essa seção é dividida em duas partes: (1) a evidência dos dados coletados pelos mecanismos de busca por meio das políticas de privacidade; (2) a coleta de dados por análise de dados de tráfego de redes de computadores, utilizando a ferramenta *Wireshark*.

6.5.1 A coleta de dados pelos mecanismos de busca: uma análise a partir das políticas de privacidade

Para demonstrar a coleta de dados pelos mecanismos de busca, adaptou-se da pesquisa de Affonso et al. (2017) o Quadro 15, onde foram inseridos os dados coletados pelo mecanismo de busca *DuckDuckgo* e realizada a classificação dos dados em: Identificadores (I); Semi-Identificadores (SI); Sensíveis (SE); Não Sensíveis (NS), a fim de verificar os tipos de dados que podem provocar ameaças à privacidade.

O Quadro 15 está estruturado da esquerda para a direita com as seguintes colunas: dados interpretados das políticas de privacidade dos mecanismos de busca; classificação dos dados em identificadores, semi-identificadores, dados sensíveis e não sensíveis; menção às políticas de privacidade; explicitação da coleta especificamente pelos mecanismos de busca. Essa categorização foi realizada em relação à coleta de dados efetivada pelos mecanismos *Google*, *Bing* e *DuckDuckgo*.

Na lateral à esquerda do quadro, os dados foram agrupados nas seguintes categorias: Contato (dados sobre o usuário); Pagamento (dados referentes a cartão de crédito); Credenciais (dados vinculados à autenticação do usuário); Demográficos (expressam características do usuário); Uso de dados (interação com os serviços); Localização; Interesses e Favoritos; Contatos e Relações; e Conteúdo (conteúdos de arquivos e comunicação) (AFFONSO et al., 2017).

Quadro 15 - Categorização dos dados identificados nas políticas de privacidade[102]

Dados interpretados das políticas de privacidade (*Google* e *Bing*)		Tipo de Dados	*Google*		*Bing*		*DuckDuckgo*	
			Menção na política	Explícito pelo mecanismo	Menção na política	Explícito pelo mecanismo	Menção na política	Explícito pelo mecanismo
Contato	Nome	I	S	N	S	N	N	N
	Sobrenome	I	N	N	S	N	N	N
	Endereço	SI	N	N	S	N	N	N
	E-mail	I	S	N	S	N	N	N
	Número de telefone	I	S	N	S	N	N	N
	Outros dados de contato	I	N	N	S	N	N	N
	Foto	I	S	N	S	N	N	N
Pagamento	Código de segurança cartão de crédito	SE	N	N	S	N	N	N
	Cartão de crédito	I	S	N	S	N	N	N
Credenciais	Senhas	I	N	N	S	N	S	S
	Dicas de senha	SI	N	N	S	N	N	N
	Informações de segurança	I	N	N	S	N	N	N
Demográficos	Idade	SI	N	N	S	N	N	N
	Sexo	SI	N	N	S	N	N	N
	País	SI	N	N	S	N	N	N
	Idioma Preferencial	NS	S	N	S	N	N	N
Uso de Dados	Modelo de *hardware*	SI	S	N	N	N	N	N
	Versão Sistema Operacional	SI	S	S	S	N	N	N
	Identificadores Exclusivos de dispositivos	I	S	N	S	N	N	N
	Informações de rede móvel	SI	S	N	S	N	N	N
	Consultas e termos de pesquisa	SE	S	S	S	S	N	N
	Entrada de voz e dados de desempenho associados à função voz	SE	N	N	S	S	N	N
	Palavra ou expressão procurada em uma página Web ou documento	SE	N	N	S	S	N	N
	Caracteres que o usuário insere em uma pesquisa	NS	N	N	S	S	N	N
	Informações de reg. de telefonia[103]	I	S	N	N	N	N	N
	Páginas que o usuário visita	SE	S	N	S	N	N	N
	Itens que o usuário adquire	SE	N	N	S	N	N	N
	Interação do usuário com anúncios	SE	S	N	N	N	N	N
	Inf. de evento de dispositivo como problemas	SE	S	N	N	N	N	N
	Dados sobre desempenho dos produtos que o usuário utiliza (tipo de problema, detalhes de *software/hardware*, conteúdo de arquivos relacionados a um erro)	SI	N	N	S	S	N	N
	Atividades de sistema	SI	S	N	S	N	N	N
	Configuração de *hardware*	SI	S	N	S	N	N	N
	Tipo de navegador/configuração navegador	SI	S	S	S	S	N	N
	Idioma do navegador	SI	S	S	S	S	N	N
	Sistema Operacional	SI	S	S	S	N	N	N
	Aplicativo exclusivo instalado no dispositivo do usuário	SI	S	N	S	N	N	N
	Data e horário de solicitação do usuário	SI	S	S	S	S	N	N
	URL de referência	SE	S	S	S	S	N	N
	Informações e Identificadores exclusivos contidos em *cookies*	SE	S	S	S	S	N	N
	Dados de armazenamento local	SE	S	N	N	N	N	N

[102] Legenda: S=SIM; N=Não; I=Identificador; SI=Semi-Identificador; SE=Sensível; NS=Não Sensível.

	Dados de suporte (dados sobre o usuário e seu *hardware*, *software*, dados de contato ou autenticação, conteúdos dos seus *chats*, condição da máquina e dos aplicativos, dados do registro e do sistema)	SE	N	N	S	N	N	N
Localização	IP (*Internet Protocol*)	SI	S	S	S	S	S[104]	S
	GPS (*Global Position System*)	SI	S	N	S	S	N	N
	Outros sensores (acelerômetro; giroscópio)	SI	S	N	N	N	N	N
	Ponto de acesso Wi-Fi e torres de celular	SI	S	N	S	N	N	N
	Cidade	SI	N	N	S	N	N	N
	CEP	SI	N	N	S	N	N	N
Interesses e favoritos	Dados sobre os interesses do usuário (time que acompanha, cidade favoritas)	SE	N	N	S	N	N	N
Contatos e relações	Dados sobre seus contatos e relacionamentos quando usa um produto Microsoft ou Google	SI	N	N	S	N	N	N
Conteúdo	Mensagens de e-mail	SE	S	N	S	N	N	N
	Perfil do G+	SI	S	N	N	N	N	N
	Fotos	SE	S	N	S	N	N	N
	Vídeos	SE	S	N	S	N	N	N
	Histórico de navegação	SE	S	N	S	N	N	N
	Pesquisas de mapas	SE	S	N	N	N	N	N
	Documentos ou outro conteúdo	SE	S	N	S	N	N	N
	Música	NS	N	N	S	N	N	N
	Comunicação com a empresa (telefone, chat, mensagens)	SE	N	N	S	N	N	N
	Mensagem instantânea	SE	N	N	S	N	N	N

Fonte: Adaptado de Affonso et al. (2017)

Os dados apresentados no Quadro 15 ilustram que, por meio da interpretação das políticas de privacidade, é possível identificar os possíveis dados que as empresas revelam coletar. No entanto, as formas como as políticas de informação disponibilizam informações para os usuários não facilitam para que os usuários possam ter conhecimento sobre o processo. Essas políticas são vagas e estimulam o usuário a entender a coleta como um benefício para o uso do serviço. Inclusive, para ter ciência do que as empresas relatam nas políticas, o usuário precisa estar disposto a ler e interpretar essas políticas de privacidade.

Para Nissenbaum (2011), as políticas de privacidade não são a melhor forma de promover consciência para o usuário, pois a maioria são longas, incompreensíveis e legalistas, o que contribui para que usuários não tenham hábito de ler políticas de privacidade.

Essas políticas de privacidade deveriam explicitar quais dados, especificamente, estão sendo coletados e compartilhados pelos mecanismos, e não apenas os dados coletados pelos serviços da empresa (AFFONSO et al., 2017), inclusive, indicando meios reais de controle sobre a coleta, tal como a anonimização de dados que o usuário não deseja que sejam coletados. Mesmo que o usuário opte por navegar em modo anônimo, a coleta de dados ainda continua

[104] É descrito na política de privacidade que o navegador Web envia automaticamente informações sobre o computador do usuário, no entanto, o DuckDuckgo afirma que não registra (armazena) essas informações.

sendo realizada. O navegador *Google Chrome* disponibiliza, no momento da abertura da janela anônima, o seguinte texto:

> Quando você está no modo invisível, as páginas que você visita não aparecem no seu histórico de navegação e de pesquisa, nem armazenam arquivos "*cookies*". Mas os downloads e favoritos continuam funcionando normalmente. O modo invisível NÃO oculta seus dados de navegação. Seu empregador, seu provedor de Internet e os *websites* visitados continuam tendo acesso a essas informações (GOOGLE CHROME, grifo do autor).

Dados referentes ao sistema operacional, dados de rede móvel, IP, configuração de hardware, estão muito distantes da consciência do usuário e das possíveis consequências dessa coleta, mesmo estando discriminados nas políticas de privacidade. Desta forma, esses dados continuam sendo coletados e de posse do detentor, tornando o usuário cada vez mais insciente e impedindo qualquer tentativa de controle seus dados.

Destaca-se que, mesmo quando os mecanismos de busca deixam explícitos em suas políticas de privacidade que são coletados dados e identificadores exclusivos contidos em *cookies* não é o suficiente para que o usuário tenha conhecimento de quais dados estão sendo coletados da sua máquina durante a interação com o serviço, impactando na insciência sobre a fase de coleta de dados.

A categorização dos dados recuperados das políticas de privacidade dos mecanismos de buscas em identificadores, semi-identificadores, sensíveis e não sensíveis, comprova quão vulnerável estão os usuários nas questões de privacidade no âmbito da coleta realizada pelos ambientes Web, fruto da sua interação nesses ambientes. Dados como URL de referência, dados do navegador, data e hora de solicitação, GPS, CEP, são considerados semi-identificadores. A ameaça à privacidade do sujeito referenciado nesses dados se perfaz quando esses dados são correlacionados com outros, podendo contribuir para a construção de perfis de usuários e para a sua identificação.

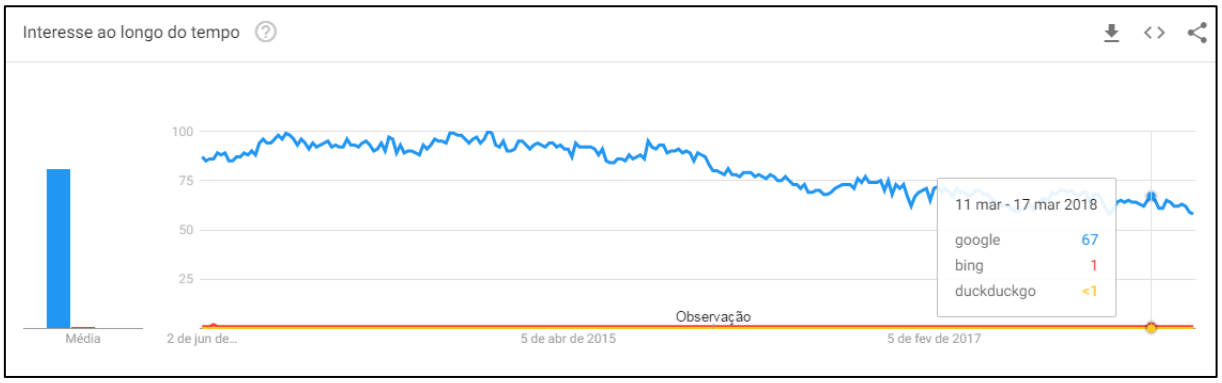
Dados como o endereço IP emergem no Regulamento (UE) 2016/679 como identificadores, pois quando combinados com identificadores únicos podem identificar os titulares dos dados: "[...] as pessoas naturais podem ser associadas a identificadores por via eletrônica, fornecida pelos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP, identificadores de *cookies* [...]" (UNIÃO EUROPEIA, 2016, p. 6).

Embora as políticas de privacidade do *Google* e do *Bing* revelam uma quantidade expressiva de dados coletados durante a interação do usuário com seus serviços, o mecanismo de busca *Google* aparece na primeira posição do ranking de *sites* mais acessados, segundo o

site Alexa[105]. O *Bing* está representado na 42º posição, enquanto o mecanismo *DuckDuckgo* sequer é uma aplicação com destaque, estando na 343º posição.

Essa representatividade dos mecanismos de busca também pode ser visualizada no interesse pelos termos "*Google*", "*Bing*" e "*DuckDuckgo*" nos últimos cinco anos no *site* do *Google Trends* (Figura 37).

Figura 37 - Interesse pelos termos *Google-Bing-DuckDuckgo* nos últimos cinco anos



Fonte: *Google Trends*

Observa-se, na Figura 37 a baixa procura pelos mecanismos *Bing* e *DuckDuckgo* e o destaque para o *Google*. Esse cenário demonstra que a coleta de dados pelos ambientes não é fator relevante para o usuário, uma vez que, ele pode ser insciente sobre essa coleta e que a miríade de benefícios e serviços, especialmente providos pela *Google*, compensam as atitudes em relação à privacidade.

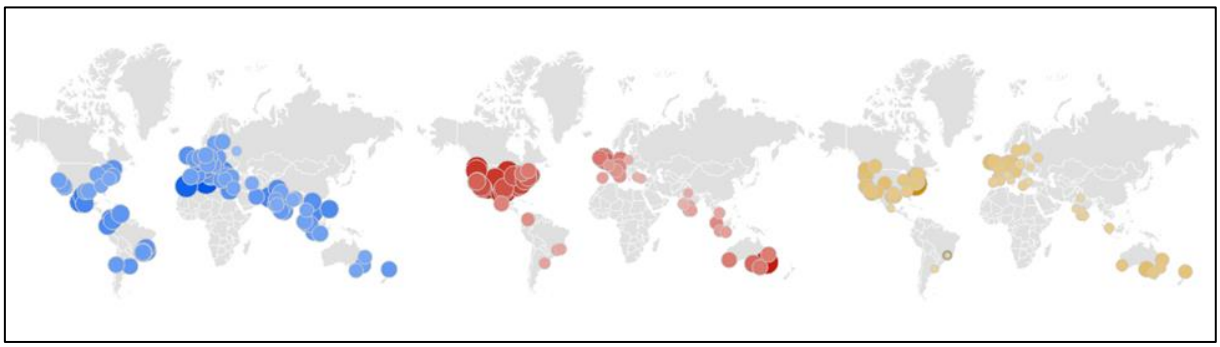
Esses benefícios podem ser vistos pela busca personalizada utilizada pelo *Google*. Ao coletar uma expressiva quantidade de dados pessoais e de interação, esse mecanismo de busca torna os resultados da busca mais relevantes e focado nas preferências dos usuários, situação que leva ao que Pariser (2012) denomina de filtro bolha. Ao contrário, o *DuckDuckgo* não utiliza a abordagem de busca personalizada, o que torna seus resultados não tão próximos do usuário e gera a falsa ideia de resultados sem relevância. No entanto, esse mecanismo de busca oferece a possibilidade de o usuário decidir o que é importante para ele na recuperação do resultado de sua pesquisa.

A Figura 38 ilustra as regiões que mais pesquisaram sobre esses mecanismos. Destaca-se que, os países que buscaram no *Google Trends* pelo termo *DuckDuckgo*, mecanismo que promete não armazenar os dados e garantir proteção à privacidade do usuário, são na maioria, aqueles que, de acordo com o Capítulo 4, apresentam números representativos em pesquisas

[105] Disponível em: <https://www.alexa.com/siteinfo>. Acesso em: 23 jul. 2017.

sobre privacidade, especificamente no contexto da anonimização de dados, tais como, Estados Unidos, Alemanha, Austrália, Coreia do Sul, e Índia. Inclusive, muitos desses países possuem legislações específicas que amparam à proteção de dados pessoais (Capítulo 5), assim, a presença de regulamentos específicos pode ser um fator que configura a busca pelas garantias de privacidade, resultando em consciência sobre as implicações em relação à coleta de dados, armazenamento e compartilhamento de dados pessoais.

Figura 38 - Interesse pelos termos por regiões



(a) Google (b) Bing (c) *DuckDuckgo*

Fonte: *Google Trends*

Esta seção buscou evidenciar os dados que são coletados pelos mecanismos de busca, por meio das menções desses mecanismos nas políticas de privacidade, a fim de verificar como suas políticas contribuem para minimizar a insciência do usuário sobre a coleta de dados.

6.5.2 A coleta de dados pelos mecanismos de busca: uma análise a partir dos dados de tráfego da interação do usuário com o ambiente Web

Ao interagir com o ambiente Web o usuário solicita informação e o servidor responde, atividade baseada no modelo cliente-servidor. A coleta de dados se efetua durante essa interação, perpassando as camadas de abstração, que na maioria das vezes, as entrelinhas desse processo se tornam opaca para o usuário. Nesta seção são apresentadas evidências da abstração da coleta de dados em relação ao usuário, por meio do acesso a páginas dos mecanismos *Bing*, *Google* e *DuckDuckgo.*

Foi solicitado, respectivamente, o acesso à página dos mecanismos de busca para verificar o processo de coleta de dados. A interação com o ambiente consistiu-se na digitação do termo "*big data*" no campo de busca do mecanismo. Esse processo foi acompanhado pelo *software Wireshark e* resultou nos seguintes dados:

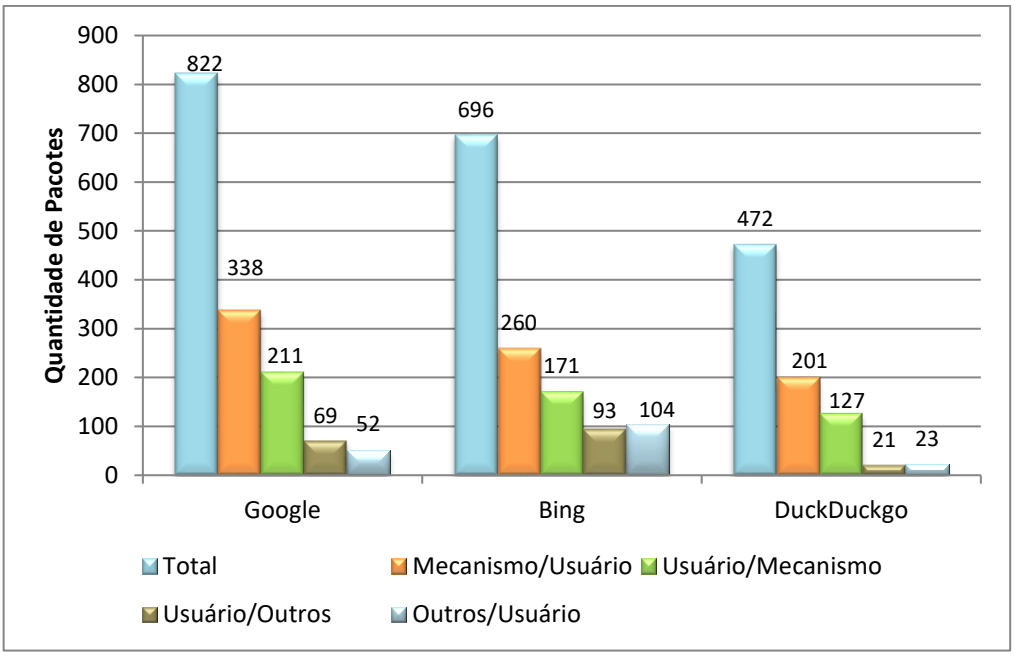
- ✓ ***Google*:** Foram coletados durante a interação 822 pacotes, dos quais 549 são resultantes da interação do usuário com o mecanismo de busca. Desse total, 211 pacotes foram enviados da máquina de origem (usuário) para o servidor (página do *Google*), e 338 pacotes foram enviados do servidor (página do *Google*) para a máquina do usuário**.** Ressalta-se, também, 121 pacotes derivados de envio e recebimento da máquina do usuário para destinos desconhecidos.

- ✓ ***Bing*:** O processo resultou na coleta de 696 pacotes, dos quais 431 foram diretamente identificados como pacotes da interação do usuário com o *site* do mecanismo de busca. Desse total, 171 pacotes foram enviados da máquina de origem (usuário) para o servidor (página do *Bing*), e 260 pacotes foram enviados do servidor (página do *Bing*) para a máquina do usuário**.** Observa-se que, dessa interação, obtém-se 197 pacotes que são resultados do envio e de recebimento da máquina do usuário para destinos desconhecidos.

- ✓ ***DuckDuckgo:*** Durante a interação do usuário com o mecanismo, foram obtidos 472 pacotes, dos quais 328 representam, especificamente, a interação do usuário com o *site* do mecanismo de busca. Desse resultado, 127 pacotes foram enviados da máquina de origem (usuário) para o servidor (página do *DuckDuckgo*), e 201 pacotes foram enviados do servidor (página do *DuckDuckgo*) para a máquina do usuário**.** Nesse mecanismo, o envio e o recebimento de pacotes para destinos desconhecidos resultaram em 44 pacotes de dados.

Observa-se, na Figura 39, que o mecanismo *Google* apresenta maior quantidade de pacotes gerados da interação com o usuário em relação ao *Bing* e ao *DuckDuckgo*. Em relação ao envio de dados especificamente para o mecanismo de busca (coleta usuário-mecanismo), o *Google* ainda se supera. O tempo de interação na captura de pacotes de dados pela ferramenta *Wireshark* foi o mesmo em ambos os mecanismos de busca.

Figura 39 - Quantidade de pacotes resultantes da interação com o mecanismo de busca

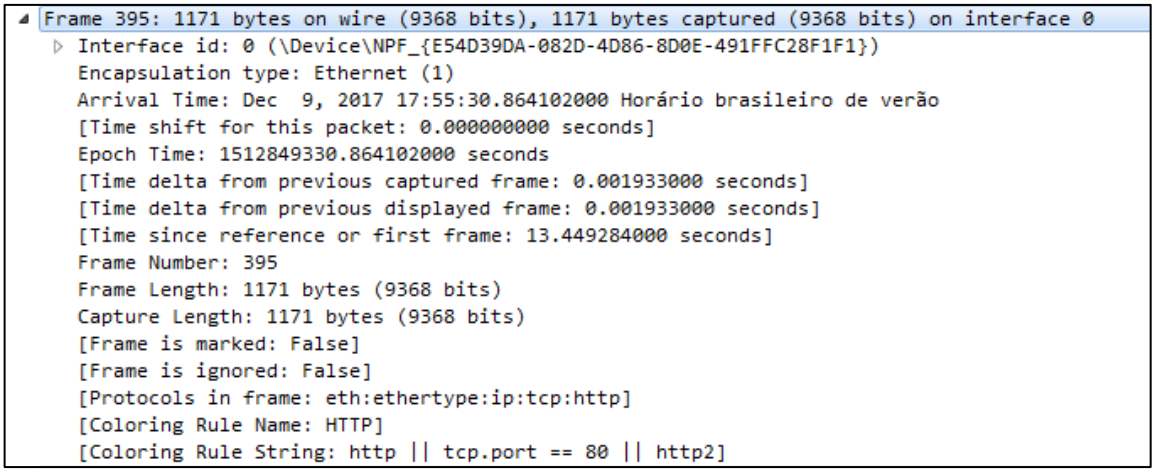


Fonte: Elaborado pela autora

Para demonstrar o processo de interação do usuário com o mecanismo de busca e os possíveis dados coletados, considerou-se um pacote HTTP por meio do método GET do mecanismo *Bing*. Esse método realiza a solicitação da busca do usuário a partir da palavra-chave.

A Figura 40 apresenta os metadados presentes no campo **Frame**, especificamente do pacote selecionado (368). É definido no Frame o campo "*interface id*", uma GUID (*Globally Unique Identifier*) que representa um valor gerado pelo sistema operacional com uma numeração de referência única para o recurso. Os metadados presentes no campo Frame representam os dados de captura do pacote durante a interação do usuário com o mecanismo de busca Bing, tais como: dados de captura, variáveis de tempo (data e hora da captura; tempo ocorrido no momento da coleta do pacote), tamanho do pacote e protocolos que atuaram nesse pacote.

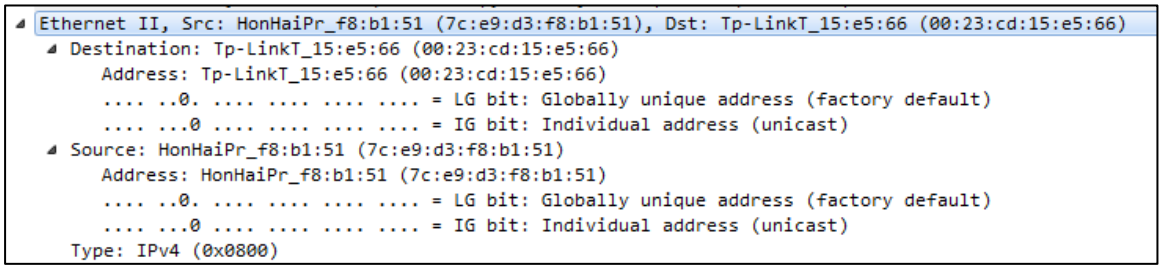
Figura 40 - Recorte do campo *Frame* no *Wireshark*



Fonte: Elaborado pela autora

A camada de enlace do modelo OSI se efetua no campo **Ethernet II** (Figura 41), representando o caminho entre a origem e o destino no qual é transportado o pacote de dados por meio de **protocolos. Nesse campo** estão presentes o endereço MAC de origem e destino, sendo esse endereço um valor exclusivo para cada dispositivo, permitindo desta forma a identificação do dispositivo envolvido na comunicação dos dados. Nesse caso, o endereço MAC da placa do usuário Src: HonHairPr_f8:b1:51 (7c:e9:d3:8:b1:51) e o endereço MAC destino Dst: Tp-linkT-15:e5:66 (00:23:cd:15:e5:66).

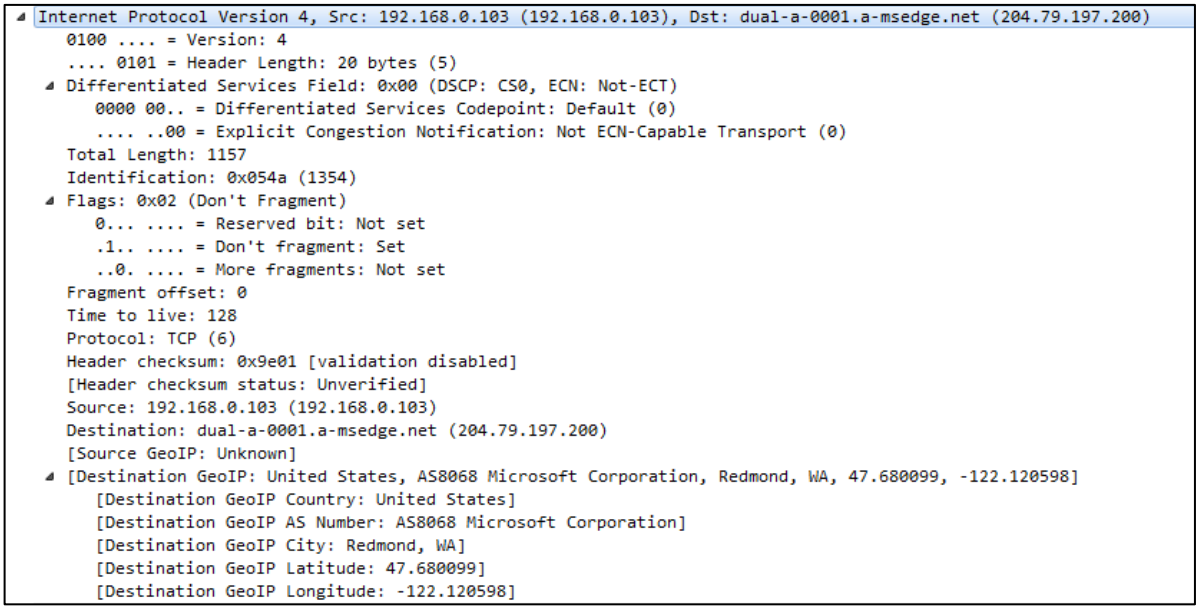
Figura 41 - Recorte do campo *Ethernet II* no *Wireshark*



Fonte: Elaborado pela autora

O campo ***Internet Protocol Version* 4** (Figura 42) representa a camada de rede, nessa camada acontece o roteamento de pacotes entre o destino e a origem. Para que aconteça esse roteamento os pacotes são identificados nessa camada por meio do endereço IP de origem e de destino: do lado usuário o IP 192.168.0.103, e do lado da página do Bing o IP 204.79.197.200. Mediante os atributos *Source GeoIP* e *Destination GeoIP* são especificados os dados referentes à geolocalização da origem e do destino. Esses dados quando combinados com outros podem levar a muitas descobertas durante a interação do usuário com o ambiente dos mecanismos de busca.

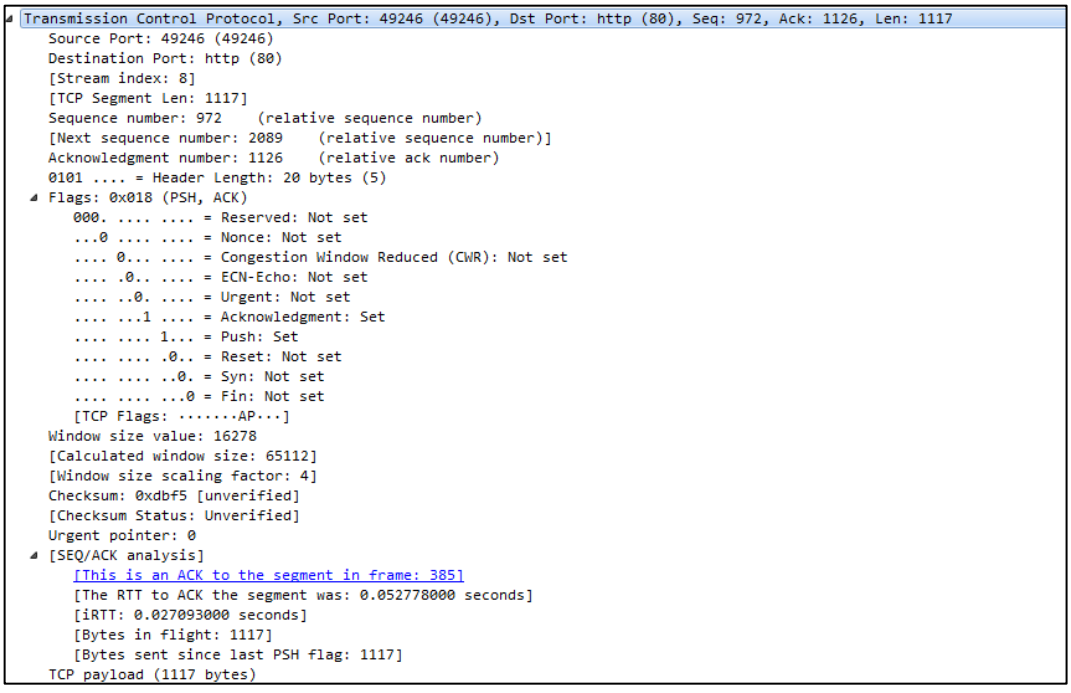
Figura 42 - Recorte do campo *Internet Protocol Version 4* no *Wireshark*



Fonte: Elaborado pela autora

A camada de transporte do modelo OSI é representada pelo campo ***Transmission Control Protocol*** (TCP) (Figura 43), com propósito de permitir a comunicação entre duas máquinas mediante o número de portas, considerando seus programas ou processos. Na Figura 42 nota-se a presença do protocolo TCP, que opera a comunicação por meio da porta de origem Src Port: (49246) e da porta de destino Dst Port: http (80).

Figura 43 - Recorte do campo *Transmission Control Protocol* no *Wireshark*



Fonte: Elaborado pela autora

A única camada tipicamente perceptível pelo usuário no modelo OSI é a camada de aplicação, que permite a comunicação de dados entre *browsers* e servidores, essa camada é representada na Figura 44 pelo campo ***HyperText Transfer Protocol*** (HTTP). O protocolo HTTP é dos que atua nesta camada, enviando comandos da camada de aplicação entre cliente e servidor. Também se encontram na camada de aplicação os *cookies* enviados da máquina do usuário no momento da coleta para aplicação Web e; cabeçalhos *user-agent* com informações do navegador.

Os dados digitados pelo usuário no campo de busca estão explícitos no pacote analisado pelo *Wireshark*, presente no campo *HyperText Transfer Protocol* no *Wireshark*, respectivamente, referente a camada de aplicação, a mais próxima do usuário.

Figura 44 - Recorte do campo *HyperText Transfer Protocol* no *Wireshark*

Fonte: Elaborado pela autora

Dessa forma, a percepção do usuário em relação à coleta de seus dados nesse ambiente recai, especificamente, aos dados que ele transmitiu para a aplicação, no entanto, muitos outros dados são abstraídos pelas camadas da rede de comunicação durante o processo de solicitação de uma página (Figura 41). Ao utilizar um analisador de pacote tipo *sniffer*, neste caso o *Wireshark*, outros elementos estão presentes na coleta, tais como data e hora da solicitação, endereço de IP, dados de localização, informações do navegador e do sistema operacional, e *cookies* que ficam escondidos do usuário.

Para evidenciar a abstração existente no processo de coleta de dados em ambientes digitais, especificamente durante a interação do usuário com o mecanismo de busca, apresenta-se, no Quadro 16, a correlação desses dados com a camada OSI e a possível percepção do usuário em relação a essa coleta.

Assim, as informações no Quadro 16 estão especificadas da esquerda para a direita, respectivamente, pelos seguintes atributos: *site* (mecanismo de busca); protocolo de dados; camada OSI; campo do *Wireshark;* atributos do campo; valor do atributo; e o grau de consciência sobre a coleta desses dados.

Para a realização do estudo, foi selecionado o pacote nº 395, resultado da operação com o protocolo *http* por meio do método GET. Esse método é utilizado quando o usuário solicita algo para o servidor. Neste caso, solicita o retorno de páginas de acordo com o termo digitado no campo de busca. Posteriormente, foi selecionado o pacote nº 1554, rotulado como dados da aplicação do mecanismo *Google* e o pacote nº 1223 do mecanismo *DuckDuckgo*.

Quadro 16 - Dados presentes na captura durante a interação com o mecanismo de busca

Site	**Protocolo**	**Camada OSI**	**Campos *Wireshark***	**Atributos do Campo**		**Valor**	**Consciência**
Bing	http	Enlace	*Ethernet II*	*Src:*		*HonHaiPr_f8:b1:51 (7c:e9:d3:f8:b1:51)*	Baixa
				Dst:		*Tp-LinkT_15:e5:66 (00:23:cd:15:e5:66)*	Baixa
		Rede	*Internet Protocol Version*	*Src:*		*192.168.0.103*	Baixa
				Dst:		*a-0001.a-msedge.net (204.79.197.200)*	
				0100 .... =		*Version: 4*	
				.... 0101 =		*Header Length: 20 bytes (5)*	
				Differentiated Services Field:		*0x00 (DSCP: CS0, ECN: Not-ECT)*	
				Total Length:		*1157*	
				Identification:		*0x054a (1354)*	
				Flags:		*0x02 (Don't Fragment)*	
				Fragment offset:		*0*	
				Time to live:		*128*	
				Protocol:		*TCP (6)*	
				Header checksum:		*0x9e01 [validation disabled]*	
				Header checksum status		*Unverified*	
				Source:		*192.168.0.103 (192.168.0.103)*	
				Destination:		*a-0001.a-msedge.net (204.79.197.200)*	
				Source GeoIP		*Unknown*	
				Destination GeoIP:	*Destination GeoIP Country:*	*United States*	
					Destination GeoIP AS Number:	*AS8068 Microsoft Corporation,*	
					Destination GeoIP City:	*Redmond, WA,*	
				Destination GeoIP:	*Destination GeopIP Latitude:*	*47.680099,*	Baixa
					Destination GeoIP Longitude	*-122.120598*	

Bing	http	Transporte	*Transmission Control Protocol*	*Src Port:*	*49246 (49246)*	Baixa
				Dst Port:	*http (80)*	
				Stream index	*8*	
				TCP Segment Len	*1117*	
				Sequence number	*972*	
				Next sequence number	*2089*	
				Acknowledgment number	*1126*	
				Header length	*20 bytes (5)*	
				Flags	*0x018 (PSH, ACK)*	
				Window size value	*16278*	
				Calculated window size	*65112*	
				Windows size scaling fator	*4*	
				Checksum	*0xdbf5(Unverified)*	
				Checksum status	*Unverified*	
				Urgente pointer	*0*	
				SEQ/ACK analysis — *The RTT to ACK the segment was*	*0.052778000 seconds*	
				SEQ/ACK analysis — *iRTT*	*0.027093000 seconds*	
				SEQ/ACK analysis — *Bytes inflight*	*945*	Baixa
				SEQ/ACK analysis — *Bytes sent since last PSH flag*	*1117*	
				TCP payload	*1117 bytes*	
		Aplicação	*Hypertext Transfer Protocol*	*GET*	*search?**q=big+data**&qs=n&form=QBLH&sp=-1&ghc=1&pq=big+data&sc=8-8&sk=&cvid=8F287045526849BC9177929B9C9E8AC8 HTTP/1.1*	Alta
				Host	*www.bing.com*	Alta
				Connection	*keep-alive\r\n*	Baixa
				Upgrade-Insecure-Requests	*1\r\n*	

				User-Agent	*Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36\r\n*	Baixa
				Accept	*text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n*	
				DNT	*1*	Baixa
				Referer	***http://www.bing.com/search?q=big+data&qs=AS&pq=big+d&sc=8-5&cvid=43E95DB1C29F45AF9990DFDE91CB4ABA&FORM=QBLH&sp=1&ghc=1\r\n***	Alta
				Accept-Encoding	*gzip, deflate, sdch*	Baixa
				Accept-Language	*pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4*	Baixa
				Cookie	_ : _EDGE_V=1; MUID=025A703366B86D0B154D7B1F67716CCE; MUIDB=025A703366B86D0B154D7B1F67716CCE; SRCHD=AF=NOFORM;	
Google	https	Enlace	*Ethernet II*	*Src:*	*HonHaiPr_f8:b1:51 (7c:e9:d3:f8:b1:51)*	Baixa
				Dst:	*Tp-LinkT_15:e5:66 (00:23:cd:15:e5:66)*	Baixa
		Rede	*Internet Protocol Version 4*	*Src:*	*192.168.0.103 (192.168.0.103)*	Baixa
				Dst:	*gru10s02-in-f163.1e100.net (172.217.29.163)*	
				0100 .... =	*Version: 4*	
				.... 0101 =	*Header Length: 20 bytes (5)*	
				Differentiated Services Field:	*0x00 (DSCP: CS0, ECN: Not-ECT)*	
				Total Length:	*193*	
				Identification:	*0x0838 (2104)*	
				Flags:	*0x02 (Don't Fragment)*	
				Fragment offset:	*0*	
				Time to live:	*128*	
				Protocol:	*TCP (6)*	
				Header checksum:	*0x1ae3 [validation disabled]*	

Google	https	Transporte	*Transmission Control Protocol*	*Header checksum status*		*Unverified*	Baixa
				Source:		*192.168.0.103 (192.168.0.103)*	
				Destination:		*gru10s02-in-f163.1e100.net (172.217.29.163)*	
				Source GeoIP		*Unknown*	
				Destination GeoIP:	*Destination GeoIP Country:*	*United States*	
					Destination GeoIP AS Number:	*AS1569 Google Inc.*	
				Destination GeoIP:	*Destination GeoIP City:*	*Mountain View, CA*	Baixa
					Destination GeoIP Latitude:	*37.4192201*	
					GeoIP Longitude:	*-122.057404*	
				Source Port:		*49277 (49277)*	Baixa
				Destination Port:		*https (443)*	
				Stream index		*1*	
				TCP Segment Len		*153*	
				Sequence number		*414*	
				Next sequence number		*567*	
				Acknowledgment number		*925*	
				Header length		*20 bytes (5)*	
				Flags		*0x018 (PSH, ACK)*	
				Window size value		*16477*	
				Calculed window size		*16306*	
				Windows size scaling fator		*-1 (unknown)*	
				Checksum		*0xe9fe (Unverified)*	
				Checksum status		*Unverified*	
				Urgente pointer		*0*	
					Bytes in flight	*153*	
					Bytes sent since last PSH flag	*153*	
				TCP payload		*153 bytes*	

		Apresentação	*Secure Sockets Layer*	*TLSv1.2 Record Layer:*	*Application Data Protocol: http-over-tls*	Baixa
				Contente Type	*Application Data (23)*	
				Version	*TLS 1.2 (0x0303)*	
				Length	*148*	
				Encrypted Application Data	*a81a0c5a6b5701f1a7710c57dce9f70094303ad7ca8a6116...*	
DuckDuckgo	https	Enlace	*Ethernet II*	*Src:*	*HonHaiPr_f8:b1:51 (7c:e9:d3:f8:b1:51)*	Baixa
				Dst:	*Tp-LinkT_15:e5:66 (00:23:cd:15:e5:66)*	
				Type	*IPv4 (0x0800)*	
		Rede	*Internet Protocol Version 4*	*Src:*	*192.168.0.101 (192.168.0.103)*	
				Dst:	*ec2-184-72-106-52.compute-1.amazonaws.com (184.72.106.52)*	
				0100 .... =	*Version: 4*	
				.... 0101 =	*Header Length: 20 bytes (5)*	
				Differentiated Services Field:	*0x00 (DSCP: CS0, ECN: Not-ECT)*	
				Total Length:	*162*	
				Identification:	*0x0ada (2778)*	
				Flags:	*0x02 (Don't Fragment)*	Baixa
				Fragment offset:	*0*	
				Time to live:	*128*	
				Protocol:	*TCP (6)*	
				Header checksum:	*0x0bf0 [validation disabled]*	
				Header checksum status	*Unverified*	
				Source:	192.168.0.103 (192.168.0.103)	Baixa
				Destination:	*ec2-184-72-106-52.compute-1.amazonaws.com (184.72.106.52)*	
				Source GeoIP	*Unknown*	
				Destination GeoIP: / *Destination GeoIP Country:*	*United States*	

DuckDuckgo	Htpps				*Destination GeoIP AS Number:*	AS14618 *Amazon.com, Inc*.	
					Destination GeoIP City	Ashburn, Va	Baixa
					Destination GeoIP Latitude	39.048100	
					Destination GeoIP Longitude	-77.472801	
		Transporte	*Transmission Control Protocol*	*Source Port:*		49296 (49296)	
				Destination Port:		https (443)	
				Stream index		2	
				TCP Segment Len		122	
				Sequence number		1	
				Next sequence number		123	
				Acknowledgment number		1	
				Header length		20 bytes (5)	
				Flags		0x018 (PSH, ACK)	Baixa
				Window size value		16560	
				Calculed window size		16560	
				Windows size scaling fator		*-1 (unknown)*	Baixa
				Checksum		*0x4d35 (Unverified)*	
				Checksum status		*Unverified*	
				Urgente pointer		0	
				SEQ/ACK analysis	*Bytes in flight*	122	
					Bytes sent since last PSH flag	122	
				TCP payload		122 bytes	
		Apresentação	*Secure Sockets Layer*	*TLSv1.2 Record Layer:*		*Application Data Protocol: http-over-tls*	Baixa
				Content Type		*Application Data (23)*	
				Version		*TLS 1.2 (0x0303)*	
				Length		200	
				Encrypted Application Data		5c953cea6ce97cbba09314c33ccb747db2d866a43bd1cccc...	

Fonte: Elaborado pela autora

Os dados apresentados no Quadro 16 foram extraídos de pacotes de dados de tráfego durante a interação do usuário com os mecanismos de busca. Observa-se que os dados de tráfego de rede podem relevar informações sobre a atividade do usuário e, consequentemente, ameaçar a privacidade dos indivíduos referenciados nesses dados, sem que esses tenham consciência sobre a coleta de dados.

Os dados de tráfego podem representar um conteúdo potencialmente sensível e se tornam ativos valiosos para vários interessados, como organizações públicas e privadas (AURA; ZUGENMAIER, 2004; LIN; LIN, 2012; LIN et al., 2016). Por exemplo, é possível associar a um indivíduo apenas pelos registros de data e hora da interação e informações adicionais da conta, o que conduz a quebras de privacidade (DUCKDUCK, 201-).

Observa-se, no Quadro 16, a possível presença de dados sensíveis, tais como os valores presentes nos atributos *host*, *cookies* e *encrypted application data*; e a presença de dados semi-identificadores, tais como os atributos IP, *Time-to-Live*, *Source GeoIP; Destination GeoIP*; *Src Port* e *Dst Port;* e ainda dados que são identificadores únicos, presentes no campo Ethernet II, como o atributo Src, por exemplo, representando o valor MAC da máquina do usuário. Ressalta-se que esses dados seguem o padrão estipulado pela estrutura da ferramenta *Wireshark*, o que sugere que outros dados podem estar presentes durante a coleta e não são abarcados pela ferramenta.

Há uma miríade de opções de combinação dos dados presentes nos pacotes de rede que podem implicar em ameaças à privacidade do usuário. Segundo Lin e Lin (2012) e Lin et al. (2016), determinar quais campos representam ameaças à privacidade ou devem ser anonimizados se torna um grande esforço, devido à semântica de todos os campos sensíveis e semi-identificadores, resultado da grande quantidade de dados extraídos dos pacotes coletados. Portanto, a ocorrência dessa atividade não está visível para o usuário, tornando-o insciente sobre a fase de coleta, limitando as suas ações para proteção da privacidade.

Para elucidar as possíveis brechas de privacidade e a insciência do usuário sobre a coleta de dados, descreve-se, a seguir, as camadas de abstração do modelo OSI e os principais campos coletados.

A camada física não fica visível pela captura no *sniffer*, pois consiste no conjunto de *bits* e sinais elétricos gerados durante a conexão com a Internet. Pode-se considerar que é alta a insciência sobre os dados que circulam nessa camada.

Na camada de enlace estão presentes os dados referentes ao equipamento do usuário, neste caso, o número do endereço MAC. Esse endereço, determinado pelo número da interface da rede, está presente nas três capturas, determinando o número do endereço MAC do

computador do usuário. Esse endereço é único, assim, as questões de privacidade estão ameaçadas se um observador da rede tiver acesso ele. Para Aura e Zugenmaier (2004) e Cunche (2014), o endereço MAC de um indivíduo pode ser usado para conhecer informações de sistemas e identificar o dispositivo do usuário. Mesmo que a carga útil dos pacotes seja criptografada, o cabeçalho é sempre transmitido, isso significa que o endereço MAC dos dispositivos pode ser coletado e usado para identificar, de forma exclusiva, o dispositivo do proprietário (CUNCHE, 2014). Não é perceptível para o usuário que, durante a interação com aplicações Web, o endereço da sua máquina está sendo coletado e poderá ser utilizado para identificação posterior.

Na camada de rede, o pacote carrega os endereços IP origem e IP destino, que caracteriza dados que podem possibilitar a identificação do indivíduo. Para Heidemann e Papadopoulos (2009), os atributos com valores de endereço IP representam ameaças à privacidade porque é possível relacioná-los com a identidade dos indivíduos. É importante notar que os endereços IP, por si só, não identificam os usuários, mas a combinação com informações externas, como registro de usuário, registros do protocolo DHCP (*Dynamic Host Configuration Protocol*) ou dados de *cookies*, podem ser utilizados para mapear o usuário.

Também se encontra o atributo TTL (*Time-to-Live*) na camada de rede. Por meio do seu valor, é possível adivinhar quantos saltos o pacote realizou (PEUHKURI, 2001). Com essa informação, pode ser conhecido o sistema operacional que o usuário utiliza, já que cada sistema operacional possui seu TTL padrão. Essa correlação de informação pode implicar na violação da privacidade do indivíduo.

Embora os dados de TTL não indiquem, diretamente, ameaças à privacidade, eles podem ser utilizados para *fingerprint*, termo definido na RFC 6973 como um conjunto de elementos de informação que identifica um aplicativo ou dispositivo, ou para *fingerprinting*, definido como o processo de um observador identificar exclusivamente um dispositivo ou aplicação baseada em um conjunto de múltiplas informações (COOPER et al., 2013).

Nesse contexto, Saraiva et al. (2014) atribui a *fingerprinting* o conjunto amplo de tecnologias e técnicas que podem receber o nome de *Device Intelligence*, *Machine Fingerprinting*, *Browser Fingerprinting*, *Web Fingerprinting* ou *Device Fingerprinting*. Mediante essas técnicas ou tecnologias é possível acessar a um conjunto de configurações e dados, tais como tamanho da tela do dispositivo, versão de *softwares* e outros dados, tornando-se possível identificar o usuário ou seu dispositivo.

Na camada de transporte encontram-se os campos referentes à porta de origem e de destino (80/http e 443/https), esses campos determinam o término da conexão e podem ser

utilizados para identificar a aplicação utilizada pelo usuário (PEUHKURI, 2001). Por exemplo, a porta 80 indica a transferências de páginas www, a porta 110/TCP é usada para recebimento de e-mail, e a porta 443/TCP é usada para transferência de páginas seguras. Portanto, a presença de portas de comunicação revela algo sobre a atividade do usuário e, quando combinada com outros dados, caracteriza também ameaça à privacidade.

O comprimento total do *datagrama* IP (*TCP Segment Len)* e o campo *checksum*[106] presentes nessa camada também podem revelar informações sobre os protocolos ou a carga útil do pacote quando combinado com outros campos (PEUHKURI, 2001). Os campos *Sequence number*, *Windows size value*, *Calculed Windows Size*, *Windows Size Scaling fator* são utilizados na numeração dos dados enviados e no controle do fluxo, e em combinação com outros dados podem ser utilizados na identificação do sistema operacional, denominados descoberta por *Operating System fingerprinting* (PEUHKURI, 2001).

Embora muitos desses campos não sejam considerados sensíveis, eles podem se tornar bastantes influentes, pois muitos se caracterizam como semi-identificadores. As diversas combinações desses campos podem ampliar o conhecimento sobre o processo e sobre o indivíduo pelos detentores de dados, e consequentemente, impulsiona quebras de privacidade e acentua a insciência do usuário sobre o processo de coleta de dados.

A camada de aplicação é a mais próxima do usuário. Nela, é possível notar, na interação com o serviço *Bing*, dados de solicitação do usuário. Como o serviço não estava operando com criptografia, os dados ficaram visíveis nessa camada, inclusive a presença de *cookies* coletados da máquina do usuário para o serviço do mecanismo de busca.

Por meio do comando GET, o cliente (192.168.0.101) envia um pacote para o servidor (204.79.197.200); esse comando é utilizado quando o usuário solicita algo à página (no caso, o termo de busca). Dentre as informações especificadas no método GET, estão a URI (*Uniform Resource Identifier*) da página do mecanismo, endereço para onde os dados estão sendo enviados; cabeçalho *user-agent*[107], com informações sobre navegador e sistema operacional; cabeçalho *referer*, que indica a URL (*Uniform Resource Locator*) onde o pedido foi originado; e o cabeçalho *accept-language*, que informa ao servidor o idioma que a máquina cliente estará utilizando.

[106] Denominado de campo soma de verificação (*checksum*) tem a finalidade de identificar se o pacote foi transmitido sem erros.

[107] Identifica o navegador do usuário e fornece determinados detalhes do sistema operacional aos servidores que hospedam os sites que o usuário visita (MICROSOFT, 2017).

Por meio do cabeçalho *user-agent*, cada vez que o usuário entra no mecanismo de busca, ele revela exatamente o navegador que o usuário está utilizando e mais alguns dados. Essas informações podem ajudar a distinguir os usuários da Internet um dos outros.

Uma pesquisa realizada pela *Electronic Frontier Foundation* (EFF) sobre *fingerprinting* do *browser*[108] verificou como as informações presente no atributo *user-agent* poderiam ser usadas para rastrear pessoas, mesmo que tivessem excluído os *cookies*. Dessa forma, o experimento verificou se o *user-agent* sozinho, ou combinado com outros dados, seria suficiente para permitir que um *site* identificasse o usuário. Como resultado, obteve-se que a sequência de *user-agent* carrega em média 5-15 bits de dados de identificação e revela que apenas uma pessoa em 1.500 terá o mesmo *user-agent*. Segundo a pesquisa, esse resultado não significa que o *user-agent* é suficiente para rastrear pessoas, mas em combinação com dados de geolocalização ele se torna um verdadeiro problema de privacidade (ECKERSLEY, 2010).

Assim, a pesquisa da EFF conclui que o cabeçalho *user-agent*, ao revelar dados do navegador, implica em ameaças à privacidade. Isso indica que a maioria dos usuários da Internet pode ser rastreada usando exclusivamente os dados de configuração e a versão dos navegadores que são disponibilizados para os *sites*. Esses tipos de dados podem ser considerados identificadores, da mesma forma que os *cookies*, os endereços IP e os *supercookies* (ECKERSLEY, 2010).

Segundo a W3C (2015), a *fingerprinting* do browser é uma ameaça potencial à privacidade dos usuários da Web, devido à possibilidade de identificação do usuário; ao correlacionamento das atividades de navegação do usuário; ao rastreamento das suas atividades, sem que ele tenha consciência ou controle.

Devido aos mecanismos de busca *Google* e *DuckDuckgo* utilizarem de criptografia, surge o campo *Secure Sockets Layer* (SSL), que atua na camada de apresentação do modelo OSI, em que os dados são transformados para serem enviados e lidos pela camada de aplicação. O campo SSL faz referência ao uso do protocolo TLS v1 (*Transport Layer Security*) [109], responsável pelo processo de criptografia dos dados. Embora a criptografia seja utilizada para promover a segurança durante a comunicação, impedindo a intercepção por terceiros, o fato dos dados estarem criptografados não torna possível visualizar os dados da interação, ampliando ainda mais

[108] Definida pela W3C (2015) como a capacidade de um site identificar ou reidentificar um usuário visitante, *user-agent* ou dispositivo por meio de configurações ou outras características, podendo prejudicar a privacidade do usuário.

[109] Esse protocolo tem a finalidade de proporcionar privacidade e integridade dos dados entre duas aplicações (DIERKS; RESCORLA, 2008).

a insciência sobre o processo, pois nas políticas de privacidade não é mencionado quais dados são criptografados e durante a análise de pacotes não é possível ter ciência sobre esses dados.

Mediante o uso de *cookies*, é possível armazenar dados de sessão, dados de *login*, fornecer recursos de personalização, no entanto, eles também podem ser usados para rastrear a atividade de um usuário (MCKINLEY, 2008). Segundo Schoen (2009), os *cookies* ainda são um problema de privacidade para os usuários da Web, pois são um dos principais mecanismos que as empresas publicitárias, como o *Google*, usam para rastrear e criar perfis de usuários em todos os *sites* e ao longo do tempo. O *cookie* tradicional é um cookie HTTP, mas muitos navegadores implementam vários mecanismos semelhantes aos *cookies*, que são difíceis de notar e muito mais difícil de controlar. Assim, essas atividades resultam na coleta de dados pessoais do indivíduo, invadindo sua privacidade, sem que eles ao menos tenham consciência do teor desses dados (SCHOEN, 2009).

A consciência do usuário é maior na camada de aplicação, por caracterizar a interação do usuário com página Web, e diminui à medida que se estende até a camada física. Embora a camada de aplicação promova uma interface mais amigável para o usuário, ela pode promover uma consciência fictícia. Por exemplo, o envio de *cookies*, dados do navegador e sistema operacional para o destino não são claramente perceptíveis para o usuário. Por exemplo, o usuário pode ter a ciência de que há a coleta de *cookies*, pois está explícito nas políticas de privacidade; no entanto, não está perceptível o que representa, semanticamente, o conteúdo dos *cookies*, o que torna o usuário insciente sobre a coleta.

6.6 Considerações Finais

Neste capítulo foram expostos os possíveis dados coletados pelos mecanismos de busca, tanto pelas menções nas políticas de privacidade quanto pela análise dos dados coletados com ferramenta *Wireshark* (dados de tráfego de rede), resultantes da interação do usuário com os mecanismos de busca. Por meio desses resultados, é possível demonstrar como a insciência do usuário se configura na fase de coleta, indicando as possíveis ameaças à privacidade.

Observa-se que o cenário da coleta de dados pelos ambientes digitais, no caso desta pesquisa, pelos mecanismos de busca, descaracteriza muitas das determinações presentes nas legislações, pois as leis que amparam as questões de proteção de dados determinam diretrizes, para proporcionar a consciência sobre a coleta de dados, por meio do consentimento informado e da transparência sobre essa atividade.

No entanto, o que se tem são políticas de privacidade rasas ao indicar os possíveis dados que a aplicação terá acesso, e que não deixam explícita a indicação do potencial destinatário e os dados coletados por cada serviço oferecido ao usuário.

A maioria dos dados coletados pelos mecanismos de busca são os semi-identificadores, situação que pode ampliar ainda mais ameaça a privacidade, devido à possibilidade de correlação desses dados, e com isso, a construção de perfis de indivíduos. O que prevalece é um uso além do necessário para o motivo que foi coletado, desconfigurando a minimização dos dados. Conforme citado na política de privacidade do DuckDuckgo, "os mecanismos de busca não são legalmente obrigados a coletar informações pessoais em primeiro lugar. Eles fazem isso por sua própria vontade" (DUCKDUCKGO, 201[-]).

A insciência do usuário sobre a coleta de dados em ambientes digitais é acentuada, devido à abstração presente na própria interface das redes de computadores, que resulta em uma opacidade sobre os elementos que participam dessa atividade. Essa interface abstrai situações que torna a coleta de dados imperceptível para o usuário, o que resulta em brechas de privacidade, ainda não mensuradas, indo muito além dos dados coletados pelos detentores, tal como a interceptação por terceiros e as ações por meio de *fingerprints*.

A proteção de dados pessoais é muito alinhada às questões de segurança da informação, tal como os danos causados por intercepção de terceiros (invasores) às máquinas e arquivos de usuários, cenário que o usuário aparenta ter mais ciência sobre a necessidade de medidas e aplicações para salvaguardas de privacidade.

Entretanto, a segurança não é garantia de privacidade de dados. Como demonstrado na coleta de dados pelos mecanismos de busca, os metadados de comunicação compõem as técnicas de *fingerprinting,* que permite que empresas rastreie o indivíduo, sem que ele tenha conhecimento sobre essa atividade. Inclusive, os dados que são criptografados podem apresentar garantias de segurança à interceptação, mas não garantias à privacidade do usuário, pois o usuário não tem conhecimento de quais dados estão saindo da sua máquina e indo para o destino. Não é possível controlar e impedir que esses dados sejam criptografados ou ainda impedir a coleta. Desta forma, o usuário se torna insciente sobre os elementos presentes nesse processo de coleta de dados pelas aplicações, ampliando, ainda mais, as brechas de privacidade.

Face ao exposto, "***a abstração na fase de coleta de dados, promovida pela própria interface das redes de computadores e pela falta de clareza das políticas de privacidade"*** pode contribuir para um cenário que propicia a insciência na fase de coleta de dados nos ambientes digitais, insciência esta que pode ter impactos em questões de privacidade.

Ciente dos possíveis dados coletados pelos ambientes digitais, exposto neste capítulo mediante a menção nas políticas de privacidade e pelos dados de tráfego durante a interação do usuário com os mecanismos de busca, o próximo capítulo versa sobre as principais ameaças à privacidade em relação aos mecanismos de busca.

7 AMEAÇAS À PRIVACIDADE DOS USUÁRIOS NA INTERAÇÃO COM MECANISMOS DE BUSCA

> *Em cada patamar, diante do poço do elevador, o rosto enorme fitava-o da parede. Desses retratos de tal maneira conseguidos que os olhos nos seguem os movimentos. O GRANDE IRMÃO ESTÁ A VER-TE, rezava por baixo a legenda (ORWELL, 2009, p. 7).*

A fase de coleta de dados é a gênese para as próximas fases do ciclo de vida dos dados. Logo, os relatos mencionados em relação à coleta de dados pelos mecanismos de busca e outras aplicações web impactam a privacidade dos usuários no armazenamento, na recuperação e até no descarte desses dados. Indubitavelmente, a insciência sobre a fase de coleta de dados resulta em negligências nas ações para proteção de dados pessoais. Diante desse cenário, este capítulo aborda as principais ameaças à privacidade em relação aos mecanismos de busca.

7.1 Resultados e Discussões

Baseado no framework proposto por Solove (2006) identifica-se neste capítulo as ameaças à privacidade do usuário que interagem com os mecanismos de busca, considerando: as fases de Coleta (Vigilância e Interrogatório), Processamento de Informação (Agregação, Identificação, Insegurança; Uso Secundário e Exclusão; Disseminação de Informação (Quebra de Sigilo; Divulgação; Exposição; Aumento do Acesso; Chantagem; Apropriação e Distorção); e Invasão (Intromissão e Interferência Decisional). A análise realizada tem a finalidade de demonstrar que quando a insciência do usuário transcorre na fase de coleta pode impactar nas outras fases do ciclo de vida dos dados.

7.1.1 Fase de coleta da informação

No âmbito dos mecanismos de busca, a **vigilância** se efetua no momento em que são coletados os termos de busca e os dados da interação usuário-mecanismo. Para Affonso et al. (2017, p. 428) “[...] com o resultado dessa interação, os mecanismos obtêm mais dados sobre o usuário do que ele imagina”. Por meio do Quadro 15 foi possível constatar dados coletados pelos mecanismos de busca, que só se tornam perceptíveis para o usuário quando ele se propõe a ler e a interpretar as políticas de privacidade, salvo os dados que ele disponibiliza cientemente. Por outra perspectiva, o Quadro 16 descreveu os possíveis dados coletados e identificados por meio de ferramentas para análise de pacotes de redes, cuja semântica dos dados e suas

correlações com outros dados estão muito distante da ciência do usuário. Ao acompanhar esses dados de toda interação do usuário com o mecanismo de busca, o usuário fica sob um estado de vigilância constante.

> Um aspecto importante da privacidade para os indivíduos [...] é a capacidade de se movimentar de hora em hora. Pois um aspecto importante da vigilância física depende de saber onde o "sujeito" está em todos os momentos, e especialmente para onde ele vai quando quer ficar sozinho, a sombra física tem sido uma técnica de vigilância desde a antiguidade. O que a nova tecnologia acrescenta é a maneira de "marcar" as pessoas para que elas possam ser seguidas de maneira mais eficiente e com menos riscos de descobertas[110] (WESTIN, 1967, p.73).

Para que o usuário tenha maior relevância nos resultados disponibilizados pelo mecanismo de busca, nas configurações do serviço é sugerido que, durante a interação com o ambiente, o usuário esteja conectado à sua conta; para isso, ele precisa ter realizado, anteriormente, algum tipo de cadastro para ter acesso ao serviço. "Quando o usuário está conectado à sua Conta do *Google* e está com o Histórico da Web ativado, pode receber resultados de pesquisa mais relevantes com base no seu Histórico da Web" (GOOGLE, 201-). Esse cenário pode ser caracterizado como atividade de **interrogatório**, em que, ao contrário da vigilância, o usuário tem consciência sobre a coleta dos seus dados (SOLOVE, 2006).

Tanto o mecanismo de busca *Google* quanto o *Bing* justificam em suas políticas de privacidade que a coleta de dados do usuário é importante para proporcionar melhores resultados na busca:

> Usamos as informações que coletamos em todos nossos serviços para fornecer, manter, proteger e melhorar esses serviços, desenvolver novos e proteger a Google e nossos usuários. Também usamos essas informações para oferecer ao usuário um conteúdo específico, por exemplo, fornecer resultados mais relevantes de pesquisa e anúncios" (GOOGLE, 201-).

Assim, a fase de coleta pode estar atrelada ao grau de poder entre detentores e titulares de dados, criando uma assimetria informacional. Mayer-Schönberger (2011) ressalta que os detentores ampliam seu poder sobre a situação ao ganhar acesso à informação, principalmente

---

[110] *A major aspect of privacy for individuals […] is the ability to move about anonymously from time to time. Because a major aspect of physical surveillance depends on knowing where the "subject" is at all times, and especially where he goes when wants to be alone, physical shadowing has been a technique of surveillance since antiquity. What the new technology adds is ways to "tag" persons so that they can be followed more efficiently and with less risk of discovery*

quando o titular dos dados não tem consciência sobre a coleta e não permitiu a atividade, implicando na perda de poder e controle sobre seus dados.

7.1.2 Fase de processamento da informação

Nos mecanismos de buscas, a **agregação** de dados tem a intenção de disponibilizar melhores resultados para o usuário. Por exemplo, ao realizar uma busca sobre uma determinada faculdade, o mecanismo de busca combina dados de IP e de localização, recuperando nos primeiros resultados as faculdades mais próximas geograficamente do usuário. No mecanismo *Google*, é exibido na barra lateral informações sobre a faculdade pesquisada pelo usuário, recurso utilizado pela *Google* para apresentar o resultado da busca de forma mais rápida e interessante para o usuário. Outra situação de agregação de dados pode ser observada quando o usuário realiza uma pesquisa por determinado produto no mecanismo de busca e, posteriormente, ao entrar em uma rede social, são disponibilizados vários anúncios e *post* relacionados com essa busca. Observa-se que tal atividade amplia o poder dos detentores de dados em relação ao conhecimento que ele tem sobre o indivíduo, pois dados isolados passam a compor o conjunto e, com o perfil do usuário, consequentemente, ampliam-se as ameaças à privacidade.

> Podemos combinar informações pessoais de um serviço com informações (pessoais inclusive) de outros serviços da Google para facilitar o compartilhamento de informações com pessoas que o usuário conhece, por exemplo. Dependendo das configurações da conta, as atividades do usuário em outros *sites* e apps podem ser associadas às informações pessoais dele para melhorar os serviços da Google e os anúncios fornecidos por ela (GOOGLE, 201-).

Ao utilizar recurso baseado em cliques e endereço IP, os mecanismos de busca **identificam** o usuário nos mais diversos contextos, e os próximos resultados da busca e da divulgação de anúncios são determinados por esse relacionamento identificação-contexto. Os dados de IP e *fingerprints* também permitem a identificação do usuário quando combinados com outros dados de interação.

Durante a interação do usuário com mecanismo de busca pode ocorrer à interceptação de terceiros por meio de *softwares* de análise de pacotes de redes, os denominados *sniffers*. Com esse acesso ao fluxo de dados que circula na rede, pode haver roubo de dados e de informações confidenciais, dependendo, assim, de ações para inibir ameaças à privacidade dos indivíduos. Inclusive, se o servidor for invadido, são anuladas as garantias de privacidade, uma vez que, ao utilizar os mecanismos de busca, o usuário deposita toda sua necessidade e intenção

de busca na caixa de pesquisa, revelando muitas vezes seus segredos mais íntimos, que ficam sob a tutela do mecanismo. Esses relatos podem ou deveriam gerar ao usuário **insegurança** na interação com o serviço.

Na política de privacidade do *Google*, são descritas questões referentes ao compartilhamento de dados. Consequentemente, o **uso secundário** desses dados não é explícito. Não se sabe, portanto, quem são os parceiros mencionados na política de privacidade com quem o Google irá compartilhar as informações.

> Podemos compartilhar informações de identificação não pessoal publicamente e com nossos parceiros – como editores, anunciantes, desenvolvedores ou detentores de direitos. Por exemplo, compartilhamos informações publicamente para mostrar tendências sobre o uso geral dos nossos serviços. Também permitimos que parceiros específicos coletem informações do seu navegador ou dispositivo para fins de publicidade e medição usando os próprios *cookies* ou tecnologias semelhantes (GOOGLE, 201-).

Nos mecanismos de busca, as políticas de privacidade se propõem a garantir a consciência para evitar a **exclusão** do usuário sobre as atividades realizadas com os seus dados, de forma que o usuário saiba quais dados são coletados, como são coletados e o uso desses dados. No entanto, a política traz informações referentes aos serviços da empresa *Google* e não retrata as especificações de coleta do mecanismo, ao contrário do mecanismo *Bing*, que é estipulada na política da *Microsoft* um tópico para descrever possíveis dados que são coletados com a interação do usuário com o serviço de busca (AFFONSO et al., 2017).

7.1.3 Fase de disseminação da informação

Em relação à divulgação de dados a terceiros, o mecanismo de busca *Google* menciona na sua política de privacidade:

> Fornecemos informações pessoais a nossas afiliadas ou outras empresas ou pessoas confiáveis para processá-las para nós, com base em nossas instruções e em conformidade com nossa Política de Privacidade e quaisquer outras medidas de segurança e de confidencialidade adequadas (GOOGLE, 201-).

Para Thomson (1975), se um indivíduo fornece informações sob a condição de que elas não devem ser compartilhadas, e isso não acontece, o direito à confidencialidade é violado, sejam essas informações pessoais ou não. Caso a informação seja pessoal, também ocorre à violação do direito à privacidade, o ponto é válido se o motivo para compartilhar a informação é maliciosa ou gere lucros. O ato de fornecer informações a outros, sendo esses outros parceiros ou afiliados, resulta no **aumento de acesso** aos dados dos indivíduos, caracterizando ameaça à privacidade.

Ao utilizar mecanismo de busca, o usuário acredita que toda a interação ocorre apenas com o provedor do serviço, sem que se forneçam informações pessoais a outras empresas. Porém ao utilizar o serviço e, principalmente, se estiver logado em sua conta, mais dados pessoais do usuário podem estar sendo fornecidos para outras empresas, e o usuário não tem consciência e nem poder de decidir sobre o fornecimento desses dados.

Na política de privacidade do mecanismo de busca *Google*, fica explícita a questão de violação da **confidencialidade** (quebra de sigilo) ao descrever:

> Também coletamos o conteúdo que você cria, de que faz upload ou que recebe de outras pessoas ao usar nossos serviços. Isso inclui e-mails enviados e recebidos, fotos e vídeos salvos, documentos e planilhas criados e comentários feitos em vídeos do YouTube" (GOOGLE, 201-).

Na ameaça da **divulgação**, o *Bing* anonimiza os dados da interação após 18 meses. "Removemos a identificação de consultas de pesquisa armazenadas ao excluir todo o endereço IP ao fim de 6 meses, bem como IDs de *cookies* e outros identificadores cruzados de sessões de pesquisa ao fim de 18 meses" (BING, 201-). Essa questão da anonimização de dados é efetuada na fase de recuperação, no momento da coleta não há menção de anonimização pelos mecanismos de busca.

A ameaça de **apropriação** é resultado da coleta e do compartilhamento de dados, pois, ao obter os dados, os mecanismos de busca ou terceiros passam a ter propriedade sobre o conjunto de dados do indivíduo, principalmente sem a consciência do usuário. Assim, para Solove (2006), a violação da apropriação está relacionada à proteção dos direitos de propriedade.

No âmbito dos mecanismos de busca, a **distorção** pode acontecer na medida em que os dados do indivíduo são utilizados para montar perfil de acordo com a interação no ambiente, ou quando há o uso dos dados entre empresas parceiras, que podem utilizar esses dados em outros contextos, não especificamente com o mesmo objetivo de quando o usuário os disponibilizou. A distorção se caracteriza quando o mecanismo de busca insere o usuário no que Pariser (2012) denomina de "filtro bolha", resultados baseados naquilo que o mecanismo acredita que é importante para o usuário.

Ao pesquisar um termo de busca no mecanismo, observa-se que o assunto pesquisado retorna em forma de anúncios durante a sua interação com outros *sites*, o que, indiretamente, está relacionado à coleta realizada pelo mecanismo de busca. Inclusive, as ações de *fingerprinting*, ao identificar o usuário, implica em rastreio, o que se caracteriza, posteriormente, como uma **intromissão** durante a permanência do usuário na Web.

Quando há a necessidade de compartilhamento de informações com o governo, caracteriza-se a **interferência decisional.** Essa interferência, de acordo com Solove (2006), envolve a incursão do governo nas decisões pessoais quando relacionadas a causas privadas do indivíduo. Na política do *Bing* ficam evidentes as situações em que podem ocorrer interferência decisional: [...] retemos, acessamos, transferimos, divulgamos e guardamos dados pessoais, incluindo seus conteúdos [...] quando acreditamos de boa-fé que isso é necessário para: cumprir a lei ou responder a processos legais [...] (BING, 201-).

A fase de **chantagem** e **exposição** não estão explícita na interação com os mecanismos de busca, de acordo com a abordagem dada por Solove (2006). Ao resgatar as ameaças determinadas por Solove (2006), observa-se que muitas ameaças de privacidade estão presentes durante a interação com os mecanismos de busca, sendo que a fase de coleta de dados é crucial e decisória para outras fases do ciclo de vida dos dados. Nos mecanismos de buscas, a interação do usuário com o ambiente pode perpassar esses grupos e subgrupos estipulados na taxonomia, caracterizando as possíveis quebras de privacidade, em que o usuário é insciente sobre a coleta e sobre as possíveis ameaças à privacidade.

7.2 Considerações Finais

Este capítulo abordou sobre as possíveis ameaças quando o usuário utiliza dos mecanismos de busca, no entanto, essas ameaças podem se efetuar em vários outros ambientes digitais.

Para essa identificação utilizou-se o framework proposto por Solove (2006), que desenvolveu essa taxonomia para delimitar atividades que impactam a privacidade nas fases de coleta, processamento de informação, disseminação e invasão, pois o autor considera que o termo privacidade era vago para que juristas pudessem tomar as decisões quando ocorriam agravos em relação à proteção de dados dos indivíduos.

Assim, melhorias para essas ameaças de privacidade dependem de como o ordenamento jurídico irá conduzir essas questões, uma vez que, para as organizações estarem em conformidade com regulamentos é necessária à concretização de políticas de privacidade e adoção de técnicas para proteger dados pessoais, medidas que quando adotadas podem minimizar quebras de privacidade e fomentar novas investigações e aplicações científicas.

8 CONCLUSÕES

> *Existem momentos na vida onde a questão de saber se se pode pensar diferentemente do que se pensa, e perceber diferentemente do que se vê, é indispensável para continuar a olhar ou refletir [...] (FOUCAULT, 1984, p. 13).*

A coleta de dados realizada no ciberespaço acentua as questões envolvidas com quebra de privacidade, reflexo do rastreio imediato durante as interações do usuário e que oportuniza o uso dos dados pelos detentores em diversas situações, sem que o usuário tenha a percepção sobre essa atividade, tornando-o insciente sobre a fase de coleta de dados.

A insciência do usuário sobre sua interação com os ambientes digitais diminui a autonomia para controlar seus dados, podendo impactar inclusive na formação de sua opinião em determinados contextos. Considerou-se neste trabalho que a insciência do usuário diante a fase de coleta de dados é fato, confirmada por vários relatos nos quais o usuário não tem conhecimento sobre as ações que estão envolvidas com seus dados.

Este trabalho investigou fatores que configuram o cenário que propicia a insciência do usuário enquanto alvo de fases de coleta de dados durante sua interação nos ambientes digitais, uma vez que, essa insciência pode ser fator de relevo na precarização do seu direito à privacidade. Mediante os resultados obtidos e explanados no decorrer deste trabalho, afirma-se que o cenário que propicia a insciência do usuário na fase de coleta de dados pode ser determinado pelos seguintes fatores:

a) Carência de pesquisas sobre proteção de dados pessoais na fase de coleta de dados

Há uma carência de pesquisas na fase de coleta de dados no âmbito da anonimização, principal medida no que tange a proteção de dados pessoais, pois impede a possibilidade de associação, direita ou indireta, a um indivíduo referenciado em um conjunto de dados. Essa carência foi revelada mediante seleção e análise de documentos resultado da revisão sistemática de literatura, a qual demonstrou que pesquisadores têm concentrado esforços para produzirem conjunto de dados anonimizados no domínio da recuperação de dados, de forma que o seu compartilhamento seja útil para a sociedade. É emblemático e válido esse esforço, pois muitas pesquisas podem ser replicadas com os dados compartilhados, principalmente na área da saúde, evitando a redundância da coleta de dados, assim, as possíveis ameaças à privacidade nesse

contexto decorrem da exposição do sujeito referenciado em situação de constrangimento e do descabido uso dos seus dados.

No entanto, a investigação científica não deve prevalecer apenas na fase de recuperação de dados, pois, o detentor é o primeiro a possuir dados do usuário, o que oportuniza esses detentores a construir perfis de indivíduos, podendo resultar no uso e compartilhamento de dados que vão muito além da consciência do usuário e, consequentemente, ampliando brechas de privacidade.

No que se refere ao contexto no qual a anonimização foi abordada nos trabalhos selecionados, sobressaem-se os dados de localização do usuário, totalizando 65% das pesquisas, um número de relevo, e, ainda, principalmente durante a interação do usuário com serviços LBS. Esses dados podem revelar informações além do posicionamento do usuário, pois quando combinados com outros dados permitem um rico conhecimento sobre vida do indivíduo.

Os dados de localização aparentam mais suscetíveis a ameaças à privacidade, e com isso os estudos científicos tem se concentrado nesse contexto. No entanto, essa situação remete a impressão de que as ameaças à privacidade acontecem apenas pela coleta realizada por ambientes digitais e dispositivos no contexto de dados de localização. Assim, esse cenário demonstra que possíveis ameaças à privacidade de indivíduos que utilizam os mais diversos serviços que, por sua vez, coletam dados de interação, tais como, mecanismo de busca, *e-commerce*, redes sociais, não são destaques nos documentos analisados.

Dessa forma, questiona-se a interação do usuário com esses ambientes também não carecem de técnicas e modelos para proporcionar proteção de dados no momento da coleta, buscando a garantia de minimizar brechas de privacidade. O nível de maturidade das pesquisas em relação à coleta ainda está em fase embrionária, pode-se notar que o contexto de *Privacy by design*, cuja finalidade é tratar as questões de privacidade na concepção das aplicações apresenta pouca incidência nos trabalhos analisados.

Em relação aos modelos que prevalecem para promover a proteção de dados pessoais, o modelo k-anonimato tem se destacado, sua essência é referência para a elaboração de outros modelos e medidas para proteção da privacidade. As técnicas predominantes nos trabalhos são a criptografia e o *spatial cloaking*, seguido de técnicas não perturbativas, como generalização e supressão, e técnicas perturbativas, como permutação e randomização. Destaca-se que uso da criptografia segue acompanhado de outras técnicas para anonimização, tais como a generalização e adição de ruído.

A maioria dos países que emergem nos trabalhos analisados apresenta em sua legislação amparo à proteção de dados pessoais. Logo, a presença de leis pode ser um fator estimulante

para que pesquisadores investiguem e proponham novas técnicas e modelos para minimizar violações de privacidade. Ao desenvolverem medidas para a proteção de dados, pesquisadores contribuem para que organizações públicas e privadas estejam em conformidade com legislações, a fim de não sofrer sanções.

Desta forma, a exiguidade de trabalhos que versam sobre anonimização na fase de coleta pode caracterizar-se como um fator que determina o cenário que leva a insciência do usuário sobre a fase de coleta pelos ambientes digitais. Notou-se nos trabalhos analisados que apenas o intitulado "*Efficient Time-Stamped Event Sequence Anonymization"* dos autores Sherkat e Mamoulis (2013) abordam ameaças à privacidade em relação aos mecanismos de busca e redes sociais, ao tratar sobre anonimização de dados de *timestamp*. Esse resultado indica oportunidades para futuras pesquisas e estudos de técnicas e modelos para impedir que influentes serviços de tecnologias continuem a coleta de dados que não são justificáveis para o uso do serviço.

Quando a ciência dissemina suas pesquisas sobre proteção de dados, ela pode contribuir para que a insciência do usuário sobre a coleta de dados seja minimizada, e ainda, torna mais perceptível os danos provocados por essa atividade, que podem ser irreversíveis quando não amparados por medidas de proteção.

- ✓ **Generalização dos aspectos de coleta de dados pessoais em legislações**

Nas leis e projetos de leis as questões de privacidade na fase de coleta estão envolvidas com a transparência sobre as atividades realizadas com dados, notificação clara sobre a coleta de dados, e o consentimento do usuário. Esses elementos são recorrentes nas leis e projetos de leis, seguidos da justificativa e minimização da coleta.

Comprovou-se que as leis ao abordarem elementos que estão envolvidos com a fase de coleta, apresentam esses conceitos muitas vezes de forma generalizada, principalmente em relação ao consentimento sobre a coleta, medidas para proteção dos dados (anonimização), e a própria menção a atividade de coleta, que emerge na maioria das leis como tratamento. Essa situação pode comprometer a interpretação durante a aplicação das leis, que irá refletir nos mecanismos vinculados diretamente ao usuário, como as políticas de privacidade e a interface de interação nos sites e aplicativos, contribuindo para ampliar sua insciência do usuário sobre a coleta de seus dados.

Em relação ao consentimento do usuário a respeito da coleta de seus dados, observou-se que, embora o consentimento seja uma medida de relevo nas leis, detalhes sobre essa medida não são comuns em muitos documentos. A generalização dessa questão se efetua quando leis regulam nas suas diretrizes apenas que o usuário deve dar consentimento, não explicitando, por

exemplo, o meio que deve ser utilizado (físico ou digital); forma do consentimento (escrito ou online); fase do ciclo de vida dos dados que deve se efetuar (coleta, armazenamento ou recuperação). A exceção recai sobre Regulamento (UE) 2016/679 e a PIPEDA, que especificam o consentimento informado em relação aos aspectos de validade e a modalidade do consentimento.

A anonimização como medida para proteção de dados pessoais emerge em algumas leis internacionais e no PL 5.276/2016. No entanto, quando a anonimização está presente nas legislações, não fica explícita a intenção de garantir a privacidade na fase de coleta de dados. Assim, quando as leis não explicitam a necessidade de anonimização na fase de coleta, ou enfatizam apenas na fase de recuperação de dados, corrobora com os resultados do capítulo 2, o qual revelou que as preocupações com as questões de privacidade tem se efetuado na fase de recuperação de dados e não na fase de coleta.

Outra situação de relevo é a pouca ênfase na menção sobre dados semi-identificadores, tão explorados por Sweeney (2001) ao abordar sobre anonimização. As leis não destacam esse tipo de dado como ameaçador a privacidade do indivíduo, elas versam sobre a proteção de dados sem especificação dos tipos de dados, exceção para dados sensíveis que são recorrentes nas leis, devido ser um tipo de dado mais perceptível e de maior impacto em relação a quebras de privacidade.

Desta forma, notou-se que semi-identificadores, por exemplo, *user agent*, *Source GeoIP*, *Destination GeoIP*, não são mencionados de forma específica nas legislações, se tornando desmerecidos quando se aborda sobre proteção na coleta de dados. Essa circunstância pode acentuar os danos em relação a brechas de privacidade.

Na maioria das leis identificadas neste trabalho a fase de coleta de dados é referenciada pelo termo “tratamento”, que ainda abarca outras atividades, tais como: armazenamento, consulta e o processamento. Essa generalização para várias atividades que envolvem os dados pode dificultar a identificação de quais diretrizes são especificamente voltadas para o momento da coleta, uma vez que, violações de privacidade ocorridas nessa fase implicam em possíveis novas ameaças, podendo implicar no armazenamento, processamento, recuperação ou no descarte dos dados.

A maioria das leis não regulamentam diretrizes para que detentores de dados informem o propósito do *cookie* e o seu conteúdo semântico, tornando essa questão opaca e, consequentemente impactando na consciência do usuário sobre a coleta de seus dados.

Diante do exposto, observa-se que a generalização das questões técnicas envolvidas na fase de coleta de dados pelas legislações, mediante a adoção de conceitos unitários, pode

impactar na forma como as instituições formulam suas políticas de informação, por exemplo, Affonso et al (2017) relatam que ao analisar a política de privacidade do mecanismo *Google*, essas tratam os aspectos de coleta de dados pelos seus serviços da mesma forma, com únicas orientações, independente se o serviço é um mecanismo de busca ou serviço de e-mail, o que torna a identificação de dados coletados por cada serviço o tanto quanto incompreensível. Esse posicionamento do *Google,* nas suas políticas de privacidade, pode ser fruto da aderência a uma legislação que também generaliza seus conceitos, situação que, indubitavelmente, pode causar a insciência do usuário ao interagir com ambientes digitais e ter acesso às políticas de privacidade. A política de privacidade do Google, mesmo descrevendo suas atividades em conformidade com o Regulamento (UE) 2016/679, ainda trata a coleta de dados por todos os seus serviços de forma única[111].

Considerando o aumento de aplicações e de meios de vigilância com o poder de coletar uma miríade de dados de indivíduos, torna-se imprescindível que casos que ampliam quebras de privacidade sejam representados especificamente com suas devidas regulamentações e medidas para proteção de dados. Assim, os aspectos técnicos se tornam elementos preponderantes que devem ser considerados no desenvolvimento de leis que tenham o propósito de impedir violações de privacidade.

No levantamento de legislações realizado neste trabalho, o Brasil é o único país que não possui uma lei específica para essas questões, situação que acentua ainda mais o impacto sobre cenário que leva a insciência do usuário. A garantia à privacidade do sujeito alvo e referenciado em conjuntos de dados se efetua a partir de leis esparsas, como a Lei nº 7.232/1984 (Plano Nacional de Informática); Lei nº 9.507/1997 (*Habeas Data*); Lei nº 9.472/1997 (Lei Geral das Telecomunicações); Lei nº 12.414/2011 (Lei do Cadastro Positivo); Lei nº 12.527/2011 (Lei de Acesso à informação); Lei nº 12.737/2012 (Lei Carolina Dickeman); Lei nº 12.965/2014 (Marco Civil da Internet). Normalmente, essas leis estão vinculadas a problemas específicos, o que torna a generalização muito maior para questões de privacidade, fato que corrobora com a necessidade de uma lei específica para a proteção de dados pessoais.

Ainda, ressalta-se que a proteção de dados pessoais vai muito além da aprovação de leis e decretos. É necessário um maior entendimento do processo de proteger dados pessoais, que envolve uma série de questões, como: avaliar como será conduzido o consentimento informado; como os dados permanecem armazenados; o que será disponibilizado, compartilhado ou descartado; quais técnicas e modelos serão utilizadas para anonimização dos dados na fase de

[111] Segundo relato de atualização da política no dia 25 de maio de 2018.

coleta, inclusive se os detentores de dados têm competências e habilidades para lidar com essas atividades.

Além da carência de pesquisas na fase de coleta de dados e da generalização dos aspectos de coleta de dados em legislações, o cenário que propicia a insciência do usuário na fase de coleta pode ser determinado pela:

c) Abstração na fase de coleta de dados, promovida pela própria interface das redes de computadores e pela falta de clareza das políticas de privacidade

As camadas de abstração, resultado do modelo OSI, ao organizar e ao simplificar seu contexto complexo, encapsulam detalhes de comunicação nas redes de computadores, tornando oculto o fluxo de coleta em que os usuários estão inconscientemente inseridos.

Mediante a análise de pacotes de dados durante o acesso às páginas Web, observa-se que a opacidade nesse cenário promove, além da baixa consciência do usuário, sobre a fase de coleta, incalculáveis violações de privacidade, uma vez que, muitos dados que trafegam nas redes podem resultar na identificação do indivíduo. Outros aspectos também podem ser preocupantes, como a possível correlação dos dados com outras bases de dados, considerando que cada vez se torna mais difícil identificar a natureza de um dado e, determinar se ele pode ou não violar a privacidade de um indivíduo.

A fase de coleta se inicia no momento em que o usuário solicita o serviço para aplicação Web, e a percepção do usuário sobre a coleta de dados é baseada nos dados disponibilizados cientemente. Não é explícito que, encapsulados nas camadas da rede, outros dados sejam coletados e podem ser dotados de semântica, aumentando a abstração para o usuário sobre esse processo. Dados como *user agent*, endereço IP, *cookies*, formam um conjunto de dados que, quando observados silenciosamente por técnicas de *fingerprinting*, tornam o usuário ainda mais insciente sobre a coleta de dados.

Por outra perspectiva, amplia-se o conhecimento do detentor sobre os dados que perpassam as camadas de redes e, certamente, a abstração presente na fase de coleta de dados fortalece a assimetria informacional entre detentores de dados e usuários, quando esses utilizam diversos serviços na Web, tais como: redes sociais; mecanismo de buscas ou; compras em *sites* de comércio eletrônico.

Assim, a consciência em relação à coleta é maior para aqueles que detêm o controle sobre a coleta do que para o usuário, o que torna muitas aplicações, como no caso dos mecanismos de buscas, inseridas na onisciência, enquanto os usuários estão imersos na insciência sobre a coleta de dados. Ressalta-se, ainda, que nesse processo pode ainda ocorrer à interceptação de outros interessados nos dados, emergindo novas e até indesejadas coletas. O fato dessa abstração se

efetuar durante toda a interação do usuário com o ambiente digital contribui para o cenário que leva a insciência do usuário em relação a fase de coleta de dados.

Observa-se que essa abstração impede o indivíduo de ter autonomia pessoal sobre seus dados, pois como citado por Westin (1967), a ameaça mais séria à autonomia de um indivíduo é a possibilidade de permitir que o invasor conheça seus segredos extremos. Será que os ambientes digitais não estão fazendo indivíduos perderem autonomia sobre seus segredos, tornando-os vulneráveis ao uso de seus dados, sem justificativas e permissão, dando o controle àqueles que conhecem seus dados? Segundo Westin (1967), a capacidade do indivíduo de decidir quando revelar seus segredos ao público é um aspecto crucial para o sentimento de autonomia. Desta forma, ao perder essa autonomia, a coleta realizada pelos detentores de dados fere o direito à privacidade dos usuários e dos referenciados, ainda que, a insciência sobre o momento da coleta fortalece ou torna essa questão complexa para o lado do usuário.

Face ao exposto**,** existem fatores que contribuem para um cenário que propicia insciência do usuário na fase de coleta de dados nos ambientes digitais, insciência esta que pode ter impactos em questões importantes como a da privacidade. Dentre os quais, evidenciou-se neste trabalho a carência de pesquisas sobre proteção de dados pessoais na fase de coleta de dados, especificamente por meio de anonimização de dados; generalização dos aspectos técnicos de coleta de dados pessoais em legislações e; abstração na fase de coleta de dados, promovida pela própria interface das redes de computadores e pela falta de clareza das políticas de privacidade.

O meio acadêmico e os formuladores de leis podem proporcionar melhorias para esse cenário, posto que, um pode impactar na esfera do outro. Quando existe uma demanda para proteger dados pessoais, ocasionada pelas determinações das leis, essas fomentam pesquisas no que tange o aprimoramento de técnicas e modelos para garantir a proteção de dados pessoais. Em contrapartida, o meio científico ao disseminar suas pesquisas mediante produtos e serviços contribui para que organizações estejam alinhadas ao ordenamento jurídico, e se, construídos de forma específica, considerando os detalhes técnicos das tecnologias e suas vertentes, podem proporcionar melhorias no domínio de minimizar a insciência do usuário quanto à atividade de coleta de dados. Tanto a esfera acadêmica quanto a esfera jurídica devem considerar nas suas abordagens a coleta de dados realizada de modo ciente e insciente pelo ambiente digital.

Ressalta-se que, elementos que consideram questões de privacidade no âmbito da coleta de dados de forma rasa e não dispõem de medidas ou estudos para proporcionar percepção ao usuário, deixam os usuários susceptíveis aos mais variados meios de violações de privacidade, iniciando com a vigilância e interrogatório, perpassando a agregação, a exclusão, a

identificação, até se perfazer a fase de divulgação de dados. Violações que foram exemplificadas por meio do *framework* de Solove (2006) em relação à coleta realizada pelos mecanismos de buscas, mas que se concretizam também em outras aplicações da Web.

A privacidade em relação à coleta de dados nos ambientes digitais pode começar a se fortalecer a partir do momento em que o usuário se torna ciente sobre essa atividade, situação que é determinada pelas políticas de informação, leis e pelo meio acadêmico, atores que se configuram como participativos para minimizar a insciência do usuário.

Almeja-se como trabalho futuro, analisar o impacto do Regulamento (UE) 2016/679 nas políticas de privacidade de serviços como mecanismo de buscas e redes sociais, a fim de identificar especificamente, como o consentimento informado e questões de controle sobre os dados tem se efetuado nesses ambientes em relação à coleta de dados.

REFERÊNCIAS

ABADE, A. S.; ALVES, J. D. Política de privacidade e dados pessoais: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. *Revista FACISA On-Line*, v. 6, n. 1, p. 123-144, 2017.

ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. *Science*, v. 347, n. 6221, p. 509-514, 2015.

AFFONSO, E. P.; MONTEIRO, E. C. S. A.; CAMARGO, F. B. Aplicativos móveis na agricultura e as implicações nas questões de privacidade. In: ENCONTRO COMPETÊNCIAS DIGITAIS PARA AGRICULTURA FAMILIAR, 3., 2016, Tupã. *Anais...* Tupã: CoDAF, 2016. p. 47-56.

AFFONSO, E. P.; OLIVEIRA, S. C.; SANT'ANA, R. C. G. Análise do equilíbrio entre privacidade e utilidade no acesso a dados. *Informação & Sociedade: Estudos*, v. 27, n. 1, p. 81-92, 2017.

AFFONSO, E. P.; SANT'ANA, R. C. G. Anonimização de metadados de imagem digital por meio do modelo k-anonimato. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 16., 2015, João Pessoa. *Anais...* João Pessoa: ANCIB, 2015.

AFFONSO, E. P.; SANT'ANA, R. C. G. Preservação da privacidade no acesso a dados por meio do modelo k-anonimato. *PontodeAcesso*, v. 11, n. 1, p. 20-41, 2017.

AFFONSO, E. P. et al. Mecanismos de busca e as implicações nos aspectos de privacidade. *Revista Ibero-Americana de Ciência da Informação*, v. 10, n. 2, p. 422-442, 2017.

AFFONSO, E.P.; SANT'ANA, R. C. G. The issue of privacy awareness in digital libraries in the collection phase of the data life cycle. *IFLA Journal*, special issue on privacy, 2018. No prelo.

AFFONSO, E. P.; MONTEIRO, E. C. S; SANT'ANA, R. C. G. Coleta de dados por aplicativos e seu impacto sobre a privacidade. In: ENCONTRO INTERNACIONAL DE INFORMAÇÃO, CONHECIMENTO E AÇÃO, 10., 2018, Marília. *Anais...* No prelo

AGRAWAL, R.; SRIKANT, R. Privacy-preserving data mining. In: ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT OF DATA, 2000, Dallas. *Proceedings...* New York: ACM, 2000. p. 439-450.

AKERLOF, G. A. The market for "lemons": quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, v. 84, n. 3, p. 488-500, 1970.

ALECRIM, E. Google Brasil terá que se explicar à Justiça sobre a coleta indevida de dados pelos carros do Street View. *Tecnoblog*, 2013. Disponível em: <https://tecnoblog.net/144694/google-brasil-coleta-indevida-dados-street-view/>. Acesso em: 15 nov. 2017.

ALEMANHA. Federal Ministry of Justice and Consumer Protection. Federal Data Protection Act, promulgated on 14 January 2003. This Act serves to implement directive 95/46/EC of the

European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Federal Law Gazette I*, p. 66, 2003.

ALEMANHA. Telemedia Act (TMA). *Federal Gazette I*, p. 179, 26 fev. 2007.

ALEMANHA. Federal Ministry of Justice and Consumer Protection. Federal Data Protection Act of 30 June 2017. *Federal Law Gazette I*, p. 2097, 2017.

ALLARD, T.; NGUYEN, B.; PUCHERAL, P. METAP: revisiting Privacy-Preserving Data Publishing using secure devices. *Distributed and Parallel Databases*, v. 32, n. 2, p. 191-244, 2014.

ALVES, R. C. V.; SANTOS, P. L. V. A. C. *Metadados no domínio bibliográfico*. Rio de Janeiro: Intertexto, 2013.

ARAÚJO, A. M. R. As transferências transatlânticas de dados pessoais: o nível de proteção adequado depois de Schrems. *Revista Direitos Humanos e Democracia*, v. 5, n. 9, p. 201-236, 2017.

ASIMOV, I. The last question. *Science Fiction Quarterly*, 1956.

ASRODIA, P.; PATEL, H. Network traffic analysis using packet sniffer. *International Journal of Engineering Research and Applications*, v. 2, n. 3, p. 854-856, 2012.

AURA, T.; ZUGENMAIER, A. Privacy, control and internet mobility. In: INTERNATIONAL WORKSHOP ON SECURITY PROTOCOLS, 12., 2004, Cambridge. *Papers...* Berlin: Springer, 2004. p. 133-145.

AUSTRÁLIA. Australian Government. Privacy Act 1988. An Act to make provision to protect the privacy of individuals, and for related purposes. *Federal Register of Legislation*, compilation nº 77, 22 fev. 2018.

ÁUSTRIA. Federal Ministry for Digital and Economic Affairs. Federal Act concerning the Protection of Personal Data (DSG 2000). *Federal Law Gazette I*, n. 165, 1999.

ÁUSTRIA. Federal Ministry for Digital and Economic Affairs. Telecommunications Act 2003 (TKG 2003). Federal Act enacting the Telecommunications Act and amending the Federal Act on Labour Inspection for Transport. *Federal Law Gazette I*, n. 70, 2003.

ÁUSTRIA. Federal Ministry for Digital and Economic Affairs. Federal Act concerning the Protection of Personal Data (DSG 2000). *Federal Law Gazette I*, n. 165, 1999 as amended by *Federal Law Gazette I*, n. 120, 2017. Date of the version: 25 May 2018. Disponível em: <https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Erv&Dokumentnummer=ERV_1999_1_165>. Acesso em: 31 maio 2018.

BAHŞI, H.; LEVI, A. k-anonymity based framework for privacy preserving data collection in wireless sensor networks. *Turkish Journal of Electrical Engineering & Computer Sciences*, v. 18, n. 2, p. 241-272, 2010.

BARDIN, L. *Análise de conteúdo*. 4. ed. Lisboa: Edições 70, 1977.

BARDIN, L. *Análise de conteúdo*. Ed. rev. e atual. Lisboa: Edições 70, 2009.

BATTELLE, J. *A busca*: como o Google e seus competidores reinventaram os negócios e estão transformando nossas vidas. Rio de Janeiro: Elsevier, 2006.

BAUMAN, Z. *44 cartas do mundo líquido moderno*. Rio de Janeiro: Zahar, 2011.

BAUMAN, Z. *Vigilância líquida*. Rio de Janeiro: Zahar, 2014.

BÉLGICA. Act on the protection of privacy in relation to the processing of personal data, 8 dez. 1992. *Belgian Official Journal*, 18 mar. 1993.

BÉLGICA. Service Public Federal Justive. 3 decembre 2017 - Loi portant creation de l'Autorité de protection des données. *Moniteur Belge*, 10 jan. 2018

BÉLGICA. Service Public Federal. Economie, P.M.E., Classes Moyennes et Energie. Loi relative aux communications électroniques, 13 juin 2005. *Moniteur Belge*, 20 jun. 2005.

BELSHE, M.; PEON, R.; THOMSON, M. Hypertext Transfer Protocol Version 2 (HTTP/2). *Internet Engineering Task Force (IETF)*, maio 2015. Disponível em: <https://tools.ietf.org/html/rfc7540>. Acesso em: 23 maio 2017.

BENNETT, C. J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992.

BERGSTRÖM, A. Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behaviour*, v. 53, p. 419-426, 2015.

BETTINI, C.; RIBONI, D. Privacy protection in pervasive systems: state of the art and technical challenges. *Pervasive and Mobile Computing*, v. 17, p. 159-174, 2015.

BJERKE, P.; SANDTRØ, J. Norway. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 5 maio 2018.

BLACKMORE, N. Data protection in Hong Kong: overview. *Thomson Reuters Practical Law*, 1 ago. 2017. Disponível em: <https://uk.practicallaw.thomsonreuters.com/9-505-7567?navId=812C69879F58CC34E8CD48B0EECBACE1&comp=pluk&transitionType=Default&contextData=(sc.Default)>. Acesso em: 28 abr. 2018.

BLANCO-JUSTICIA, A.; DOMINGO-FERRER, J. Privacy-preserving loyalty programs. In: DPM INTERNATIONAL WORKSHOP ON DATA PRIVACY MANAGEMENT, 9., 2014, Wroclaw. *Papers*..,[S.l.]: Springer, 2015. p. 133-146.

BOFF, S. O.; FORTES, V. B. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Seqüência: Estudos Jurídicos e Políticos*, v. 35, n. 68, p. 109, 2014.

BRAGA, R. 200 Crônicas Escolhidas. 17ª edição, Rio de Janeiro: Record, 2001.

BRASIL. Presidência da República. Casa Civil. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 30 set. 1984.

BRASIL. Constituição Federal (1988). *Constituição da República Federativa do Brasil*. Promulgada em 5 out. 1988. Brasília, DF, Senado Federal, 5 out. 1988.

BRASIL. Presidência da República. Casa Civil. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 12 set. 1990.

BRASIL. Presidência da República. Casa Civil. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 13 nov. 1997a.

BRASIL. Presidência da República. Casa Civil. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 17 jul. 1997b.

BRASIL. Presidência da República. Casa Civil. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 10 jun. 2011a.

BRASIL. Presidência da República. Casa Civil. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 18 nov. 2011b.

BRASIL. Presidência da República. Casa Civil. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 3 dez. 2012.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 4060, de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. *Câmara dos Deputados*, 2012b. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 20 dez. 2016.

BRASIL. Senado Federal. Projeto de Lei do Senado nº 330, de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. *Senado Federal*, 2013. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 10 nov. 2016

BRASIL. Senado Federal. Projeto de Lei do Senado nº 131, de 2014. Dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiras a organismos estrangeiros. *Senado Federal*, 2014a. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/116969>. Acesso em: 10 nov. 2016.

BRASIL. Senado Federal. Projeto de Lei do Senado nº 181, de 2014. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais. *Senado Federal*, 2014b. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/117736>. Acesso em: 10 nov. 2016.

BRASIL. Presidência da República. Casa Civil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 24 abr. 2014c.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Apelação nº 20130110719195APC (0018676-70.2013.8.07.0001). Apelante: Decio Nery de Lima. Apelado: Google Brasil Internet Ltda. Relator: Gislene Pinheiro. Brasília, 3 de dezembro de 2014d. *Diário da Justiça Eletrônico*, Brasília, 15 dez. 2014d. Disponível em: <https://tj-df.jusbrasil.com.br/jurisprudencia/157964666/apelacao-civel-apc-20130110719195-df-0018676-7020138070001/inteiro-teor-157964683?ref=juris-tabs>. Acesso em: 10 mar. 2018

BRASIL. Tribunal de Justiça de São Paulo. Agravo de Instrumento nº 2153598-52.2014.8.26.0000. Agravante: Paulo Roberto Barbosa de Oliveira. Agravado: Google Internet do Brasil Ltda. Relator: Alcides Leopoldo e Silva Júnior. São Paulo, 7 de outubro de 2015a. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_21535985220148260000_07102014.pdf>. Acesso em: 20 mar. 2018.

BRASIL. Tribunal de Justiça de São Paulo. Sentença do Processo nº: 1013430-56.2015.8.26.0008. Requerente: Gilberto Trama. Requerido: Google Brasil Internet Ltda e outros. Relator: Juíza Ana Carolina Vaz Pacheco de Castro. São Paulo, 4 de outubro de 2015b. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2015/sp_10134305620158260008_07102015.pdf>. Acesso em: 20 mar. 2018.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 5.276, de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. *Câmara dos Deputados*, 2016a. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 10 nov. 2016.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 6.291, de 2016. Altera o Marco Civil da Internet, no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de internet. *Câmara dos Deputados*, 2016b. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2113796>. Acesso em: 20 dez. 2016.

BRASIL. Tribunal de Justiça de São Paulo. Agravo de Instrumento nº 2261625-95.2015.8.26.0000. Agravante: Facebook Serviços Online do Brasil Ltda. Agravada: Cláudia Maria Nogueira de Souza. Relator: Maia da Cunha. São Paulo, 22 de fevereiro de 2016. *Diário de Justiça do Estado de São Paulo*, São Paulo, 3 mar. 2016c. Disponível em:

<https://tj-sp.jusbrasil.com.br/jurisprudencia/308032416/agravo-de-instrumento-ai-22616259520158260000-sp-2261625-9520158260000>. Acesso em: 30 mar. 2018.

BRASIL. Tribunal de Justiça do Paraná. Despacho Saneador do Processo nº: 0005900-84.2016.8.16.0194. Autor: Cesar Eduardo Isaacson Buffara representado por Robinson Marcal Kaminski e outros. Réu: Privacy Protection Service INC. Relator: Juiz Marcos Vinícius da Rocha Loures Demchuk. Curitiba, 13 de junho de 2016. Data da Publicação: 22 jun. 2016d. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2016/pr_00059008420168160194_16062016.pdf>. Acesso em: 19 mar. 2018.

BRASIL. Tribunal de Justiça de São Paulo. Agravo de Instrumento nº 2247265-24.2016.8.26.0000. Agravante: Facebook Serviços Online do Brasil Ltda. Agravada: Anna Hartman Rzyski da Silva. Relator: Viviani Nicolau. São Paulo, 2 de março de 2017a. Disponível em: <https://tj-sp.jusbrasil.com.br/jurisprudencia/435230247/agravo-de-instrumento-ai-22472652420168260000-sp-2247265-2420168260000/inteiro-teor-435230266?ref=topic_feed>. Acesso em: 25 mar. 2018.

BRASIL. Tribunal de Justiça de São Paulo. Sentença do Processo Digital nº 1026719-03.2017.8.26.0100. Requerente: Danilo Gentili Junior. Requerido: Facebook Serviços Online do Brasil Ltda. Relator: Tonia Yuka Kôroku. São Paulo, 29 de junho de 2017b. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2017/sp_10267190320178260100_29062017.pdf>. Acesso em: 10 abr. 2018.

BRASIL. Tribunal de Justiça de São Paulo. Sentença do Processo nº: 1112509-86.2016.8.26.0100. Requerente: Geraldo José Rodrigues Alckmin Filho. Requerido: Twitter Brasil Rede de Informação Ltda. Relator: Juiz Guilherme Ferreira da Cruz. São Paulo, 8 de junho de 2017c. Disponível em: <http://www.omci.org.br/jurisprudencia/185/figura-publica-e-identificacao-de-usuarios/>. Acesso em: 25 mar. 2018.

BRASIL. Justiça Federal do Piauí. Sentença do Processo nº 25463.45.2016.4.01.4000. Autor: Ministério Público Federal. Réu: Google Brasil Internet Ltda. Relator: Márcio Braga Magalhães. Teresina, 29 de janeiro de 2018a. Disponível em: <http://www.omci.org.br/jurisprudencia/189/escaneamento-de-emails-e-consentimento-previo/>. Acesso: 19 mar. 2018.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Decisão Interlocutória do Processo nº 0702128-96.2018.8.07.0018. Autor: 99 Tecnologia Ltda. Réu: Distrito Federal. Relator: Juiz Roque Fabricio Antonio de Oliveira Viel. Brasília, 15 de março de 2018b. Disponível em: <http://www.omci.org.br/jurisprudencia/240/servicos-de-transporte-e-protecao-de-dados/>. Acesso em: 16 abr. 2018.

BRASIL. Tribunal de Justiça de São Paulo. Ação Civil Pública nº: 5009507-78.2018.4.03.6100. Autor: Ministério Público Federal. Réu: Microsoft Informática Ltda, União Federal. Relator: Cristiane Farias Rodrigues dos Santos. São Paulo, 27 de abril de 2018c. Disponível em: <http://www.omci.org.br/jurisprudencia/250/coleta-de-dados-pessoais-sem-autorizacao/>. Acesso em: 25 mar. 2018.

BREKNE, T.; ÅRNES, A.; ØSLEBØ, A. Anonymization of ip traffic monitoring data: attacks on two prefix-preserving anonymization schemes and some proposed remedies. In: PETS:

INTERNATIONAL SYMPOSIUM ON PRIVACY ENHANCING TECHNOLOGIES SYMPOSIUM, 5., 2005, Cavtat. *Papers…* Berlin: Springer, 2005. p. 179-196.

BUCHMANN, E. et al. Re-identification of smart meter data. *Personal and Ubiquitous Computing*, v. 17, n. 4, p. 653-662, 2013.

BUNNIG, C.; CAP, C. H. Ad hoc privacy management in ubiquitous computing environments. In: INTERNATIONAL CONFERENCE ON ADVANCES IN HUMAN-ORIENTED AND PERSONALIZED MECHANISMS, TECHNOLOGIES AND SERVICES, 2., 2009, Porto. *Proceedings*... [S.l.]: IEEE, 2009. p. 85-90.

CADWALLADR, C.; GRAHAM-HARRISON, E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, 17 mar. 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 17 mar. 2018.

CAMENISCH, J. et al. (Ed.). *Privacy and identity management for life*. Heidelberg: Springer, 2011.

CANADÁ. Minister of Justice. Privacy Act. An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves. *Revised Statutes of Canada*, 1985.

CANADÁ. Minister of Justice. Personal Information Protection and Electronic Documents Act. An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act. *Statutes of Canada*, 2000.

CANADÁ. Office of the Privacy Commissioner. Overview of privacy laws in Canada. *OPC*, 31 jan. 2018. Disponível em: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/>. Acesso em: 9 fev. 2018.

CAPURRO, R. Rafael Capurro: depoimento. *O Globo*, 4 dez. 2014. Entrevista concedida a Sérgio Matsuura. Disponível em: <http://oglobo.globo.com/sociedade/conte-algo-que-nao-sei/rafael-capurro-filosofo-ha-uma-esquizofrenia-entre-mundo-real-digital-14738635>. Acesso em: 2 mar. 2016.

CARVALHO, A. P. G. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. *Revista de Direito do Consumidor*, v. 46, p. 77-119, 2003.

CASTELLS, M. A galáxia Internet: reflexões sobre a Internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CHAUÍ, M. Convite à filosofia. Ática: São Paulo, 1995.

CHOW, C.-Y.; MOKBEL, M. F.; AREF, W. G. Casper: query processing for location services without compromising privacy. *ACM Transactions on Database Systems*, v. 34, n. 4, p. 2009.

CHOW, C.-Y.; MOKBEL, M. F.; LIU, X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: ACM INTERNATIONAL SYMPOSIUM ON ADVANCES IN GEOGRAPHIC INFORMATION SYSTEMS, 14., 2006, Arlington. *Proceedings*... New York: ACM, 2006. p. 171-178

CHOW, C.-Y.; MOKBEL, M. F.; HE, T. A privacy-preserving location monitoring system for wireless sensor networks. *IEEE Transactions on Mobile Computing*, v. 10, n. 1, p. 94-107, 2010.

CHOW, C.-Y.; MOKBEL, M. F.; LIU, X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *GeoInformatica*, v. 15, n. 2, p. 351-380, 2011.

CHOW, C.-Y. et al. Query-aware location anonymization for road networks. *GeoInformatica*, v. 15, n. 3, p. 571-607, 2011.

CIRIANI, V. et al. Microdata protection. In: YU, T. JAJODIA, S. (Ed.). *Secure data management in decentralized systems*. [S.l.]: Springer US, 2007a. p. 291-321.

CIRIANI, V. et al. Fragmentation and encryption to enforce privacy in data storage. In: EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY, 12., 2007, Dresden. *Proceedings*... Berlin: Springer, 2007b. p. 171-186.

CIRIANI, V. et al. Theory of privacy and anonymity. In: ATALLAH, M.; BLANTON, M. (Org). *Algorithms and theory of computation handbook*: special topics and techniques. 2. ed. CRC Press, 2009. cap. 18.

CISCO. Cisco visual networking index: global mobile data traffic forecast update, 2016-2021. *Cisco*, 7 fev. 2017. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>. Acesso em: 20 nov. 2017.

CLARKE, R. The digital persona and its application to data surveillance. *The Information Society*, v. 10, n. 2, p. 77-92, 1994.

CLAUSE, J.; ORSO, A. Camouflage: automated anonymization of field data. In: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, 33., 2011, Honolulu. *Proceedings*... New York: ACM, 2011. p. 21-30.

CLELAND, S.; BRODSKY, I. *Search & destroy*: why you can't trust Google Inc. St. Louis, MO: Telescope Books, 2011.

COMITÊ GESTOR DA INTERNET NO BRASIL. Resolução CGI.br/RES/2009/003/P. Princípios para a governança e uso da internet. *CGI.br*, 2009. Disponível em: <http://www.cgi.br/resolucoes/documento/2009/003>. Acesso em: 13 jul. 2017.

COLONIZAÇÃO DE POVOAMENTO. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Coloniza%C3%A7%C3%A3o_de_povoamento&oldid=52395471>. Acesso em: 18 jun. 2018.

COOPER, A. et al. Privacy Considerations for Internet Protocols. *Internet Architecture Board (IAB)*, jul. 2013. Disponível em: <https://tools.ietf.org/html/rfc6973>. Acesso em: 23 maio 2017.

CORAGGIO, G. Italy. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 4 fev. 2018.

CORBET, R. et al. Data protection in Ireland: overview. *Thomson Reuters Practical Law*, 1 mar. 2018. Disponível em: <https://uk.practicallaw.thomsonreuters.com/6-505-8262?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1>. Acesso em: 23 abr. 2018.

COREIA DO SUL. Korean Government. Act on promotion of information and communications network utilization and information protection, etc. [*Personal Information Protection Comission*], 16 Jan 2001.

COREIA DO SUL. Korean Government. Law on the protection and use of location information. [*Personal Information Protection Comission*], 27 jan. 2005.

COREIA DO SUL. Korean Government. Personal Information Protection Act, promulgated on 29 Mar 2011. [*Personal Information Protection Comission*], 30 Sep 2011.

CORREIA, P. M. A. R.; JESUS, I. O. A. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. *Revista Direito, Estado e Sociedade*, n. 43, p. 135-161, 2013.

COUNCIL OF EUROPE. Parliamentary Assembly. Human rights and modern scientific and technological developments: text adopted by the Assembly on 31st January 1968 (16th Sitting). *Assembly Debate*, 31 jan. 1968. Disponível em: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en>. Acesso em: 24 abr. 2018.

CUNCHE, M. I know your MAC address: targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques*, v. 10, n. 4, p. 219-227, 2014.

CUTILLO, L. A.; MOLVA, R.; STRUFE, T. Privacy preserving social networking through decentralization. In: INTERNATIONAL CONFERENCE ON WIRELESS ON-DEMAND NETWORK SYSTEMS AND SERVICES, 6., 2009, Snowbird. *Proceedings...* [S.l.]: IEEE, 2009. p. 145-152.

D'HULST, T.; KENGEN, L. Data protection in Belgium: overview. 2017. *Thomson Reuters Practical Law*, 1 out. 2017. Disponível em: <https://uk.practicallaw.thomsonreuters.com/2-502-2977?transitionType=Default&contextData=(sc.Default)>. Acesso em: 23 mar. 2018.

DALENIUS, T.; REISS, S. P. Data-swapping: a technique for disclosure control. *Journal of Statistical Planning and Inference*, v. 6, n. 1, p. 73-85, 1982.

DE CAPITANI DI VIMERCATI, S. et al. Data privacy: definitions and techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, v. 20, n. 6, p. 793-817, 2012.

DECEW, J. W. The scope of privacy in law and ethics. *Law and Philosophy*, v. 5, n. 2, p. 145-173, 1986.

DENZIN, N. K. Triangulation in educational research. In: KEEVES, J. P. (Ed.). *Educational research, methodology, and measurement*: an international handbook. Oxford: Pergamon Press, 1988. p. 318-322.

DENZIN, N. K.; LINCOLN, Y. S. *O planejamento da pesquisa qualitativa*. Porto Alegre: Penso, 2006.

DEPARTAMENTO DE ESTADO DOS ESTADOS UNIDOS. Um esboço da História Americana. Escritório de Assuntos Públicos, 2012. Disponível em: < https://photos.state.gov/libraries/amgov/30145/publications-portuguese/OutlineofUSHistory>. Acesso em: 03 jul. 2018.

DIAS, G. A.; VIEIRA, A. A. N. Big Data: questões éticas e legais emergentes. *Ciência da Informação*, v. 42, n. 2, p. 174-184, 2015.

DIERKS, T.; RESCORLA, E. The Transport Layer Security (TLS) Protocol: version 1.2. *Internet Engineering Task Force (IETF)*, ago. 2008. Disponível em: <https://tools.ietf.org/ html/rfc5246>. Acesso em: 4 maio 2017.

DIRIK, A. E.; SENCAR, H. T.; MEMON, N. Analysis of seam-carving-based anonymization of images against PRNU noise pattern-based source attribution. *IEEE Transactions on Information Forensics and Security*, v. 9, n. 12, p. 2277-2290, 2014.

DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2017. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 20 jul. 2017.

DOMINGO-FERRER, J. Microaggregation for database and location privacy. In: INTERNATIONAL WORKSHOP ON NEXT GENERATION INFORMATION TECHNOLOGIES AND SYSTEMS, 6., 2006, Kibbutz Shefayim. *Proceedings...* Berlin: Springer, 2006. p. 106-116.

DOMINGO-FERRER, J.; SEBÉ, F.; CASTELLÀ-ROCA, J. On the security of noise addition for privacy in statistical databases. In: INTERNATIONAL WORKSHOP ON PRIVACY IN STATISTICAL DATABASES, 2004, Barcelona. *Proceedings*... Berlin: Springer, 2004. p. 149-161.

DOMINGO-FERRER, J.; TORRA, V. Ordinal, continuous and heterogeneous k-anonymity through microaggregation. *Data Mining and Knowledge Discovery*, v. 11, n. 2, p. 195-212, 2005.

DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, D. Privacidade e transparência no acesso à informação pública. In: MEZZAROBA, O.; GALINDO, F. (Org.). *Democracia eletrônica*. Zaragoza: Prensas Universitárias de Zaragoza, 2010. p. 179-216.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, 2011.

DOTTI, R. A. Tutela jurídica da privacidade. In: DIAS, A. L. et al. *Estudos jurídicos em homenagem ao Professor Washington de Barros Monteiro*. São Paulo: Saraiva, 1982. p. 333-352.

DUCKDUCKGO. Política de privacidade. [201-]. Disponível em: <https://DuckDuckgo.com/privacy>. Acesso em: 20 set. 2017.

DWORK, C. Differential privacy: a survey of results. In: INTERNATIONAL CONFERENCE ON THEORY AND APPLICATIONS OF MODELS OF COMPUTATION, 5., 2008, Xi'an. *Proceedings*... Berlin: Springer, 2008. p. 1-19.

DWORK, C.; ROTH, A. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, v. 9, n. 3-4, p. 211-407, 2014.

DYBA, T.; DINGSOYR, T.; HANSSEN, G. K. Applying systematic reviews to diverse study types: an experience report. In: INTERNATIONAL SYMPOSIUM ON EMPIRICAL SOFTWARE ENGINEERING AND MEASUREMENT, 1., 2007, Madrid. *Proceedings*... [S.l.]: IEEE, 2007. p. 225-234.

DYSON, A.; MCKEAN, R. United Kingdom. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 5 maio 2018.

ECKERSLEY, P. Is every browser unique? Results fom the panopticlick experiment. *Electronic Frontier Foundation*, 17 maio 2010. Disponível em: <https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick>. Acesso em: 20 nov. 2017.

EECKE, P. Belgium. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 7 maio 2018.

EFTHYMIOU, C.; KALOGRIDIS, G. Smart grid privacy via anonymization of smart metering data. In: IEEE INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS, 1., 2010, Gaithersburg. *Proceedings*... [S.l.]: IEEE, 2010. p. 238-243.

ELECTRONIC CODE OF FEDERAL REGULATIONS. *Part 99 - Family educational rights and privacy*. 2018. Disponível em < https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33#se34.1.99_12 >. Acesso em: 28 mai. 2018.

ELECTRONIC PRIVACY INFORMATION CENTER. *The Fair Credit Reporting Act*. 2018. Disponível em: < https://epic.org/privacy/fcra/>. Acesso em: 5 nov. 2017.

ELECTRONIC PRIVACY INFORMATION CENTER. *The Privacy Act of 1974*. Disponível em: <https://epic.org/privacy/1974act/#introduction>. Acesso em: 5 nov. 2017

ENDSLEY, M. R. Design and evaluation for situation awareness enhancement. In: HUMAN FACTORS AND ERGONOMICS SOCIETY ANNUAL MEETING, 32., 1988, Los Angeles. *Proceedings...* Santa Monica: SAGE Publications, 1988. p. 97-101.

ESPANHA. Ministério de la Presidencia y para las Administraciones Territoriales. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *Boletín Oficial del Estado*, nº 298, 14 dez. 1999.

ESPANHA. Ministério de la Presidencia y para las Administraciones Territoriales. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *Boletín Oficial del Estado*, nº 166, 12 jul. 2002.

ESTADOS UNIDOS. U.S. Department of Justice. The Privacy Act of 1974. To amend title 8, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained Im Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes. *Public Law*, 31 dez. 1974.

ESTADOS UNIDOS. U.S. Department of Justice. The Privacy Act of 1974. 2015. Disponível em: <https://www.justice.gov/opcl/privacy-act-1974>. Acesso em: 20 set. 2017.

EUROPEAN COURT OF HUMAN RIGHTS. *European convention on human rights*. Strasbourg: Council of Europe, [2018?].

EU GENERAL DATA PROTECTION REGULATION. GDPR Portal: site overview. *GDPR Portal*, [201-]a. Disponível em: <http://www.eugdpr.org/>. Acesso em: 5 nov. 2017.

EU GENERAL DATA PROTECTION REGULATION. GDPR key changes. *GDPR Portal*, [201-]b. Disponível em: <http://www.eugdpr.org/key-changes.html>. Acesso em: 24 nov. 2017.

EUROPEAN COMMISION. Directorate-General for Justice and Consumers. *Guide to the EU-U.S. Privacy Shield*. [Belgium]: European Union, 2016.

FACEBOOK. Políticas de privacidade do Facebook. [201-]. Disponível em: <https://www.facebook.com/privacy/explanation?pnref=lhc>. Acesso em: 8 maio 2017.

FAIRFIELD, P. *Public/private*. Maryland: Rowman & Littlefield, 2005.

FEHRINGER, S.; PANIC, S. Austria. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 7 maio 2018.

FEDERAL TRADE COMMISSION. *Fair credit reporting act*. 1970, revised May 2016. Disponível em: <https://www.ftc.gov/system/files/fcra_2016.pdf.> Acesso em: 15 ago. 2017.

FEDERAL TRADE COMMISSION. *Children's online privacy protection act (COPPA)*. 1998a. Disponível em: <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>. Acessível em: 20 maio 2018.

FEDERAL TRADE COMMISSION. *Privacy online*: a report to congress. 1998b. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>. Acesso em: 13 jul. 2017.

FIEGERMAN, S. Yahoo says 500 million accounts stolen. *CNN Tech*, 23 set. 2016a. Disponível em: <http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/index.html>. Acesso em: 20 out. 2017.

FIEGERMAN, S. Yahoo says data stolen from 1 billion accounts. CNN Tech, 15 dez. 2016b, online. Disponível em: <http://money.cnn.com/2016/12/14/technology/yahoo-breach-billion-users/index.html>. Acesso em: 20 out. 2017.

FIGARO, R. A triangulação metodológica em pesquisas sobre a comunicação no mundo do trabalho. *Fronteiras - Estudos Midiáticos*, v. 16, n. 2, p. 124-131, 2014.

FLICK, U. Introdução à pesquisa qualitativa. 3. ed. Porto Alegre: Artmed, 2008.

FLORIDI, L. The ontological interpretation of informational privacy. *Ethics and Information Technology*, v. 7, n. 4, p. 185-200, 2005.

FOUCAULT, M. História da sexualidade II: o uso dos prazeres. Rio de Janeiro: Edições Graal, 1984.

FOUCAULT, M. Vigiar e punir: nascimento da prisão. Petrópolis: Vozes, 1987.

FRANCESCHI-BICCHIERAI, L. Este app de selfies estilo anime está coletando seus dados pessoais. *Motherboard*, 24 jan. 2017. Disponível em: <https://motherboard.vice.com/pt_br/article/9ad538/app-de-selfies-estilo-anime-esta-coletando-seus-dados-pessoais>. Acesso em: 10 out. 2017.

FRANÇA. L'Assemblée nationale et le Sénat ont adopté. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *Journal Officiel de la République Française*, 7 jan. 1978. Disponível em: <*https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460*>. *Acesso em: 24 abr. 2018.*

FRANÇA. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *Legifrance.gouv.fr*, dernière modification au 25 mai 2018, version consolidée au 04 juin 2018. Disponível em: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte= JORFTEXT000000886460>. Acesso em: 31 maio 2018

FRIEDMAN, K.; HUNTER, T. Canada. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 6 maio 2018.

FRIEDMAN, A.; WOLFF, R.; SCHUSTER, A. Providing k-anonymity in data mining. *The VLDB Journal*, v. 17, n. 4, p. 789-804, 2008.

FUNG, B. C. M. et al. Privacy-preserving data publishing: a survey of recent developments. *ACM Computing Surveys*, v. 42, n. 4, 2010.

GAMIZ, M. S. F. Privacidade e intimidade: doutrina e jurisprudência. Curitiba: Juruá, 2012.

GAO, S. et al. Balancing trajectory privacy and data utility using a personalized anonymization model. *Journal of Network and Computer Applications*, v. 38, p. 125-134, 2014.

GARANTE PRIVACY. Simplified arrangements to provide information and obtain consent regarding *cookies* - 8 may 2014. *Garante per la Protezione dei Dati Personale*, 8 maio 2014. Disponível em: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654>. Acesso em: 8 fev. 2018.

GARCIA-RIVADULLA, S. Personalization vs. privacy: an inevitable trade-off? *IFLA Journal*, v. 42, n. 3, p. 227-238, 2016.

GAVISON, R. Privacy and the limits of law. *The Yale Law Journal*, v. 89, n. 3, p. 421-471, 1980.

GEDIK, B.; LIU, L. Location privacy in mobile systems: a personalized anonymization model. In: IEEE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, 25., 2005, Columbus. *Proceedings*... [S.l.]: IEEE, 2005. p. 620-629.

GEDIK, B.; LIU, L. Protecting location privacy with personalized k-anonymity: architecture and algorithms. *IEEE Transactions on Mobile Computing*, v. 7, n. 1, p. 1-18, 2008.

GELLMAN, R. Fair information practices: a basic history. *SSRN*, 10 abr. 2017. Disponível em: <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2415020>. Acesso em: 20 nov. 2017.

GHINITA, G. et al. A reciprocal framework for spatial k-anonymity. *Information Systems*, v. 35, n. 3, p. 299-314, 2010.

GIANI, A. Identification with zero knowledge protocols. *SANS Institute Reading Room*, 2001. Disponível em: <https://www.sans.org/reading-room/whitepapers/vpns/identification-zero-knowledge-protocols-719>. Acesso em: 23 nov. 2017.

GIBSON, W. Google‘s Earth. *The New York Times*, 31 ago. 2010. Disponível em: <http://www.nytimes.com/2010/09/01/opinion/01gibson.html>. Acesso em: 23 jul. 2017.

GIL, A. C. Como elaborar projetos de pesquisa. 5. ed. São Paulo: Atlas, 2010.

GONG, Y.; FANG, Y.; GUO, Y. Private data analytics on biomedical sensing data via distributed computation. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, v. 13, n. 3, p. 431-444, 2016.

GOOGLE. *Políticas de privacidade do Google*. [201-]. Disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/>. Acesso em: 8 maio 2017.

GOOGLE CHROME. [Modo de navegação anônima]. Acesso em: 10 maio 2017.

GRENTZENBERG, V.; MEENTS, J.; POHLE, J. Germany. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 7 maio 2018.

GRESSIN, S. The equifax data breach: what to do. *Consumer Information*, 8 set. 2017. Disponível em: <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>. Acesso em: 1 nov. 2017.

GUSTAV, Y. H. et al. Velocity similarity anonymization for continuous query location based services. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL PROBLEM-SOLVING, 2013, Jiuzhai. *Proceedings...* [S.l.]: IEEE, 2013. p. 433-436.

HAJIAN, S.; DOMINGO-FERRER, J. A study on the impact of data anonymization on anti-discrimination. In: IEEE INTERNATIONAL CONFERENCE DATA MINING WORKSHOPS, 12., 2012, Brussels. *Proceedings...* [S.l.]: IEEE, 2012. p. 352-359.

HALPERT, J; KASHATUS, J; LUCENTE, K. United States. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 6 maio 2018.

HASHEMI, M.; MALEK, M. R. Protecting location privacy in mobile geoservices using fuzzy inference systems. *Computers, Environment and Urban Systems*, v. 36, n. 4, p. 311-320, 2012.

HEALTH & HUMAN SERVICES. Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule. *HHS*, 26 nov. 2012. Disponível em: <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>. Acesso em: 10 out. 2017.

HEALTH & HUMAN SERVICES. Summary of the HIPAA Privacy Rule. *HHS*, 26 jul. 2013. Disponível em: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>. Acesso em: 10 out. 2017.

HEIDEMANN, J.; PAPADOPOULOS, C. Uses and challenges for network datasets. In: IEEE CYBERSECURITY APPLICATIONS & TECHNOLOGIES CONFERENCE FOR HOMELAND SECURITY, 2009, Washington. [S.l.]: IEEE, 2009. p. 73-82.

HONG KONG. Chapter 486 personal data (privacy) ordinance. *Hong Kong e-Legislation*, 1996. Disponível em: <https://www.elegislation.gov.hk/hk/cap486>. Acesso em: 23 abr. 2018.

HOLANDA. Dutch Telecommunications Act: act of 19 October 1998, containing rules regarding telecommunication. *Dutch Staatsblad*, text applying on 7 June 2012. Disponível em: <https://www.government.nl/documents/policy-notes/2012/06/07/dutch-telecommunications-act>. Acesso em: 31 maio 2018.

HUANG, K. L.; KANHERE, S. S.; HU, W. A privacy-preserving reputation system for participatory sensing. In: CONFERENCE ON LOCAL COMPUTER NETWORKS, 37., 2012, Clearwater. *Proceedings...* [S.l.]: IEEE, 2012. p. 10-18.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 25237:2017*: Health informatics - Pseudonymization. Genebra, 2017.

IRLANDA. Data protection act, 1988. An act to give effect to the convention for the protection of individuals with regard to automatic processing of personal data done at strasbourg on the 28th day of january, 1981, and for that purpose to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically. *Irish Statute Book*, number 25 of 1988, 13 jul. 1988.

IRLANDA. Data Protection Act 2018. An Act to establish a body to be known as An Coimisiún um Chosaint Sonraí or, in the English language, the Data Protection Commission... *Irish Statute Book*, number 7 of 2018, 24 maio 2018.

ITÁLIA. Personal data protection code. Legislative Decree no. 196 of 30 June 2003. *Garante per la Protezione dei Dati Personale*, 2003. Disponível em: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4814258>. Acesso em: 23 abr. 2018.

JÄNDEL, M. Decision support for releasing anonymised data. *Computers & Security*, v. 46, p. 48-61, 2014.

JOHNSON, C. What to do if you suspect your child's identity has been stolen. *Clark*, 6 nov. 2017. Disponível em: <http://clark.com/protect-your-identity/identity-theft-child-kid-what-to-do/>. Acesso em: 3 dez. 2017.

JONES, P. Australia. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 6 maio 2018.

JUTLA, D. N.; BODORIK, P.; ALI, S. Engineering privacy for big data apps with the unified modeling language. In: IEEE INTERNATIONAL CONGRESS ON BIG DATA, 2013, Santa Clara. *Proceedings*... [S.l.]: IEEE, 2013. p. 38-45.

KARAKÜÇÜK, A.; DIRIK, A. E. Adaptive photo-response non-uniformity noise removal against image source attribution. *Digital Investigation*, v. 12, p. 66-76, 2015.

KARGUPTA, H. et al. Random-data perturbation techniques and privacy-preserving data mining. *Journal Knowledge and Information Systems*, v. 7, n. 4, p. 387-414, 2005.

KIFT, P. To have or not to have: the true privacy question. *Internet Policy Review*, v. 2, n. 4, p. 1-7, 2013.

KIM, J. J. A method for limiting disclosure in microdata based on random noise and transformation. In: SECTION ON SURVEY RESEARCH METHODS, 1986, Chicago. *Proceedings*... Washington: American Statistical Association, 1986. p. 303-308.

KIM, J. J.; WINKLER, W. E. Multiplicative noise for masking continuous data. Washington: U.S. Bureau of the Census, 2003.

KIM, Y. et al. Hilbert-order based spatial cloaking algorithm in road network. *Concurrency and Computation: Practice and Experience*, v. 25, n. 1, p. 143-158, 2013.

KITCHENHAM, B. *Procedures for performing systematic reviews*: joint technical report. Keele: Keele University, 2004.

KORTH, H. F.; SILBERSCHATZ, A. *Sistemas de banco de dados*. São Paulo: Makron Books, 1993.

KURBALIJA, J. *Uma introdução à governança da internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

KUROSE, J. F.; ROSS, K.W. Redes de Computadores e a Internet: uma abordagem top-down. Tradução Opportunity translations; revisão técnica Wagner Zucchi – 5ª edição – São Paulo: Addison Wesley, 2010.

KUROWSKA-TOBER, E; CZYNIENIK U. Poland. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://wwwqa.dlapiperdataprotection.com/index.html>. Acesso em: 8 maio 2018.

KURTH A. H. Belgium adopts law reforming the Belgian privacy commission. *Hunton Andrews Kurth Privacy & Information Security Law Blog*, 18 jan. 2018. Disponível em: <https://www.huntonprivacyblog.com/2018/01/18/belgium-adopts-law-reforming-belgian-privacy-commission/>. Acesso em: 23 mar. 2018.

LANE, A. *Understanding and selecting data masking solutions*: creating secure and useful data. Phoenix: Securosis, 2012.

LAPERDRIX, P.; RUDAMETKIN, W.; BAUDRY, B. Beauty and the beast: diverting modern web browsers to build unique browser fingerprints. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2016, San Jose. *Proceedings...* [S.l.]: IEEE, 2016. p. 878-894.

LARSON, S. Instagram hackers are selling user emails and phone numbers. *CNN Tech*, 1 set. 2017. Disponível em: <http://money.cnn.com/2017/09/01/technology/business/instagram-hack/index.html>. Acesso em: 3 nov. 2017.

LEBEAU-MARIANNA, D. France. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 8 maio 2018.

LEE, D. South Korea. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 5 maio 2018.

LEI, P. et al. Dummy-based schemes for protecting movement trajectories. *Journal of Information Science and Engineering*, v. 28, n. 2, p. 335-350, 2012.

LEONARDI, M. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2011.

LÉVY, P. *As tecnologias da inteligência*: o futuro do pensamento na era da informática. Rio de Janeiro: Ed. 34, 1993.

LI, N.; LI, T.; VENKATASUBRAMANIAN, S. t-closeness: privacy beyond k-anonymity and l-diversity. In: INTERNATIONAL CONFERENCE ON DATA ENGINEERING, 23., 2007, Istanbul. *Proceedings...* [S.l.]: IEEE, 2007. p. 106-115.

LIBRARY OF CONGRESS. Erasure of online information: Norway. *Library of Congress*, 2018. Disponível em: <https://www.loc.gov/law/help/erasure-online-info/norway.php>. Acesso em: 5 maio 2018.

LIBRARY OF CONGRESS. Online Privacy Law: Germany. *Library of Congress*, 2018. Disponível em: < https://www.loc.gov/law/help/online-privacy-aw/2017/germany.php#Data>. Acesso em: 30 jun. 2018.

LIN, H. et al. CAM: cloud-assisted privacy preserving mobile health monitoring. *IEEE Transactions on Information Forensics and Security*, v. 8, n. 6, p. 985-997, 2013.

LIN, P.; LIN, Y. Towards packet anonymization by automatically inferring sensitive application fields. In: INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION TECHNOLOGY, 14., 2012, PyeongChang. *Proceedings...* [S.l.]: IEEE, 2012. p. 87-92.

LIN, Y. et al. Pcaplib: a system of extracting, classifying, and anonymizing real packet traces. *IEEE Systems Journal*, v. 10, n. 2, p. 520-531, 2016.

LIOUDAKIS, G. V. et al. A middleware architecture for privacy protection. *Computer Networks*, v. 51, n. 16, p. 4679-4696, 2007.

LOUKIL, F. et al. Privacy-aware in the IoT applications: a systematic literature review. In: ON THE MOVE TO MEANINGFUL INTERNET SYSTEMS, 2017, Rhodes. *Proceedings...* [S.l.]: Springer, 2017. p. 552-569.

LOURO, P.; GARCIA, J.; ROMANO, P. Multipathprivacy: enhanced privacy in fault replication. In: EUROPEAN DEPENDABLE COMPUTING CONFERENCE, 9., 2012, Sibiu. *Proceedings...* [S.l.]: IEEE, 2012. p. 203-211.

MCGGEE, T. Equifax Data Breach: Has Amercia Given Up on Privacy? *TargetMarketing*, 13 set. 2017. Disponível em: < https://www.targetmarketingmag.com/post/has-america-given-up-on-privacy/>. Acesso em: 3 dez. 2017

MACHADO, J.; BIONI, B. R. A proteção de dados pessoais nos programas de nota fiscal: um estudo de caso da Nota Fiscal paulista. *Liinc em Revista*, v. 12, n. 2, p. 351-365, 2016.

MACHANAVAJJHALA, A. et al. L-diversity: privacy beyond k-anonymity. In: INTERNATIONAL CONFERENCE ON DATA ENGINEERING, 22., 2006, Atlanta. *Proceedings...* [S.l.]: IEEE, 2006. p. 24.

MANO, K.; MINAMI, K.; MARUYAMA, H. Protecting location privacy with k-confusing paths based on dynamic pseudonyms. In: IEEE INTERNATIONAL CONFERENCE ON

PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, 2013, San Diego. *Proceedings...* [S.l.]: IEEE, 2013. p. 285-290.

MARTÍNEZ, S.; SÁNCHEZ, D.; VALLS, A. A semantic framework to protect the privacy of electronic health records with non-numerical attributes. *Journal of Biomedical Informatics*, v. 46, n. 2, p. 294-303, 2013.

MASON, R. O. Four ethical issues of the information age. *MIS Quarterly*, v. 10, n. 1, p. 5-12, 1986.

MAYER-SCHÖNBERGER, V. Delete: the virtue of forgetting in the digital age. Princeton University Press, 2011.

MATHYS, R. et al. Switzerland. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 30 abr. 2018.

MCKINLEY, K. Cleaning up after *cookies*: version 1.0. *iSEC Partners Whitepapers*, p. 1-12, 31 dez. 2008. Disponível em: <https://www.nccgroup.trust/us/our-research/cleaning-up-after-*cookies*/>. Acesso em: 1 dez. 2017.

MICROSOFT. User-agente string. *Microsoft*, 11 mar. 2017. Disponível em: <https://msdn.microsoft.com/en-us/library/hh920767(v=vs.85).aspx>. Acesso em: 3 jun. 2017.

MINA *COOKIES*. *Recommendation on the use of cookies and comparable technology*. 2011. Disponível em: <http://www.mina*cookies*.se/wp-content/uploads/2011/11/Rekommendation_-*cookies*_nov18_2011_English_version.pdf>. Acesso em: 10 maio 2018.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. Comissão de Proeção dos Dados Pessoais. [201-]. Disponível em: <http://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-e-grupos/comissao-de-protecao-dos-dados-pessoais>. Acesso em: 4 abr. 2018.

MIVULE, K. Utilizing noise addition for data privacy, an overview. In: THE INTERNATIONAL CONFERENCE ON INFORMATION AND KNOWLEDGE ENGINEERING, 2012, Las Vegas. *Proceedings...* [S.l.]: CSREA Press, 2012. p. 65-71.

MIVULE, K. *An investigation of data privacy and utility using machine learning as a gauge*. 2014. 262 p. Dissertation (Doctorate in Science) - Graduate School of Bowie State University, Bowie, Maryland, 2014.

MIVULE, K. On the generation of privatized synthetic data using distance transforms. In: INTERNATIONAL CONFERENCE ON ADVANCED COGNITIVE TECHNOLOGIES AND APPLICATIONS, 7., 2015, Nice. *Proceedings...* [S.l.]: IARIA, 2015.

MONTEIRO, S. D. As múltiplas sintaxes dos mecanismos de busca no ciberespaço. *Informação & Informação*, v. 14, n. 1, p. 68-102, 2009.

MONTEIRO, S. D. et al. Em busca da compreensão da “busca” no ciberespaço. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 12., 2011, Brasília. *Anais...* Brasília: ANCIB, 2011. p. 2536-2551.

MOOR, J. H. Using genetic information while protecting the privacy of the soul. In: TAVANI, H. T. (Ed.). *Ethics, computing, and genomics*. Sudbury: Jones and Bartlett Publishers, 2006. p. 109-119.

MOORE, A. Defining privacy. *Journal of Social Philosophy*, v. 39, n. 3, p. 411-428, 2008.

MOORE, A. *Privacy rights*: moral and legal foundations. Pennsylvania: The Pennsylvania State University Press, 2010.

MORVILLE, P.; CALLENDER, J. *Search patterns*: design for discovery. Sebastopol: O'Reilly Media, 2010.

MULLEN, J.; FIEGERMAN, S. Yahoo tops the list of largest ever data breaches. *CNN Tech*, 4 out. 2017. Disponível em: <http://money.cnn.com/2017/10/04/technology/yahoo-biggest-data-breaches-ever/index.html>. Acesso em: 10 nov. 2017.

MURALIDHAR, K.; SARATHY, R. Data shuffling: a new masking approach for numerical data. *Management Science*, v. 52, n. 5, p. 658-670, 2006.

MURALIDHAR, K.; SARATHY, R.; DANDEKAR, R. Why swap when you can shuffle? A comparison of the proximity swap and data shuffle for numeric data. In: INTERNATIONAL CONFERENCE ON PRIVACY IN STATISTICAL DATABASES, 2006, Rome. *Proceedings...* Berlin: Springer, 2006. p. 164-176.

NERGIZ, A. E.; CLIFTON, C. Query processing in private data outsourcing using anonymization. In: IFIP ANNUAL CONFERENCE ON DATA AND APPLICATIONS SECURITY AND PRIVACY, 25., 2011, Richmond. *Proceedings...* Berlin: Springer, 2011. p. 138-153

NERGIZ, M. E.; GÖK, M. Z. Hybrid k-anonymity. *Computers & Security*, v. 44, p. 51-63, 2014.

NIKKEL, B. J. Generalizing sources of live network evidence. *Digital Investigation*, v. 2, n. 3, p. 193-200, 2005.

NISSENBAUM, H. A contextual approach to privacy online. *Daedalus*, v. 140, n. 4, p. 32-48, 2011.

NOLAN, P. Ireland. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 8 maio 2018.

NORBERG, P. A.; HORNE, D. R.; HORNE, D. A. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, v. 41, n. 1, p. 100-126, 2007.

NORUEGA. Justis- og beredskapsdepartementet. Lov om elektronisk kommunikasjon (ekomloven). 25-07-2003. Disponível em: < https://lovdata.no/dokument/NL/lov/2003-07-04-83>. Acesso em: 30 abr. 2018.

NORUEGA. Justis- og beredskapsdepartementet. Lov om behandling av personopplysninger (personopplysningsloven). 25-05-2018. Disponível em: < <https://lovdata.no/dokument/ISL/isl/2018-05-28-54>. Acesso em: 3 jun. 2018.

OBSERVATÓRIO DO MARCO CIVIL DA INTERNET. *Jurisprudência*. [201-]. Disponível em: <http://www.omci.org.br/jurisprudencia/>. Acesso em: 30 maio 2017.

O'BRIEN, S. A. Giant equifax data breach: 143 million people could be affected. *CNN Tech*, 8 set. 2017. Disponível em: <http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html>. Acesso em: 4 nov. 2017.

O'HARA, K.; SHADBOLT, N. *The spy in the coffee machine*: the end of privacy as we know it. London: Oneworld Publications, 2014.

OREBAUGH, A. D. et al. *Ethereal packet sniffing*. Rockland: Syngress Publishing, 2004.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Comissão Interamericana de Direitos Humanos. *Convenção americana sobre direitos humanos*: assinada na Conferência Especializada Interamericana sobre Direitos Humanos, San José, Costa Rica, em 22 de novembro de 1969. 1969. Disponível em: <https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm>. Acesso em: 24 abr. 2018.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *The OECD privacy framework*. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 10 ago. 2017.

ORWELL, G. 1984. São Paulo: Companhia das Letras, 2009.

PACKARD, V. Don't tell it to the computer. *New York Times Magazine*, 8 jan. 1967.

PACKARD, V. *The hidden persuaders*. New York: IG, 1982.

PAIVA, M. A. L. Os institutos do direito informático. *Âmbito Jurídico*, v. 6, n. 14, 2003. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_Art.s_leitura&Art._id=5487>. Acesso em: 20 abr. 2018.

PALANISAMY, B.; LIU, L. Mobimix: protecting location privacy with mix-zones over road networks. In: INTERNATIONAL CONFERENCE ON DATA ENGINEERING, 27., 2011, Hannover. *Proceedings...* [S.l.]: IEEE, 2011. p. 494-505.

PALANISAMY, B. et al. Road network mix-zones for anonymous location based services. In: INTERNATIONAL CONFERENCE ON DATA ENGINEERING, 29., 2013, Brisbane. *Proceedings...* [S.l.]: IEEE, 2013. p. 1300-1303.

PALANISAMY, B. et al. Anonymizing continuous queries with delay-tolerant mix-zones over road networks. *Distributed and Parallel Databases*, v. 32, n. 1, p. 91-118, 2014.

PANDIT, A.; POLINA, P.; KUMAR, A. CLOPRO: a framework for context cloaking privacy protection. In: INTERNATIONAL CONFERENCE ON COMMUNICATION SYSTEMS AND NETWORK TECHNOLOGIES, 4., 2014, Bhopal. *Proceedings...* [S.l.]: IEEE, 2014. p. 782-787.

PANDIT, A. et al. CAPPA: context aware privacy protecting advertising: an extension to CLOPRO framework. In: IEEE INTERNATIONAL CONFERENCE ON SERVICES COMPUTING, 2014, Anchorage. *Proceedings...* [S.l.]: IEEE, 2014. p. 805-812.

PARENT, W. A. Privacy, morality, and the law. *Philosophy & Public Affairs*, v. 12, n. 4, p. 269-288, 1983a.

PARENT, W. A. A new definition of privacy for the law. *Law and Philosophy*, v. 2, n. 3, p. 305-338, 1983b.

PARESCHI, L. et al. Composition and generalization of context data for privacy preservation. In: ANNUAL IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS, 6., 2008, Hong Kong. *Proceedings...* [S.l.]: IEEE, 2008. p. 429-433.

PARISER, E. *O filtro invisível*: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PARKER, R. B. A definition of privacy. *Rutgers Law Review*, v. 27, n. 1, p. 275-296, 1974.

PATIL, S.; KOBSA, A. Privacy considerations in awareness systems: designing with privacy in mind. In: MARKOPOULOS, P.; DE RUYTER, B.; MACKAY, W. (Ed.). *Awareness systems*. London: Springer, 2009. p. 187-206.

PEPPET, S. R. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Texas Law Review*, v. 93, p. 1-85, 2014.

PEREIRA, M. C. *Direito à intimidade na Internet*. Curitiba: Juruá, 2003.

PEUHKURI, M. A method to compress and anonymize packet traces. In: ACM SIGCOMM WORKSHOP ON INTERNET MEASUREMENT, 1., 2001, Burlingame. *Proceedings...* New York: ACM, 2001. p. 257-261.

PINGLEY, A. et al. Protection of query privacy for continuous location based services. In: INFOCOM, 2011, Shanghai. *Proceedings...* [S.l.]: IEEE, 2011. p. 1710-1718.

POLICARPO, P.; BRENNAND, E. *Cibercrimes na e-democracia*. Belo Horizonte: Editora D'Plácido, 2017.

POLÔNIA. Act of August 29, 1997 on the Protection of Personal Data. *Journal of Laws*, n. 133, 1997.

POLÔNIA. Telecommunications Act of 16 July 2004. *Journal of Laws*, 3 ago. 2004

PORTUGAL. Assembleia da República. Lei nº 67/98 de 26 de Outubro. Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.o 95/46/CE, do

Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados). *Diário da República*, n. 247, 26 out. 1998.

PORTUGAL. Assembleia da República. Lei n.º 41/2004, de 18 de Agosto. Transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. *Diário da República*, n. 194, 18 ago. 2004.

POST, R. C. Three concepts of privacy. *Georgetown Law Journal*, v. 89, p. 2087, 2001.

PÖTZSCH, S. Privacy awareness: a means to solve the privacy paradox? In: IFIP SUMMER SCHOOL ON THE FUTURE OF IDENTITY IN THE INFORMATION SOCIETY, 4., 2008, Brno. *Proceedings...* Berlin: Springer, 2008. p. 226-236.

PRIVACY SHIELD. Privacy shield program overview. *Privacy Shield Framework*, [201-]a. Disponível em: <https://www.privacyshield.gov/Program-Overview>. Acesso em: 10 nov. 2017.

PRIVACY SHIELD. *EU-U.S. Privacy shield framework principles*. Washington: U.S. Department of Commerce, [201-]b. Disponível em: < https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>. Acesso em: 10 nov. 2017.

PRIVACY SHIELD. *EU-U.S. Privacy shield framework principles*. Washington: U.S. Department of Commerce, [201-]c. Disponível em: < https://www.trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf >. Acesso em: 10 nov. 2017.

PRIYA, E. M.; MANI, G. Privacy for location based system in mobile p2p environment. *Procedia Engineering*, v. 38, p. 2179-2185, 2012.

PROVÉRBIOS. In: BÍBLIA SAGRADA. 131 ed. São Paulo: Ave Maria, 1999. p. 778-816.

QUINTA, J. C. Portugal. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 5 maio 2018.

QUISQUATER, J. et al. How to explain zero-knowledge protocols to your children. In: CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOLOGY, 1989, Santa Barbara. *Proceedings...* New York: Springer, 1989. p. 628-631.

RAMOS, D. Spain. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 8 maio 2018.

RASS, S. et al. How to protect privacy in floating car data systems. In: ACM INTERNATIONAL WORKSHOP ON VEHICULAR INTER-NETWORKING, 5., 2008, San Francisco. *Proceedings...* New York: ACM, 2008. p. 17-22.

READ, B. How much do your dating apps know about you? *Vogue*, 27 set. 2017. Disponível em: <https://www.vogue.com/article/dating-apps-privacy>. Acesso em: 13 nov. 2017.

REBOLLO-MONEDERO, D.; FORNÉ, J.; SORIANO, M. An algorithm for k-anonymous microaggregation and clustering inspired by the design of distortion-optimized quantizers. *Data & Knowledge Engineering*, v. 70, n. 10, p. 892-921, 2011.

REINO UNIDO. Data protection act 2018: chapter 12. *legislation.gov.uk*, 2018. Disponível em: < http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf>. Acesso em: 26 maio 2018.

REINO UNIDO. The privacy and electronic communications (EC Directive) regulations 2003. *legislation.gov.uk*, 2003. Disponível em: <http://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf>. Acesso em: 5 maio 2018.

RIGG, J. Google fined $190.000 in Germany for illegal Wifi snooping with Street View cars. *Engadget*, 22 abr. 2013. Disponível em: <https://www.engadget.com/2013/04/22/google-street-view-fine-germany/>. Acesso em: 20 mar. 2017.

RODOTÀ, S. *Tecnologie e diritti*. Bologna: Il Mulino, 1995.

RODOTÀ, S. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES, F. A. *Coleta de dados em redes sociais*: privacidade de dados pessoais no acesso via Application Programming Interface. 2017. 678 f. Tese (Doutorado em Ciência da Informação) - Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2017.

RUBINSTEIN, I. S.; HARTZOG, W. Anonymization and risk. *Washington Law Review*, v. 91, p. 703-760, 2015.

RUFFING, T.; MORENO-SANCHEZ, P.; KATE, A. CoinShuffle: practical decentralized coin mixing for bitcoin. In: EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY, 19., 2014, Wroclaw. *Proceedings...* [S.l.]: Springer, 2014. p. 345-364.

RUN, C. et al. Protecting privacy using k-anonymity with a hybrid search scheme. *International Journal of Computer and Communication Engineering*, v. 1, n. 2, p. 155, 2012.

RUPPEL, P. et al. Anonymous user tracking for location-based community services. In: INTERNATIONAL WORKSHOP ON LOCATION-AND CONTEXT-AWARENESS, 2., 2006, Dublin. *Proceedings...* Berlin: Springer, 2006. p. 116-133.

SAMARATI, P. Protecting respondents identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, v. 13, n. 6, p. 1010-1027, 2001.
SAMARATI, P.; SWEENEY, L. *Protecting privacy when disclosing information*: k-anonymity and its enforcement through generalization and suppression. Technical report. [S.l.]: SRI International, 1998.

SÁNCHEZ, D.; BATET, M. C-sanitized: a privacy model for document redaction and sanitization. *Journal of the Association for Information Science and Technology*, v. 67, n. 1, p. 148-163, 2015.

SANDERS, C. *Practical packet analysis*: using wireshark to solve real-world network problems. San Francisco: No Starch Press, 2017.

SANT'ANA, R. C. G. Ciclo de vida dos dados e o papel da Ciência da Informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 14., 2013, Florianópolis. *Anais...* Florianópolis: ANCIB, 2013.

SANT'ANA, R. C. G. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. *Informação & Informação*, v. 21, n. 2, p. 116-142, 2016.

SARAIVA, A. et al. Device fingerprinting: conceitos e técnicas, exemplos e contramedidas. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 14., 2014, Belo Horizonte. *Minicursos...* Belo Horizonte, MG: SBC, 2014.

SCHAIK, R. WIT, R. Netherlands. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 3 maio 2018.

SCHOEN, S. New cookie technologies: harder to see and remove, widely used to track you. *Electronic Frontier Foundation*, 14 set. 2009. Disponível em: <https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide>. Acesso em: 20 nov. 2017.

SCHUSTER, S. et al. Mass surveillance and technological policy options: improving security of private communications. *Computer Standards & Interfaces*, v. 50, p. 76-82, 2017.

SCHWABE, J. *Cinquenta anos de jurisprudência do Tribunal Constitucional Alemão*. Montevidéo: Fundación Konrad-Adenauer, 2005.

SCLAVOS, J.; SIMONI, N.; ZNATY, S. Information model: from abstraction to application. In: IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 1994, Kissimmee. *Proceedings...* [S.l.]: IEEE, 1994. p. 183.

SHERKAT, R.; LI, J.; MAMOULIS, N. Efficient time-stamped event sequence anonymization. *ACM Transactions on the Web*, v. 8, n. 1, p. 1-4, 2013.

SHETH, S.; KAISER, G.; MAALEJ, W. Us and them: a study of privacy requirements across North America, Asia, and Europe. In: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, 36., 2014, Hyderabad. *Proceedings...* New York: ACM, 2014. p. 859-870.

SHIN, H.; VAIDYA, J.; ATLURI, V. Anonymization models for directional location based service environments. *Computers & Security*, v. 29, n. 1, p. 59-73, 2010.

SHRIVASTVA, K. M. P.; RIZVI, M. A.; SINGH, S. Big data privacy based on differential privacy a hope for big data. In: INTERNATIONAL CONFERENCE ON

COMPUTATIONAL INTELLIGENCE AND COMMUNICATION NETWORKS, 2014, Bhopal. *Proceedings*... [S.l.]: IEEE, 2014. p. 776-781.

SOBEK. *Home*. [201-]. Disponível em: <http://sobek.ufrgs.br/try-sobek-online.html>. Acesso em: 4 jan. 2017.

SOLOVE, D. J. Conceptualizing privacy. *California Law Review*, v. 90, n. 4, p. 1087-1155, 2002.

SOLOVE, D. J. A taxonomy of privacy. *University of Pensylvania Law Review*, v. 154, n. 3, p. 477, 2006.

SOLOVE, D. J. *Understanding privacy*. Cambridge: Harvard University Press, 2008.

SONG, D. et al. A privacy-preserving continuous location monitoring system for location-based services. *International Journal of Distributed Sensor Networks*, v. 11, n. 8, 2015. doi:10.1155/2015/815613

SPIEKERMANN, S.; CRANOR, L. F. Engineering privacy. *IEEE Transactions on Software Engineering*, v. 35, n. 1, p. 67-82, 2009.

SUÉCIA. *Personal data protection*: information on the personal data act. 4. ed. Stockholm: Fritzes kundtjänst, 2006.

SUÉCIA. Miljö- och energidepartementet. Lag (2018:551) med kompletterande bestämmelser till EU:s däckmärkningsförordning. *Svensk författningssamling*, 24 maio 2018.

SUÍÇA. The Federal Council. Federal Act on Data Protection, of 19 June 1992. *The Federal Council*, 1 jul. 1993. Disponível em: <https://www.admin.ch/opc/en/classified-compilation/19920153/index.html>. Acesso em: 6 maio 2018

SUÍÇA. Federal Act on Data Protection: draft published on September 15, 2017. [Switzerland]: Walder Wyss, 2017. Disponível em: <https://www.walderwyss.com/publications/2149.pdf>. Acesso em: 06 Mai. 2018.

SUÍÇA. The Federal Council. Swiss-US Privacy Shield: better protection for data transferred to the USA. *The Federal Council*, 5 jan 2016. Disponível em: <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65210.html>. Acesso em: 10 nov. 2017.

SUNDBERG, J.; THÖRN, J. Sweden. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 5 maio 2018.

SVENSSON, A. F.; ADVOKATBYRÅ, H. Data protection in Sweden: overview. *Thomson Reuters Practical Law*, 1 fev. 2018. Disponível em: <https://uk.practicallaw.thomsonreuters.com/8-5020348?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1>. Acesso em: 23 abr. 2018.

SWEENEY, L. K-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, v. 10, n. 5, p. 557-570, 2002.

SZANIAWSKI, E. *Os direitos de personalidade e sua tutela*. São Paulo: Revista dos Tribunais, 1993.

TANENBAUM, A. S. Redes de computadores. 4. ed. Rio de Janeiro: Campus, 2003.

TANENBAUM, A. S.; WETHERALL, J. D. Redes de computadores. 5. ed. Rio de Janeiro: Pearson, 2011.

TAVANI, H. T. Informational privacy: concepts, theories, and controversies. In: HIMMA, K. E.; TAVANI, H. T. (Ed.). *The handbook of information and computer ethics*. New Jersey: John Wiley & Sons, 2008. p. 131-164.

TELLES, G. Política de privacidade da Uber. *Uber Newsroom*, 8 dez. 2014. Disponível em: <https://newsroom.uber.com/politica-de-privacidade-da-uber/>. Acesso em: 5 out. 2017.

THIEL, S.; BIGG, C. Hong Kong. In: DLA PIPER. *Data protection laws of the world*: full handbook. [S.l.]: DLA Piper, 2018. Disponível em: <https://www.dlapiperdataprotection.com/index.html>. Acesso em: 3 fev. 2018.

THOMSON, J. J. The right to privacy. *Philosophy & Public Affairs*, v. 4, n. 4, p. 295-314, 1975.

TOR. *Anonymity online*. [201-]. Disponível em: <https://www.torproject.org/>. Acesso em: 3 jul. 2017.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial das Comunidades Europeias*, n. 50, 23 nov. 1995.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). *Jornal Oficial das Comunidades Europeias*, n. 50, 31 jul. 2002.

UNIÃO EUROPEIA. Directiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas. *Jornal Oficial das Comunidades Europeias*, n. 50, 18 dez. 2009.

UNIÃO EUROPEIA. European Parliament. Council of Europe. Regulation (EU) 2016/679 of the European Parliament and of the Council. *EUR-Lex*, 27 abr. 2016.
UNIÃO EUROPEIA. COM/2017/010 final - 2017/03 (COD). Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas). *Jornal Oficial das Comunidades Europeias*, n. 50, 10 jan. 2017.

UNITED NATIONS. *Universal declaration of human rights*. 1948. Disponível em: <http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf>. Acesso em: 24 abr. 2018.

UNITED NATIONS. Office of the High Commissioner for Human Rights. *International Covenant on Civil and Political Rights*. 1966. Disponível em: <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>. Acesso em: 24 abr. 2018.

VERGARA-LAURENS, I. J.; LABRADOR, M. A. Preserving privacy while reducing power consumption and information loss in lbs and participatory sensing applications. In: IEEE GLOBECOM WORKSHOPS, 2011, Houston. *Proceedings...* [S.l.]: IEEE, 2011. p. 1247-1252.

VERGARA-LAURENS, I. J.; MENDEZ, D.; LABRADOR, M. A. Privacy, quality of information, and energy consumption in participatory sensing systems. In: IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS, 2014, Budapest. *Proceedings...* [S.l.]: IEEE, 2014. p. 199-207.

VYGOTSKY, L. S. *Obras escogidas III*. Madri: Visor, 1995.

WACKS, R. *Privacy*: a very short introduction. New York: Oxford University Press, 2015.

WALLACE, K. A. Anonymity. *Ethics and Information Technology*, v. 1, n. 1, p. 21-31, 1999.

WALLACE, K. A. Online anonymity. In: HIMMA, K. E.; TAVANI, H. T. (Ed.). *The handbook of information and computer ethics*. New Jersey: John Wiley & Sons, 2008. p. 165-189.

WANG, H. *Protecting privacy in China*: a research on China's privacy standards and the possibility of establishing the right to privacy and the information privacy protection legislation in modern China. New York: Springer, 2011.

WANG, Y.; KOBSA, A. A PLA-based privacy-enhancing user modeling framework and its evaluation. *User Modeling and User-Adapted Interaction*, v. 23, n. 1, p. 41-82, 2013.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890.

WEI, Y.-C.; CHEN, Y.-M.; SHAN, H.-L. RSSI-based user centric anonymization for location privacy in vehicular networks. In: INTERNATIONAL WORKSHOP ON SECURITY IN EMERGING WIRELESS COMMUNICATION AND NETWORKING SYSTEMS, 1., 2009, Athens. *Proceedings...* Berlin: Springer, 2009. p. 39-51.

WERSIG, G.; NEVELING, U. The phenomena of interest to information science. *The Information Scientist*, v. 9, n. 4, p. 127-140, 1975.

WESTIN, A. F. *Privacy and freedom*. New York: Atheneum, 1967.

WIGAND, C.; VOIN, M. European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. *European Comission*, 12 jul 2016. Disponível em: http://europa.eu/rapid/press-release_IP-16-2461_en.htm. Acesso em: 20 jun. 2017.

WIRESHARK. *Wireshark user's guide*. [201-]. Disponível em: <https://www.wireshark.org/docs/>. Acesso em: 5 maio 2017.

WONG, R. C.-W. et al. (α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing. In: ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING, 12., 2006, Philadelphia. *Proceedings...* New York: ACM, 2006. p. 754-759.

WOO, J. The right not to be identified: privacy and anonymity in the interactive media environment. *New Media & Society*, v. 8, n. 6, p. 949-967, 2006.

WORLD WIDE WEB CONSORTIUM. Hypertext Transfer Protocol -- HTTP/1.1. *Network Working Group*, jun. 1999. Disponível em: <http://www.w3.org/Protocols/rfc2616/rfc2616.txt>. Acesso em: 23 maio 2017.

WORLD WIDE WEB CONSORTIUM. Fingerprinting guidance for web specification authors (draft). *W3C Interest Group Note*, 24 nov. 2015. Disponível em: <https://www.w3.org/TR/fingerprinting-guidance/>. Acesso em: 20 nov. 2017.

XIAO, X.; TAO, Y. Anatomy: simple and effective privacy preservation. In: INTERNATIONAL CONFERENCE ON VERY LARGE DATA BASES, 32., 2006, Seoul. *Proceedings...* [S.l.]: VLDB Endowment, 2006. p. 139-150.

XU, Yang et al. A survey of privacy preserving data publishing using generalization and suppression. *Applied Mathematics & Information Sciences*, v. 8, n. 3, p. 1103-1116, 2014.

XUE, M. et al. Distributed privacy preserving data collection. In: INTERNATIONAL CONFERENCE ON DATABASE SYSTEMS FOR ADVANCED APPLICATIONS, 16., 2011, Hong Kong. *Proceedings...* Berlin: Springer, 2011. p. 93-107.

ZHANG, C.; HUANG, Y. Cloaking locations for anonymous location based services: a hybrid approach. *GeoInformatica*, v. 13, n. 2, p. 159-182, 2009.

ZHANG, Q.; LAZOS, L. Collusion-resistant query anonymization for location-based services. In: IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS, 2014, Sydney. *Proceedings...* [S.l.]: IEEE, 2014. p. 768-774.

ZHANG, Q. et al. Aggregate query answering on anonymized tables. In: IEEE INTERNATIONAL CONFERENCE ON DATA ENGINEERING, 23., 2007, Istanbul. *Proceedings...* [S.l.]: IEEE, 2007. p. 116-125.

ZHONG, S.; YANG, Z.; CHEN, T. k-Anonymous data collection. *Information Sciences*, v. 179, n. 17, p. 2948-2963, 2009.

ZUBERI, R. S.; LALL, B.; AHMAD, S. N. Privacy protection through k-anonymity in location-based services. *IETE Technical Review*, v. 29, n. 3, p. 196-201, 2012.

APÊNDICE A - Sumarização dos trabalhos inclusos na revisão sistemática[112]

Art.	Autor (es)	Ano	Citação	Escopo e Característica do Estudo
1	GEDIK E LIU	2008	210	- É proposta uma arquitetura baseada no modelo k-anonimato para anonimizar dados de localização de usuários que utiliza serviços LBS; - A arquitetura é formada por um cliente móvel (usuário), servidor de anonimato confiável e um canal seguro protegido por criptografia. - A comunicação dos usuários com o servidor de anonimato acontece por meio de conexão autenticada e criptografada. - O servidor de anonimato executa perturbação nas mensagens antes de enviar ao LBS e remove dados identificadores. - O *spatial cloaking* refere-se a substituir a localização por intervalo espacial (generalização). - Considera o espaço temporal e local, e o termo perturbação se refere a camuflagem espacial e cloaking temporal; - Baseia-se no modelo k-anonimato, nas técnicas de criptografia e na generalização.
2	GEDIK E LIU	2005	127	- Desenvolveram um modelo k-anonimato personalizado para proteção da privacidade de indivíduos que utilizam serviços LBS; - O sistema LBS é formado por nós móveis, servidor de anonimato e servidor LBS; -Utiliza técnicas de perturbação para variáveis de espaço e tempo, e remoção da identidade; - Cada usuário pode especificar o nível de k-anonimato e pode alterar a granularidade por mensagem; - A comunicação dos usuários com o servidor de anonimato acontece por meio de conexão autenticada e criptografada; - O servidor de anonimato remove qualquer identificador, tais como endereço IP, e perturba a informação de localização por meio de camuflagem espaço-temporal. E encaminha a mensagem anonimizada para o provedor LBS; - Anonimização acontece em um servidor confiável. - Baseia-se no k-anonimato, nas técnicas de supressão, *spatial cloaking* e criptografia.
3	EFTHYMIOU E KALOGRIDIS	2010	96	- Descreve um método para anonimizar dados de energia elétrica que são coletados de residências por meio de medidores inteligentes - Mecanismo permite coletar dados minimizando associação de dados coletados com um cliente específico; - Utiliza servidor de terceiro para autenticar a leitura e gerar dados pseudoanônimos[113]. O terceiro pode ser o fabricante do medidor inteligente ou um terceiro confiável. - Baseia-se no uso de criptografia e pseudônimos
4	SPIEKERMANN e CRANOR [114]	2009	67	- É apresentada uma revisão de literatura para evidenciar as atividades que ameaçam a privacidade no contexto da coleta, armazenamento e processamento de dados. - Posteriormente, é proposta uma metodologia baseada na *Fair Information Practices* (FIP), e discutem como esse contexto pode ser apoiado por meio de privacidade por política e privacidade por *design* (minimiza a coleta de dados pessoais identificáveis e enfatiza a anonimização no lado do cliente), enfocando mecanismos de aviso e consentimento. - Aborda o modelo k-anonimato e *l-diversity*.
5	CHOW; MOKBE; AREF	2009	45	- Proposto um framework denominado Casper, com finalidade de permitir que usuários móveis utilizem LBS sem revelar dados pessoais; - O framework permite que usuário utilizem serviços especificando seu perfil de privacidade; - O Casper tem dois componentes principais, o anonimizador de localização e o processador de consulta (servidor LBS). - O serviço LBS não precisa ter dados exatos de localização;

[112] Os textos citados neste apêndice compõem a lista de referência desta tese.
[113] Técnica de anonimização de identidade, onde a identidade real do veículo é substituída por um pseudônimo (BALDINI; GIULIANI; PONS, 2017)
[114] Art. que realiza revisão, desta forma não foi evidenciado as categorias do quadro. p

				- O nível de privacidade é apoiado pelo modelo K-anonimato, e o servidor de anonimização de localização utiliza um algoritmo para desfocar as áreas de localização, removendo qualquer identidade do individuo. - O processador de consulta ao invés de retornar a resposta exata, retorna uma lista de resposta para usuários que estão na área anonimizada. - a anonimização ocorre mediante modelo k-anonimato e as técnicas de *spatial cloaking* e supressão.
6	CHOW; MOKBEL; LIU	2011	42	- Os autores propõem um algoritmo utilizando *Spatial Cloaking* e abordagens do k-anonimato em ambientes P2P móvel, que permite que usuários móveis compartilhem suas informações de localização com outros pares, reduzindo a sobrecarga de comunicação; - O modelo é composto pelos usuários móveis e pelo servidor baseado em localização; - O foco é na consulta instantânea, sendo que cada consulta recebe um identificador pseudônimo; - Cada usuário especifica seus requisitos de privacidade, podendo mudar seu perfil de privacidade a qualquer momento, tanto em relação às questões temporais, espaciais e/ou restrição interdependente (nível do anonimato e área coberta). - O servidor baseado em localização executa o algoritmo P2P *Spatial Cloaking* para desfocar localização do usuário da área *cloaked* e, enviar sua consulta juntamente com a área desfocada para o LBS, a fim de receber os serviços. - Baseado no modelo k-anonimato e nas técnicas de *spatial cloaking* e pseudônimo.
7	PALANISAMY e LIU	2011	42	- Descreve o framework *Mobimix* para proteção de dados localização de usuários que utilizam dispositivos móveis e que viajam em redes rodoviárias. - A abordagem do *Mobimix* é interromper a continuidade da localização do usuário utilizando *mix-zones* (regiões onde um nó veicular pode mudar sua identidade temporária (pseudônimo[115]) sem ser rastreado, assim não é possível acompanhar os movimentos do usuário). - Um *mix-zone* de k-participantes se refere à região k-anônima, na qual os usuários podem alterar seus pseudônimos de tal forma que o mapeamento entre os pseudônimos anteriores e novos não são revelados. - Aborda duas situações do mix-zone: quando o usuário permanece um tempo aleatório dentro da zona aleatório e, quando o usuário segue uma probabilidade de entrar e sair da zona. - É apresentado modelos de ataque e medidas de anonimato. - Aborda o modelo k-anonimato.
8	CHOW: MOKBEL; HE	2011	26	- É proposto um sistema de monitoramento de localização de indivíduos para proteger a privacidade em redes de sensores sem fio; - O sistema é baseado no modelo k-anonimato e utiliza histograma espacial; - No sistema, cada indivíduo é indistinguível entre k indivíduos, onde cada nó do sensor será perturbado e é informado ao servidor apenas informações de localização agregada, que se encontra na área desfocada. Para apoiar o monitoramento de serviços - São propostos dois algoritmos de anonimização de localização (*The Resource-Aware Algorithm e The Quality-Aware Algorithm*), que requerem que os nós colaborem uns com os outros para desfocar área, de modo que cada área contenha pelo menos k-pessoas para constituir uma área k-anônima. - É proposto um histograma espacial que analisa os locais agregados para estimar a distribuição das pessoas monitoradas no sistema. - A arquitetura do sistema é composta por três elementos: nós de sensores, servidor e usuários do sistema. - O servidor é responsável pela coleta das localizações referente aos nós dos sensores, utilizando um histograma espacial para estimar a distribuição dos objetos monitorados.

[115] Uso de identidades temporárias autenticáveis, Esta alternativa exige que cada nó veicular seja equipado com um conjunto de certificados, um para cada pseudônimo, que deve ser emitido por uma terceira parte confiável.

				- O servidor só sabe que um remetente é um nó dentro de uma área anonimizada, mas não tem informação da sua localização. - Baseado no modelo k-anonimato, nas técnicas de spatial cloaking e microagregação
9	LIN et al.	2013	28	- Foi desenvolvido um monitoramento *para Cloud-Assisted MHealth* (CAM), identificando problemas de design na proteção da privacidade e posteriormente as soluções. - O CAM consiste em quatro partes: servidor da nuvem; empresa que fornece o serviço de monitoramento de *mHealth* (prestador de serviços de saúde), clientes individuais e uma autoridade semi-confiável (responsável por distribuir chaves privadas aos clientes individuais). - CAM adota técnica de criptografia homomórfico e, para proteger os programas dos prestadores de serviços mHealth, foi utilizado permutação e randomização.
10	DOMINGO-FERRER	2006	22	- Utiliza-se de microagregação e k-anonimato para proteção da privacidade de localização; - Faz uso de um terceiro confiável *free*, que não exige que os usuários divulguem sua localização exata ou suas consultas; - Uso do k-anonimato para localização e perturbação de dados confidenciais do usuário, tais como a latitude e longitude, sendo que o próprio usuário perturba a sua localização por meio da adição de ruído com distribuição Gaussiana; - É proposto o modelo *p-sensitive* baseado em microagregação que não utiliza de supressão e nem de generalização. - O p-sensitive é uma evolução do k-anonimato cujo objetivo é evitar que registros compartilhem um ou mais atributos confidenciais. - Baseado no modelo k-anonimato e uso das técnicas de micro agregação e randomização.
11	PINGLEY et al	2011	20	- São investigadas questões relacionadas à privacidade de consulta contínua em LBS, buscando evitar que servidor LBS correlacione atributos de serviços com identidade de indivíduos. - Foi proposta solução chamada DUMMY que utiliza técnicas de perturbação, e protege a privacidade durante a consulta a um LBS, pois gera consultas falsas; - Foi proposto um esquema baseado em *quad-tree* para reduzir necessidade de armazenamento e capacidade computacional da DUMMY; - A arquitetura do DUMMY-Q consiste em quatro componentes: previsão da trajetória, POOL-BUILDER (algoritmos para gerar valores falsos), recuperação de grid/contexto e geração de consulta; - A solução não requer a presença de um terceiro confiável. - para anonimização utiliza da técnica de randomização
12	GHINITA et al	2010	18	- Aborda sobre o *spatial k-anonymity* (SKA), cujo objetivo é substituir a localização exata de um usuário por uma região anonimizada *(anonymizing spatial region (*ASR*));* - Foi proposto um framework para implementar algoritmos recíprocos utilizando índice espacial existentes nas localizações de usuário; - A anonimização acontece por meio de um terceiro confiável (anonimizador) que envia os dados de solicitação (consultas de usuários distribuídos geograficamente) anonimizados para o provedor de serviço. O anonimizador que recebe as consultas de usuários remove a identificação dos usuários, esconde suas localizações e encaminha para a ASR para o LBS, onde cada consulta tem um grau variável de k-anonimato. - O anonimizador indexa os locais dos usuários por hierarquia (ex: Quad-tree). - Para anonimização utiliza de *spatial cloaking* com base no modelo k-anonimato.
13	ZHONG; YANG; CHEN	2009	16	- É estudado o *k-Anonymous Data Collection* (KADC), *uma* técnica de criptografia voltada para proteção da privacidade na fase de coleta dos dados, que permite que usuários enviem dados anonimamente, mesmo que os dados tenham informações de identificação; - O kADC permite que o minerador de dados colete uma versão anonimizada do conjunto de dados de entrevistados, mas não devem ser capazes de vincular os dados sensíveis aos indivíduos;

				- O kADC não depende de nenhuma informação de identificação; - Foi criado protocolo básico do kADC baseando-se em modelo semi-honesto, modelo malicioso e, um protocolo que permite suprimir menos dados semi-identificadores; - Utiliza técnica de supressão para alcançar o k-anonimato, assinaturas digitais, randomização, permutação e protocolo *zero-knowledge proofs* para prevenir ataques.
14	PEPPET	2014	15	- Este artigo mostra aspectos das tecnologias baseadas em sensores, internet das coisas e as como proceder para proteger a privacidade. - O autor exemplifica as questões da Internet das coisas por meio do dispositivo *Breathometer*, que mede, registra e analisa diferentes aspectos da vida diária do individuo. - É realizada uma reflexão nas questões envolvidas sobre a propriedade dos dados coletados, segurança, consciência das implicações legais, direito ao esquecimento, quais dados os dispositivos podem ser coletados, como esses dados podem ser usados e qual o controle do usuário sobre os dados. Os dados de sensores de automóveis também são incluídos na reflexão deste Artigo
15	CHOW; MOKBEL; LIU	2011	15	- Neste trabalho foi proposto um algoritmo de anonimização de dados de localização para rede rodoviária, baseando-se no algoritmo *Spatial Cloaking.* - O algoritmo considera o custo de execução da consulta no servidor de banco de dados e da qualidade da consulta, ou seja, o número de objetos retornados aos usuários pelo servidor, durante o processo de anonimização da localização. - No Artigo os autores se concentram no *spacial cloaking*, sensores de rede, dados de trajetórias e consultas contínuas. - A ideia principal da proposta é desfocar a localização do usuário em uma área que foi utilizada *spatial cloaked* e que satisfaça o requisito de privacidade por meio do modelo k-anonimato. - Arquitetura do sistema é composta de usuários móveis, anonimizador de localização e servidor LBS. - Os usuários móveis se inscrevem no sistema especificando seus requisitos de privacidade de modo personalizado, ou seja, no mínimo k-anônimo, indistinguível entre os usuários de K. - O anonimizador de localização é um terceiro confiável colocado entre o usuário e o servidor LBS que também remove a identidade do usuário para garantir a pseudoanonimização da informação de localização, assim ele envia para o LBS a consulta anonimizada e com dados de localização desfocados. - O LBS retorna uma lista de resposta ao invés de uma resposta exata, de acordo com a região que foi anonimizada. - Utiliza o modelo k-anonimato e técnicas de randomização, supressão e microagregação.
16	REBOLLO-MONEDERO; FORNE; SORIANO	2011	13	-Apresenta uma solução para os problemas de microagregação e cluster anônimo, tanto para recuperação da informação privada baseada em dados de localização, quanto em banco de dados. - A solução é baseada no modelo k-anonimato, utilizando técnicas perturbativas otimizada para dados de localização; - A arquitetura é composta pelo usuário, pelo anonimizador de localização e pelo provedor LBS; - O algoritmo proposto denominado de *probability-constrained Lloyd (PCL)* faz uma modificação no algoritmo do Lloyd, voltado para otimizar a distorção e adequado para microagregação e agrupamento; - Os princípios da pseudoanonimização e anonimização são mesclados, e os dados de localização são coletados por um terceiro confiável para criar a perturbação e remover qualquer dado de identificação do usuário. - O terceiro confiável é considerado um anonimizador de localização que coleta dados precisos sobre a localização dos usuários, executa o agrupamento k-anônimo, ou seja, locais agrupados por meio de centroides comuns a k dispositivos próximos. - Utiliza modelo k-anonimato, e as técnicas de spatial cloaking e randomização.
17	ZHANG; HUANG	2009	13	- Este trabalho propõe um framework chamado HiSC cujo objetivo é equilibrar a tarefa entre o servidor de anonimização e os clientes móveis quando utilizam LBS. - Um cliente móvel pode solicitar um serviço ao servidor de anonimização (*cloaking* centralizado) ou utilizar uma abordagem P2P utilizando *Spatial Cloaking*, com base em privacidade personalizada.

				- O sistema HiSC pode distribuir a carga de trabalho entre o servidor de anonimização e o cliente móvel, proporcionando o anonimato na consulta. -A arquitetura do sistema é composta pelos usuários móveis, um servidor de anonimização e o servidor LBS. - O servidor de anonimização é confiável e tem conhecimento sobre o usuário, as solicitações de serviço móvel e a localização exata. -O servidor LBS são considerados não confiáveis, eles não tem conhecimento do identificador de um usuário móvel que solicita um serviço especifico e, não conhecem a localização precisa do solicitante do serviço, apenas conhecem a região que foi camuflada (*cloaking region*) – que consiste em uma região que contém pelo menos k clientes móveis. - Quando a anonimização por spacial cloaking é centralizada a tarefa é do servidor de anonimização, e quando é tratada pelos clientes móveis é por meio da abordagem P2P, comunicação entre pares. - Utiliza do modelo k-anonimato, técnicas de randomização e *spatial cloaking.*
18	CLAUSE; ORSO	2011	11	- É apresentado um protótipo denominado *Camouflage* para tornar dados anônimos automaticamente na coleta dos dados, antes de enviar para os desenvolvedores; - As técnicas abordadas diminui a quantidade de informação que é revelada na entrada original, garantindo a privacidade; - Utiliza-se de duas novas técnicas *path condition relaxation* e *breakable input conditions*, essas técnicas diminuem o valor das informações que são reveladas quando coletadas, tornando mais difícil reconstruir os dados originais; - Foi verificado o tempo necessário para gerar dados anonimizados e a qualidade da anonimização. - Utiliza de técnicas de supressão.
19	VERGARA-LAURENS; MENDEZ; LABRADOR	2014	9	- Aborda sobre detecção participativa, dados obtidos por meio de participação voluntária de usuários com dispositivos inteligentes; -Foi desenvolvido um mecanismo híbrido para proteção da privacidade que combina anonimização por meio de randomização de dados e técnicas de criptografia para aumentar a qualidade da informação, proteger a privacidade e manter o consumo de energia de aplicativos móveis; -A arquitetura do sistema é composta de: nós móveis, representado pelos dispositivos com poder de computação e capacidade de comunicação suficiente para executar a transmissão dos dados para o servidor de aplicativos; corretor de dados, responsável pelo envio da lista de ponto de interesse (*Points of Interest* – POI) para os nós móveis, recebendo os relatórios de dados sensíveis, validando assinatura de celulares, realizando agregação inicial de dados e encaminhando os dados anônimos para o servidor do aplicativo; servidor de aplicação, responsável por realizar o processo de inferência e fornecer a informação aos usuários finais; servidor de POI responsável por dividir a área alvo em células e atribuir localização aos pontos de interesse. - O mecanismo de privacidade é composto pela combinação de POI para ofuscar a localização real dos participantes, antes de informar o corretor de dados, o dispositivo altera a localização real pela localização do POI mais próximo. - Utiliza de técnicas de randomização e criptografia.
20	HUANG; KANHERE; HU	2012	9	- Foi desenvolvido um *proxy* para transferir valores entre comunicações anônimas, e um *schema* de anonimização para divulgação de informações, reduzindo a probabilidade dos usuários serem monitorados. - Neste trabalho as medidas de proteção da privacidade foram para dados de sensores de participação, nos quais os cidadãos comuns coletam dados de seu meio, usando dispositivo de mão e envia-os para um servidor de aplicativos, por meio de infraestrutura de comunicação; - Foi utilizado um servidor confiável para transferir dados de participação, realizando atribuição de reputação, que funciona como medida de confiança nos dados fornecidos, e o servidor também mantém uma lista da identidade real do usuário com seus pseudônimos. Desta forma, para cada contribuição anônima feita por um usuário, o servidor atualiza o valor da reputação. - A arquitetura do sistema é composta pelo usuário, terceiro confiável e servidor de aplicativos, utilizou-se arquitetura centralizada ao invés de abordagem distribuída. - Utiliza técnicas de randomização e pseudônimo e baseia-se no modelo k-anonimato

21	RUPPEL et al	2006	8	- Foi apresentada uma técnica de anonimato para *location-based community services* (LBCSs) que utiliza transformada de distância e pseudônimos para proteção da privacidade; - A técnica apoia o anonimato do usuário, tanto em relação ao provedor local, que coleta as alterações de posições, quanto ao provedor LBS. - Um provedor de localização intermediário é responsável pela coleta e armazenamento em cache das posições dos alvos, ofuscamento dos dados e transferências para o provedor LBS. - A abordagem suporta dois modelos diferentes de confiança, tanto o cenário P2P,quanto terceiro confiável. - utiliza o modelo k-anonimato, randomização e transformada da distância.
22	DIRIK; SENCAR; MEMON	2014	5	- É abordado anonimização para imagens e vídeos, devido o problema da atribuição do PRNU na fonte (*photo-response non-uniformity*), um padrão único que está presente em imagens ou frames capturado pelo sensor de imagem - No estudo, foi investigado o desempenho da anonimização baseado em *seam-carving* e ruído PRNU atribuído na fonte; - - Propõe dois ataques de de-anonimização. - utiliza de randomização para anonimizar dados
23	RUFFING; MORENO-SANCHEZ; KATE	2014	5	- Foi proposto um protocolo de mixagem descentralizado para o uso de *Bitcoin*, que permite que usuários façam uso do serviço de forma anônima; - Não requer nenhum terceiro confiável para realizar a anonimização. - O protocolo *CoinShuffle* é completamente descentralizado e permite eu usuários combinem suas moedas com as de outros usuários, o protocolo requer criptografia e faz uso de técnicas de *shuffle*.
24	ZUBERI	2012	5	-Realiza uma revisão de literatura sobre o modelo k-anonimato para LBS, indicando três perspectivas: k-anonimato baseado na arquitetura, com base nos algoritmos de anonimato, e nos tipos de k-anonimato.
25	LEI et al.	2012	5	- É realizada uma reflexão sobre LBS e o problema do monitoramento de padrões de movimento do usuário, denominada de movimento de trajetória; - Propõe uma abordagem para permitir que os usuários configurem seu perfil de privacidade por meio de falsos locais e desvio de distância, assim, os autores consideram os problemas de anonimização baseada no cliente. - A partir do perfil de privacidade do usuário, é gerada localizações falsas, utilizando *Random Pattern Scheme* (gera *dummies* aleatórios (valores falsos- com movimentos consistentes) e um *Intersection Pattern-based Scheme* (cria interseção entre as trajetórias). Assim, a cada trajetória de movimento frequente de um usuário é gerado um esquema de padrão aleatório e um padrão de interseção. Utiliza de randomização
26	SHIN; VAIDYA; ATLURI	2010	5	- Os autores ressaltam que além da localização do usuário, a direção do seu movimento deve ser considerada para garantir o anonimato. - Neste trabalho, os autores estendem a noção do k-anonimato para localização, incorporando a direção do movimento do usuário enquanto utiliza um LBS, especificamente generalizando a localização e a direção na medida especifica pelo usuário. - A arquitetura é proposta em três camadas: usuário (envia solicitação por meio de conexão segura) para um servidor de localização confiável (anonimizador de localização) que remove qualquer identificação e substitui a localização pela região anonimizada, e a consulta é enviada para o provedor LBS, que recebe o pedido e envia novamente para o servidor confiável, que envia o resultado para o usuário. - Os autores consideram os provedores LBS não confiáveis. O foco do trabalho não é privacidade na comunicação de redes, mas na privacidade de localização do provedor LBS. - aborda o modelo k-anonimato, e as técnicas de generalização e randomização.
27	PARESCHI et al	2008	5	- É proposto um mecanismo baseado no contexto do usuário e na agregação de dados para preservar a privacidade dos usuários, por meio de técnicas de anonimização e ofuscação.

				- As técnicas utilizadas baseiam-se na generalização dos dados de solicitação, como também nos dados de contexto fornecidos ao aplicativo. - Antes de chegar a um provedor de serviço, cada pedido é transformado em um pedido generalizado onde os dados que identificam um indivíduo foram transformados para garantir o anonimato; - Cada solicitação de usuário é filtrada pelo módulo *context-aware privacy module* (CPM), que transforma a identificação do usuário em um pseudônimo utilizado para identificar o pedido e executar a autenticação, e remove os semi-identificadores antes de encaminhar o pedido ao provedor LBS. - provedor LBS solicita dados de contexto, e encaminha para o gerenciador de perfil local (SPPM); - O CPM recupera as políticas de privacidade e os dados de contexto do usuário, e combina o contexto recebido com os possíveis dados que darão conflito, e generaliza e ofusca dados de contexto de acordo com a política de privacidade. - Então, ele envia o resultado da solicitação ao provedor de contexto, que obtém o agregado de dados e envia ao aplicativo lógico, que envia ao CPM, que encaminha ao usuário. - utiliza do modelo k-anonimato e as técnicas de generalização, supressão e pseudoanonimato
28	WANG e KOBSA	2015	4	- No artigo foi proposto uma um framework para proteção da privacidade de consultas contínuas em redes rodoviárias, o framework baseia-se nos conceitos de k-anonimato e l-diversity. - Autores ressaltam que a maioria das aplicações para proteger a privacidade em redes rodoviárias tem a desvantagem do custo de tempo; - Foi desenvolvida uma hierarquia Snet baseada na quantidade de usuários, traços históricos e topologias de redes rodoviárias para acelerar o processo de *cloaking* realizado no servidor de anonimização. - São projetados dois tipos de algoritmos de *cloaking*, para um único usuário e um para um lote de usuários. - A arquitetura é composta pelos seguintes elementos: usuários móveis; servidor de anonimização confiável e o provedor LBS. - baseado no modelo k-anonimato el-diversity, juntamente com a técnica *spatial cloaking*.
29	PALANISAMY et al.	2013	4	- Foi proposto uma estrutura, denominada de MobiMix, que utiliza Mix-zones para proteger a privacidade de localização de usuários que viajam em redes rodoviárias, de modo que nenhuma aplicação pode rastrear os movimento do usuário - O objetivo das mix-zones é quebrar a continuidade da exposição local do usuários, de modo a não permitir o movimento dos usuários. - é definido que o mix-zone de k participantes refere-se a uma área k-anônima, na qual os usuários podem alterar seus pseudônimos sem ser revelado, e esses usuário podem sair da área de modo a desvincular-se de seus eventos; - No MobiMix, as mix-zones são construídas levando em consideração a geometria das zonas, a estatística do comportamento do usuário, as restrições espaciais sobre os padrões de movimento dos usuários e dados temporais e espaciais. - Foi demonstrado no artigo como a anonimização por mix-zone rompe a continuidade da localização do usuário para proteger a privacidade. - modelo k-anonimato e mix-zone, utiliza de técnica de pseudônimo.
30	NERGIZ; CLIFTON	2011	4	- Foi desenvolvido um processo de consulta para conjunto de dados relacional que impede que o servidor aprenda algo sobre o cliente; - Utiliza técnica de anatomização, separando dados identificadores dos dados confidenciais; - O link entre dados identificadores e informações sensíveis são criptografados; - Apenas o cliente tem a possibilidade de descriptografar os dados; - O cliente primeiro anonimiza o banco de dados por meio de anatomização, e depois os links individualmente identificáveis são criptografados.

				- Os proprietários dos dados enviam o banco de dados modificado para um terceiro semi-confiável (servidor) para realizar a maior parte do processamento da consulta, e o servidor não modifica o banco de dados que o proprietário dos dados enviou no início do protocolo. - A abordagem foi minimizar a criptografia e garantir questões de privacidade. - aborda modelo *l-diversity* e de criptografia, anatomização e generalização.
31	BAHSI; LEVI	2010	4	- É proposto um método de anonimização por agrupamento K(k-ACM), que minimiza perda de dados, mantém o consumo de energia dentro do limite razoável e satisfaz as ameaças no requisito de privacidade. - O foco é a proteção da privacidade na coleta de dados de redes de sensores sem fio; - Considera dois níveis de privacidade, um nível básico, que é fornecido para os dados compartilhados com servidores semi-confiável e um nível mais complexo de privacidade que é fornecido contra espiões; - O framework é baseado no modelo k-anonimato, onde alguns dados são criptografados e o restante é generalizado. - Por meio da generalização é possível reduzir o tamanho dos dados transmitidos na rede, resultando na economia de energia ao custo da perda de informação e, por outro lado, a criptografia fornece anonimização sem perda de informação e sem economia de energia. - Utiliza o método de *clustering* para minimizar a perda de informação e aumentar a economia de energia; - Para os autores, os usuários podem não querer que um servidor central conheça informações espaço-temporal exata, assim a proteção da privacidade em relação ao servidor também é necessário, pois este pode não ser confiável ou pode haver outras partes não confiáveis, como as escutas. - O modelo tem dois critério de privacidade, o k1-anonimato, para os dados recebidos pelo servidor semi-confiável, e o k2-anonimato para os dados transmitidos na rede, e que podem ser capturados pelos não confiáveis.
32	KARAKUCUK; DIRIK,	2015	3	- Neste trabalho foi apresentado um método para otimização do PRNU contra identificação da câmera de origem com a finalidade de proteger a privacidade. - Os autores ressaltam que o objetivo principal da anonimização da fonte de imagem é proteger a identidade do fotógrafo contra qualquer tentativa de identificar o dispositivo de câmera de origem por meio da análise de ruído PRNU. - Considera-se que o padrão de ruído PRNU pode ser considerado como um identificador de sensor intrínseco. Uma maneira de impedir a atribuição da fonte da imagem é suprimir tanto quanto possível o ruído PRNU. - Por meio de análise experimental os autores demonstram que é possível impedir a identificação da câmera fonte pela supressão de ruído PRNU - É explanado sobre a identificação da câmera baseada em PRNU e a supressão de fingerprint - É proposto anonimização da fonte de imagem por meio de três métodos: remoção do *fingerprint; denoisign* (APD-1) que utiliza filtragem para remover o ruído PRNU; e o método proposto (APD-2), que emprega *wavelet domain filtering* para estimar o ruído do sensor durante a anonimização. - o método proposto produz imagens anonimizadas, com menos ruído e melhor qualidade na imagem.
33	VERGARA-LAURENS; LABRADOR	2011	3	- É apresentado um esquema para proteção da privacidade e economia de energia para aplicações LBS e *Participatory Sensing (PS) systems*, combinando técnicas de anonimização (ruído) e criptografia. - Esses sistemas dependem dos usuários para transmitir os dados para um site central, pois os usuários concordam em transmitir dados que serão utilizados para solucionar problemas coletivos, no entanto, essas atividades têm causado preocupações em relação à privacidade dos indivíduos. - Um exemplo deste tipo de sistema são os que envolvem a detecção e comunicação de medidas de qualidade do ar para avaliar a poluição de um determinado lugar, no entanto, a informação temporal e espacial dos usuários devem ser preservadas para que a participação do usuário tenha resultados satisfatórios;

				- Foi desenvolvido um algoritmo que divide o conjunto de dados em dois conjuntos, o primeiro conjunto utiliza método de criptografia dupla que não modifica a dimensão espacial ou temporal, com a finalidade de garantir a precisão das informações de localização. O segundo conjunto usa anonimização por meio de adição de ruído. - Ao combinar esses dois conjuntos o esquema consegue privacidade e precisão desejada dos dados de localização, enquanto é eficiente em termos de energia. - Arquitetura é composta com os seguintes elementos: nós móveis; servidor de aplicação (responsável pelo processamento do relatório de dados); corretor de dados (responsável pelo envio da lista de pontos de interesse para os nós móveis, validando a assinatura dos celulares e encaminhando dados criptografados ou locais anônimos para o aplicativo do servidor); Servidor gerador de pontos de interesse: responsável por dividir área alvo em células e atribuir locais de interesse. – aborda o modelo l-diversity e as técnicas de randomização, criptografia.
34	RASS et al	2008	3	- Aborda a coleta de dados de tráfego de veículos (*Floating Car Data* (FCD), por meio de dados de posição e velocidades que são enviados a um servidor central; - É apresentado um método para anonimizar dados de *Floating Car Data* (FCD) por meio de derivação de pseudônimos e ocultação da identidade do driver, protegendo a privacidade do usuário. - Aborda técnicas de criptografia, randomização e pseudônimo.
35	XUE et al.	2011	3	- Este Art. relata aspectos de proteção da privacidade na coleta de dados por um coletor de dados não confiável (por exemplo, um instituto de pesquisa médica) que deseja coletar dados de um grupo de entrevistados (pacientes). Cada respondente envia para o coletor um registro com informações sensíveis e não sensíveis (semi-identificadores). - Para os autores há proteção da privacidade quando o coletor obtém uma versão do conjunto de dados k-anônima ou l-diversificada sem revelar os registros originais do adversário. - É proposto um protocolo de coleta de dados distribuídos que gera um conjunto de dados anonimizados por generalização de atributos semi-identificadores, e emprega técnicas criptográficas homomórficas, recuperação privada de informações e computação multipartidária segura para garantir a proteção da privacidade no processo de coleta de dados. - Para os autores as técnicas tradicionais de anonimização não são aplicáveis no problema proposto, pois assumem que existe uma única parte confiável que tenha acesso a todos os registros da tabela, caso essa parte confiável seja comprometida, então a privacidade dos indivíduos referenciados nos conjuntos de dados também é comprometida. - Nesta pesquisa cada respondente possui seu próprio registro e não transmite suas informações para qualquer parte antes da anonimização. - O sistema emprega arquitetura cliente-servidor - O protocolo proposto alcança tanto o k-anonimato, quanto o l-diversity e considera que o coletor de dados não é confiável. - Realiza anonimização por meio de generalização e criptografia.
36	BUNNIG; CAP; CH	2009	3	- Os autores argumentam sobre a necessidade dos usuários de aplicações ubíquas consigam ter privacidade de forma dinâmica e intuitiva; - É apresentado um protótipo para avaliar o conceito de privacidade ad hoc, observando a interação do usuário com serviço de computação ubíqua. - É enfatizado as vantagens de controlar o fluxo de informação pessoais em ambientes inteligentes, pois libera o usuário para se atentar as preocupações de privacidade antes do uso real do sistema, podendo realizar configurações de privacidade de acordo com suas preferências, no entanto, essa abordagem pode causar sobrecarga da atenção do usuário; - O protótipo consiste em uma ou mais estações base e dispositivos de usuário, onde cada serviço fornece descrição da sua finalidade e quais dados requerem do usuário e, o usuário pode interpretar essas informações e responder aos pedidos de coleta de dados;

37	ALLARD; NGUYEN; PUCHERAL	2014	2	- É proposto um metaprotocolo genérico, distribuído e escalonável denominado MetAp. - Esse protocolo distribuído permite que o próprio participante anonimize seus dados de forma independente, pois o titular dos dados deve ter o controle durante a coleta, de acordo com a confiança no destinatário, de modo não dependa do servidor central para anonimizar os dados. - Ressalta que o servidor central pode ser um ponto vulnerável para ataques de privacidade. - Para anonimização utiliza randomização e criptografia, e os algoritmos para anonimização *Mondrian* baseado no k-anonimato (trabalha com os semi-identificadores), *Bucketization* no *l-diversity* (trabalha com os dados sensíveis) e o algoritmo *αβ-Algorithm* baseado no modelo (d, γ)-*Privacy* (relacionamento de igualdade entre os registros). - Ilustra os algoritmos também com os modelos t-cloness e privacidade diferencial - São verificadas as possíveis violações de privacidade pelo participante e descreve uma metodologia para implementar algoritmos de proteção de privacidade na divulgação usando os protocolos desenvolvidos - Verifica a latência durante a anonimização na fase de coleta, por meio do número de total de conexões, para isso utiliza-se distribuição gaussiana, e ressalta que a latência no lado do destinatário é insignificante. - aborda os modelos k-anonimato, l-*diversity*, privacidade diferencial e t-*closeness.*
38	PALANISAMY et al.	2014	2	- Este Art. apresenta um framework baseado em Mix-zone (*delay-tolerant mix-zone framework*) para proteger a privacidade de localização de usuários móveis contra ataques de correlação de consulta contínua e tolerante ao atraso. - Os usuários expõem locais perturbados localmente ou temporal - Um Mix-zone refere-se a uma região k-anônima em que os usuários podem alterar seus pseudônimos - São abordados os possíveis ataques quando um usuário realiza um consulta contínua, mesmo que tenha sido utilizado pseudônimo e os pontos fortes da anonimização de Mix-Zone, e posteriormente apresentam três tipos de Mix-zone para rede rodoviária (temporais, espaciais e espaço-temporal). - Ao utilizar *delay-tolerant mixzones* os locais dos usuários (são anonimizados por região mascarada em vez da localização exata) são enviados instantaneamente e o adversário não consegue saber o tempo exato da trajetória do usuário. - No *spatio-temporal* e *delay-tolerant* mix-zone, as localizações dos usuários são perturbadas usando tanto um atraso temporal quando uma região espacial em vez do ponto exato. - Aborda mix-zone por meio de k-anonimato, e as técnicas de randomização, pseudônimo e *spatial cloaking*.
39	GAO, SHENG et al.	2014	2	- O conhecimento da trajetória do usuário em LBS pode revelar informações confidenciais e levar a danos. - O principal desafio na anonimização de trajetória tem sido selecionar um conjunto de trajetória k-anônima. - Foi proposto um modelo de anonimização personalizado para selecionar trajetória k-anônima, a fim de garantir utilidade e privacidade nos dados de trajetória. - São explicitadas as propriedades básicas em relação ao espaço-temporal para dados de trajetória e seus problemas. - Os autores consideram que todas as trajetórias são de locais de origem precisos e verdadeiros. - O processo de anonimato da trajetória de localização é realizado por meio de sistema off-line, mas são anonimizadas antes de informar para a aplicação do detentor. - O processo de anonimização utiliza três modelos: a coleta da trajetória, a anonimização da trajetória e análise de dados e aplicação. O foco do artigo é no módulo de anonimato da trajetória para proteção da privacidade da trajetória e da utilidade dos dados. - Baseia-se no modelo k-anonimato, garantindo semelhança nas trajetórias selecionada. De acordo com as configurações do usuário, foi construído um modelo de anonimização personalizado a partir da teoria dos grafos para encontrar uma trajetória k-anônima. - baseado no modelo k-anonimato e nas técnicas de generalização e randomização.

40	WANG et al.[116]	2013	2	- Foi desenvolvido um framework (*software product line architecture* (PLA) que seleciona métodos de personalização durante o tempo de interação do usuário com sites Web, atendendo restrições de privacidade e permitindo que o usuário configure tanto as opções de privacidade quanto os métodos de personalização que podem operar nessas restrições de privacidade. - A arquitetura do framework é composta por um servidor de modelagem de usuário (*user modeling server)* LDAP-*basead*, que gerencia um componente de modelagem de usuário (*user modeling componente* (UMC)), um *scheduler* e um cache de banco de dados. - Foi desenvolvido um painel de controle *Privacy Control Panel* (PCP) que permite que os usuários indiquem suas restrições de privacidade. - No PCP é permitido que o usuário visualize as opções de privacidade e as consequências de personalização. - No PCP tem uma lista de preferências de privacidade que o usuário pode especificar, tais como: acompanhamento das interações do usuário no site; e opções de consentimento informado em relação ao site acompanhar a interação do usuário. Por padrão todas as opções de privacidade são desmarcadas. - Um PCP é mostrado em todas as páginas de um site, para que usuário possam alterar suas configurações de privacidade. - Os usuários que utilizam o PCP julgaram a ferramenta útil. - menciona técnica de randomização.
41	KIM; YONG-KI et al.	2013	2	- Foi proposto um algoritmo de cloaking H-Star para proteger a privacidade de usuários em rede rodoviária, de modo que mesmo que os adversários estejam fisicamente presente em uma rede, também foi proposto algoritmo de processamento de consulta de vizinhos mais próximos na região anonimizada. - foi definida uma rede rodoviária baseado em grafo consistindo em um conjunto de bordas, representando segmentos rodoviários. - utilizou-se da abordagem do k-anonimato de localização para garantir a privacidade dos usuários de LBS sob o modelo de rede, o que garante a indistinguibilidade de um usuário entre um conjunto de usuários. - Um cliente móvel envia um consulta com um perfil de privacidade (k-anonimato e tolerância espacial) para um servidor confiável que com base nos requisitos do usuário e posição, anonimiza as informações de localização antes de transmitir ao servidor LBS e posteriormente, envia a resposta ao cliente. - Foi observado que quando o k-anonimato é alto, é muito difícil cumprir os requisitos do usuário e criar uma área de anonimização. - menciona o modelo k-anonimato e a técnica de *spatial cloaking.*
42	HASHEMI; MALEK; MR	2012	2	Art. aborda questões de privacidade em serviços LBS e os autores propõem uma nova abordagem proteger a privacidade de dados de localização com base no seu contexto espaço-temporal e em um grupo de usuários, por meio de sistemas de inferência *fuzzy.* - A arquitetura é composta: pelo usuário que solicita um serviço remoto; servidor de localização confiável (que recebe a localização exata do usuário e entrega ao provedor depois de anoninimizar os dados); e pelo provedor do servidor. - No sistema *fuzzy*, a precisão espacial é atribuída ao usuário de acordo com seu contexto, grupo de usuários e tipo de serviço solicitado. O método proposto obscurece a localização do usuário como ele deseja.
43	WEI; CHEN; SHAN	2010	2	- Foi proposto o modelo R-anonimato centrado no RSSI (*Received Signal Strength Indicator*) do usuário para melhorar as questões relacionadas à privacidade de localização e a segurança no trânsito. - O modelo R-Anonimato utiliza de métrica de distância para proteger a privacidade de localização, a privacidade é preservada perturbando seletivamente os valores reais dos veículos, como posição, direção e velocidade.

[116] Desenvolve um framework para personalização de privacidade

				- Estes dados perturbados evita que o adversário tenha o rastreamento preciso de um veículo. - Para ter um parâmetro para garantir o anonimato foi utilizado o método RSSI (*received signal strength indication*), que fornece uma estimativa da distância entre veículos. O modelo é centrado no usuário, sem a necessidade de um terceiro confiável. - Para anonimização utiliza medidas de distância e randomização.
44	CUTILLO; MOLVA; STRUFE	2009	2	- Neste Art. os autores propuseram uma rede social on-line utilizando arquitetura *peer-to-peer*, evitando a necessidade de um controle centralizado (provedor de serviços). - A arquitetura P2P atende a preocupação básica em relação à privacidade, evitando o controle centralizado por provedores de aplicativos potencialmente mal intencionados. Cada participante está associado a um nó da rede, e cada nó, por sua vez é identificado de forma exclusiva por um pseudônimo e um identificador de nó. - A visão geral do sistema consiste em três componentes principais: Vários *matryoshka*s (consiste na visão de nós no sistema, nos quais os nós estão localizados em anéis concêntricos), uma rede *peer-to-peer* e um serviço de identificação confiável (concederá a cada usuário e seu nó um único pseudônimo, um identificador de nó exclusivo e dois certificados para autenticação do nó). - Para autenticação de usuários foi utilizado criptografia *end-to-end* e criptografia de chave pública e pseudônimos.
45	BLANCO-JUSTICIA; DOMINGO-FERRER	2015	1	- Aborda as questões de privacidade nos programas de fidelidade, devido dados resultantes de cadastros que podem ser utilizados pelos detentores para montar perfis de usuários. - No artigo é proposto um protocolo que permite o anonimato, de forma que nenhuma informação sobre o usuário é obtida pelo servidor durante o uso do protocolo. - O protocolo utiliza *token* anônimos, por meio de protocolo zero-conhecimento, e generalização de históricos de compras e perfis. - Os *tokens* enviados não podem ser vinculados à identidade de um solicitante, devido o uso de protocolo zero-conhecimento, quando um *token* é emitido, o valor de identificação é conhecido apenas pelo *token* que gerou a assinatura parcialmente cega. - A qualquer momento, um cliente pode enviar uma lista de recibos de compra ou versão generalizada deles para o fornecedor e obter pontos de fidelidade, para cada produto comprado no histórico de compras, o cliente envia o *token* de recebimento correspondente ao nível de generalização que ela deseja. - Quando os clientes usam pouco ou nenhuma generalização nos recibos de compra, renunciam parte de sua privacidade. - - Os clientes têm o poder de decidir quais informações privadas elas querem divulgar e quão precisa será essa informação. - O cliente deve utilizar medidas adicionais de anonimização, como navegação anônima, oferecido pelo TOR, métodos de envio anônimo e métodos de pagamentos anônimos. - O mecanismo proposto segue a abordagem descentralizada.
46	SONG; SIM; PARK; SONG	2015	1	- O Art. propõe um modelo de sistema *cloaking* chamado *anonymity of motion vectors* (AMV), na qual oferece anonimato para consultas espaciais. - O propósito do AMV é permitir consultas de usuários com base em dados de localização - O modelo AMV considera os movimentos do usuário para criar uma área k-anônima e suporta as consultas espaciais com localização *cloaked* (camadas). - O modelo tem três componentes: o servidor LBS centralizado, o anonimizador de localização e o usuário, sendo o anonimizador de localização um terceiro confiável que é colocado entre o cliente e o servidor LBS e utiliza o modelo k-anonimato para anonimização de dados. - Para obter o serviço de localização, o usuário envia sua consulta juntamente com sua localização para o anonimizador, que recebe periodicamente as atualizações de localização do usuário móvel e impede os locais exatos dos usuários em CR (*cloaked region*), enviando a consulta junto com o CR para o servidor LBS. - O anonimizador cria uma identificação de sessão válida durante todo o serviço para o LBS, que processa a consulta baseada em CR, e retorna uma lista de respostas para o anonimizador. - O anonimizador calcula a resposta exata da consulta da lista e envia para o usuário.

				- O usuário pode fornecer informações de movimento quando informa a localização e informações de parâmetro k-anônimo para o servidor LBS. - O AMV proposto gera um CR k-anônimo, prevendo a localização futura do cliente com base no vetor de movimento. - Para anonimização se baseia no modelo k-anonimato e na técnica de *spatial cloaking*.
47	PANDIT; POLINA; KUMAR	2014	1	- É proposto um framework chamado de CLOPRO (*A Context Cloaking Privacy Protecting Framework*) que garante a privacidade de usuário móvel que utiliza LBS, protegendo dados de identidade, localização e hora de solicitação. - Utiliza de criptografia para garantir que a identidade não seja revelada e converte um consulta original em uma consulta genérica, fornecendo proteção a privacidade em relação a consulta enviada pelo usuário. - A estrutura CLOPRO é composta pelo usuário móvel; servidor de anonimização de localização; servidor de anonimização de consulta e provedor de serviço de localização. - O sistema utiliza servidores de anonimato de terceiros confiáveis, é utilizada uma arquitetura distribuída com dois servidores confiáveis: um para alcançar privacidade de localização e o segundo para a privacidade de consulta. - O processo perturba automaticamente a hora real da solicitação de serviço. - Durante a geração da consulta para solicitar o serviço, o usuário insere a consulta, o nível desejado do K anonimato e o tempo de expiração da consulta. - O módulo de construção da consulta gera um par de referências de solicitação exclusiva para cada solicitação de serviço para identificar de forma exclusiva a solicitação, este componente está criptografado para obter maior privacidade. - O framework CLOPRO permite que usuários obtém serviços baseados em localização e ao mesmo tempo em que a privacidade do usuário está protegida e o link entre a identidade, o contexto e a consulta real do usuário nunca é exposto. - Baseia-se no modelo k-anonimato e nas técnicas de generalização e randomização.
48	PANDIT et al	2014	1	- Os autores abordam serviços de aplicativos que utilizam perfil de usuários para envio de anúncios que ameaçam a privacidade. - No trabalho, os autores estendem o framework CLOPRO que permite a privacidade de identidade, de localização e de consulta e, por meio *Context Aware Privacy Preserving Advertising* (CAPPA) torna-se possível a entrega de anúncios ou cupons com base nos interesses de usuários, especificados no momento de registro e no contexto atual do usuário, sem revelar detalhes ao provedor de serviços. - A extensão do k-anonimato para é que a consulta do usuário e a localização deve ser indistinguível de k-1 outros usuários. - Quando o LBS envia resultados para o anonimizador com base na consulta genérica, ele também envia anúncios de propaganda relevantes ao conteúdo e localização da consulta. - As solicitações de serviços originais são modificadas pela estrutura CLOPRO usando conceitos de cluster e generalização, e a criptografia impede que a identidade do sujeito seja revelada.
49	ZHANG; LAZOS	2014	1	- O Art. aborda o problema proteção da privacidade e o anonimato de localização do usuário ao acessar LBS - Os autores ressaltam as desvantagens do servidor anonimizador (terceiro confiável), no qual a privacidade pode ser ameaça, caso esse seja invadido. - Essas deficiências podem ser resolvidas por abordagens descentralizadas, que eliminam o terceiro confiável, anonimizando as consultas de modo distribuído por P2P, no entanto, existe o problema da colusão, pois a privacidade de localização não é preservada entre os membros do grupo P2P. - Foi desenvolvido uma nova forma de anonimização de consultas, chamado MAZE, que é resiste à colusão, e oferece a privacidade por meio de grupos P2P, sem a necessidade de um servidor anonimizador confiável; as consultas dos usuários são k-anônimas; o LBS pode autenticar os usuários que enviam as consultas. - A arquitetura MAZE é formada por três fases: formação do grupo de usuário (forma um grupo P2P que satisfaça o perfil de privacidade de cada usuário participante); anonimização da consulta (os membros do grupo anonimizam suas consultas, transformando-as, e é enviada coletivamente para o LBS) e fase do serviço da consulta (O LBS autentica cada membro do grupo,

				e prepara um conjunto de respostas criptografadas, sem poder associar a consulta ao usuário que realizou), cada membro do grupo descriptografa sua resposta individualmente. - O MAZE foi estendido para um protocolo multi-estágio chamado LMAZE, que é resiste à colusão de até (L-1) usuário com o LBS, esse protocolo utiliza criptografia e técnicas de permutação e/ou embaralhamento *(shuffling)* que impedem o rastreamento de mensagens. O usuário faz o papel do remetente que deseja anonimizar a consulta, e o receptor é o conjunto de usuários e o LBS. A desassociação do usuário da consulta evita o problema da colusão. - Para anonimização baseia-se no modelo k-anonimato e nas técnicas de criptografia, permutação e *shuffling*.
50	SHERKAT; LI; MAMOULIS	2013	1	- Aborda sobre o fluxo de dados coletados pelos provedores de internet, e que para evitar violação de privacidade por meio de ligação do *timestamp*, um provedor de internet pode anonimizar dados, substituindo o tempo por intervalos generalizados. - O objetivo do Art. é estudar a anonimização das sequências do evento de *timestamp* usando tempo e generalização de eventos. - ressalta as diferenças de anonimizar sequencias de *timestamp* com outros tipos de dados conforme pesquisado em outros trabalhos. Pois a sequencia de *timestamp* não apresenta um esquema de comprimento fixo e limite bem definido entre semi-identificadores e atributos sensíveis. - foi aplicada generalização para a dados de *timestamp* e generalização de eventos para URL usando taxonomia de eventos. - consideraram dois tipos de ataques: identificação de sequencia e previsão de eventos. Para o primeiro ataque foi utilizado o k-anonimato, de modo que nenhum adversário pode associar qualquer sequencia com menos de k-sequencia. Para quantificar o risco de ataque de previsão de eventos foi utilizado o modelo l-diversity - Foi apresentado resultados de uma avalição empírica dos algoritmos em dados reais e sintéticos. Foi comparado e eficiência, perda de informação, redução de calculo, e qualidade dados anônimos. - Para medir a utilidade dos dados anônimos, foram consideradas as consultas de predição de tempo, por exemplo, o Google quer saber a probabilidade de alguém visitar a Amazon após 5 minutos de visita no Google ou inversamente, a probabilidade de alguém visitar o Bing 5 minutos antes de visitar o Google. - Baseado no modelo k-anonimato e l-diversity, juntamente com as técnicas de supressão e generalização.
51	GUSTAV et al.	2013	1	- Neste Art., os autores apresentam um novo algoritmo de privacidade para consultas, denominado de *cloaking algorithm* (DSDCA) voltados a consultas contínuas de LBS, considerando usuários com direção similar, velocidade semelhante e viajando com o mesmo meio de transporte. - Os autores enfatizam o problema da consulta contínua em serviços LBS, que podem ameaçar a privacidade dos indivíduos. - A arquitetura é composta por três partes o cliente móvel, o servidor de anonimização e o servidor LBS, sendo que o servidor de anonimização possui seis partes: o mecanismo *cloaking;* o refinador de resultados; o repositório *Cloaked*; o armazenamento de perfil; o armazenamento de transporte e o registro de dados de localização. - Utiliza de técnicas de *spatial cloaking*, supressão e agregação e baseia-se no modelo k-anonimato.
52	JUTLA; ALI [117]	2013	1	- É demonstrado como a UML de um sistema pode ser ampliada para integrar os requisitos de privacidade, seja para Big Data ou outro contexto, ajudando engenheiros a inserir rapidamente requisitos de privacidade em seus modelos de análise. - Os autores ressaltam que importantes ferramentas como a UML será essencial para garantir sistemas seguros e privados em relação ao fluxo de informação, contribuindo com engenheiros de software, usuários do sistema e outras partes interessadas em torno das questões de privacidade - Abordam sobre a importância da minimização de dados, da generalização e supressão para casos de anonimização no contexto de big data. .- Foi desenvolvido por meio do Visual Visio um caso de uso, chamada Privacy by Design (PbD) para incorporar privacidade nas fases iniciais do desenvolvimento de software, também propõe adicionar anonimato e pseudoanonimização.

[117] Aborda questões de privacidade na fase de planejamento (análise de sistemas)

				- Foi proposto um container que irá hospedar os controles de privacidade necessários para um diagrama de caso de uso. Possui três controle de privacidade: primeiro especifica o requisito de mostrar o aviso de uso de dados pelo programa (aviso de privacidade); segundo especifica o requisito de pseudoanonimização de dados antes de serem utilizados pelo programa; terceiro controle especifica que anonimização precisa ser aplicada na saída de dados do programa. - É considerado no caso de uso condições de consentimento informado.
53	MANO; MINAMI; MARUYAMA	2013	1	- Neste Art., os autores apresentam um esquema de pseudônimo dinâmico para construção de conjuntos de dados de localização que esconde os caminhos de informações dos usuários, preservando a privacidade de sua localização. - É apresentado um algoritmo para determinar se cada usuário em um determinado conjunto de dados de localização tem um número suficiente de caminhos possíveis para disfarçar os verdadeiros movimentos do usuário. - O servidor de localização baseado em pseudônimos recebe de vários usuários seus dados de localização identificáveis, substitui suas identidades por pseudônimos, e fornecer aos LBS, como aplicativos de monitoramento de tráfego dados de localização pseudoanonimizados. - O algoritmo divide o caminho do usuário em múltiplos segmentos com diferentes pseudônimos, assim é possível alterar os pseudônimos dinamicamente para evitar ataques.
54	LOURO; GARCIA; ROMANO	2012	1	- Os autores evidenciam ameaças a privacidade em relação aos relatórios de erros de aplicativos enviados pelos usuários, cujo envio depende da disponibilização de informações detalhadas sobre o uso real da aplicação, e esse processo de coleta de dados suscita graves problemas de privacidade, pois é provável que os relatórios de erros incluam informações pessoais, - Os autores abordam a questão de como projetar mecanismo de ofuscação de dados visando anonimizar os relatórios de erros gerados por mecanismos com problemas, sem comprometer a reprodutibilidade dos erros. - Foi proposto uma solução denominada de *MultiPathPrivacy*, cuja finalidade é ampliar o grau de ofuscação. - A arquitetura do MultiPathPrivacy contém os seguintes elementos, o cliente e servidor, sendo o usuário e a equipe de manutenção. - Quando o cliente detecta uma falha em determinada linha de código envia ao servidor, o servidor tem a função de transferir as informações do cliente (relatório de erro final do cliente) para o lado da manutenção. - Os desenvolvedores de aplicativos serão capazes de ter acesso aos erros do usuário (um bug que ocorreu na aplicação), mas utilizando dados de entrada ofuscados. - Foram realizados testes de avalição em relação a perda de privacidade, sobrecarga de desempenho e escalabilidade. - Para anonimização faz uso de randomização.
55	GONG; FANG; GUO	2016	1	- Objetiva-se em promover a privacidade em algoritmos de aprendizagem de máquina, o foco é na regressão logística, muito utilizada para técnicas de aprendizado de máquina. - Foi proposto um esquema de aprendizagem colaborativo para proteção da privacidade utilizando regressão logística para mHealth.. - O esquema permite que usuários da *mHealth* controlem seus dados brutos e compartilhem apenas resultados intermediários durante o processo de treinamento. - Os usuários de *mHealth* podem manter seus dados privados localmente e apenas fazer upload de resultados intermediários (criptografados) para o servidor *mHealth* para o treinamento do modelo. - A arquitetura do sistema se concentra em sistemas *mHealth* centrados no pacientes, onde os paciente compartilham seus dados de detecção privados com um servidor *mHealth*, o paciente é monitorado continuamente por vários sensores, gerando um grande volume de dados, como taxas cardíacas, níveis de hidratação, níveis de glicose. Esses sensores são conectados a um dispositivo móvel, que coleta e armazena os dados detectados. - A tarefa do servidor *mHealth* é construir um modelo de regressão logística que permite construir um novo vetor de características, o modelo é construído de forma colaborativa, usando um conjunto de dados de múltiplos pacientes.

				- O servidor não aprende nada além do resultado agregado de cada interação. Os dados de cada paciente são mascarados antes de disponibilizá-los. - Para anonimização utiliza da criptografia e das técnicas de *spatial cloaking.*
56	PRIYA; MANI	2012	1	- Neste artigo é proposto um algoritmo de *Spatial Cloaking* para ambientes móveis P2P - Foi desenvolvido um esquema de compartilhamento de informações, que permite que usuários de dispositivos móveis compartilhem suas informações de localização em pares, de forma a reduzir a sobrecarga de comunicação; e um esquema de localização histórica que permite que usuários móveis utilizem informações de localizações em pares obsoletas para superar o problema da partição da rede. - A arquitetura do sistema proposto possui dois elementos: cliente móvel e o servidor baseado em localização, sendo que cada cliente móvel específica seu nível desejado de privacidade. - O principal objetivo do algoritmo é permitir que quando usuário deseja enviar uma consulta a um LBS, ele colabora com outros pares para borrar sua localização em uma área *cloaked*, garantindo o k-anonimato. - baseia-se no modelo k-anonimato e na técnica de *spatial cloaking*
57	CUTILLO; MOLVA; STRUFE	2009	1	- Neste Art. são abordada questões de privacidade em redes sociais - Os autores ressaltam que mesmo que se tenha um conjunto completo de medidas de segurança e privacidade, ainda os usuários de redes sociais estariam expostos a possíveis violações de privacidade pelo onisciente provedor de serviços das redes sociais. - Foi proposta uma arquitetura distribuída denominada *Safebook*. A arquitetura é composta de dos seguintes componentes: várias *matryoshkas*; arquitetura P2P; serviço de identificação confiável (fornece a cada nó um pseudônimo exclusivo), com a finalidade de proteger a privacidade de usuários em relação a intrusos, evitando a centralização por meio do controle dos prestadores de serviços. - para anonimização utiliza de pseudônimos.

Fonte: Elaborada pela autora

APÊNDICE B - Legislação Brasileira com abordagem a proteção de dados pessoais

Lei	Atores	Art.s	Processo	Conceitos
7.232 (BRASIL, 1984)	Titular dos dados	Art. 2º Inciso VIII	"Estabelecimento de mecanismos e instrumentos legais e técnicos para proteção dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas".	-
		Art.2º Inciso IX	"Estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas"	
8.078 (BRASIL, 1990)	Titular dos dados	Art.43º	"O consumidor, [...], terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".	-
		Art.43º § 1º	"Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão [...]"	
		Art. 43º § 2º	"A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele".	
		Art. 43º § 3º	"O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção [...]".	
		Art. 43º § 4	"Os bancos de dados e cadastros relativos consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público".	
9.507 (BRASIL, 1997)	Titular dos dados	Art. 7º Inciso I	Conceder-se-á *habeas data*: "para a assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público".	-
		Art. 7º Inciso II	Conceder-se-á *habeas data*:"para a retificação de dados [...]".	
9.472 (BRASIL, 1997)	Titular dos dados	Art. 3º Inciso V	O usuário de serviços de telecomunicações tem direito "à inviolabilidade e ao segredo de sua comunicação [...]".	-
		Art. 3º Inciso IX	O usuário de serviços de telecomunicações tem direito "ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço".	
		Art. 72º § 1º	"A divulgação das informações individuais dependerá da anuência expressa e específica do usuário".	
		Art. 72º § 2º	"A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade"	

12.414 (BRASIL, 2011)	Titular dos dados	Art. 3º § 3º	Em relação às informações de adimplemento do cadastrado, ficam proibidas as anotações de: "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".	"**informações sensíveis**, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" (Art.º 3 § 3º inciso II).
		Art. 4º	"A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado [...]".	
		Art. 5º Inciso I	São direitos do cadastrado "a obter cancelamento do cadastro"	
		Art. 5º Inciso II	Tem o direito de "acessar gratuitamente informações sobre ele existente no banco de dados, inclusive o seu histórico [...]".	
		Art. 5º Inciso III	Tem o direito de "solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados".	
		Art. 5º Inciso IV	Tem o direito de "conhecer os elementos e critérios considerados para análise de risco, resguardado o segredo empresarial".	
		Art. 5º Inciso V	Tem o direito de "ser informado previamente sobre o armazenamento, identidade do gestor, objetivo de tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento".	
		Art. 5º Inciso VI	Tem o direito de "solicitar ao consulente a revisão de cada decisão realizada exclusivamente por meio automatizados"	
		Art. 5º Inciso VII	Tem o direito de "ter seus dados pessoais utilizados somente de acordo com a finalidade para a qual foram coletados".	
		Art. 9º	"O compartilhamento de informação de adimplemento só é permitido se autorizado expressamente pelo cadastrado [...]."	
		Art. 15º	"As informações sobre o cadastrado constantes dos bancos de dados somente poderão ser acessadas por consulentes que com ele mantiverem ou pretenderem manter relação comercial ou creditícia".	
	Gestor	Art. 5º Inciso II	Cabe ao gestor "manter sistemas seguros, por telefone ou por meio eletrônico para informar as informações de adimplemento".	
		Art. 6º Inciso I	Deve fornecer ao cadastrado "todas as informações sobre ele constantes de seus arquivos, no momento da solicitação".	
		Art. 6º Inciso II	Deve fornecer ao cadastrado "indicação das fontes relativas às informações de que trata o inciso I, incluindo endereço e telefone para contato".	
		Art. 6º Inciso III	Deve indicar "gestores de banco de dados com os quais as informações foram compartilhadas".	

	Gestor	Art. 6º Inciso IV	Deve indicar "indicação de todos os consulentes que tiveram acesso a qualquer informação sobre ele nos 5 (seis) meses anteriores à solicitação".	
		Art. 6º Inciso V § 1º	É proibido aos gestores de banco de dados "estabelecerem políticas ou realizarem operações que impeçam, limitem ou dificultem o acesso do cadastrado preciso no inciso II do Art. 5º".	
		Art. 9º § 4º	"O gestor deverá assegurar, sob pena de responsabilidade, a identificação da pessoa que promover qualquer inscrição ou atualização de dados relacionados com o cadastrado, registrando a data desta ocorrência, bem como a identificação da fonte, do nome do agente [...]".	
	Fontes	Art. 8º Inciso I	São obrigações das fontes: "manter os registros adequados para demonstrar que a pessoa natural ou jurídica autorizou o envio e a anotação de informações em banco de dados";	
		Art. 8º Inciso II	"Comunicar os gestores de banco de dados acerca de eventual exclusão ou revogação de autorização do cadastrado".	
		Art. 8º Inciso III	"Verificar e confirmar, ou corrigir, [...], informação impugnada, sempre que solicitado por gestor de banco de dados ou diretamente pelo cadastrado".	
		Art. 8º Inciso IV	"Fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de banco de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros banco de dados."	
		Parágrafo Único	"É vedado às fontes estabelecerem políticas ou realizarem operações que impeçam, limitem ou dificultem a transmissão a banco de dados de informações de cadastrados que tenham autorizado a anotação de seus dados em banco de dados"	
12.527 (BRASIL, 2011)	Titular dos dados	Art. 31º	"O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem [...]".	"**Informação pessoal:** aquela relacionada à pessoa natural identificada ou identificável." (Art. 4º IV). "**Tratamento da Informação:** conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, eliminação, avaliação, destinação ou controle da informação"(Art. 4º V).
		Art. 31º Inciso II	As informações pessoais "poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem"	
	Órgão Público	Art. 6º Inciso III	Cabe aos órgãos e entidades do poder público "proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso".	
		Art. 34º	"Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais [...]".	

Lei nº 12.737 (2012) [118]	Titular dos dados	Art. 2º	O titular dos dados é amparado se um terceiro "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita":	-
Lei 12.965 (BRASIL, 2014)	Titular dos dados	Art. 7º Inciso I	O usuário tem direito a: "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação".	-
		Art. 7º Inciso II	O usuário tem direito a: "Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei".	
		Art. 7º Inciso III	O usuário tem direito a: "inviolabilidade e sigilo de suas comunicações pela internet, salvo por ordem judicial".	
		Art. 7º Inciso VI	O usuário tem direito a: "informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade".	
		Art. 7º Inciso VII	O usuário tem direito a: "não fornecimento a terceiros de seus dados pessoais, registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre [...]".	
		Art. 7º Inciso VIII	Direito a "informações claras sobre a coleta, uso, armazenamento e tratamento e proteção de seus dados pessoais [...]".	
		Art. 7º Inciso IX	"Consentimento expresso sobre a coleta, uso, armazenamento e tratamento de dados pessoais [...]".	
		Art. 7º Inciso X	Direito "a exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet [...], ressalvadas as hipóteses de guarda obrigatória de registros previstos nesta lei".	
		Art. 8º	"A garantia do direito à privacidade e à liberdade de expressão nas comunicações [...]".	
	Provedor	Art. 10º	"A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas."	
		Art. 10º § 1º	"O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou terminal, mediante ordem judicial [...]".	-
		Art. 10º § 2º	"O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial [...]".	
		Art. 10º § 4º	"As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais".	
		Art. 11º	"Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a	

[118] Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências, acrescentando os 154-A e 154-B no Capítulo VI. (BRASIL, 2012)

			legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros".	
		Art. 11º § 3º	"Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações".	
		Art. 14º	"Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet".	
	Administrador de sistema autônomo	Art. 13º	"Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento".	
		Art. 13º § 1º	A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros	
	Provedor de aplicações de internet	Art. 15º	"[...] deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança [...]".	
		Art. 16º Inciso I	É vedada a guarda: "dos registros de acesso a outras aplicações de internet em que o titular dos dados tenha consentido previamente ..]".	
		Art. 16º Inciso II	"é vedada a guarda "de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dados consentimento pelo seu titular".	
	Juiz	Art. 23º	"Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário".	

Fonte: Elaborado pela autora

APÊNDICE C - Regulamentos e conceitos do PL 12.965

Atores	Legislação	Processo	Conceitos
Titular dos dados	Art. 6º Inciso I	"Tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informar ao **titular** [...]".	**Dado Pessoal:** "dado relacionado à pessoal natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa" (Art. 5º, inciso I). **Tratamento:** "Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (Art. 5º, inciso II). **Dados Sensíveis:** "dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos" (Art. 5, inciso III). **Dados anonimizados:** "Dados relativos a um titular que não possa ser identificado". (Art. 5, inciso IV) **Titular:** "A pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". (Art. 5, inciso VI). **Consentimento:** "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". (Art. 5, inciso VII). **Responsável**: "A pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais". (Art. 5, inciso VIII). **Operador:** "A pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável". (Art. 5, IX).
	Art. 6º Inciso II	"[...] tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do **titular** [...]".	
	Art. 6º Inciso IV	Garante "aos **titulares** consultada facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados"	
	Art. 6º Inciso V	"[...] devem ser garantidas aos **titulares** a exatidão, a clareza, relevância e a atualização dos dados [...]."	
	Art. 6º Inciso VI	"[...] devem ser garantidas aos **titulares** informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento".	
	Art. 7º Inciso I	O tratamento de dados pessoais somente poderá ser realizado "mediante o fornecimento pelo **titular** de consentimento livre, informado e inequívoco".	
	Art. 7º Inciso V	O tratamento de dados pessoais somente poderá ser realizado "quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o **titular** [...]".	
	Art. 7º Inciso VII	O tratamento de dados pessoais somente poderá ser realizado "para a proteção da vida ou da incolumidade física do **titular** [...]".	
	Art. 7º Inciso IX	O tratamento de dados pessoais somente poderá ser realizado "para atender aos interesses legítimos do responsável [...], exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do **titular** que exijam a proteção dos dados pessoais [...]".	
	Art. 8º	"Deverá ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizada de forma clara, adequada e ostensiva [...]".	
	Art. 8º Inciso VII	Direito do **titular** "(a) acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; (b) denunciar ao órgão competente o descumprimento de disposição desta lei; (c) não fornecer o consentimento [...]"	
	Art. 8º § 3º	"Nas atividades que importem em coleta continuada de dados pessoais, o **titular** deverá ser informado periodicamente sobre as principais características do tratamento [...]".	
	Art. 8º § 4º	"Quando o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o **titular** será informado com destaque sobre tal fato e sobre meios pelos quais poderá exercer controle sobre o tratamento de seus dados".	
	Art. 11º Inciso I	"O tratamento de dados sensíveis somente poderá ser realizado: com fornecimento de consentimento inequívoco, expresso e específico pelo **titular**".	
	Art. 15º Inciso III	O término do tratamento de dados pessoais ocorrerá mediante: "comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento [...]".	
	Art. 17º	O titular tem direito "a titularidade dos dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade [...]".	
	Art. 18º Inciso I	Titular dos dados pessoais tem direito "a confirmação da existência de tratamento"	
	Art. 18º Inciso II	Titular dos dados pessoais tem direito "acesso aos dados".	
	Art. 18º Inciso III	Titular dos dados pessoais tem direito "a correção de dados incompletos, inexatos ou desatualizados".	

	Art. 18º Inciso IV	Titular dos dados pessoais tem direito "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei".	**Encarregado**: "pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente". (Art. 5, X). **Anonimização**: "qualquer procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". (Art. 5, XII) **Bloqueio:** "guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento". (Art. 5, XIII). **Eliminação:** "exclusão definitiva de dado ou de conjunto de dados armazenados em banco de dados, independentes do procedimento empregado". (Art. XIV). **Uso compartilhado de dados**: "a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou o tratamento compartilhado de banco de dados pessoais por órgão e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamentos delegados por esses entes públicos" (Art. 5, XV).
	Art. 18º Inciso V	Titular dos dados pessoais tem direito "a portabilidade, mediante requisição, de seus dados pessoais a outro fornecedor de serviço ou produto".	
	Art. 18º Inciso VI	Titular dos dados pessoais tem direito: "eliminação de seus dados pessoais, cujo tratamento tenha consentido".	
	Art. 18º Inciso VII	Titular dos dados pessoais tem direito: "aplicação das normas de defesa do consumidor, quando for o caso, na tutela da proteção de dados pessoais".	
	Art. 18º § 1º	"o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento [...]".	
	Art. 19º	"Quando o tratamento tiver origem no consentimento do titular [...] poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente [...]."	
	Art. 20º	"Titular dos dados pessoais tem direito a solicitar revisão de decisões tomada unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses [...]".	
	Art. 33º Inciso VII	Em relação à transferência de dados internacional será permitida "quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação [...]".	
	Art. 40º	"A comunicação de dados pessoais entre responsáveis ou operadores de direito privado dependerá do consentimento do titular [...]"	
Responsável	Art. 7º § 1	"Deverá informar ao titular as hipóteses em que será admitido o tratamento de seus dados"	
	Art. 8º § 2	"O responsável deverá comunicar ao titular as informações de contato atualizadas"	
	Art. 9º § 2º	"Cabe ao responsável o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei."	
	Art. 10º § 2	"O **responsável** deverá adotar medidas para garantir transparência do tratamento de dados [..]	
	Art. 10º § 3	"Quando o tratamento for baseado no legítimo interesse do **responsável,** somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados [...]"	
	Art. 41º	"O responsável deverá indicar um encarregado pelo tratamento de dados pessoais"	
	Art. 37º	"O responsável e o operador devem manter registros das operações de tratamento de dados pessoais que realizarem"	
	Art. 47º	"O responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares".	
	Art. 50º	"Os responsáveis pelo tratamento de dados pessoais [...], poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações educativas [...]".	

	Art. 50º § 1º	"O responsável e o operador levarão em consideração a natureza, escopo e finalidade do tratamento e dos dados, bem como a probabilidade e gravidade dos riscos de danos aos indivíduos"	
Encarregado	Art. 41º § 2º Inciso I	"Receber reclamações e comunicações dos titulares prestará esclarecimentos e adotar providências"	
	Art. 41º § 2 Inciso II	"Receber comunicações do órgão competente e adotar providências"	
	Art. 41º § 2 Inciso III	"Orientar os funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais"	
Operador	Art. 45º	"O operador deve adotara medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".	
Administração Pública	Art. 7º Inciso III	O tratamento de dados somente poderá ser realizado "pela **administração pública**, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas [...]".	
Poder Público	Art. 23º	"O tratamento de dados pessoais pelas pessoas jurídicas de direito público [...] deverá ser realizado para atendimento de sua finalidade pública [...]."	
	Art. 24º	"Os órgão do poder público darão publicidade às suas atividades de tratamento de dados pessoais por meio de informações claras, precisas e atualizadas em veículos de fácil acesso [...]".	
Poder Público	Art. 24º § 1º	"Os órgãos do Poder Público que realizem operações de tratamento de dados pessoais deverão indicar um encarregado [...]."	
	Art. 26º	"O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando os princípios da proteção de dados pessoais elencados no Art. 6º desta Lei".	
	Art. 26º Parágrafo único	"É vedado ao Poder público transferir a entidades privadas dados pessoais constantes de base de dados a que tenha acesso [...]".	
	Art. 9º § 7º	"O órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos."	
	Art. 10º § 4º	"O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo."	
	Art. 12º	"O órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento, ou solicitar a apresentação de impacto à privacidade".	
	Art. 13º § 2	"O **órgão competente** poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de segurança".	
	Art. 13º § 3º	"O compartilhamento e o uso que se faz de dados anonimizados deve ser objeto de publicidade e de transparência, sem prejuízo do órgão competente poder solicitar ao responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento".	
	Art. 15º Inciso IV	O término do tratamento de dados pessoais ocorrerá pela "determinação do órgão competente, quando houver violação da legislação em vigor a respeito".	

Órgão competente	Art. 15º Parágrafo único	"O órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica."	
	Art.19º § 4º	"O órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular"	
	Art. 24º	"Deverá informar as hipóteses em que, realizam o tratamento de dados pessoais, disponibilizando informações claras e atualizadas sobre essas atividades em veículos de fácil acesso."	
	Art. 29º	"O órgão competente poderá solicitar, a qualquer momento, às entidades do Poder Público que realizam operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado [...]".	
	Art. 30º	"O órgão competente poderá estabelecer normas complementares para as atividades de comunicação de dados pessoais"	
	Art. 32º	"O órgão competente poderá solicitar a agentes do poder público que publiquem relatórios de impacto de privacidade e sugerir adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público"	
	Art. 33º Inciso IV	Em relação à transferência internacional de dados, será permitida "quando o órgão competente autorizar a transferência".	
	Art. 33º Parágrafo único	Em relação a transferência internacional de dados "o nível de proteção de dados do país será avaliado pelo órgão competente [...]".	
	Art. 34º § 1º	"O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados [...]".	
	Art. 37º Parágrafo Único	"O órgão competente poderá dispor sobre o formato, estrutura e tempo de guarda do registro".	
	Art. 39º	"O órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados [...]".	
	Art. 41º § 3º	"O órgão competente poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado".	
	Ar. 48º	Em relação a incidentes com dados pessoais "o órgão competente verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao responsável à adoção de outras providências [...]".	
	Art. 45º § 1	"O órgão competente poderá dispor sobre padrões técnicos e organizacionais [..], levando em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis"	
	Art. 50º § 2	"As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente".	
	Art. 51º	"O órgão competente estimulará a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais".	
	Art. 53º	"O órgão competente designado para zelar pela implementação e fiscalização da lei terá as seguintes atribuições".	
	Art. 53º Inciso I	"Zelar pela proteção dos dados pessoais [...]	
	Art. 53º Inciso II	"Elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade"	
	Art. 53º Inciso IV	"Promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade"	

Órgão competente	Art. 53º Inciso V	"Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais"	
	Art. 53º Inciso VI	"Promover ações de cooperação com autoridade e proteção de dados pessoais de outros países [...]".	
	Art. 53º Inciso VII	"Elaborar relatório anuais acerca de suas atividades".	
	Art. 53º Inciso VIII	"Editar normas sobre proteção de dados pessoais e privacidade"	
	Art. 53º Inciso IX	"Realizar demais ações dentro de sua esfera de competência [...]".	
	Art. 56º Parágrafo único	"O órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta lei, considerada a complexidade das operações de tratamento e a natureza dos dados"	
Juiz	Art. 42º §Parágrafo único	"O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa"	
Conselho Nacional de Proteção de Dados Pessoais	Art. 55º Inciso I	"Fornecer subsídios para elaboração da Política Nacional de Proteção de Dados e da Privacidade"	
	Art. 55º Inciso II	"Elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade"	
	Art. 55º Inciso III	"Sugerir ações a serem realizadas pelo órgão competente"	
	Art. 55º Inciso IV	"Realizar estudos e debates sobre a proteção de dados pessoais e da privacidade"	
	Art. 55º Inciso V	"Disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral"	

Fonte: Elaborado pela autora[119]

[119] Com base na coleta de dados realizada no documento do Projeto de Lei nº 5.276, de 2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

APÊNDICE D – Casos julgados sobre proteção de dados pessoais nos tribunais brasileiros

Tema	Data do julgamento	Art. do Marco Civil	Ementa	Temas envolvidos
Escaneamento de e-mails e consentimento prévio	29/01/2018	Art. 7º, IX	"Trata-se de Ação Civil Pública ajuizada pelo Ministério Público Federal, na qual se pretende provimento judicial no sentido de que seja suspensa, por parte da ré, a análise (escaneamento) do conteúdo dos e-mails dos usuários do Gmail, em todo o território nacional, enquanto não for colhido o consentimento prévio, expresso, e destacado do titular da conta de e-mail, inclusive para o envio de publicidade comportamental. Inicial instruída com vasta documentação. Contestação anexada às fls. 230/273 Decisão de fls. 350/353 indeferindo o pedido liminar. Réplica oferecida pelo órgão ministerial às fls. 370/392. Notícia de Agravo interposto em razão da referida decisão, conforme cópia do referido instrumento às fls. 416/493. Após a realização de audiência, houve a suspensão do feito para eventual tentativa de acordo, sendo a mesma frustrada conforme noticiam as partes (...)".	Privacidade, Provedores de aplicações, Dados pessoais, Intimidade, Direito do consumidor, Segurança da informação, Interesse público, Algoritmos.
Coleta de dados pessoais sem autorização	27/04/2018	Art. 7º, VI, VII, VIII, IX, e X, e artigo 8º, "caput"	"(...) Vislumbra-se em parte, todavia, a plausibilidade parcial do direito invocado, no tocante a determinar-se que a Microsoft adote procedimentos específicos, no prazo de 30 (trinta) dias, de modo a permitir que o usuário do sistema operacional Windows 10, em caso de não autorizar o uso de seus dados, tenha ferramenta operacional que permita o exercício de tal opção de forma tão simples e fácil quanto a que permite a atualização com a autorização dos dados.[...]	Privacidade, Dados pessoais, Intimidade, Danos morais, direito do consumidor, segurança da informação e interesse público.
Perfil falso em aplicativo de transporte	12/03/2018	Art. 10º, § 1º Art. 19	"Trata-se de ação movida por (...) em face de UBER DO BRASIL TECNOLOGIA LTDA. Alegou o autor que buscou cadastrar-se como motorista no aplicativo da requerida em novembro de 2016, porém não logrou êxito pois outro indivíduo já havia efetuado cadastro utilizando seus dados pessoais. Alegou que, diante deste fato, contatou a requerida para que fornecessem informações acerca do perfil falso, o que foi negado pelas rés. Requereu o julgamento da ação como procedente para que a requerida sejam compelida a fornecer o número de IP, datas e horários, porta lógica de origem dos acessos, chave de identificação e senha atribuídos ao motorista cadastrado com seu nome, além de informações sobre repasses decorrentes de viagens realizadas. (...)"	Provedores de aplicações, Registros de conexão, Dados pessoais, Registros de acesso a aplicações, Dados cadastrais, Porta lógica de origem.
Serviços de transporte e proteção de dados	15/03/2018	Art. 5º, VIII Art. 15 e § 3º	"99 TECNOLOGIA LTDA. pede tutela de urgência, de natureza antecipada, para que o DISTRITO FEDERAL: a) se abstenha de exigir da 99 o cumprimento das obrigações de coletar, fornecer ou permitir o acesso da SEMOB/DF ou de qualquer outro órgão ou agente do DF a dados pessoais dos motoristas parceiros, usuários do aplicativo da 99, mapas de calor das viagens realizadas pelos seus usuários, informações sobre quantidade de viagens, distância percorrida entre pares de origem e destino (Matriz Origem-Destino) e veículos cadastrados; e b) se abstenha de aplicar à 99 e aos motoristas parceiros quaisquer sanções ou empecilhos ao regular desenvolvimento das suas atividades, pelo não cumprimento das obrigações acima referidas e também em decorrência da não obtenção do Certificado Anual de Autorização (CAA). (...)"	Privacidade, Provedores de aplicações, Dados pessoais, Registros de acesso a aplicações, Intimidade.
Quebra de sigilo e cooperação internacional	12/12/2017	Art. 7º Art. 8º	"Recurso ordinário em mandado de segurança. Inquérito policial. Quebra de sigilo telemático. Descumprimento de ordem judicial. Alegações de ausência de indícios de autoria delitiva e de	Provedores de aplicações, Dados pessoais, Registros de acesso a

		Art. 10º, §§ 1º e 2º Artº. 11 §§ 1º, 2º e 3º Artº. 12	violação a direito de terceiro. Não cabimento. Aplicação de multa diária. Empresa situada no país. Submissão à legislação nacional. Marco civil da internet . Incidência 1. Consta dos autos ter sido instaurado o Inquérito Policial nº 58728-34.2012.4.01.3400 com o objetivo de investigar a prática dos crimes tipificados no Art. 10 da Lei nº 9.296/1996 (Lei de interceptação) e Art. 153, § 1º-A, do Código Penal – CP. Situação em A YAHOO! DO BRASIL INTERNET LTDA alega que o acórdão impugnado efetuou interpretação equivocada do Art. 10, § 1º, do Marco Civil da Internet e que ela tem o direito líquido e certo de não ser obrigada a fornecer dados pelos quais não é responsável pela guarda. 2. É incabível, em sede de mandado de segurança – que na sua essência visa preservar direito líquido e certo – discutir indícios de autoria delitiva, matéria afeta ao Juízo criminal, que, ademais, demanda a análise dos elementos de prova colhidos na investigação. Precedentes. Para a impetração do mandamus é imprescindível que a prova do direito seja pré-constituída, sendo inviável imiscuir-se em matéria fática, mormente no caso concreto, em que a investigação não recai sobre a impetrante, mas sobre terceiros. A propósito, esta Corte Superior já se manifestou no sentido de que a destinatária da interceptação de dados não pode invocar direitos fundamentais de terceiros para eximir-se se cumprir a decisão judicial. Precedente. 3. Conforme jurisprudência do Superior Tribunal de Justiça "por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo" (RMS 55.109/PR, Rel. Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 07/11/2017, DJe 17/11/2017) 4. Observe-se, ainda, que não há qualquer ilegalidade no fato de o delito investigado ser anterior à vigência do Marco Civil da Internet. Isto porque a Lei n.º 12.965/2014 diz respeito tão somente à imposição de astreintes aos descumpridores de decisão judicial, sendo inequívoco nos autos que a decisão judicial que determinou a quebra de sigilo telemático permanece hígida. Com efeito, a data dos fatos delituosos é relevante para se aferir apenas a incidência da norma penal incriminadora, haja vista o princípio da anterioridade penal, sendo certo que o inquérito policial investiga condutas que se encontram tipificadas no Art. 10 da Lei nº 9.296/1996 (Lei de interceptação) e Art. 153, § 1º-A, do Código Penal – CP e não na Lei n. 12.965/2014. 5. Recurso ordinário em mandado de segurança ao qual se nega provimento."	aplicações, Multa diária, Direito penal, Quebra de sigilo.
Inexistência de ilícito e liberdade de expressão	21/12/2017	Art. 10º "caput" e § 1º Art 19, § 1º Art. 22, I	"ORDEM DOS ADVOGADOS DO BRASIL - SEÇÃO DE SÃO PAULO ajuizou ação de obrigação de fazer com pedido de tutela de urgência em face de FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA Aduz que tomou ciência da existência da página no Facebook intitulada "Advogado: sinônimo de roubo e falcatrua", por meio da qual a honra e imagem da classe dos advogados está sendo violada, uma vez que ridiculariza, julga, denigre, ofende e generaliza todos os advogados. Pede que o réu seja condenado a fornecer todos os dados necessários à identificação do titular da referida página e a excluir o seu conteúdo, objetivando impedir novos acessos, publicações e/ou compartilhamentos. A antecipação dos efeitos da tutela foi deferida em parte para determinar que o réu fornecesse toda e qualquer informação que permita a identificação do titular da página indicada na inicial, incluindo os dados pessoais ou cadastrais, se houver, mas principalmente os registros de acesso e conexão (IPs), objetivando a completa identificação dos(a) responsáveis(a) pela publicação, restando indeferido o pedido de exclusão da página. Citado, o réu aduziu, em preliminar, ilegitimidade de parte; no mérito, que somente por meio de ordem judicial pode fornecer dados e retirar conteúdo	Liberdade de expressão, Provedores de aplicações, Dados pessoais, Dados cadastrais, Identificação clara e inequívoca, Redes sociais, Remoção de conteúdos, Intimidade, Direito de imagem, Interesse público, Liberdade de manifestação do pensamento.

			de páginas. Pede a extinção do processo sem exame do mérito e, subsidiariamente, que a demanda seja julgada improcedente, nos termos do Art. 487, I, do CPC, e que não seja condenada nos ônus da sucumbência, por se tratar de procedimento necessário no caso em questão. (...)"	
Provedores de aplicação e porta lógica	12/12/2017	Art. 5º, VII Art. 7°, III Art. 10º, § 1° Art. 15º Art. 22º	"CIVIL E PROCESSUAL CIVIL. AGRAVO DE INSTRUMENTO. REDE SOCIAL. TUTELA DE URGÊNCIA. FORNECIMENTO DOS DADOS DA PORTA LÓGICA DE ORIGEM. - Os dados referentes à porta lógica de origem consistem em informação relacionada a registro de conexão, por complementar o endereço IP, de modo que seu armazenamento não é competência dos chamados provedores de serviços de aplicação, como a rede social agravante, que disponibiliza um conjunto de funcionalidades, que podem ser acessadas por meio de um terminal conectado à internet (Art. 5º, VII, Lei n. 12.965/2014). - Os dados cujo fornecimento pretende a Agravada são fornecidos por provedores de conexão ou de acesso, que fornecem os serviços que possibilitam o acesso à Internet por intermédio de seus terminais - Recurso conhecido e provido, em harmonia com o parecer ministerial."	Provedores de aplicações, Dados pessoais, Registros de acesso a aplicações, Dados cadastrais, Redes sociais, Multa diária, Porta lógica de origem.
Pessoa pública e mero aborrecimento	29/06/2017		"DANILO GENTILI JUNIOR moveu a presente ação de requisição judicial de registros c/c pedido de exclusão de conteúdo publicado na rede social em face de FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. alegando, em síntese, que em uma publicação do canal Comedy Central Brasil em seu perfil da rede social ré recebeu vários comentários lesivos a sua honra, nome e imagem. Requer, assim, a condenação a ré a fornecer os endereços de IP descritos na inicial, bem como os dados cadastrais e dados pessoais e a determinação para que os 16 comentários transcritos na inicial sejam indisponibilizados. (...)"	Liberdade de expressão, Provedores de aplicações, Dados pessoais, Registros de acesso a aplicações, Dados cadastrais, Identificação clara e inequívoca, Redes sociais, Segredo de justiça, Anonimato, Remoção de conteúdos, Direito de imagem, Liberdade de manifestação do pensamento, Pessoas públicas.
Ataque DDoS e identificação de autoria	25/12/2017	Art. 15º	"AGRAVO DE INSTRUMENTO - Ação cominatória - Decisão que determina que a agravante forneça os dados de cadastro de usuário e registros eletrônicos disponíveis de usuários responsáveis pelos IP's apontados em tabela anexa à inicial - Inadmissibilidade - Prazo legal para armazenamento dos dados já decorrido quando da intimação do recorrente (Art. 15 do Marco Civil da Internet Lei nº 12.965/14 - Ademais, autor poderá obter referidos dados dos outros requeridos - Decisão reformada - Recurso provido."	Provedores de conexão, Provedores de aplicações, Registros de conexão, Dados pessoais, Registros de acesso a aplicações, Dados cadastrais, Redes sociais, Segredo de justiça, Multa diária, Interesse público, *Hackers.*
Direito a exclusão de dados pessoais	15/12/2017	Art. 3º II e III Art. 5º X Art. 7º X Art. 10º	"Relação entre usuário e aplicação na internet - PAGSEGURO. Lei 12.965/14 – Marco Civil da Internet. Direito à exclusão dos dados pessoais mantidos pela aplicação da internet – Art. 7º, X. Direito à privacidade. Dever de exclusão após o término da relação entre as partes. Sentença parcialmente mantida. Recurso Parcialmente Provido."	Privacidade, provedores de aplicações, dados pessoais, intimidade, direito do consumidor.
Violação da intimidade e prova ilícita	05/12/2017	Art. 7º II e III	"Penal e processo penal. Recurso em habeas corpus . Furto e quadrilha. Aparelho telefônico apreendido. Vistoria realizada pela polícia militar sem autorização judicial ou do próprio investigado.	Privacidade, provadores de aplicações, dados pessoais, redes

			Verificação de mensagens arquivadas. Violação da intimidade. Prova ilícita. Art. 157 do CPP. Recurso em habeas corpus provido. 1. Embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação telefônica, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no Art. 5º, inciso XII, da CF, houve sim violação dos dados armazenados no celular do recorrente (mensagens de texto arquivadas - WhatsApp). 2. No caso, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista a garantia, igualmente constitucional, à inviolabilidade da intimidade e da vida privada, prevista no Art. 5º, inciso X, da CF. Dessa forma, a análise dos dados telefônicos constante dos aparelhos dos investigados, sem sua prévia autorização ou de prévia autorização judicial devidamente motivada, revela a ilicitude da prova, nos termos do Art. 157 do CPP. Precedentes do STJ 3. Recurso em habeas corpus provido, para reconhecer a ilicitude da colheita de dados do aparelho telefônico dos investigados, sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos."	sociais, intimidade, direito penal, quebra de sigilo.
Baleia Azul e investigação criminal	03/10/2017	Art. 12º	"Mandado de segurança. Facebook. “desafio da baleia azul”. fornecimento de conteúdo de comunicações privadas e reativação de perfil fictício para investigação criminal. multa diária e suspensão das atividades. descabimento. 1) A questão principal dos autos gira em torno do fornecimento do conteúdo das comunicações privadas de usuários do Facebook suspeitos de integrarem organização criminosa voltada para a prática do denominado “Jogo da Baleia Azul” ou “Desafio da Baleia Azul”. Trata-se de suposto jogo que coopta adolescentes em redes sociais na internet, propondo-lhes uma sequência de desafios a cada etapa mais difíceis e cuja superação traz risco de lesões corporais e suicídio. O indigitado “jogo” recentemente chamou a atenção da sociedade e fez deflagrar investigação policial em vários estados da federação, dentre os quais o Rio de Janeiro, onde foram detectados casos suspeitos e seus possíveis “curadores” (assim chamados os aliciadores dos menores). Nesse contexto, com o escopo de infiltrar-se dentre seus adeptos, a autoridade policial criou um perfil fictício no Facebook para simular adolescente suscetível a participar do jogo. Outrossim, requereu em juízo que o Facebook Serviços Online do Brasil Ltda., ora Impetrante, fornecesse os dados cadastrais dos suspeitos, registros de criação e acesso aos perfis de usuário, além do conteúdo armazenado nas respectivas páginas. Deferidos os requerimentos, a empresa Impetrante foi oficiada e se reportou às empresas Facebook Inc. e Facebook Ireland Limited (operadores do site) e, através destas, obteve e forneceu os perquiridos dados cadastrais e registros. Não obstante, informou a impossibilidade técnica e jurídica de fornecer o conteúdo das páginas, armazenados em provedor localizado nos Estados Unidos da América, cuja legislação exige autorização de juízo federal daquela país para a quebra de sigilo. 2) Mediante a juntada de seus atos constitutivos, a Impetrante demonstra que se cuida apenas de uma representante comercial, vale dizer, uma negociante de espaços publicitários, não gerindo o conteúdo das informações existentes na rede social. Decerto causa certa perplexidade o fato de o grupo empresarial atuar de forma bastante expressiva no Brasil e não manter aqui os seus respectivos registros, incluindo o conteúdo das páginas virtuais. Malgrado, a Lei 11.965/2014 (Marco Civil da internet), a despeito de prever o dever de armazenamento de dados por provedores, não dispôs acerca da obrigatoriedade da guarda desses dados em território nacional. Despropositado avaliar aqui se a guarda dos dados em localidade	Privacidade, provedores de aplicações, registros de acesso a aplicações, dados cadastrais, redes sociais, multa diária, direito penal, interesse público.

			estrangeira se assenta em dificuldades técnico-operacionais ou decisão estratégica do grupo Facebook, ou em uma conjugação de ambos os fatores. O ponto é que a empresa brasileira não detém esses dados, o que torna impossível fornecê-los e, assim, cumprir integralmente a determinação judicial. Por conseguinte, descabido impor-lhe quaisquer medidas coercitivos, as quais, como sabido, não possuem finalidade punitiva. Ademais, nos termos do Art. 12 da Lei 12.965/2014, trata-se a suspensão temporária das atividades de sanção voltada a coibir violação ao direito à privacidade do usuário do serviço e ao sigilo das comunicações – hipótese exatamente contrária ao caso em análise – ao passo que a imposição de multa diária em procedimento investigatório criminal sequer encontra previsão na legislação pátria. 3) Para dar efetividade ao provimento judicial, resta recorrer-se aos mecanismos de cooperação internacional através do Ministério da Justiça, conforme disposto no Decreto Presidencial nº 3.810/2001, que promulgou o Acordo de Assistência Judiciária em Matéria Penal entre os Governos da República Federativa do Brasil e dos Estados Unidos da América – onde sediada uma das empresas detentoras dos perquiridos dados. 4) Descabido forçar à Impetrante a reativar perfil fictício, posto contrariar os termos de uso do serviço privado, ao qual se jungiu o usuário ao se cadastrar na rede social. Quiçá possa o grupo Facebook voluntariamente estabelecer exceção em seus termos de uso, ou firmar acordo com as autoridades brasileiras, com quem a Impetrante afirma colaborar, de molde a permitir a criação de perfil fictício em hipóteses como a presente. Contudo, obrigar a Impetrante ou as operadoras a tanto, não evidenciado o dolo de obstruir a investigação, ofende o princípio da legalidade disposto na Constituição da República (Art. 5º, inciso II, da CRFB). Concessão da segurança."	
Acesso indevido e direitos individuais	03/08/2017	Art. 3º II e III Art. 25	"Trata-se de ação ordinária/outras proposta pela união federal em face de Sazso Sistemas LTDA-ME, objetivando, em sede de tutela antecipada, “que seja expedida ordem obrigando a requerida a cessar imediatamente a venda de dados protegidos e acessos ilegal aos dados do DENATRAN, suspendendo ainda o funcionamento do site www.carchek.com.br”. Como provimento final, requer seja a Ré “condenada a cessar os acessos ilícitos ao banco de dados do DENATRAN e subsequente divulgação, sob pena de multa e, na ineficácia desta, de retirada compulsória do site da internet, sem prejuízo de outras medidas executivas necessárias a cessar a divulgação” (...)."	Privacidade, provedores de aplicações, dados pessoais, dados cadastrais, liberdade dos modelos de negócios, direito à informação, interesse público.
Conteúdo difamatório e mecanismo de busca	19/07/2017	Art. 19º § 1º Art. 32º	"Apelação cível. Obrigação de fazer cumulada com indenização por danos morais. Responsabilidade civil. Danos à imagem e à honra. Sítio de busca Google search. Disponibilização de informações que vinculam o nome dos autores a predicativos que depreciam a sua honra. Sentença de procedência. Prevenção da câmara. Réu que é parte legitima para figurar em ação que visa a remoção de conteúdo ofensivo, veiculado na internet. Nulidades, arguidas sob o fundamento de inobservância da lei 12.965/2014, rejeitadas. Marco civil da internet (lei 12.965 /2014). Inaplicabilidade aos casos anteriores a sua vigência. Notificação extrajudicial para exclusão do conteúdo difamatório, não atendida. Deferimento da tutela de urgência antecipada para determinar ao réu que retire a mensagem ofensiva. Violação do direito da personalidade que enseja a reparação por dano moral. Direito ao esquecimento. Desnecessidade de indicação da url. Autores que apresentaram informações suficientes para a localização do conteúdo ofensivo. Provedor que possui meios para desvincular a pesquisa do nome dos autores das páginas, indicadas. Precedentes do stj. Dano moral, configurado. Majoração da verba indenizatória. Honorários advocatícios, fixados em valor proporcional ao trabalho exercido e complexidade da causa. Majoração dos honorários advocatícios em sede recursal, na forma do Art. 85, § 11 do ncpc. Manutenção do valor das astreintes. Erro material no pronunciamento do termo inicial da multa pelo descumprimento da obrigação de fazer. Termo a quo	Privacidade, provedores de aplicações, identificação clara e inequívoca, remoção de conteúdos, multa diária, direito de imagem. Danos morais, provedores de pesquisa, direito ao esquecimento, interesse público, indenização.

			que se dá a partir da intimação pessoal do devedor para cumprimento da obrigação. Precedentes do stj. Multa, aplicada por ato atentatório à dignidade da justiça, no percentual de 20% por cento. Desprovimento do recurso do réu. Parcial provimento do recurso dos autores."	
Governo digital e auditoria operacional	12/07/2017	Art. 3º II; Art. 7º VII; Art. 24º II, III, V	"Relatório de auditoria natureza operacional. Avaliação dos serviços prestados aos cidadãos de forma eletrônica. Identificação de oportunidades de melhoria. Recomendações."	Privacidade, provedores de aplicações, dados pessoais, dados cadastrais, direito à informação, segurança da informação, interesse público.
Figura pública e identificação de usuários	08/06/2017	Art. 7º I e VII Art. 8º Art. 22º parágrafo único, I a III Art. 23º	"GERALDO JOSÉ RODRIGUES ALCKMIN FILHO forte na inviabilidade do anonimato ajuizou a presente tutela cautelar antecedente para exibição de documentos em face de Twitter Brasil rede de informação LTDA, qualificados nos autos, objetivando compelir a ré a apresentar os dados cadastrais e números de IP's dos perfis responsáveis pelas postagens para subsidiar as ações principais que (...) julgar necessárias (sic). Deferida a tutela provisória (fls. 99/100), a ré citada (fls. 138) ofertou embargos de declaração, rejeitados (fls. 136/137) e contestação (fls. 141/223). Discorre sobre a sua atuação no mercado e o Marco Civil da Internet. Entende que a quebra do sigilo de dados, por exemplo sem indício da ocorrência de ilícito, põe em risco a liberdade de expressão e de manifestação do pensamento dos respectivos usuários (sic). O caso envolve fatos de relevante interesse público e com ampla repercussão, já que o Autor possui um âmbito de proteção diminuído em relação a seus direitos da personalidade e deve se sujeitar a conteúdos que a mencionem (sic). Não dispõe dos dados cadastrais dos seus usuários, elementos não abrangidos pelo dever legal de guarda. Entende não estar sujeito à sucumbência. Houve réplica (fls. 225/230). Determinada a especificação de provas (fls. 232), manifestaram-se as partes (fls. 260/267 e 276); informando o autor o parcial provimento ao agravo (fls. 279/291), ao qual se agregou primário efeito suspensivo (fls. 272/274). (...)"	Liberdade de expressão, privacidade, provedores de aplicações, registros de acesso a aplicações, dados cadastrais, redes sociais, segredo de justiça, anonimato, quebra de sigilo, liberdade de informação, liberdade de manifestação do pensamento, pessoas públicas.
Disponibilização de dados sem autorização do usuário	24/05/2017	-	"O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, por intermédio da titular da 5ª Promotoria de Justiça de Consumo da Capital propôs AÇÃO CIVIL PÚBLICA contra Telefônica Brasil S/A (VIVO S/A), qualificado(s) nos autos, sob a alegação da prática de condutas vedadas pelo Código de Defesa do Consumidor, em especial, a de não zelar pelo cumprimento dos contratos firmados com os consumidores, cujos dados são repassado sem critérios de distinção ou identificação do receptor e sem prévia autorização do interessado. Segundo a exordial, também se faz necessária a inversão do ônus da prova. Alegando a presença dos pressupostos do periculum in mora e do fumus boni iuris requer que a ré seja liminarmente compelida a efetuar, no prazo de 24h, as seguintes condutas: A) Não disponibilizar os dados dos usuários dos seus produtos e serviços sem a devida e prévia autorização destes, mantendo-os em caráter sigiloso, conforme o quanto determina a Lei Federal n. 12.965/14, bem como o Decreto n. 8771/2016, respeitando o direito à inviolabilidade dos dados dos usuários e o sigilo do fluxo de suas comunicações;	Privacidade, provedores de conexão, dados pessoais, dados cadastrais, multa diária, direito do consumidor, interesse público, decreto 8771/16, processos históricos

			B) Adotar mecanismos e instrumentos tecnológicos de armazenamento de dados dos usuários dos seus produtos e serviços de modo a resguardar a segurança e o sigilo destes, orientando os seus funcionários e/ou terceirizados acerca do obrigatório respeito aos mecanismos e instrumentos tecnológicos de armazenamento dos dados dos usuários, realizando, inclusive, o necessário treinamento adequado e satisfatório para tal mister; C) Certificar-se da segurança dos serviços prestados por terceiros em nome da Telefônica Brasil S/A, de modo a evitar fraudes e demais condutas ilícitas, afetando os interesses e direitos dos consumidores; D) Zelar pela contratação de prestadores de serviços terceirizados que os executem em respeito às normas estabelecidas pelas Leis Federais n: 8.078/90 e 12.965/14, acompanhando a referida prestação a fim de averiguar seus padrões de eficiência, qualidade e segurança; E) Verificar, previamente, a veracidade das solicitações de modificação da estrutura contratual vigente, certificando-se se realmente foram requeridas pelos legítimos usuários e não, de modo ilícito, por terceiros, orientando os seus funcionários e terceirizados acerca da imprescindibilidade da verificação, com a realização de treinamentos periódicos."	
Agente público e liberdade de expressão	06/04/2017	Art. 5º VII e VIII Art. 10º §1º;	"Trata-se de ação de obrigação de fazer promovida por João Agripino da costa Doria júnior em face de Facebook serviços on line do Brasil LTDA. Requer, o autor, a retirada, da rede social da empresa ré, da página de evento marcado para o dia 13 de maio 2017, denominado "Virada Cultural na Casa de João Dorian", e de "posts" ofensivos contidos na referida página, sob a alegação de que dita página afronta a paz pública e a honra do autor. Pede, também, os dados cadastrais dos responsáveis pela criação da página, bem como da página "Deixe a esquerda livre", (fls. 1/75). Tutela de urgência indeferida (fls. 77/80). A ré ofereceu contestação, sustentando, a preliminar de ilegitimidade passiva, e, no mérito, a impossibilidade de controle prévio de conteúdo, que não se mostra ofensivo, ademais, a limitação dos dados a serem fornecidos e a falta de pretensão resistida (fls. 86/134). (...)"	Liberdade de expressão, privacidade, provedores de aplicações, dados cadastrais, redes sociais, remoção de conteúdo, pessoas públicas.
Dados além dos registros de acesso	02/03/2017	Art. 15º	"AGRAVO DE INSTRUMENTO. Ação de obrigação de fazer. Decisão agravada que deferiu a antecipação dos efeitos da tutela para determinar o fornecimento dos registros de acessos e informações de usuários de banco de dados referente a endereço eletrônico de rede social. Recurso da ré. Acolhimento. Decurso de prazo superior a seis meses entre a divulgação do conteúdo e a citação da ré, pelo que não subsiste a obrigação de guarda dos registros de acesso a aplicações de internet, nos termos do Art. 15 do Marco Civil da Internet. Ausência de obrigação de guarda de outros dados além dos registros de acesso a aplicações. Decisão revogada. RECURSO PROVIDO."(v.24694).	Privacidade, Provedores de aplicações, Registros de acesso a aplicações, Dados cadastrais, Redes sociais, Segredo de justiça.
Processo público e liberdade de imprensa	15/02/2017		"Marcela Tedeschi Araújo Temer, que, como é de conhecimento comum, é a Primeira Dama do País, ajuizou ação em face da Folha de São Paulo (Folha da Manhã S/A) e do Jornal O Globo, narrando, em breve síntese, que, em meados de 2016, teve o seu telefone celular clonado, ocasião em que o responsável teria copiado todos os arquivos da memória do aparelho, aí incluídos fotos, mensagens de texto, vídeos e outros, de conteúdo privado e íntimo. A petição inicial esclarece que o autor de tal fato foi identificado, processado e condenado à prisão. Acreditando estar resolvido o assunto na esfera judicial, a autora narrou que o Secretário Especial de Comunicação da Casa Civil da Presidência da República foi contatado pelas empresas rés, solicitando-lhe comentário do Presidente da República acerca do conteúdo clonado do celular de sua	Liberdade de expressão, Privacidade, Segredo de justiça, Intimidade, Direito de imagem, Direito penal, Quebra de sigilo, Liberdade de imprensa, Pessoas públicas.

			esposa, asseverando que esse conteúdo seria disponibilizado nos sítios da internet desses veículos de comunicação, bem como em versão impressa. Por isso, e ao argumento da proteção constitucional da privacidade e da intimidade, bem como ao amparo da proteção legal da inviolabilidade da intimidade e da vida privada, além da inviolabilidade do sigilo das comunicações privadas (Lei nº 12.965/14 – Marco Civil da Internet) – e não sem antes fazer referência à chamada "Lei Carolina Dieckmann" (Lei nº 12.737/12), que tipifica o crime de invasão de dispositivo informático –, pediu e obteve a concessão de liminar lavrada nos seguintes termos (...)"	
Perfil falso em rede de relacionamento	09/01/2017	Art. 19º	"(...) Alega que há mais de um ano recebe e-mails da ré, que possui o domínio do site Badoo no Brasil (badoo.com.br), convidando-a a acessar um link de "admiradores", convite que sempre ignorou, até que recentemente acessou esse link e teve conhecimento da criação de perfil falso em seu nome no Badoo com dados e fotos extraídas sem autorização de sua página no Facebook. Diz que recebeu diversas mensagens de desconhecidos, algumas com conteúdo libidinoso, ocasionando problemas pessoais, pois é advogada e está noiva, sendo que o perfil falso causou ofensa à sua honra e imagem. Relatou o problema à ré, sem obter resposta. Requer a retirada do perfil falso do site da ré, com inibição de envio de e-mails para sua conta (***@hotmail.com), bem como a condenação da ré ao pagamento de indenização por danos morais, estimados em R$ 30.000,00. (...)"	Privacidade, Provedores de aplicações, Redes sociais, Remoção de conteúdos, Direito de imagem, Danos morais, Propriedade intelectual, Nome de domínio, indenização.
Provedor de aplicações e código IMEI	22/02/2016	-	"Internet. Publicações ofensivas no Facebook. Decisão agravada que determinou o fornecimento do código IMEI dos usuários que proferiram as ofensas. Impossibilidade. O provedor dos sites não está obrigado a fornecer dados pessoais dos usuários que sequer são exigidos no momento do cadastro, inexistindo provas de que esses dados são armazenados pelo Facebook. Fornecimento do IP dos usuários que é suficiente para sua identificação. Jurisprudência deste E. TJSP. Decisão reformada para afastar a obrigatoriedade de fornecimento do IMEI. Recurso provido."	Provedores de aplicações, Registros de conexão, Dados pessoais, Registros de acesso a aplicações, Dados cadastrais, Remoção de conteúdos.
Fornecimento de IP e Princípio da Legalidade	29/02/2016	Art. 15º	"Recurso extraordinário com agravo. Direito civil. Google. Facebook. Blogs "reaciocinante de direita", "zé Osvaldo" e "polenta news". Determinação judicial de fornecimento dos endereços de IP. Manutenção de dados de IP por tempo determinado. Art. 15 da lei nº 12.965/2014. Alegação de ofensa ao princípio da legalidade. Súmula nº 636 do stf. Reexame do conjunto fático-probatório carreado aos autos. Impossibilidade. Súmula nº 279 do stf. Agravo desprovido."	Liberdade de expressão, Provedores de aplicações, Dados pessoais, Registros de acesso a aplicações, Dados cadastrais, Interesse público.
Fornecimento de dados e impossibilidade técnica	15/05/2016	Art. 10º §1º; Art. 19º, §1º Art. 22º	"Medida Cautelar. Facebook. Fornecimento de dados do usuário. Ausência dos requisitos do Art. 22 da Lei 12.965/2014. Improcedência mantida. Recurso a que se nega provimento."	Provedores de aplicações, Dados pessoais, Identificação clara e inequívoca, Redes sociais, Direito de imagem.
Identificação de ofensor e servidores no exterior	28/06/2016	Art. 11º Art. 22º parágrafo único.	"Cominatória. Internet. Google. Fornecimento de dados de identificação de usuário ofensor. Ofensa cometida fora do território nacional. Incidência do Art. 11, da Lei nº 12.965/2014. Cumpre observar que, para o deferimento do pedido, exige-se apenas "indícios da ocorrência do ilícito" (Art. 22, parágrafo único, da Lei nº 12.965/2014). Em outras palavras, nesta demanda, não seria pertinente o exame exauriente da ofensa, mas sim apenas potencialidade de se verificar que o quanto afirmado por usuário poderia, efetivamente, causar danos ao direito da personalidade da vítima. E, neste caso, a suposta anedota, envolvendo aspectos íntimos da vida do autor, poderia, de fato, caracterizar ofensa à honra. É o quanto basta para impor ao réu a obrigação de identificação.	Liberdade de expressão, Provedores de aplicações, Dados pessoais, Registros de acesso a aplicações, Identificação clara e inequívoca, Anonimato.

			Face ao disposto no Art. 11, da Lei nº 12.965/2014, vê-se que os provedores de hospedagem e aplicações na internet somente têm o dever de guarda e fornecimento de dados pessoais de usuários, caso os atos impugnados ocorram em território nacional, em terminais localizados no País. Daí decorre que não se pode impor a identificação ao autor, considerando-se a prova de que os dados requeridos foram mantidos em servidor localizado no exterior. Recurso provido para reconhecer a falta de interesse processual do autor."	
Divulgação de dados pessoais e bloqueio de site	06/12/2016	-	"AGRAVO DE INSTRUMENTO Tutela Provisória de Urgência Antecipada – Pedido de bloqueio de informações prestadas pelo site www.consultasocio.com relacionadas a participação societária do agravante - Não há a demonstração de plano de que houve indevido acesso a informações sigilosas da Receita Federal, uma vez que informações acerca de participação em sociedade comerciais podem ser obtidas perante as Juntas Comerciais dos Estados e perante a própria Receita Federal que disponibiliza serviço denominado "CONSULTA QUADRO DE SÓCIOS E ADMINISTRADORES NO CNPJ" – Ausência da probabilidade do direito e do periculum in mora - Recurso desprovido."	Privacidade, Provedores de aplicações, Dados pessoais, Remoção de conteúdos, Bloqueio de conteúdos, Provedores de pesquisa, Provedores de conteúdo.
Selfie e renúncia a direito individual	06/12/2016	Art. 7º	"civil. Direito protetivo à imagem. Divulgação de "selfie" a constituir aparente renúncia a esse direito. Liberdade de imprensa na divulgação da mídia, que fundamenta matéria jornalística atinente a uma operação policial. Não observada violação à intimidade da pessoa. Ponderação dos valores constitucionais ao caso concreto. I. Nos tempos atuais, quanto maior o desenvolvimento tecnológico da computação, maior risco experimenta a proteção dos direitos individuais, especialmente o de imagem, objeto de constante divulgação (e exploração) na "internet". Nessa interface, ganha projeção o que a doutrina alemã denomina de "direito de determinação sobre os próprios dados pessoais" ("die informationelle Selbstbestimmung"). Ou seja, compete ao indivíduo o direito de dispor sobre os dados (informes ou mídias) referentes à sua própria pessoa. Aqui, os dados pessoais são compreendidos não apenas os cadastrais, senão também aqueles no curso da telecomunicação-telemática. Com isso, estende-se a proteção à vida privada, à privacidade, à intimidade, à honra e à própria imagem do indivíduo. Logo, a limitação desses aspectos ao desenvolvimento da personalidade só podem estar presentes em determinadas situações legais (v.g., persecução penal), sobretudo após o marco civil regulador da "internet" (Lei n. 12.965, de 23.4.2014, Art. 7º, I), com exceção da própria renúncia (tácita ou expressa) exercida pela pessoa titular desse direito. II. No caso concreto, o próprio agente (ora recorrido), aparentemente no curso de operação policial, teria tirado uma "selfie". Isolada alegação do recorrido de voluntária transmissão da respectiva imagem a um grupo formado por policiais. Não elucidada a circunstância de disposição dessa mídia na "internet". Renúncia ao citado "direito de determinação sobre os próprios dados pessoais". Respectiva imagem, que não expõe aspectos centrais da vida privada (intimidade) do recorrente, objeto de reportagem no sítio "radar on line da veja.com.", sob o título "Registro da ocorrência". No ponto, não se extrai qualquer responsabilidade da recorrente na captação da mídia, livremente disposta na "internet", e a utilizar para fins jornalísticos. III. Ademais, a fotografia ("sem cortes") e a correspondente matéria jornalística estariam dentro de um espectro do exercício regular e ponderado da liberdade da imprensa, porque a) o recorrido agia na qualidade de servidor público e em área pública; b) há notícia de concomitante ocorrência de grave delito (sequestro), em cuja respectiva apuração policial, o recorrente poderia estar em atividade; c) a imagem do "selfie" não teria experimentado qualquer adulteração ou falsificação ou (re)montagem; d) para preservar a própria imagem, bastaria o recorrido ter utilizado bala clava, como sói acontecer nas operações policiais de destaque; e) aparentemente, não se tratava de foto para "registro de informações técnicas e de estudo de posicionamento enviada para um grupo de exclusivo	Privacidade, Dados pessoais, Redes sociais, Intimidade, Direito de imagem, Danos morais, Direito ao esquecimento, Liberdade de imprensa, Interesse público.

			de policiais envolvidos na operação" (f.7), até porque essa circunstância não foi comprovada; f) a experiência comum revela que um "selfie" não é o meio mais comum para esse desiderato (Lei n. 9.099/95, Art. 5º); g) exatamente por ser uma situação extraordinária é que veio a ser classificada como "inconveniente" pela direção policial (f. 132). Em outros termos, a divulgação da aludida imagem, sem cortes (como disponibilizada na "internet") (necessidade), é que conferia credibilidade ao inusitado fato noticiado, tornando-se, pois, aspecto essencial à matéria jornalística (adequação), a qual não teria ultrapassado o campo do excesso, a não configurar violação ao princípio da proporcionalidade (em sentido estrito), uma vez que não foram inseridos ou explorados outros dados pessoais do ora recorrido. IV. E quanto ao conteúdo da matéria jornalística, a começar pelo título ("Registro da ocorrência"), observa-se no desenrolar do historiado, um texto que retrata os fatos (aparente posicionamento de duas pessoas, com trajes e instrumentos policiais, num teto de edifício) com extraordinária "fina ironia". Eis o teor: "Enquanto as forças de segurança do Distrito Federal não piscavam os olhos e o país acompanhava pela televisão o sequestro do mensageiro de um hotel, ontem, em Brasília, parte da turma da Polícia Civil concentrava-se no que, de fato, considera importante: o registro da ocorrência. Um policial, aparentemente atirador de elite, destacado em cima do prédio vizinho ao edifício onde ocorria o crime, sacou uma de suas armas: o telefone celular. Virou a cabeça para o lado e, pimba, fez um selfie. A imagem, com outro policial ao fundo segurando uma arma, já começou a correr solta nas redes sociais e, lógico, gerar todo tipo de piada" (f. 123). No particular, há uma correspondência do caráter extraordinário, tanto da "ironia" (matéria), quanto do fato reportado. Ademais, a tirada jornalística não fez qualquer menção à qualificação do ora recorrido, nem à sua competência ou honra profissional, muito menos lançou adjetivos ou dúvidas sobre a imagem, isoladamente considerada. Logo, o tom crítico teria sido proporcional, à época da retratação dos fatos, à inusitada situação documentada. V. Em síntese, não se observa, pois, violação à vida privada, à intimidade e aos atributos da personalidade, especialmente o direito à honra e à imagem do recorrido, tendo a recorrente atuado dentro dos padrões da razoabilidade em cumprir seu mister de informar à época dos fatos (CF, Art. 5º, IV, IX, XIV e Art. 220, caput, §§ 1º e 2º). VI. Por fim, não se dessume interesse público, em se permitir a continuidade de exploração da imagem (e consequente matéria jornalística), como tal captada e noticiada pela recorrente, se a parte interessada (ora recorrido) agora alega constrangimento profissional, o que é factível em razão do longo período ao fato documentado. Caso contrário, se teria uma insuficiência à concretude da proteção dos "dados pessoais". Nesse contexto, o recorrido faz jus ao esquecimento (direito comparado: Acórdão C-131/12, Tribunal de Justiça da União Europeia). Cristalino, pois, o direito do recorrido ao esquecimento de tal reportagem, uma vez que estão ausentes razões especiais como o papel desempenhado pela recorrida na vida pública a justificar um interesse preponderante do público em ter acesso a tal matéria (precedente: TJDFT, Acórdão n. 908629, 1ª T. Cível, em 19.11.2015). No ponto, a sentença deve ser mantida por seus próprios fundamentos. Recurso conhecido e parcialmente provido. Excluída a condenação de danos morais e respectiva publicação, na íntegra, da sentença condenatória. Mantida, no entanto, a obrigação à exclusão da matéria e da imagem, como reportadas, do sítio eletrônico da requerida (item "b" - f. 141-v), em atenção ao "direito ao esquecimento". Sem custas, nem honorários (Lei n. 9.099/95, Art. 46 e 55)."	
Custódia de dados e regras de segurança	06/12/2016	Art. 15º Art. 13º	"Obrigação de fazer, internet, fornecimento de dados de acesso de aplicações, perdas e danos, Sentença de procedência, condenando a ré a fornecer os dados cadastrais e informações de um perfil criado na rede social, assim como os registros de logs de acesso e números de ips do usuário da conta.	

		Art. 14º Art. 15º Art. 16º do Decreto nº 8.771/16	Fixação de multa por descumprimento da ordem liminar confirmada, no valor de R$ 5.000,00 (cinco mil reais) diários, até o limite de R$ 500.000,00 (quinhentos mil reais). Irresignação da ré 1. Nulidade da sentença. Não configuração. Embargos declaratórios rejeitados por decisão anterior à sentença. Embargos opostos contra decisão liminar, e não à sentença. Preclusão da impugnação da nulidade, pela não interposição de recurso contra a decisão que rejeitou os embargos de declaração. Inteligência do Art. 278 do CPC/2015. Nulidade afastada. 2. Fornecimento de dados de registro de acesso de aplicações. Fatos relatados pela autora ocorridos em março de 2016, já na vigência da Lei 12.965/2014 (Marco Civil da Internet). Obrigação de custódia dos dados de registro de acessos a aplicações, por seis meses (Art. 15, Lei 12.965/2014). Norma que não é de eficácia contida. Regulamentação posterior, pelo Decreto 8.771/2016, que apenas previu as regras de segurança da guarda das informações. Obrigação já existente anteriormente. Alegação da ré de impossibilidade de cumprimento. Conversão em perdas e danos (Art. 248, CC, e Art. 499, CPC/2015). Fixação em R$ 5.000,00 (cinco mil reais), corrigidos monetariamente desde essa fixação (Súmula 362, STJ), e com juros de mora de 1% (um por cento) ao mês da data da citação (Art. 240, CPC/2015). Sentença reformada em parte, convertendo a obrigação de fazer em perdas e danos. Manutenção da sucumbência da ré. Recurso provido em parte."	
Ofensas por aplicativos e celular profissional	15/11/2016	Art. 7º, III	"(...) ROBERTA e Eduardo foram casados de maio de 2006 a julho de 2013 (fls. 115/116) e são pais de Guilherme e Fernando (com 8 e 6 anos de idade, respectivamente), os quais têm como babá, desde o ano de 2008, a ré IVONETE. Após o divórcio, JAMILE e Eduardo constituíram união estável, tendo este constatado, ao examinar aparelho celular que teria sido dado a IVONETE em razão do trabalho, que as rés, em mensagens trocadas via WhatsApp, ofendiam copiosamente a honra da autora. Meses após tal constatação, um dos filhos de Eduardo e ROBERTA, durante reunião familiar, dirigiu ofensa à autora com conteúdo assemelhado às ofensas proferidas pelas rés em mensagens trocadas via WhatsApp. A prova havida mediante acesso ao aparelho celular de IVONETE. Questão decisiva a ser desde logo desatada diz com a validade dos dados e informações colhidos por Eduardo (e por ele transmitidos à autora) no aparelho celular utilizado por IVONETE. (...)"	Privacidade, Provedores de aplicações, Dados pessoais, Redes sociais, Segredo de justiça, Intimidade, Danos morais Quebra de sigilo, Indenização.
Bloqueio do WhatsApp e direito à comunicação	27/10/2016	Art. 3º I e V	"(...) Na sociedade moderna, a internet é, sem dúvida, o mais popular e abrangente dos meios de comunicação, objeto de diversos estudos acadêmicos pela importância que tem como instrumento democrático de acesso à informação e difusão de dados de toda a natureza. Por outro lado, também é fonte de inquietação por parte dos teóricos quanto à possível necessidade de sua regulação, uma vez que, à primeira vista, cuidar-se-ia de um “território sem lei”. No Brasil, contudo, já se procurou dar contornos legais à matéria. A Lei 12.965/2014 surgiu, exatamente, com o propósito de estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil”. Em seu Art. 3º, I, o citado diploma dispõe que o uso da internet no País tem como um dos princípios a “garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal”. Além disso, há expressa preocupação com “a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas” (Art. 3º, V). Ora, a suspensão do serviço do aplicativo WhatsApp, que permite a troca de mensagens instantâneas pela rede mundial de computadores, da forma abrangente como foi determinada, parece-me violar o	Liberdade de expressão, Privacidade, Provedores de conexão, Provedores de aplicações, Redes sociais, Bloqueio de aplicativos, Interesse público, Criptografia, Processos históricos.

			preceito fundamental da liberdade de expressão aqui indicado, bem como a legislação de regência sobre o tema. Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa. (...)"	
Registro de Conexão e prática de ilícitos	20/10/2016	Art. 15º	"Neste juízo de cognição sumária, nos termos dos Art.s 298 e 300, do CPC, resta somente aferir se presentes os requisitos necessários à concessão da providência urgente, quais sejam, a probabilidade do direito e o perigo de dano irreparável ou o risco ao resultado útil do processo. Pretende a autora o fornecimento das informações indispensáveis à identificação dos usuários de linhas telefônicas, com acesso à internet, que integram uma rede de websites destinados à comercialização ilícita de transmissão de canais de TV por assinatura, evidenciando-se a prática criminosa. A medida pretendida não implica violação à garantia constitucional de sigilo das comunicações de dados, diante da ofensa a direito. A par da garantia da livre manifestação do pensamento, a Constituição Federal também veda o anonimato. Como consabido, nos dias atuais o cognominado Marco Civil da Internet, a Lei nº 12.965, de 23.04.2014, em seu Art. 15, disciplina expressamente a guarda de registros de acesso a aplicações da internet enquanto obrigação legal que pesa sobre tais prestadores de serviços. Ademais, não se pretende a quebra de sigilo de dados e comunicações tutelados pela Lei nº 9.296/96, mas sim e tão somente o acesso a dados cadastrais de agentes potencialmente responsáveis pela prática de ilícitos, cuja elucidação se persegue."	Privacidade, Provedores de conexão, Registros de conexão, Dados cadastrais, Identificação clara e inequívoca, Direito penal, Quebra de sigilo, Liberdade de manifestação do pensamento
Violação às garantias e nulidade da prova	29/09/2016	Art. 7º III	"Apelação. Associação para o tráfico de drogas. Desrespeito às garantias da inviolabilidade da intimidade, do sigilo de correspondência de dados e comunicações telefônicas. Nulidade. Absolvição. Assiste razão à Defesa ao pretender a nulidade da sentença por violação ao disposto no Art. 5º, incisos X e XII, da Constituição Federal, cujo texto consagra outras garantias fundamentais, como a inviolabilidade da intimidade, o sigilo das comunicações telegráficas, de dados e das comunicações telefônicas, cabendo ressaltar, ainda, que a Lei nº 12.965/14, estabelece os princípios, garantias e deveres para o uso da Internet no Brasil, e prevê, em seu Art. 7º, inciso III, dentre os direitos assegurados aos usuários da rede mundial, "a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial". Assim, conclui-se que os dados armazenados nos aparelhos celulares estão resguardados pelo direito fundamental à intimidade, e, a despeito de não gozar de caráter absoluto, tais prerrogativas individuais, somente, são passíveis de sofrer restrições pelos órgãos estatais em casos de relevante interesse público, ou em situações que se revelem imprescindível para assegurar outros direitos constitucionais, o que não ocorreu nestes autos, porque sua violação se deu sem a autorização do recorrente e ao arrepio do Art. 5º, inciso X, da Constituição da República, de forma a justificar a declaração de nulidade da prova obtida durante a diligência policial, maculando os demais elementos probatórios subsequentes e dela dependentes, com a consequente absolvição do recorrente. Precedente do STJ. PROVIMENTO DO RECURSO"	Privacidade, Provedores de aplicações, Segredo de justiça, Intimidade, Direito penal, Quebra de sigilo.
Provedores de pesquisa e responsabilidade estrita	19/09/2016	Art. 19º §1º	"AGRAVO DE INSTRUMENTO. Publicação de decisão judicial com conteúdo sigiloso veiculada em sites de busca. Concessão de medida antecipatória para obrigar a agravante a remover os links publicados sob pena de multa. Responsabilidade estrita ao caso de omissão, quando devidamente indicado o conteúdo indevido, inclusive com apontamento da URL específica. Impossibilidade de serviços de busca na internet monitorar previamente o conteúdo editado pelos usuários. Inteligência do Art. 19, §1º do Marco Civil da Internet. Decisão reformada. Agrado provido."	Privacidade, Identificação clara e inequívoca, Segredo de justiça, Remoção de conteúdos, Intimidade, Multa diária, Provedores de pesquisa, Provedores de conteúdo.

Apreensão de smartphone e acesso a dados	15/09/2016	Art. 7º, III	"Processual penal. Operação "lava-jato". Mandado de busca e apreensão. Apreensão de aparelhos de telefone celular. Lei 9296/96. Ofensa ao Art. 5º, xii, da constituição federal. Inocorrência. Decisão fundamentada que não se subordina aos ditames da lei 9296/96. Acesso ao conteúdo de mensagens arquivadas no aparelho. Possibilidade. Licitude da prova. Recurso desprovido. I - A obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9296/96. II - O acesso ao conteúdo armazenado em telefone celular ou smartphone, quando determinada judicialmente a busca e apreensão destes aparelhos, não ofende o Art. 5º, inciso XII, da Constituição da República, porquanto o sigilo a que se refere o aludido preceito constitucional é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos. III - Não há nulidade quando a decisão que determina a busca e apreensão está suficientemente fundamentada, como ocorre na espécie. IV - Na pressuposição da ordem de apreensão de aparelho celular ou smartphone está o acesso aos dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal. V - Hipótese em que, demais disso, a decisão judicial expressamente determinou o acesso aos dados armazenados nos aparelhos eventualmente apreendidos, robustecendo o alvitre quanto à licitude da prova. Recurso desprovido."	Privacidade, Dados pessoais, Segredo de justiça, Direito penal, Quebra de sigilo, Interesse público
Ataque cibernético e dados cadastrais	10/08/2016	Art. 4º Art. 15º Art. 22º I e II.	"Trata-se de ação de obrigação de fazer com pedido de antecipação de tutela movida por BANCO DAYCOVAL S/A contra GLOBAL VILLAGE TELECOM S/A, alegando, em síntese, que em 26/04 e 27/04 de 2016 o seu departamento de TI identificou ataques virtuais a partir do IP de nº 179.185.142.243, do que resultou na liquidação indevida do empréstimo consignado do Governo do Estado da Paraíba, sendo o autor o credor deste negócio jurídico. Afirma que a ré é a empresa provedora de acesso do referido IP e, portanto, visando a identificação do responsável pelos ataques cibernéticos e a consequente adoção das medidas judiciais cabíveis, pleiteia, também em sede de tutela antecipada, o fornecimento por parte da requerida dos dados cadastrais (nome, endereço e demais informações) pertencentes ao IP fornecido. Juntou documentos."	Privacidade, Provedores de conexão, Dados cadastrais, Quebra de sigilo.
Descumprimento de ordem de autoridade	20/07/2016	Art. 7º, Art. 11º e Art. 12º	"Processual civil. Ação civil pública. Ministério público federal. Lei nº 12.965/2014 (marco civil da internet). Requisição de informações por autoridade brasileira. Limitação prevista pelo Art. 7º. Ordem judicial. Obrigatoriedade. Eventual descumprimento de ordens emanadas de autoridades judiciais. Ausência de interesse de agir. Atribuição exclusiva dos magistrados prolatores das decisões supostamente não atendidas, a quem cabe impor as medidas coercitivas previstas no Art. 12 da lei nº 12.965/2014. Inadequação da tutela coletiva. Apelação desprovida. 1. Irrelevante o fato de a MM. Magistrada prolatora do decisum em debate ter decidido a lide apenas após a manifestação do demandado, com acolhimento de suas ponderações. Aliás, não merece reparo ter a MM. Magistrada sentenciante se servido do previsto no Art. 2º da Lei nº 8.437/1992 que, além de permitir o exercício do contraditório, permite ao julgador aprimorar sua cognição acerca do objeto da demanda, o que não lhe pode ser vedado à luz do princípio do livre convencimento. 2. Conforme consignado na sentença guerreada, "não pode o autor pretender que toda e qualquer autoridade brasileira obtenha acesso a dados que possuem proteção a respeito de seu sigilo garantida	Privacidade, Provedores de aplicações, Registros de conexão, Dados pessoais, Redes sociais, Remoção de conteúdos, Intimidade, Quebra de sigilo, Interesse público.

			a constitucionalidade e sobre os quais, por tais motivos, recai a reserva de jurisdição para o devido acesso, conforme reconhecido legalmente" (fls. 362). 3. Portanto, a expressão "autoridades brasileiras", por demasiadamente ampla e em descompasso com o previsto no Art. 11 da Lei nº 12.965/2014, inquina a pretensão inicial de juridicamente possível, mesmo que a análise de seu conteúdo seja ultimada apenas em tese. 4. O cumprimento das ordens judiciais exaradas nos diversos casos concretos deve ser engendrado pelos próprios Magistrados oficiantes, com esteio nos instrumentos legislativos dissuasórios existentes no ordenamento jurídico, tais como a fixação de multas e a tomada de medidas assemelhadas. 5. Cabe aos juízes, a toda evidência, fazerem valer suas decisões e dar-lhes o devido cumprimento. Trata-se inclusive de uma dedução solar que se extrai do próprio conceito de jurisdição, cujo esvaziamento seria incontestável diante de entendimento diverso. Em suma, parece desnecessário (daí a falta de interesse de agir), para que não se diga absurdo, que outro magistrado, em ação diversa, deva expressamente reconhecer in abstrato algo tão comezinho e evidente per se. 6. Em momento algum da petição inicial o autor deixa transparecer a ideia de que os sucessivos descumprimentos a ordens judiciais teriam gerado um dano coletivo passível de ser indenizado sob as normas da Lei da Ação Civil Pública, seja em termos de causa de pedir, seja quanto ao pedido propriamente dito. A alegação apenas em sede de apelação impede o Tribunal de decidir a lide sob esse prisma 7. Não há necessidade de uma tutela coletiva que venha apenas repetir o que a lei já determina, cabendo ao magistrado sopesar a aplicação das sanções do Art. 12 da Lei nº 12.965/2014 em cada caso concreto 8. Apelação desprovida."	
Registro de acesso e prazo superado	28/06/2016	Art. 5º VI e VIII Art. 7º I, II e III Art. 13º § 2º Art. 15º Art. 22º Art. 13º § 2º do Decreto 8771/16	"Apelação cível – requisição judicial de registros – lei nº 12.965/2014 – registros de acesso a aplicações de internet – prazo de armazenamento (6 meses) superado à data do ingresso do pedido – impossibilidade no cumprimento da ordem judicial – honorários – matéria não conhecida – prejudicialidade – recurso da empresa requerida provido – recurso do requerente não conhecido. Com o advento da Lei n. 12.965/2014 (Marco Civil), os pedidos judiciais com propósito de formar conjunto probatório em processo judicial (Art. 22, Lei 12.965/2014), devem seguir o procedimento da lei especial, o que ocorre na especificidade do caso concreto. A requisição de registro de acesso a aplicações de internet após o prazo assinalado no Art. 15 da Lei n. 12.965/2014 (6 meses), torna impossível ao provedor fornecê-lo, em razão de a legislação exigir o armazenamento por prazo certo. O provimento do recurso da requerida, desobrigando-a de apresentar os documentos requisitados, prejudica a análise do recurso do ex adverso, que discute honorários de sucumbência."	Privacidade, Provedores de aplicações, Registros de acesso a aplicações, Redes sociais, Quebra de sigilo, Decreto 8771/16.
Domain privacy" e bloqueio no backbone	16/06/2016	Art. 3º Art. 7º	"1. Trata-se de ação de obrigação de fazer ajuizada em face de Privacy Protection Service Inc. em que os autores alegam, em síntese, a ilegalidade da exploração comercial e exposição não autorizada de seus dados pessoais e das sociedades que compõem junto ao “www.consultasocio.com” (ID:	Privacidade, Provedores de conexão, Dados pessoais, Dados cadastrais, Segredo de justiça,

		Art. 11º	2012741661_DOMAIN_COM-site VRSN). Aduziu que as informações fornecidas pelo site violam direito fundamental à intimidade, vida privada, honra e imagem (Art. 5º, X, CF), bem como à disciplina estabelecida nas Leis 12.965/2014, 12.414/2011, e 12.527/2011 quanto à utilização de informações cadastrais e restrição de acesso às informações relativas à vida privada sem consentimento. Sustentou a ausência de caráter informativo ou conteúdo relevante nas informações divulgadas no site. Disse que o mesmo se presta a consultar CPF, CNPJ, e verificar se determinada pessoa integra o quadro societário de alguma empresa, e então divulgar qual sua participação societária, o ramo de atividade exercido, qual a razão social e o nome fantasia, qual o capital social, quem são os demais sócios, qual o CNPJ da empresa, o endereço, telefone e endereço de e-mail do responsável. Alegou tratar-se de reformulação das ferramentas do site "tudo sobre todos", retirado do ar por determinação da Justiça Federal em 2015 Pugnou pela concessão de antecipação dos efeitos da tutela a fim de que: "seja solicitado ao Estado da Austrália, através do setor de Recuperação de Ativos/Secretaria Nacional de Justiça/Ministério da Justiça do Brasil, que interrompa a exibição dos dados pessoais dos demandantes, e não volte a fazê-lo até o julgamento final da demanda", bem como "informem os dados completos das pessoas físicas e jurídicas que criaram e mantém o site www.consultasocio.com, bem como que integram a empresa demandada, incluindo os respectivos IPs, logs de acesso e endereços de e-mails"; e ainda, "sejam as empresas que administram no Brasil os serviços de acesso a blackbones2 , serviço móvel pessoal (SMP) e serviço telefônico fixo comutável (STFC), intimadas a inserir obstáculos tecnológicos capazes de inviabilizar, até o julgamento da demanda, acesso ao site www.consultasocio.com (a exemplo do que já foi determinado judicialmente em relação a outro site similar, www.tudosobretodos.com, ou, alternativamente, a quaisquer informações pessoais, assim definidas em lei, associadas aos nomes próprios dos demandantes, sob pena de ineficácia do provimento"."	Intimidade, Bloqueio de conteúdos, Direito à informação, Interesse público.
Porta lógica e provedores de aplicação	12/05/2016	Art. 5º Art. 6º Art. 10º § 1°	"Ação de obrigação de fazer. Decisão que impôs ao provedor de aplicação (Google) o dever de informar o número da "porta lógica de origem" de determinados "IPs". Medida sem a qual haverá a impossibilidade de identificação de usuários que praticam ilícitos na rede mundial de computadores. Dever de fornecimento decorrente da interpretação conjunta dos dispositivos e princípios do marco civil da internet (lei n° 12.965/2014) Art.s 5º, 6º e 10). Rol do Art. 5º meramente exemplificativo. Decisão mantida. Recurso desprovido."	Privacidade, Provedores de aplicações, Dados pessoais, Dados cadastrais, Identificação clara e inequívoca, Redes sociais, Segredo de justiça, Anonimato, Direito de imagem, Porta lógica de origem.
Acesso ao WhatsApp em celular apreendido	19/04/2016	Art. 7º I, II e III	"Penal. Processual penal. Recurso ordinário em habeas corpus. Tráfico de drogas. Nulidade da prova. Ausência de autorização judicial para a perícia no celular. Constrangimento ilegal evidenciado. 1. Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial. 2. Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos."	Privacidade, Provedores de aplicações, Intimidade, Direito penal, Quebra de sigilo.
Envio de spam e ausência de interesse de agir	05/11/2015	Art. 2º I a VI.	"Responsabilidade civil. Envio de e-mail. Spam. Publicidade. Propaganda. Ato ilícito. Dano moral. Interesse jurídico. O interesse jurídico possui relação com a necessidade de ser ajuizada ação para solucionar um litígio. No caso, a situação, relacionada ao recebimento de e-mail ou mensagem de publicidade, pode ser solucionada por outros meios. Apelação não provida."	Privacidade, Provedores de aplicações, Danos morais, Spam, Danos materiais.

Direito ao esquecimento e sites de buscas	07/10/2015	Art. 19º	"Trata-se de ação de obrigação de fazer c/c danos morais e pedido liminar, alegando o autor que em 1999 fora investigado e denunciado em processo crime denominado pela mídia como "Máfia dos Fiscais", mas já teve extinta sua punibilidade em decorrência da prescrição da pretensão punitiva. Diz que através de pesquisas realizadas em seu nome nos sites de busca das rés "Google,", "Bing" e "Yahoo", existem diversos resultados vinculando-o às matérias jornalísticas publicadas na época e ao aludido fato pretérito, o que vem lhe causando sérios inconvenientes nos âmbitos pessoal, profissional e familiar. Afirma que apesar de notificadas, as rés se negaram a suspender a veiculação. (...). Deve-se prestigiar, no presente caso, o direito ao esquecimento (Enunciado 531 da VI Jornada de Direito Civil sobre o Art. 11 do Código), que visa a proteger, precipuamente, a dignidade da pessoa humana na sociedade da informação, em detrimento à liberdade de informação, uma vez que não se vislumbra interesse público na permanência da notícia nos sites de busca das rés (...)"	Privacidade, Provedores de aplicações, Intimidade, Provedores de pesquisa, Direito ao esquecimento.
Direito ao esquecimento e notícia desabonadora	07/10/2015	Art. 7º II	"Apelação cível. Direito civil. Lesão a direito da personalidade. Ação indenizatória c/c obrigação de fazer. Veiculação de notícia desabonadora atrelada à imagem dos autores. Pretensão que, além da compensação por danos morais, tem por escopo de evitar a associação do nome dos demandantes às notícias que envolvam supostas fraudes na emissão de carteiras falsas de juiz por tribunal arbitral e, ainda, em relação ao denominado "golpe do emprego na Petrobras", de acordo com o qual o primeiro autor prometia salário de r$ 1,5 mil, cobrava r$ 30,00 para dar uma palestra e mandava os candidatos esperarem em casa até convocação da empresa, a qual jamais ocorreria. Sentença de improcedência do pedido que merece reforma, sob enfoque do direito ao esquecimento 1- hipótese que possui assento constitucional e legal, considerando que é uma consequência do direito à vida privada (privacidade), intimidade e honra, assegurados pelo Art. 5º, v e x da cf e pelo Art. 21 do cc, sendo inclusive prevista no marco civil da internet (Art. 7º, i da lei nº 12.965/2014), com reflexos no tocante à dignidade da pessoa humana (Art. 1º, iii, da cf; en. Doutrinário 531 da iv jornada de direito civil do CJF). 2- matérias jornalísticas, ainda divulgadas nos sites vinculados ao sistema globo de comunicações, que possuem estrito cunho informativo, sem qualquer intenção de difamar os envolvidos, retratando investigação deflagrada pela polícia federal, que redundou em denúncia em razão dos ilícitos penais, em tese, praticados, dos quais, posteriormente, foram absolvidos (Art. 386, iii do CPP). 3- logo, embora não se cogite de abuso do direito de informar (Art. 220 cf c/c 187 do CC) e, com isso, afaste-se a pretensão lesão por danos morais (Art. 5º, x da CFC/c 17 do CC), sob a perspectiva do direito ao esquecimento, prospera o inconformismo dos recorrentes, haja vista a inexistência de interesse pela historicidade do fato. 4- autores absolvidos da prática dos ilícitos penais que lhes foram imputados. Daí ser legítimo o direito de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores, de natureza criminal, nos quais se envolveram, mas que, posteriormente, foram inocentados. 5- assim, embora não seja possível desvincular o nome do primeiro autor daqueles fatos, pois pulverizados em sites não vinculados ao sistema globo de comunicação (Art. 472 do CPC), é, ao menos viável, tal exclusão dos sítios mantidos ou divulgados pela apelada de qualquer notícia ou relato que os vincule aos episódios referidos na inicial, de cujos crimes foram absolvidos, fixando-se, para tanto, o prazo de cinco dias, após o trânsito em julgado, sob pena de multa diária de r$ 10 mil Art. 461, § 4º do CPC c/c súmula nº 410 do STJ) . Recurso a que se dá parcial provimento.	Privacidade, Provedores de aplicações, Remoção de conteúdos, Intimidade, Multa diária, Danos morais, Provedores de pesquisa, Direito ao esquecimento.
Direito ao esquecimento e interesse público	07/10/2015	Art. 2º	"AGRAVO DE INSTRUMENTO - Antecipação da Tutela - Referências ao autor em matéria jornalística – Pretensão que a Google crie mecanismos para quando se buscar seu nome, o mesmo	Liberdade de expressão, Privacidade, Provedores de

		Art. 3º I.	não conste de seus mecanismos de busca, ou qualquer outro indexador de seu banco de dados - Decisão agravada que indeferiu liminar - Para concessão da antecipação da tutela não basta a relevância da fundamentação, mas há, ainda, que se demonstrar os requisitos legais e as condições da ação, pois na medida antecipada, conceder-se-á o exercício do próprio direito afirmado pelo autor, ainda que em caráter provisório É necessária a observância das garantias do contraditório e da ampla defesa para verificação de eventual ilicitude a ser coibida, não se justificando, nesta fase, a supressão das veiculações, sob pena de violação ao princípio constitucional da livre manifestação do pensamento, no que se inclui a divulgação de fatos de interesse público - Ausência dos requisitos legais - Recurso desprovido."	aplicações, Intimidade, Bloqueio de conteúdos, Provedores de pesquisa, Direito ao esquecimento, Criptografia, *Hackers.*
Informações públicas e segredo de justiça	29/09/2015	Art. 3º II Art. 7º I	"Ação de obrigação de fazer - Antecipação de tutela indeferida - Insurgência do autor - Não acolhimento - Pesquisa realizada no site da requerida apontando link (jus Brasil) com a indicação de processo criminal em nome do autor - Informações obtidas junto ao site do Poder Judiciário - Diário Eletrônico de Justiça - Informações públicas - Não preenchidos os requisitos legais que autorizam a concessão da medida para o reconhecimento do segredo de justiça, bem como da remoção do nome do autor do resultado de buscas na rede mundial de computadores - Ausência de afronta ao direito de privacidade - Requerida que, nesta fase processual, não pode ser compelida a reter conteúdos difundidos na internet em sítios eletrônicos que não são de sua propriedade - Decisão mantida - Recurso não provido."	Privacidade, Provedores de aplicações, Segredo de justiça, remoção de conteúdos, bloqueio de conteúdos, provedores de pesquisa, direito ao esquecimento.
Inquérito policial e acesso a aparelho celular	21/09/2015	Art. 22º	"(...) 09. O advento da Lei nº 12.965/2014 Marco Civil da Internet, regulou a utilização na internet no Brasil e estabeleceu direitos e deveres dos usuários e administradores da rede, além de possibilitar o acesso aos registros de conexão e de acesso dos usuários quando tal medida afigurar-se necessária ao conhecimento de dados essenciais a deslinde do litígio judicial. 10. Com efeito, o Art. 22 da referida norma dispõe, in verbis: Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. 11. Destarte, a quebra do sigilo de dados na persecução criminal será medida imperiosa à elucidação de delitos praticado na ambiência da rede mundial de computadores, notadamente para identificação correta do suposto autor do crime. 12. Impende salientar que o acesso a referidos registros para fins de identificação do autor do crime não viola o Art. 5º, X e XII, da Constituição de 1988, na medida em que não identifica a comunicação de dados, mas os dados em si os quais com aquela não se confunde, conforme melhor entendimento doutrinário e jurisprudencial. (...)"	Privacidade, Intimidade, Direito penal, Quebra de sigilo.
Nome de fantasia e titularidade de e-mail	05/08/2015	-	"Civil e processo civil - ação cominatória - provedor de internet - fornecimento - dados de conta de e-mail - usuário e senha - obrigação - ausência de previsão legal. Não há previsão legal que obrigue o provedor de internet a fornecer usuário e senha de e-mail criado por ex-funcionário da empresa requerente, mesmo que o prefixo do e-mail coincida com o nome de fantasia daquela, já que a titularidade da conta, usuário e senhas pertencem ao seu criador."	Privacidade, Provedores de aplicações, Dados cadastrais, Quebra de sigilo, Propriedade intelectual, Segurança da informação.
Remoção e Bloqueio de site sediado no exterior	30/07/2015	Art. 3º I, II e III Art. 7º I e VII	"Cuida-se de ação cautelar preparatória, movida pelo Ministério Público Federal em face da empresa TOP DOCUMENTS LLC, pessoa jurídica sediada no exterior, mediante a qual requer, em caráter liminar, sem oitiva da parte contrária, que: a) seja determinado às empresas que, no Brasil, administram serviços de acesso a backbones, que neles insiram obstáculos tecnológicos capazes de inviabilizar, até o julgamento definitivo do processo principal, o acesso ao site "TUDO SOBRE	Privacidade, Dados pessoais, Dados cadastrais, Remoção de conteúdos, Direito de imagem, Danos morais, Bloqueio de conteúdos, Interesse público.

		Art. 10º § 1º e Art. 11º § 2º.	TODOS" (http://tudosobretodos.se), em todo território nacional; b) seja determinado às empresas que, no Brasil, administram Serviço Móvel Pessoal e Serviço Telefônico Fixo Comutado, para que neles insiram obstáculos tecnológicos capazes de inviabilizar até o julgamento definitivo do processo principal, o acesso ao site "TUDO SOBRE TODOS" (http://tudosobretodos.se), em todo território nacional; c) que seja solicitado ao Reino da Suécia, via Departamento de Recuperação de Ativos/Secretaria Nacional de Justiça/Ministério da Justiça do Brasil, a retirada provisória da internet do aludido site, hospedado no toplevel domain (TLD) desse país, bem como que informe a este Juízo os dados completos das pessoas físicas que o criaram e que o mantêm, inclusive números de IP, logs de acesso e endereços de e-mail."	
Direito ao esquecimento e acesso a informação	28/07/2017	-	"Civil. Internet. Provedor de pesquisa. Google brasil. Exclusão de resultados de pesquisa. Inadmissibilidade. Direito da coletividade à informação. Art. 220, § 1.º, da constituição federal. 1. Não se mostra possível impor ao provedor de pesquisa qualquer restrição nos resultados das buscas efetuadas por seus sistemas, seja pela inviabilidade técnica e jurídica, ante o imenso volume de informações e acessos diários, seja pela impossibilidade de se obstar o livre exercício de liberdade de expressão 2. Em se aplicando o princípio da proporcionalidade e sopesando o direito da coletividade à informação, frente ao direito individual à intimidade e à privacidade, opera-se uma superposição da garantia da liberdade de informação assegurada pelo Art. 220, § 1.º, da CF. 3. Recurso conhecido e provido."	Liberdade de expressão, Privacidade, Provedores de aplicações, Provedores de pesquisa, Direito ao esquecimento, Liberdade de informação.
Auditoria operacional no INSS e Marco Civil	22/07/2015	Art. 24º III, IV e X Art. 25º	"Auditoria operacional. Avaliação dos serviços previdenciários eletrônicos disponibilizados ao cidadão pela previdência social. Oportunidades de melhoria no direcionamento, monitoramento e avaliação do programa. Recomendações ao ministério da previdência e ao instituto nacional do seguro social (...) 35. A Lei 12.965/2014, Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, e, ao dispor sobre a atuação do poder público, estabelece diretrizes para o desenvolvimento da Internet no Brasil, das quais cabe destaque no âmbito deste trabalho: a. promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos; b. prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos. c. facilidade de uso dos serviços de governo eletrônico; e d. promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;"	Privacidade, Provedores de conexão, Provedores de aplicações, Dados pessoais, Dados cadastrais, Direito à informação, Segurança da informação, Interesse público.
Fatos públicos reais e liberdade de expressão	25/06/2015	Art. 3º I e II Art. 4º II	"Agravo de instrumento. Ação de obrigação de fazer c/c indenização por danos morais e pedido de antecipação de tutela. Crítica e divulgação de fatos públicos reais na internet. Pessoa pública. Ausência de conteúdo ofensivo. Improvimento. I - A recente Lei nº 12.965, de 23 de abril de 2014, denominada Lei do Marco Civil, estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, entre eles a garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal (Art. 3º, I) e a proteção da privacidade (Art. 3º, II). Nela, também se previu que o uso da	Liberdade de expressão, Privacidade, Provedores de aplicações, Redes sociais, Remoção de conteúdos, Pessoas públicas.

			internet visa à promoção do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos (Art. 4º. II); II - [...] não induz responsabilidade civil a publicação de matéria jornalística cujo conteúdo divulgue observações em caráter mordaz ou irônico ou, então, veicule opiniões em tom de crítica severa, dura ou, até, impiedosa, ainda mais se a pessoa a quem tais observações forem dirigidas ostentar a condição de figura pública, investida, ou não, de autoridade, pois, em tal contexto, a liberdade de crítica qualifica-se como verdadeira excludente anímica, apta a afastar o intuito doloso de ofender" (STF - AI: 705630 SC , Relator: Min. CELSO DE MELLO, Data de Julgamento: 22/03/2011, Segunda Turma, DJe-065 DIVULG 05-04-2011 PUBLIC 06-04-2011 EMENT VOL-02497-02 PP-00400). III - agravo não provido."	
Ampliação da antecipação dos efeitos da tutela	03/06/2015	Art. 10º § 1º Art. 13º Art. 15º § 3º Art. 22º e parágrafo único	"Agravo de instrumento. Tutela antecipada concedida em parte. Inconformismo do autor. Pedido autoral para ampliar a antecipação de tutela. Acolhimento parcial. 1. Na esteira de precedentes desta E. Corte e sob inspiração das disposições inovadoras do Marco Civil da Internet (Lei Federal nº 12.965/2014), é o caso de se determinar a ampliação da antecipação dos efeitos da tutela, a fim de ordenar que as requeridas informem, ao juízo, os dados cadastrais e registros de navegação dos usuários indicados na forma como solicitados na minuta recursal. Necessidade de pronta identificação dos autores dos possíveis atos ilícitos cometidos presentes dos registros internos das corrés, para cruzamento com dados portados por provedores de acesso, sob pena de se transpor a garantia de sigilo de informações e privacidade do usuário como direito superior àquele que veda a manifestação em anonimato e preserva a intangibilidade e inviolabilidade da honra e imagem das pessoas, sejam elas naturais ou jurídicas. Decisão reformada. 2. Recurso provido em parte."	Privacidade, Provedores de aplicações, Registros de conexão, Dados pessoais, Registros de acesso a aplicações, Nudez ou atos sexuais, Dados cadastrais, Anonimato, Multa diária.
Direito ao esquecimento e bloqueio de resultados	21/05/2015	Art. 1º Art. 2º Art. 3º Art. 18º Art. 19º Art. 20º Art. 21º	"Apelação cível. Direito privado não especificado. Obrigações. Atos unilaterais. Ação de obrigação de fazer. Internet. Disseminação de postagens. Conteúdo ofensivo. Retirada do sistema de buscas. O interessado tem o direito de pretender que o responsável pela hospedagem na internet retire do sistema de buscas pelo seu nome o acesso a postagem que tenha por ofensiva. Não se trata de tolher a iniciativa jornalística ou a notícia, mas de preservar a privacidade e dados pessoais impedindo que sejam disseminadas em veículos sem aquele caráter por diversos do jornalístico. RECURSO PROVIDO, POR MAIORIA."	Privacidade, Provedores de aplicações, Dados pessoais, Bloqueio de conteúdos, Provedores de pesquisa, Direito ao esquecimento.
Vedação à obtenção de dados sem ordem judicial	24/04/2015	Art. 10º § 1º e § 3º	"Trata-se de Mandado de Segurança, com pedido de liminar, impetrado por TWITTER BRASIL REDE DE INFORMAÇÃO LTDA. em face do DELEGADO DE POLÍCIA FEDERAL, objetivando a obtenção de provimento jurisdicional que determine a anulação da requisição emanada da autoridade coatora que exigiu o fornecimento do máximo de dados possíveis, como o IP de acesso da máquina do responsável, datas de acesso, qualificação completa dos responsáveis e dados cadastrais do usuário (...). Requer, ainda, que seja determinado à autoridade coatora que se abstenha de instaurar inquérito policial ou adotar qualquer medida contrária à impetrante, seus representantes legais, responsáveis ou empregados, em decorrência da negativa de fornecimento de tais dados sem ordem judicial. (...)"	Liberdade de expressão, Privacidade, Provedores de aplicações, Registros de conexão, Dados cadastrais, Redes sociais, Intimidade, Interesse público.

Identificação por elementos além de URLs	24/02/2015	Art. 10º § 1º e § 3º	"agravo de instrumento - ação cautelar inominada - liminar deferida - Facebook - retirada de conteúdo ofensivo - indicação das URLs - medida dispensável - Art. 19, § 1º da lei 12.965 - indicação precisa do conteúdo - outros meios possíveis - decisão mantida - recurso não provido. - O Art. 19, § 1º da Lei 12.965/14 determina a indicação precisa do conteúdo ofensivo a ser excluído da internet, o que pode ser obtido por outros meios além da indicação das URLs. - Assim, havendo elementos suficientes para identificação precisa das publicações a serem retiradas da rede social, deve ser cumprida a ordem judicial. - Recurso não provido. Decisão mantida."	Privacidade, Provedores de aplicações, Identificação clara e inequívoca, Redes sociais, Remoção de conteúdos.
Provedor de conteúdo e contrafação autoral	03/09/2014	-	"APELAÇÃO. SUMÁRIO. RESPONSABILIDADE CIVIL. PROVEDOR DE CONTEÚDO DE INTERNET. DIREITO AUTORAL. CONTRAFAÇÃO. VÍDEO-AULAS DE CURSO DE ENSINO JURÍDICO. DANO MATERIAL E MORAL. 1. Réu que oferece serviços de internet de hospedagem, permitindo que usuários os utilizem como ferramenta para a criação e manutenção de homepages próprias. A Autora aduz que, não obstante tenha dado ciência acerca da utilização dos serviços para a prática de ato ilícito, consubstanciada na comercialização desautorizada de vídeo-aulas por ela produzidas, o provedor manteve-se inerte. Sentença que apenas confirmou a tutela antecipada, retirando a homepage do ar. Pretensão recursal da Autora de ver reparados os danos. 2. Agravo retido. Desprovimento. 2.1 Ilegitimidade ativa rejeitada. Autora que, além de ser cessionária dos direitos sobre a imagem dos professores que formam o corpo docente, produz as vídeo-aulas. 2.2. Ilegitimidade passiva afastada. Segundo a jurisprudência, embora não tenha o dever de fiscalização prévia, o provedor de conteúdo que, ciente da ilegalidade, não retira do ar a página virtual, responde solidariamente por danos causados pelo infrator, por culpa in omittendo, caso não incidam as regras do CDC. Inaplicabilidade do Art. 927, parágrafo único, do CC/02 e da responsabilidade objetiva a que se refere. Precedentes do STJ. Ademais, o Art. 104 da Lei nº 9.610/98 prevê a responsabilidade de quem perpetue a ilegalidade. 3. Não incidência das regras previstas na Lei nº 12.965/14 (Marco Civil da Internet), em respeito ao ato jurídico perfeito, reputado como aquele já consumado segundo a lei vigente ao tempo em que este foi praticado. Princípio tempus regit actum, estampado no Art. 6º da LINDB, que deve ser observado. 4. Sentença que, embora tenha reconhecido a responsabilidade do Réu, deixou de condená-lo a reparar os danos. A Lei nº 9.610/98 disciplina a proteção relativa aos direitos sobre a produção intelectual do autor. Seja qual for o modo de manifestação intelectual, afora os que são fruto de atividade intelectual de caráter abstrato e genérico (Art. 8º), são assegurados tanto direitos morais quanto os direitos patrimoniais ao autor sobre a exploração da obra criada, a teor do Art. 22 da LDA. Obras da Autora que são passíveis de proteção, conforme Art. 7º da LDA. 5. Contrafação que se caracteriza pela usurpação dos direitos do autor de obra de qualquer espécie, seja no campo literário, científico ou artístico, podendo-se falar em contrafação de obra escrita falada, televisada, contida em suportes físicos dos mais diversos, como livro, disco, DVD, CD, pen drive, site de internet etc. 6. Prática devidamente comprovada nos autos, inclusive mediante ata notarial. A veiculação do material fraudado é fisicamente imensurável, especialmente quando praticada no meio virtual, em que as mídias utilizadas permitem a duplicação constante da obra. Circunstâncias que fazem com que o dano, ainda que material e palpável, tenha um caráter difuso e incapaz de ser valorado precisamente. 7. Particularidade que foi levada em consideração pela LDA. Na impossibilidade de determinar esse número, o parágrafo único do Art. 103 da LDA confere como parâmetro para a fixação do dano o montante equivalente a três mil exemplares fraudados. Eram oferecidos 06 CDs a R$ 10,00 cada. Indenização de R$ 18.000,00. 8. Danos morais. Inocorrência.	Provedores de aplicações, Dados pessoais, Remoção de conteúdos, Direito de imagem, Direitos autorais, Danos morais, Danos materiais.

			Não obstante a possibilidade de a pessoa jurídica sofrer danos morais, a teor da súmula nº 227 do STJ, entendo que não houve danos à honra objetiva. 9. Reforma da sentença, apenas para condenar o Réu ao pagamento dos danos materiais. 10. Parcial provimento do recurso."	
Exclusão de vídeo supostamente ofensivo	03/12/2014	Art. 5º VII Art. 19º Art. 21º	"apelação cível. Obrigação de fazer. Youtube. Google. Exclusão vídeo. Conteúdo ofensivo. Mídia não juntada nos autos. Julgamento de mérito. Error in procedendo. Não configurado. Conteúdo indevido constatado por outros meios de prova. Remoção do conteúdo. Dano moral. Responsabilidade civil. Relação jurídica continuativa. Lei nova 12.965/14. Aplicabilidade. Dano decorrente de conteúdo gerado por terceiros. Provedor aplicações internet. Responsabilidade não configurada. Art. 19 e Art. 21. 1. O apontamento do endereço virtual (URL) pelo autor na exordial não se confunde com a produção da prova documental do conteúdo do vídeo, todavia, diante do regramento processual vigente (Art. 302 e Art. 334, CPC), o magistrado deve presumir verdadeiros os fatos não impugnados, bem como conhecer dos fatos que não dependem de prova. 2. A sentença que julga improcedente o pedido, com resolução de mérito, sem considerar o vídeo disponibilizado no link de internet não configura error in procedendo, ou seja, erro de procedimento do magistrado, porquanto tal prova documental não era essencial para a instrução válida do processo. 3. Constatado nos autos que o conteúdo gerado por terceiro no provedor de aplicações de internet é indevido, deve-se tornar indisponível o conteúdo apontado como infringente. 4. Aplica-se a regra de responsabilidade por danos decorrentes de conteúdo gerado por terceiros da Lei 12.965/14 à lide decorrente de conteúdo publicado por usuário na internet antes de sua vigência, desde que o conteúdo permaneça disponível, em razão dos efeitos da relação jurídica continuativa. 5. "(...) o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário." (Art. 19 da Lei 12.965/14) 6. "O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo." (Art. 21 da Lei 12.965/14) 7. Recurso conhecido, preliminar rejeitada. Apelação parcialmente provida".	Privacidade, Provedores de aplicações, Nudez ou atos sexuais, Remoção de conteúdos, Intimidade.
Crime contra a honra e violação da privacidade	13/11/2014	Art. 5º VI e VIII Art. 22º	"Apelação Criminal – crime contra a honra. Preliminares. Nulidade. Cerceamento de defesa. Inocorrência. Prova ilícita. Não configuração. Ausência de clausula de reserva jurisdicional. Não ocorrência de violação dos direitos à privacidade e intimidade. Mérito. Provas suficientes para a condenação. Oitiva das testemunhas. Bens jurídicos distintos. Honra objetiva e subjetiva. Necessidade do reconhecimento do concurso material entre os crimes atribuídos ao réu. Pena. Circunstâncias desfavoráveis. Circunstância agravante. Não configuração. Aumento. Necessidade. Afastamento da substituição da pena privativa de liberdade por restritiva de direito. Manutenção do regime aberto em face da ausência de impugnação específica. Limite ao efeito devolutivo do recurso. Parcial provimento ao apelo do querelante e negado provimento ao apelo do réu."	Privacidade, Registros de conexão, Registros de acesso a aplicações, Intimidade, Direito penal.

Exclusão de álbum com fotos íntimas	14/08/2014	Art. 7º I Art. 21º	"Trata-se de ação pelo rito ordinário, proposta por (...) em face da GOOGLE BRASIL INTERNET LTDA. em que a autora pede o deferimento de tutela antecipada para que a ré exclua o álbum de fotos da autora que se encontra no site da ré, a condenação da ré para exibir o IP do computador que hospedou as fotos íntimas da autora e de seus filhos e ao pagamento de indenização por danos morais (...)".	Privacidade, Provedores de aplicações, Dados pessoais, Nudez ou atos sexuais, Redes sociais, Remoção de conteúdos, Intimidade, Danos morais, Indenização.

Fonte: Elaborado pela autora[120]

[120] Este quadro foi organizado por meio da coleta de dados realizada no site do Observatório do Marco Civil da Internet (OBSERVATÓRIO DO MARCO CIVIL DA INTERNET, 201[-])