FACULDADE DE DIREITO DE VITÓRIA
PÓS GRADUAÇÃO STRICTU SENSU
MESTRADO EM DIREITOS E GARANTIAS FUNDAMENTAIS

GUSTAVO GOBI MARTINELLI

O DIREITO FUNDAMENTAL À PRIVACIDADE NO ESTADO CONTEMPORÂNEO: UMA ANÁLISE DA CRIPTOGRAFIA E DAS TECNOLOGIAS LIVRES

VITÓRIA
2015

GUSTAVO GOBI MARTINELLI

O DIREITO FUNDAMENTAL À PRIVACIDADE NO ESTADO CONTEMPORÂNEO: UMA ANÁLISE DA CRIPTOGRAFIA E DAS TECNOLOGIAS LIVRES

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória, como requisito para a obtenção do grau de mestre em Direito.

Orientador: Professor Doutor Aloísio Krohling.

VITÓRIA
2015

GUSTAVO GOBI MARTINELLI

O DIREITO FUNDAMENTAL A PRIVACIDADE NO ESTADO CONTEMPORÂNEO: UMA ANÁLISE DA CRIPTOGRAFIA E DAS TECNOLOGIAS LIVRES

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória, como requisito para a obtenção do grau de mestre em Direito.

Aprovada em: _____.

COMISSÃO EXAMINADORA:

_____

Prof. Dr. Aloísio Krohling.
Orientador

_____

Profa. Dra. Elda Coelho de Azevedo Bussinguer.

_____

Prof. Dr. Rodolfo da Silva Villaça

Dedico este trabalho a todos que possuem um *segredo*, e não desejam contá-lo a ninguém.

E, àqueles que acreditam que a Privacidade está chegando ao fim. Vocês desistem fácil demais.

AGRADECIMENTOS

Inicialmente, agradeço a Deus, por tudo o que sempre me proporciona, principalmente, pelas oportunidades.

Agradeço aos meus Pais, João e Therezinha, e as minhas irmãs, Fabricia e Daniela, pelo apoio, pela força e por tornarem o caminho percorrido no Mestrado mais ameno.

Agradeço à Accenture, nas pessoas dos profissionais Assen Zalfa, Odir Brasil, Marcela Costa, Luciano Pacheco e Renan Riso por terem me proporcionado todo o crescimento profissional que tive, e a oportunidade da realização desse Mestrado concedendo-me a licença necessária para isso.

Agradeço a toda a Equipe GED pelo carinho, consideração e pelas constantes trocas de conhecimento que sempre tivemos.

Agradeço à FDV – Faculdade de Direito de Vitória, nas pessoas dos Professores Antonio José Ferreira, Abikair, Paula Castello Miguel, Elda Bussinguer e Daury Cesar Fabriz, por acreditarem em meu trabalho, tornando possível a conquista do título de Mestre em Direito.

Novamente, e sempre, a Professora Elda Bussinguer, por ser essa pessoa cativante e estimulante que sempre vê no aluno os seus pontos positivos e os explora de forma a mostrar-lhe o seu verdadeiro potencial.

Ao Prof. Aloísio Krohling, pela constante orientação em todos os momentos do mestrado, sempre demonstrando que o conhecimento é um caminho seguro por onde se pode trilhar sem medo, mas não sem as mudanças positivas que ele proporciona.

Agradeço a Profa. Gilsilene Passon, pelo profissionalismo, carinho e exemplos, como professora e como pessoa, enfrentando com ternura os desafios e problemas que a vida nos impõe.

Ao Dr. Ronaldo Segundo, pois numa simples conversa conseguiu resolver uma angústia que há muito me assombrava, fazer um Mestrado de qualidade pesquisando o Direito Digital. Foi então que ele me orientou a procurar o Prof. Bruno Costa Teixeira, na FDV.

Ao Prof. Bruno Costa Teixeira, por ter me recebido e estimulado a minha entrada no Mestrado da FDV, e pelas constantes trocas de conhecimento que tivemos.

Aos Professores Alexandre Coura, Carlos Henrique Bezerra Leite, Thiago Fabres, André Filipe e João Maurício Adeodato, Ricarlos Almagro pelo profissionalismo no competente ensino do Direito em sala de aula.

Agradeço aos amigos Lorena e Lucas, por terem sido muito mais que amigos, mas verdadeiros fraternos na produção desse trabalho. Estou certo de que a vida nos reserva muitos momentos felizes e prazerosos além dos que já passamos juntos com nossas conversas. É um verdadeiro aprendizado estar com vocês.

As Amigas Elda Bussinguer, Ana Paula Luz Faria, Carolina Nunes e Luana Petry por tudo, mas, principalmente, pelo tempo que passamos juntos durante o congresso realizado no Peru, e pelo coeso trabalho em equipe que tivemos durante a organização do I Congresso Internacional de Bioética e Direitos Humanos – CONIBDH realizado na FDV.

Ao Prof. Gilberto Sudré, pela revisão das partes deste trabalho que abordam a tecnologia.

Aos Amigos Bruno Giovannotti, Emerson Scheidegger e Gilberto Sudré, por simplesmente, serem o que são, Amigos, e por terem me auxiliado de várias formas durante o caminho trabalhoso do Mestrado.

A Dra. Scheila Uliana Canal, pelo profissionalismo com que me orientou e sempre me orienta em nossas sessões de Análise.

Aos amigos Alex Canal, Alexandre Brandão, Bruno Gadelha, Caroline Simon, Danilo Negreiros, Dirce Nazaré, Fausto Gaia, Elias Canal, Elisete Meneghetti, Livia Frossard, Livia Cani, Márcio Kaó Yien, Ronaldo Félix, Sarah Rocha, Priscila Tinelli, Rafael Fávero, Wantuil Lima, por terem sido tão cordiais comigo e me recebido tão gentilmente, sendo as duas turmas das quais fiz parte por ter entrado no Mestrado no meio do ano.

“Não me refiro à confissão. Confissão não é traição. O que você faz ou diz não importa: o importante são os sentimentos. Mas se eles conseguirem me obrigar a deixar de amar você... Isso sim, seria traição.”

Ela considerou o assunto. “Não conseguem”, disse afinal. “É a única coisa que não conseguem fazer. Eles podem fazê-lo dizer qualquer coisa – *qualquer coisa* –, mas não podem fazê-lo acreditar nisso. Não podem entrar em você.”

“Não”, disse ele, um pouco mais esperançoso. “Não conseguem mesmo. É verdade. Não conseguem entrar em você. Se você conseguir sentir que vale a pena continuar humano, mesmo que isso não tenha a menor utilidade, você os venceu.”

(George Orwell, 1984, p.199)

RESUMO

O presente trabalho tem por finalidade estudar o direito fundamental à privacidade analisando os impactos que a Era da Informação trouxe sobre ele. Diante disso, questiona-se a possibilidade de se contra-utilizar a criptografia e as tecnologias livres como elementos garantidores para se reafirmar o direito fundamental à privacidade. Inicialmente, a segregação entre os domínios público e privado segundo Hannah Arendt são abordados, momento em que se analisam as esferas da política, do social e da privacidade, propondo-se a criação de mais duas esferas, a da vida privada e a da intimidade. Após isso, passa-se a analisar dois conceitos distintos de liberdade confrontado-os de forma a ressaltar qual melhor se correlaciona com a privacidade. Então, passa-se a analisar o direito fundamental à privacidade na era tecnológica segundo a legislação internacional para, assim, trazer as previsões constitucionais brasileiras desde a constituição de 1824 até os dias atuais, abordando também a legislação infraconstitucional existente. Já o segundo capítulo possui o condão de demonstrar quais as tecnologias que permeiam o cotidiano do indivíduo e como elas afrontam o direito à privacidade, da mesma forma que se trata o conteúdo das denúncias feitas pelo Snowden sobre o programa de monitoramento global dos Estados Unidos da América. Por fim, no terceiro capítulo, os impactos sobre a liberdade do ser são analisadas sob a ótica Jeremy Bentham, Glenn Greenwald e Zygmunt Bauman. Por conseguinte, a justificativa da segurança nacional como validadora da vigilância onipresente empreendida pela tecnologia é tratada. De igual modo, demonstra-se o interesse mercadológico na coleta de dados pessoais. Finalmente, a proposta de solução para o devassamento provocado pela tecnologia, que consiste no uso da Criptografia, do Software Livre e do Hardware Livre, é verificada, demonstrando como ela reafirma o direito fundamental à privacidade.

Palavras-chaves: Privacidade. Liberdade. Criptografia. Software Livre. Hardware Livre.

ABSTRACT

This research aims to study the Fundamental Right to Privacy analyzing the impacts brought over it by the Information Age. Therefore, it questions the possibility of counter-use encryption and free technologies as guarantors elements to reaffirm the fundamental right to privacy. Initially, the segregation between public and private domains from Hannah Arendt is analyzed, both, the spheres of political, social and privacy are treated, proposing the creation of two more spheres, the private life and the intimacy. After that, two distinct concepts of freedom are examined confronting them in order to point out which best correlates with privacy. So, the fundamental right to privacy in the technological age is observed under the international law to, then, bring the Brazilian constitutionals provisions, since the constitution of 1824 until nowadays, treating the existing infra legislation. In the second chapter, all the technologies that are used by, and how they affront the privacy right are understood, as well as, the Snowden's denunciation about the United States of America's global surveillance program too. Therefore, on the third chapter, the impacts over the personal freedom in the opinion of Jeremy Bentham, Glenn Greenwald and Zygmunt Bauman are analyzed. Consequently, the national security justification to allow the global surveillance is also questioned. Similarly, the market interests in the personal data collection are demonstrated. Finally, the proposed solution to the violations caused by technology, which is the use of encryption, Free Software and Free Hardware, is checked by demonstrating how it reaffirms the fundamental right to privacy.

Keywords: Privacy. Freedom. Cryptography. Free Software. Open Source Hardware.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA – *Advanced Research Projects Agency*

ASCII – *American Standard Code for Information Interchange*

CEO – *Chief Executive Officer*

EEPROM – *Electrically-Erasable Programmable Read-Only Memory*

ENIAC – *Eletronic Numerical Integrator And Computer*

FBI – *Federal Bureau of Investigation*

FSF – *Free Software Foundation*

FTP – *File Transfer Protocol*

FVEY – *Five Eyes*

HTTP – *Hypertext Transfer Protocol*

HTTPS – *Hypertext Transfer Protocol Secure*

IETF – *Internet Engineering Task Force*

IEEE – *Institute of Electrical and Electronics Engineers*

IMAP – *Internet Message Access Protocol*

IP – *Internet Protocol*

ISO – *International Organization for Standardization*

NSA – *Nacional Security Agency*

NSF – *National Science Foundation*

ONU – Organização das Nações Unidas

OSHWA – *Open Source Hardware Association*

POP3 – *Post Office Protocol v3*

PRISM – *Planning Tool for Resource Integration, Syncronization, and Management*

RFC – *Request for Comments*

RYF – *Respect Your Freedom*

TCP/IP – *Transmission Control Protocol / Internet Protocol*

SUMÁRIO

INTRODUÇÃO

As inovações tecnológicas, em especial a tecnologia da informação, trouxeram, e continuam trazendo, inúmeros benefícios para a humanidade. Talvez o primeiro deles seja a automação de atividades rotineiras, onde o usuário[1] entrega suas informações para que um computador realize diversas atividades sobre ela. Pode-se elencar ainda, como segundo benefício, o encurtamento das distâncias, grande parte devido a Internet, permitindo a qualquer pessoa estabelecer contato com outra em qualquer parte do globo terrestre. E isso com ou sem a utilização de câmeras com a transmissão da imagem dos interlocutores. Ainda nesse sentido, por meio dos avanços técnicos é possível saber, com uma pequena margem de erro, qual é a geolocalização[2] em tempo real de um indivíduo. Exemplos não faltam para continuar demonstrando como a tecnologia mudou vários aspectos do cotidiano, entretanto, não são apenas os benefícios que se observam.

Um aspecto relevante se encontra na forma como as pessoas estão utilizando a tecnologia, onde, a todo momento, elas provém informações privadas sem que, para isso, se certifiquem sobre o uso que será feito com seus dados. Cumpre salientar, desde já, que ainda assim, o fornecimento destas informações deriva de um ato de vontade do usuário. O ato de vontade aqui referenciado corresponde a liberdade que a pessoa possui em fornecer ou não uma informação pessoal. Quando alguém fornece seu endereço residencial, este entregou a outrem a possibilidade de se colocar na porta de sua casa. No entanto, as informações que estão dentro dela continuam sob a proteção e em poder do proprietário daquele imóvel. Transferindo esse exemplo simples para o mundo virtual, numa analogia muito pertinente, quando se fornece o endereço eletrônico (*e-mail*) para alguém, também se abriu uma possibilidade para que esse indivíduo venha a ter acesso ao interior de sua casa, ou melhor dizendo, ao computador, que é um concentrador de informações, contendo diversos dados sobre o proprietário do referido endereço eletrônico. Diferente do endereço residencial, aqui os limites físicos não se impõem ao que é virtual.

1 O termo usuário ou internauta designam pessoas físicas ou jurídicas que utilizam a tecnologia, em especial, a Internet.
2 Geolocalização diz respeito as coordenadas estabelecidas dentro da planeta Terra, segundo a latitude e longitude de uma pessoa ou objeto.

Além disso, de forma mais comum, quando um internauta navega[3] na rede mundial, vários sites realizam uma verdadeira monitoração para coletar dados sobre o que ele visualizou e quanto tempo permaneceu em determinada página, ocorrendo também, o compartilhamento dessas informações com outras empresas, que se valem delas para mapear o perfil desse usuário, podendo propor produtos ou serviços especificamente para ele.

Vale citar também, as redes sociais, como, por exemplo, o Facebook[4], o Instagram[5] ou o LinkedIn[6] que, a todo momento, possuem o poder de vigiar seus usuários em suas conversas privadas, bem como as interações que eles realizam com as informações que são exibidas nessas mídias. Sobreleva ressaltar ainda, o constante dos termos de uso desses sites, que informam que os dados de seus usuários podem ser vendidos ou compartilhados com seus parceiros. E várias são as fontes de informação sobre o indivíduo. Por exemplo, a rede Instagram proporciona interações entre pessoas através de imagens. O LinkedIn é um ambiente virtual para relacionamentos de contatos profissionais. Caso os dados de todas essas fontes sejam coletados e processados, muitas informações sobre um indivíduo se tornarão públicas, ainda que contra a sua vontade. Isso permitirá o conhecimento de várias características sobre um usuário, assim como, as manifestações de vontade e opiniões que ele, porventura, tenha realizado.

Nota-se, então, os esforços para se conseguir qualquer tipo de dado sobre quem esteja utilizando um determinado serviço. A hipérbole que afirma que “informação é poder” se confirma, principalmente, na era da informação. No momento em que nossas informações pessoais se transformam em mercadoria – e as pessoas em produto – entre várias empresas de diferentes nacionalidades, importando, inclusive, para governos, verifica-se que é preciso protegê-las. Esse é o ponto principal deste trabalho, pois serão analisadas as questões que envolvem o direito fundamental à privacidade sob a ótica do impacto da tecnologia.

---

3 Navegar na Internet significa está conectado à rede mundial de computadores.
4 O link de acesso para o Facebook é https://www.facebook.com .
5 O link de acesso para o Instagram é https://instagram.com .
6 O link de acesso para o LinkedIn é https://www.linkedin.com .

Ressalte-se, novamente, o interesse que muitas nações estão desenvolvendo no monitoramento das informações que trafegam diariamente pela Internet. Logo, é preciso analisar até que ponto esse monitoramento se mostra nocivo aos usuários da grande rede.

Fica claro, assim, que se os dados pessoais possuem valor no cenário atual, é preciso protegê-los como forma de se reafirmar o direito fundamental à privacidade, uma vez que, a norma jurídica, por si só, não tem conseguido reduzir o alcance intrusivo da tecnologia.

Para o computador, os dados são um objeto de trabalho que servirão para a execução de análises diversas. E quando se verifica a existência de métodos para essa tarefa, nasce a preocupação sobre como isso será feito. Pois não se sabe qual é a finalidade da coleta dessas informações. O que pode gerar, inclusive, um estado de exceção permanente.

Portanto, o diferencial desta pesquisa se encontra no estudo realizado sobre como a tecnologia pode assegurar o direito fundamental à privacidade na era da informação, partindo da premissa de inteligência e contrainteligência, ou seja, se pelo uso da tecnologia, direitos fundamentais são fragilizados, é preciso entender como se pode contra-utilizar a tecnologia de forma a garanti-los. Logo, o objetivo deste trabalho é analisar o direito fundamental à privacidade de forma a responder a seguinte questão: com o advento da era da informação, a contra-utilização de tecnologias como a criptografia, o software livre e o hardware livre servem como elementos garantidores para se reafirmar o direito fundamental à privacidade?

Para isso, o presente estudo se digna a atingir os seguintes objetivos específicos:

- Apresentar a importância da distinção entre o domínio público e privado a partir da visão de Hannah Arendt;
- Analisar as diferenças entre a liberdade em Robert Alexy e a liberdade em Jean-Paul Sartre;

- Apresentar um breve histórico sobre o computador e a Internet, descrevendo as principais tecnologias de interceptação e análise de dados pessoais, identificando como elas fragilizam a privacidade;
- Apresentar o evento do monitoramento global denunciado por Edward Snowden, analisando-o segundo as críticas de Glenn Greenwald;
- Analisar como a criptografia e as tecnologias livres podem reafirmar o direito fundamental à privacidade;

Propõem-se a hipótese de que a própria tecnologia pode ser utilizada para reafirmar o direito fundamental à privacidade.

O quadro teórico do presente trabalho busca como fundamentos o pensamento em Hannah Arendt e em Jean-Paul Sartre.

Para tanto, no primeiro capítulo, são apresentadas as características que demonstram a importância da existência das esferas do público e do privado. Assim, passa-se a analisar dois conceitos distintos de liberdade confrontado-os de forma a ressaltar qual melhor se correlaciona com a privacidade. Diante disso, aprofundam-se as questões do privado, analisando a sua segregação entre privacidade, vida privada e intimidade. De modo a observar os direitos e garantias fundamentais, as principais normas internacionais e brasileiras, constitucionais e infraconstitucionais, que asseguram a privacidade são trazidas ao bojo deste trabalho.

No segundo capítulo, é feita a relação entre o romance 1984, de George Orwell, e o uso da tecnologia na atualidade. Então, um breve histórico do computador é apresentado demonstrando os motivos que o levam a ser fonte de confiança para seus usuários, onde estes depositam, cada vez mais, suas informações privadas e íntimas. Por conseguinte, o histórico da Internet e a sua forma de funcionamento também são tratados, desvelando, especificamente, onde ela fere o direito fundamental à privacidade. Logo após, as principais tecnologias utilizadas atualmente são abordadas de forma discriminada, tais como: os *cookies*, as Smart TVs, os *Smartphones*, as Mídias Sociais, a Computação em Nuvem, o Big Data e os

Algoritmos Preditivos, bem como, a Internet das Coisas. Outrossim, é explicado como ocorre o monitoramento global realizado pelos Estados Unidos da América, momento em que, demonstra-se o aparelhamento estatal com essa finalidade.

Por fim, no terceiro capítulo, as contribuições desta pesquisa são obtidas. Em primeiro lugar, os danos do monitoramento global e da coleta de dados pessoais são explicados. Em conformidade com isso, o Panóptico de Jeremy Bentham é abordado. Em seguida, são analisadas as considerações de Glenn Greenwald e Zygmunt Bauman. A partir daí, a hipótese e a justificativa se confirmam, onde são abordados o histórico da criptografia, suas principais técnicas, e, como ela assegura o sigilo das comunicações e dos dados pessoais. De forma a corroborar com a importância da criptografia, é feito um breve relato de movimentos que se fundam nela, como os Cypherpunks, o site Wikileaks e a Internet Profunda, também conhecida como *Deep Web*. De igual modo, os conceitos de software e hardware livre são explanados demonstrando como eles se prestam a resguardar as informações de seus usuários. Concluindo, constata-se a necessidade e efetividade da criptografia e das tecnologias livres como forma de reafirmar o direito fundamental à privacidade.

Por esse motivo, o presente estudo se justifica, uma vez que, é possível notar interesses sobre o controle das informações para se ter acessos aos dados pessoais de forma indiscriminada, e, em muitos casos, sob o subterfúgio da segurança nacional. De forma a corroborar, com isso, vale mencionar a declaração de Vint Cerf (TC, 2013), considerado um dos fundadores da Internet, que é bastante impactante, pois, para ele: “A privacidade pode ser uma anomalia[7].”

Ainda nesse sentido, observando-se como a tecnologia propicia todo o tipo de monitoramento, umas das poucas formas de se proteger o direito fundamental à privacidade na era tecnológica, que é a criptografia, vem sendo alvo de críticas onde, inclusive, alguns governantes sugerem a existência de uma forma na qual a polícia tenha acesso a uma “chave mestra” cuja qual, seja capaz de revelar qualquer conteúdo que tenha sido cifrado. Essa foi a declaração feita pelo Presidente dos

7 No original: *Privacy may be an anomaly*.

Estados Unidos da América, Barack Obama, após reunir-se com o Primeiro Ministro Britânico, David Cameron (EXAME, 2015).

Finalmente, foi escolhida uma metodologia que melhor se aplica ao atendimento do problema formulado e dos objetivos especificados de forma a enfrentar todas essas complexas questões, que é o método do Múltiplo Dialético, pois este se presta como fio condutor, a analisar as oposições e contradições relativas a tão recente temática que correlaciona os problemas observados entre o direito fundamental à privacidade e a tecnologia.

1. ESPAÇOS LIMÍTROFES: A SEGREGAÇÃO DOS DOMÍNIOS PÚBLICO E PRIVADO E A IMPORTÂNCIA DA EXISTÊNCIA DA PRIVACIDADE.

Antes que se trate os impactos da tecnologia sobre a privacidade, é preciso, primeiro, definir o que é privacidade e analisar os limites das esferas público, social e privado, evidenciando a importância da existência e mantença do espaço privado, cujo estudo de Hannah Arendt, em sua obra A Condição Humana, é feito com profundidade, servindo como pedra angular[8] do presente trabalho.

A partir daí, os conceitos de liberdade em Robert Alexy e Jean-Paul Sartre são confrontados para que a correta acepção da palavra liberdade, quando relacionada com a privacidade, seja obtida.

Após isso, uma análise sobre os elementos da privacidade é feita de forma a questionar a existência de uma segregação entre privacidade, vida privada e intimidade, demonstrando qual a relação entre elas, e a necessidade de se classificarem dessa forma. Nesse momento, uma breve definição sobre o que vem a ser privacidade é feita.

Em seguida, o regramento existente sobre a privacidade é analisado, evidenciando-se as principais previsões legais internacionais e nacionais sobre ela.

Desta feita, após tratar todos esses pontos, passa-se a análise sobre como a tecnologia vem dilapidando a privacidade.

Contudo, é de extrema importância que, inicialmente, faça-se uma abordagem sobre o método utilizado como fio condutor da elaboração e solução das questões aqui analisadas. Trata-se do Múltiplo Dialético, de autoria do Prof. Dr. Aloísio Krohling (2014).

8 O termo Pedra Angular significa alicerce, uma vez que, a pesquisa realizada sobre o privado partiu das considerações feitas por Hannah Arendt no segundo capítulo de sua obra A Condição Humana.

1.1. DA METODOLOGIA: O MÚLTIPLO DIALÉTICO

A palavra grega *Méthodos* nasce da junção de dois outros termos, quais sejam, *metá* e *hodós*. Segundo Krohling (2014, p. 28-29), a palavra *metá* significa “ir além do factual”, onde o termo *hodós* traduz-se em caminho, direção. Diante disso, método é o caminho certo ou o caminho escolhido dentre outras opções. Logo, o múltiplo dialético é o caminho escolhido por se mostrar o mais adequado para nortear as questões e soluções acerca do direito fundamental à privacidade.

Isso porque, os próprios dizeres de Hannah Arendt (2014, p.31) ressaltam a importância do discurso, afirmando que “[...] o ato de encontrar as palavras certas no momento certo, independentemente, da informação ou comunicação que transmitem, constitui uma ação.” Vale citar que para a referida autora, ação quer dizer a “[...] única atividade que ocorre diretamente entre os homens, sem a mediação das coisas ou da matéria, corresponde à condição humana da pluralidade, ao fato de que os homens, e não o Homem, vivem na Terra e habitam o mundo.” (ARENDT, 2014, p. 9)

Sobreleva ressaltar que, para Krohling (2014, p. 35), o fundador da Múltiplo Dialético foi Anaximandro de Mileto (611 – 547 A.C.), pois suas teorias são “[...] sinônimo de pluralismo e multiplicidade”. Como forma de demonstrar isso, para o referido filósofo, o princípio que deu origem a todas as coisas se trata de algo ilimitado, que, em determinados momentos, se “[...] confunde com o *kháos* [...]”. Lembrando-se que *kháos*, para os gregos, não significa desordem, mas sim, criatividade. “*Kháos* é uma imagem mítica que no seu bojo tem o ser e o não-ser.” É por esse motivo que “a dialética como tensão ou oposição entre contrários já aparece em Anaximandro.” (KROHLING, 2014, p. 36).

Logo, a argumentação e o debate, são peças fundamentais para a interação humana. A dialética demonstra a busca do conhecimento por meio de oposições, como dia e noite, e contradições, como real e não-real, afirmação e negação.

Entretanto, para que isso seja possível, é condição *sine qua non* a presença do múltiplo. Isso porque, alguns filósofos refutam o múltiplo, se limitando ao uno.

Tem-se, como exemplo, Parmênides de Eleia (530 – 460 A.C.), considerado o fundador do uno *stricto sensu*. Isso quer dizer que, "o ser é uno, eterno, não gerado e imutável." (KROHLING, 2014, p. 38). Ou seja, para Parmênides, existe apenas o ser, jamais chegando a existir o não-ser. Isso impede a oposição e a contradição, tão necessários a dialética.

É com Heráclito de Éfeso (540 – 470 A.C.) que o dinamismo é introduzido no pensamento grego, pois, para ele, tudo se transforma. "O não-ser, a alteridade e o **múltiplo** exitem em todo ser e produzem a mudança constante." (KROHLING, 2014, p. 39). Símbolo de sua teoria, um de seus ensinamentos ecoa na multiplicidade, pois dentro de seu pensamento "ninguém se banha duas vezes na mesma água do rio, pois tudo corre, tudo flui." Para Krohling (2014, p. 40), "Heráclito propunha o **múltiplo dialético**; Parmênides, o **uno** *stricto sensu*."

O primeiro autor a utilizar o termo dialética foi Zenão de Eleia (490 – 430 A.C.). Mas foi com os Sofistas (Séc. V e IV A.C.) que a dialética se iniciou como diálogo (KROHLING, 2014). Todavia, a construção da dialética teve a contribuição de Sócrates (470 – 399 A.C.), Platão (428 – 347 A.C.), Aristóteles (385 – 322 A.C.), tendo, inclusive, este último, insculpido a contradição e a oposição de opostos à dialética. Já os Estoicos e os Céticos utilizaram a dialética como método da lógica.

Na Idade Média, Nicolau de Cusa (1401 – 1464) compatibilizou a unidade com a diversidade, ou seja, a correlação entre os opostos. Assim, Krohling (2014, p. 58) conclui que este "[...] é um movimento que aponta na direção do que hoje designaríamos como múltiplo dialético e pluralismo."

Entretanto, é na Modernidade que a dialética tem seu estudo aprofundado, como o realizado por Hegel (1770 – 1831), que

> utiliza todas as filosofias existentes antes da sua. Ele mesmo é uma espécie de síntese do pensamento ocidental. Para ele, o universo, a realidade, é

> racional. Portanto, deve-se buscar uma razão e não somente uma causa para o universo. Com isso quer se mostrar que este mesmo mundo não é o efeito de um princípio e, sim, uma consequência que vem de uma razão. (KROHLING, 2014, p. 64)

É dele a tríade tese, antítese e síntese. Para Hegel, mudar é uma etapa do processo dialético, com as coisas evoluindo por conterem em seu interior, a sua própria negação. Nesse sentido, há dialética em tudo segundo uma razão.

Contudo, Marx (1818 – 1883), profundo conhecedor de Hegel, interpretou a dialética hegeliana ao que se combinou chamar de dialética invertida, pois "[...] Marx virou Hegel de cabeça para baixo [...]" (KROHLING, 2014, p. 68), uma vez que, Hegel acreditava que tudo possuía uma razão, mas Marx o contesta afirmando que a razão não é capaz de administrar todas as variáveis do real. "O real é complexo demais. E dinâmico demais, pois tudo é sempre movimento. O íngreme e plano. Existe tríade: a tese, a antítese e a síntese." (KROHLING, 2014, p. 69)

O diferencial de Marx se encontra na utilização da história da humanidade como forma de se compreender o presente e o futuro, analisando criticamente o passado. Convencionou-se chamar esse método de histórico-dialético.

Essa observação de Marx da história da humanidade representa um rompimento, segundo ele, com a filosofia tradicional. É dele a famosa frase: "até agora os filósofos limitaram-se a interpretar o mundo; trata-se agora é de transformá-lo."

Mas é com a reinterpretação de Marx, feita por Gramsci (1891 – 1937), que se verifica que a "[...] história não tem um único significado, bem como a verdade não se confunde com dogma nem com monismo. Em tudo se verifica o múltiplo, o pluralismo, a diversidade." (KROHLING, 2014, p. 75). Isso porque, Gramsci encarou a dialética como uma nova forma de entender a lógica clássica (KROHLING, 2014).

Deve destacar que a história é repleta de acontecimentos que revelam contradições e oposições que podem ser transportadas para a dialética. A ideia do múltiplo nos contextos histórico e dos direitos humanos e fundamentais revela seu atributo mais importante, a interculturalidade. "É essa dimensão histórica repleta de contradições

que nos revela o fio condutor da história que estamos chamando de múltiplo dialético.” (KROHLING, 2014, p. 75). Frise-se que a dialética em Gramsci contempla a tríade tese, antítese e síntese.

Além disso, Gramsci trouxe a importante contribuição de incorporar o devir, permitindo que a dialética permaneça aberta a mudanças, propiciando uma síntese mais próxima da verdade (KROHLING, 2014).

De igual modo, a dialética negativa de Teodoro Adorno (1903 – 1969) e de Enrique Dussel (1934 –), com sua analética e anadialética, foram de enorme contribuição e também integram o múltiplo dialético.

Por esse motivo que ao se tratar do direito fundamental à privacidade na era da informação, foi preciso escolher um método que possuísse o alcance necessário a sua compreensão. O múltiplo dialético perpassa as dialéticas, dialogando com estas, permitindo uma análise mais profundas a questões ligadas aos direitos e garantias fundamentais.

> Numa visão de perspectiva, dentro de uma análise crítica da história, a dialética auxilia uma compreensão mais adequada, e de uma maneira mais eficiente, que nos proporciona uma pavimentação da longa estrada que temos de percorrer, possibilitando que a humanidade, numa postura ética, consiga superar as contradições e se entender, superando sempre os obstáculos históricos impeditivos de uma interculturalidade e consequente reaproximação entre os povos, facilitando assim a diminuição dos abismos existentes para a concretização e efetivação dos direitos e das garantias fundamentais. (KROHLING, 2014, p. 78)

Ainda nesse sentido, Krohling (2014, p. 91) ensina que “[...] os direitos humanos fundamentais são construídos dialética e historicamente na perspectiva cultural de cada povo e Estado nacional.” Portanto, ainda que outros métodos apontem suportar as contradições e oposições verificadas na pesquisa sobre o direito fundamental à privacidade na era da informação, o múltiplo dialético é aquele que se mostrou mais adequado a analisar, dentre outras proposições, os paradigmas rompidos com o surgimento da tecnologia.

Isso, *de per si*, demonstra a necessidade do múltiplo dialético, pois não há que se falar em direitos humanos e fundamentais num método que não se presta a trazer ao bojo do debate, a multiplicidade, o multiculturalismo, a alteridade e o interculturalismo, pilares necessários para a mais correta e justa discussão.

De acordo com Krohling (2014, p.98),

> diante dos fundamentalismos emergentes, tanto no Ocidente como no Oriente, defende-se o diálogo ou, melhor, o duólogo, entre as culturas, para o reconhecimento gradativo dos direitos humanos, fundamentado na ética da dignidade da pessoa humana e da vida digna de todos os seres viventes.

Assim sendo, o presente trabalho seguirá o caminho do múltiplo dialético por ser o fio condutor a tratar das questões que são postas na análise do direito fundamental à privacidade na era da informação.

1.2. OS DOMÍNIOS PÚBLICO E PRIVADO

Precipuamente, há que se salientar que para se analisar a temática da privacidade, antes, é preciso revisitar o estudo dessa matéria feito no segundo capítulo da obra de Hannah Arendt (2014). Em seu livro, a autora explica três atividades humanas fundamentais que, juntas, significam a expressão *vita activa*. A primeira delas é o trabalho, que se perfaz num processo natural, ou seja, aquilo que é inerente ao corpo humano. A segunda, a obra, é tudo aquilo feito na existência humana, se tratando de coisas não naturais, que se traduzem em itens produzidos pelo ser humano. Já a terceira, a ação, recebe uma atenção maior, pois é a "[...] única atividade que ocorre diretamente entre os homens, sem a mediação das coisas ou da matéria, corresponde à condição humana da pluralidade, ao fato de que os homens, e não o Homem, vivem na Terra e habitam o mundo." (ARENDT, 2014, p. 9)

Por esse motivo, a ação é responsável pela socialização do indivíduo, pois "todas as atividades humanas são condicionadas pelo fato de que os homens vivem juntos, mas a ação é a única que não pode sequer ser imaginada fora da sociedade dos

homens. […] Só a ação é prerrogativa exclusiva do homem;" (ARENDT, 2014, p. 27-28). Nesse ínterim, surge, também, a esfera do social, que permeia ambos os domínios, público e privado.

De forma catedrática, Paula (2010, p. 52) adverte que na sistematização feita por Hannah Arendt (2014), não há uma distinção clara sobre as palavras domínio e esfera, onde, em muitos momentos, estas palavras são utilizadas como sinônimos, ainda que o título do segundo capítulo de sua obra seja "os domínios público e privado" (ARENDT, 2014, p.22). Desse modo, para Paula (2010, p. 52) "[...] é possível observar que ela compreende o público e o privado como dois domínios mais amplos, dentro dos quais se localizam as esferas política, social e da privacidade […]." Sendo assim, o texto contemplará a argumentação de acordo com essa orientação.

Como já informado, Hannah Arendt (2014) organizou seu estudo sobre os domínios do público e do privado no segundo capítulo de sua obra iniciando sua análise na questão do homem enquanto animal social e político. Logo após, ela enfrenta os impactos da *pólis* sobre a família. A partir daí, ela aduz o surgimento da esfera social. Por conseguinte, ela analisa o domínio público (comum) e o privado (propriedade), e, a esfera social com o domínio privado. Por fim, termina sua análise no subtítulo "a localização das atividades humanas".

Insta destacar que não é o foco da presente dissertação atacar também a questão sobre o *zoon politikon* de Aristóteles e a política entre os homens, segundo o pensamento de Hannah Arendt[9], mas tão somente, sobressaltar o conteúdo de seus ensinamentos quanto aos domínios público e privado.

A segregação entre o público e o privado reporta-se a organização política na Grécia antiga. Para os gregos, o "lar e a família" não eram o centro da associação natural da organização política de uma cidade-Estado. Na verdade, foram criadas duas percepções, uma que se reportava ao que era próprio (*idion*) e outra que se tratava do que era comum (*koinon*). O motivo dessa dicotomia ocorreu, pois, "[...] a fundação da *pólis* foi precedida pela destruição de todas as unidades organizadas à

9 Sobre o debate entre as teorias de Aristóteles e Hannah Arendt, ver Teixeira (2012, 20-24).

base do parentesco, tais como a *phratria* e a *phylé*.” (ARENDT, 2014, p. 29-30). “Historicamente, é muito provável que o surgimento da cidade-Estado e do domínio público tenha ocorrido à custa do domínio privado da família e do lar.” (ARENDT, 2014, p. 35-36)

Contudo, ainda que não se observasse a existência de parentesco, em momento algum isso significou a ausência da família. O que se alterou, foi o laço que uniria seus entes, onde agora, “[...] os homens viviam juntos por serem a isso compelidos por suas necessidades e carências.” (ARENDT, 2014, p. 36)

Nesse sentido, a *pólis* não extinguiu a domínio privado por respeito a propriedade privada, porém, não a ela em si, mas sim, a existência de um lugar, um reduto onde se pudesse estar só, pois, “[...] sem possuir uma casa, um homem não podia participar dos assuntos do mundo porque não tinha nele lugar algum que fosse propriamente seu.” (ARENDT, 2014, p. 36)

Essa premissa se convalida ao se analisar o domínio público sem a existência do domínio privado, pois ao tornar tudo comum (*koinon*), seguindo o entendimento de Arendt (2014, p.33), a *pólis* aniquilaria o governo doméstico, retirando o poder do *paterfamilias* (*dominus*) com o qual o chefe da família governava até então a sua casa, e onde se encontravam seus escravos e familiares. É por esse motivo que “a distinção entre as esferas privada e pública da vida corresponde aos domínios da família e da política, que existiram como entidades diferentes e separadas, pelos menos desde o surgimento da antiga cidade-Estado; [...]” (ARENDT, 2014, p. 34). O poder ora referenciado é considerado pré-político, pois já pertencia ao domínio privado. Em singular registro, tem-se que, até mesmo o poder de legislar, foi cedido pela família, uma vez que, “o antigo direito não é obra de um legislador: pelo contrário, impôs-se ao legislador. Seu berço está na família. Nasceu ali espontaneamente, formado pelos antigos princípios que a constituíram”. (COULANGES, 2004, p. 93). Conclui-se, assim, que o domínio privado é o berço do nascimento do domínio público e das esferas da política e do social.

Ainda nesse sentido, também seriam retirados do chefe de família, as suas propriedades, compreendendo sua casa e demais bens, assim como, seus escravos.

Não obstante, invadir o domínio privado seria retirar a liberdade dos chefes de família. Isso porque, o domínio público, aqui também representado pelas esferas política e social, era o lugar de liberdade, onde os que ali se encontravam, eram os chefes de família, pois venciam as necessidades do lar. A esfera política não era um laser ou um compromisso esporádico dos que nela transitavam. Pelo contrário, “a política não podia, em circunstância alguma, ser apenas um meio para proteger a sociedade [...]” (ARENDT, 2014, p. 37). Portanto, o domínio da *pólis* encontra limite na entrada das propriedades privadas de seus membros, pois a própria existência do domínio público e da esfera política dependiam, diretamente, dessa fronteira.

Apenas com o mundo moderno é que as esferas do social e do político começaram a se diferenciar um pouco entre si. Isso ocorreu porque com o crescimento da sociedade, ou “[...] das atividades econômicas ao domínio público, a administração doméstica e todas as questões antes pertinentes à esfera privada da família transformaram-se em preocupação coletiva.” (ARENDT, 2014, p.40)

Nota-se, portanto, que com o advento da esfera social, assuntos antes tidos como privados, tornaram-se públicos, ou seja, de conhecimento de todos. Mas viver apenas dentro do domínio privado também se demonstra impossível, dado que, como dito, a ação é uma característica da vida entre os homens. Por esse motivo, viver na privacidade não significa apenas estar privado de algo, mas também, estar só. Dessa ideia, deriva outra que foi incorporada à natureza da privacidade, que é a intimidade.

Essa esfera da intimidade, inserta na esfera da privacidade, encontra-se “[...] nos últimos períodos da civilização romana […].” (ARENDT, 2014, p. 46). E, justamente por tornar os assuntos do domínio privado de domínio público, ou seja, com o advento do social, é que nasceu a esfera da privacidade. Vale mencionar o que já foi dito acima, de que o domínio privado também compreendia a propriedade privada,

logo, privacidade traduz-se também em coisa, em obra, mas existe outra esfera que abria o intangível, aquilo que não se pode materializar, mas que, ainda assim, refere-se a essência do indivíduo, ou seja, àquilo que lhe é próprio. Obviamente, manter fora do conhecimento do domínio público, nesse sentido, em momento algum refere-se a assuntos políticos, mas sim, à questões sociais. Por esse motivo, Arendt (2014, p. 47) explica que "o fato histórico decisivo é que a privatividade moderna, foi descoberta não como o oposto da esfera política, mas da esfera social, com a qual é, portanto, mais próxima e autenticamente relacionada."

Arendt (2014) explica que com o advento da esfera social, a ação e o discurso foram excluídos da sociedade, deslocados para dentro do domínio privado, pois o social espera que seus membros se comportem de determinada maneira, onde, para isso, inclusive, impõe regras de forma a "normalizar" esse comportamento. Em momento algum, a troca da ação pelo modo de comportar-se desfaz os vínculos sociais estabelecidos. Na verdade, ao exigir certas maneiras de se portar, a esfera social faz nascer uma igualdade, diferente daquela conhecida juridicamente, mas que permite a relação humana, pois, no social, relacionam-se pares. Logo, conclui-se que a esfera do social permeia o domínio público – sendo a igualdade a sua característica predominante – e o domínio privado – repleto de distinção e diferença.

Muito embora a ação e o discurso tenham sido transferidos para o domínio privado, a excelência[10] – atividade que permitia a uma pessoa se distinguir, sobressaindo-se, em relação as demais – por sua natureza, somente se realizava se ocorresse no domínio público. Tudo porque, ela acontecia pela exigência da presença de outros, também considerados pares do indivíduo. Isso quer dizer que ainda que a esfera social tenha surgido, em momento algum, esta ameaçou o domínio público. Para Arendt (2014, p. 61), "nem a educação, nem a engenhosidade, nem o talento podem substituir os elementos constitutivos do domínio público, que fazem dele o local adequado para a excelência humana."

10 A atividade da excelência era conhecida pelos gregos como *aretẽ* e pelos romandos como *virtus*. (ARENDT, 2014, p. 60)

A partir daí, em conformidade com o problema e a hipótese formulados para esse trabalho, é preciso entender o que é o domínio público, ou, melhor dizendo, o que é tornar uma informação ou algo público.

Para Arendt (2014), o termo público pode ser traduzido em dois fenômenos correlacionados, mas não idênticos. Em primeiro lugar, tem-se que quando algo se torna público, ele é visto e ouvido por uma ou mais pessoas[11], e, consequentemente, com a maior amplitude possível. Segundo a autora, “para nós, a aparência – aquilo que é visto e ouvido pelos outros e por nós mesmos – constitui a realidade.” (ARENDT, 2014, p. 61). Isso significa a impossibilidade de viver uma vida apenas na esfera da privacidade, pois é na convivência, no aparecer e estar entre os outros que “[...] garante-nos a realidade do mundo e de nós mesmos; [...]” (ARENDT, 2014, p. 62). Ora, em conformidade com esse entendimento, o fato de estar entre iguais é poder exteriorizar opiniões, sentenças e conjecturas tidas, antes, no domínio privado. Isso, *de per si*, esclarece questões de foro íntimo postas entre os membros da família ou perante a si mesmo, frise-se que isso ocorre por ato de vontade, ou seja, por liberdade, por escolha, onde, em nenhum momento, é realizada alguma intromissão, como, por exemplo, uma coação ou tortura.

Vale mencionar que os assuntos surgidos e tratados na esfera da privacidade não se traduzem em temas irrelevantes, pois existem situações que jamais chegarão ao domínio público, e, nem por isso, pode ser desconsideradas. Na verdade, “[...] existem assuntos muito relevantes que só podem sobreviver no domínio privado. […] O que o domínio público considera irrelevante pode ter um encanto tão extraordinário e contagiante que todo um povo pode adotá-lo como modo de vida, sem com isso alterar-lhe o caráter essencialmente privado (ARENDT, 2014, p. 63-64).

Já o segundo fenômeno trata o termo público como significado do “[...] próprio mundo na medida que é comum a todos nós e diferente do lugar que privadamente possuímos nele.” (ARENDT, 2014, p. 64). Entretanto, esse mundo comum não

11 Preferiu-se utilizar a expressão “uma ou mais pessoas” em oposição ao termo “todos” utilizado por Hannah Arendt, pois, em se tratando de privacidade, vida privada e intimidade na era da informação, o fato de apenas uma pessoa ter acesso a um dado pode ser considerada uma grande exposição com amplitudes incalculáveis e imprevisíveis.

corresponde ao planeta em si ou a natureza que é habitada, mas sim, a tudo o que o homem constrói enquanto obra, conforme o termo já definido no início desse subtópico. Logo, se diz das coisas que são obradas pelo homem que podem ser vistas e ouvidas por uma ou mais pessoas. O princípio cristão de que todos devem viver como uma família e se considerar irmãos é a primeira orientação verificada nesse sentido. E, embora nesse princípio não tenha havido o interesse em construir um lugar-comum, essa filosofia estabeleceu um vínculo forte entre as relações humanas.

Nesse sentido, ao construir o mundo como um lugar de todos e para todos, tem-se a ideia de que se ele contiver “[...] um espaço público, não pode ser construído apenas para uma geração e planejado somente para os que estão vivos, mas tem de transcender a duração da vida de homens mortais.” (ARENDT, 2014, p. 67)

Por se perfazer através de obras, naturalmente, esse lugar-comum trouxe também um reconhecimento, um status, pelo que é produzido, ou seja, visto e ouvido. Tal como o dinheiro, isso também se encontra no lugar de um ganho, um retorno, pelo que é obrado pelo homem. “É a publicidade do domínio público que pode absorver e fazer brilhar por séculos tudo o que os homens venham a querer preservar da ruína natural do tempo.” (ARENDT, 2014, p. 68). Esse “lucro” obtido é chamado de admiração pública, que “[...] é consumida pela vaidade individual da mesma forma como o alimento é consumido pela fome.” (ARENDT, 2014, p. 69). É nesse sentido que é possível fazer coisas que ficam na história, como um músico, um artista, ou até mesmo um advogado que obra de forma tão notável que seus feitos serão transmitidos durante várias gerações.

Ocorre que, a autora se limitou a analisar a durabilidade das obras, mas, em momento algum, tratou o caráter positivo ou negativo delas. Isso porque, ambos os casos têm o poder de atravessar o tempo. Esse tema será tratado posteriormente. Finalmente, pode-se concluir que erguer um lugar que perpasse a duração de uma geração é a consequência, enquanto o reconhecimento acaba sendo a sua causa.

A ideia da continuidade das obras como forma de criar um lugar-comum de todos para transcender gerações é, justamente, o oposto do que ocorre no domínio privado, pois aquilo que lá permanece, principalmente, na esfera da privacidade, tem vida breve. Vem e vai com o próprio indivíduo.

Por esse motivo, é que a palavra privado deriva do termo privação, ou seja, encontrar-se sem alguma coisa. Não é menos importante ressaltar que esse entendimento leva a asseverar que a propriedade também está intimamente ligada a isso. Mas então, se o domínio privado é um lugar próprio provido de propriedade, a qual privação se poderia assimilar essa ideia? Segundo Arendt (2014, p. 72), significa, “[...] estar privado de coisas essenciais a uma vida inteiramente humana [...]”, ou seja, principalmente, de ser visto e ouvido por outros e de obrar de forma que a existência avance as gerações futuras. “A privação da privatividade reside na ausência de outros; para estes, o homem privado não aparece, e, portanto, é como se não existisse.” (ARENDT, 2014, p. 72)

Arendt (2014, p. 72) afirma ainda que, no domínio privado, o que quer que o indivíduo “[...] faça permanece sem importância ou consequência para os outros, e o que tem importância para ele é desprovido de interesse para os outros.” Excetuando-se a questão das consequências para os outros, há que se discordar da autora pelos seus próprios argumentos, pois no momento em que ela mesma afirma que “[...] todas as questões antes pertinentes à esfera privada da família transformaram-se em preocupação coletiva” (ARENDT, 2014, p.40), tem-se que a esfera social transgrediu o domínio privado até certo limite, o que torna possível afirmar que as questões privadas são de interesse para os outros. Outrossim, também é possível demonstrar esse fato, inclusive, empiricamente na era da informação, como se verá mais à frente.

Ainda assim, é possível determinar a existência do domínio privado e da esfera da privacidade. A permanência da vida privada como constituinte do privado se deve ao “[...] extraordinário senso político do povo romano, que, ao contrário dos gregos, jamais sacrificou o privado ao público, mas, ao contrário, compreendeu que esses

dois domínios somente podiam subsistir sob a forma da coexistência.” (ARENDT, 2014, p. 73)

Sendo assim, é possível afirmar que ambos os domínios precisam existir, no mesmo momento em que asseguram a própria existência humana no sentido em que são complementares. “Parece ser da natureza da relação entre os domínios público e privado que o estágio final do desaparecimento do domínio público seja acompanhado pela ameaça de liquidação também do domínio privado.” (ARENDT, 2014, p. 75). Logo, *a priori*, a crença de que a privacidade vai desaparecer na era da informação transparece-se num mito.

Como visto anteriormente, a existência do domínio privado se deve ao íntimo relacionamento que ele possui com a propriedade, onde esta é seu elemento principal, pois como se pode estar só em um lugar que não lhe pertence?

Arendt (2014) informa ainda que a propriedade não possui relação com a riqueza ou com a pobreza, mas com possuir um lugar no mundo para si. Ela analisa esse cenário de duas formas, antes e depois do que ela chama de era moderna. Isso porque, antes da era moderna a propriedade privada possuía uma característica: a sacralidade. Possuir o seu lugar era fazer parte do corpo político por chefiar uma família, tanto que, se viesse a perder esse local, isso significava perder a “[...] cidadania, além da proteção da lei.” (ARENDT, 2014, p. 76). E não é outro o motivo do significado da palavra família ser propriedade, pois “[...] designa: o campo, a casa, dinheiro e escravos.” (COULANGES, 2004, p. 93)

Já após a era moderna, “[...] o indivíduo retira os meios de sua subsistência” (ARENDT, 2014, p. 79), onde a propriedade privada podia se traduzir em riqueza. Ainda, o indivíduo podia dispor de seus bens sem que, para isso, perdesse sua cidadania, por exemplo. Logo, a riqueza privada se tornou condição para o ingresso no domínio público, pois significava que o indivíduo “[...] não teria de se dedicar a prover para si mesmo os meios de uso e do consumo, e estava livre para a atividade pública.” (ARENDT, 2014, p. 79)

No entanto, ao invés da sociedade requerer acesso ao domínio público enquanto esfera política, preferiu-se cobrar desse domínio proteção para que fosse possível acumular mais riqueza. Foi dessa forma que os assuntos do domínio privado se tornaram de interesse comum, onde esse tipo de riqueza não se poderia transformar em comum no mesmo sentido de lugar-comum. Contudo, isso gerou um risco, “pois a riqueza, depois que se tornou preocupação pública, adquiriu tais proporções que dificilmente poderia ser controlada pela posse privada.” (ARENDT, 2014, p. 86)

Desse modo, o acúmulo de riqueza, de interesse comum, acabou por ameaçar a existência do domínio privado. “A maior ameaça aqui, porém, não é a abolição da posse privada da riqueza, mas sim a abolição da propriedade privada no sentido de um lugar tangível possuído por uma pessoa no mundo.” (ARENDT, 2014, p. 86). Sobreleva ressaltar que o fato do indivíduo não possuir uma propriedade sua revela-se, obviamente, na ausência de um lugar para estar só, onde a intimidade, sem a vida privada, desvela-se insegura, pois reside, muitas vezes, num lugar intangível. Por esse motivo, Arendt (2014, p. 86) informa que “[...] sem a propriedade, como disse Locke, “de nada nos vale o comum.”

Perder a propriedade privada é perder um refúgio onde se pode ser. É por esse motivo que se afirma que o domínio privado assegura a existência humana, pois é onde se é, sem ser visto e sem ser ouvido. Caso assim não fosse, viver-se-ia uma vida superficial, onde o domínio público, embora continue a oferecer a visibilidade, “[...] perde a qualidade resultante de vir à luz a partir de um terreno mais sombrio, que deve permanecer oculto a fim de não perder sua profundidade em um sentido muito real, não subjetivo.” (ARENDT, 2014, p. 87). Analogamente, uma vida vivida inteiramente no domínio público é como o ouro que, ao ser tocado pela luz do Sol, não reluz. “O único modo eficaz de garantir a escuridão do que deve ser escondido da luz da publicidade é a propriedade privada, um lugar possuído privadamente para se esconder.” (ARENDT, 2014, p. 87-88). Note-se que não se fala em propriedade no sentido monetário, mas no material de se possuir um *locus* onde se pode tudo dentro da esfera do ser. A explicação mais clara feita por Arendt (2014, p. 89) sobre os domínios público e privado se pauta naquilo que deve ser “[...] exibido e o que deve ser ocultado”, respectivamente.

Portanto, no segundo capítulo de sua obra, Arendt (2014) sistematiza a segregação entre os domínios público e privado, ressaltando a sua importância. Além disso, ela esquematiza também as esferas da política, do social e da privacidade, além de relacionar os princípios os quais estariam inseridos nestas. De forma a exemplificar essa estrutura, Paula (2010, p. 66), assertivamente, propôs a seguinte organização:

Domínios	Público		Privado	
Esferas	Política	Social		Privacidade
Princípios	Isonomia	Isonomia	Discriminação	Exclusividade

Tabela 1 – Segregação entre os Domínios Público e Privado.

O referido autor esclarece que não existe simetria nos campos acima, e que os limites entre eles são imaginários, não se podendo delimitar, exatamente, onde eles se encontram, devendo-se observar, apenas, as distinções estabelecidas. Importa destacar que a representação gráfica esclarece as distinções feitas por Hannah Arendt.

Antes do aprofundamento no estudo sobre a privacidade, sobreleva esclarecer um ponto primordial que se encontra na relação entre a liberdade, a privacidade, a vida privada e a intimidade. É o que se faz no tópico a seguir.

1.3. A LIBERDADE E O DIREITO DE RESISTÊNCIA DO SER: UM ENSAIO RETÓRICO SOBRE A ONTOLOGIA DA LIBERDADE PARA O DOMÍNIO PRIVADO

Antes que se enfrente a problemática das esferas inseridas no domínio privado, é preciso desconstruir o pensamento de que o indivíduo possui um direito fundamental de liberdade a fim de que aja livremente dentro desse domínio, sendo então protegido apenas por essa garantia ou por um direito de resistência. Para isso, é preciso diferenciar o direito de liberdade da liberdade ontológica do ser. Contudo, é

primordial que se assente o entendimento acerca do que vem a ser um direito fundamental[12].

Embora não seja o foco do presente trabalho abordar as várias acepções da palavra direito, uma vez que, este se constitui em um vocábulo polissêmico (FABRIZ, 2003), é preciso defini-lo dentro da temática ora tratada. Sendo assim, tem-se que a ideia de um direito nasce dentro da cultura de um povo, de onde se extrai um determinado valor, pois "pertencemos a uma determinada cultura e como tal nos reconhecemos, situamo-nos em dada comunidade e por conseguinte compartilhamos os mesmos valores." (FABRIZ, 2003, p. 147). É a partir da identificação de um valor que se vislumbra o nascimento de uma norma. Assim, um direito se dá através de uma construção que se caracteriza mediante a análise supramencionada, qual seja, cultura → valor → norma. Logo, uma norma pode ser entendida como um direito que vem a ser assegurado ou restringido.

É importante mencionar que devido ao fato da convivência em comunidade, onde se localizam vários indivíduos regidos por essa mesma norma, verifica-se também, o surgimento de deveres, pois não há como afirmar a existência de um direito sem que um ou mais indivíduos, ou até mesmo o Estado, devam cumpri-lo. "*Daí se dizer que ter um direito é ser beneficiário de deveres de outras pessoas ou do Estado.*" (VIEIRA, 2006, p. 19, grifos no original)

Uma das principais categorias de direito são os direitos da pessoa humana, que consistem numa esfera de proteção, assegurando seus valores fundamentais. Essa esfera se traduz no conjunto mínimo de direitos para a proteção de todos. A partir daí é que se encontram os termos "humanos", "fundamentais" ou "da pessoa humana" (VIEIRA, 2006). Isso porque, foi através da pessoa humana, e não só, mas principalmente para ela, que os direitos surgiram. Da mesma forma, vale-se da existência frágil e finita do ser humano (HEIDEGGER, 2013), verificando-se, assim, a necessidade da efetiva segurança de seus direitos, asseverando uma vida digna.

---

12 Analisam-se os direitos fundamentais sob a ótica do autor Oscar Vilhena Vieira ao invés de Robert Alexy, pois aquele, em sua obra, compreende "o regime jurídico dos direitos fundamentais tal como estabelecido pela Constituição de 1988" (VIEIRA, 2006, p. 37), e, Alexy, funda seu estudo sob a égide da Constituição Alemã. Pertinente, pois, escolher um autor que trate o cenário brasileiro.

> Numa definição preliminar, os direitos da pessoa humana poderiam ser compreendidos como razões peremptórias, pois eticamente fundadas, para que outras pessoas ou instituições estejam obrigadas, e portanto, tenham deveres em relação àquelas pessoas que reivindicam a proteção ou realização de valores, interesses e necessidades essenciais à realização da dignidade, reconhecidos como direitos da pessoa humana. (VIEIRA, 2006, p. 27)

Os direitos fundamentais podem ser conceituados sob dois pontos de vista, substancial e formal. Para o primeiro, os direitos fundamentais são aqueles necessários para assegurar uma vida digna ao indivíduo. Já relativo ao segundo ponto de vista, os direitos fundamentais se constituem em matrizes dos demais, fundamentando-lhes de forma a possibilitar o seu exercício. (PEDRA, 2012)

Devido a essa característica protetiva, os direitos fundamentais encontram-se positivados numa Constituição, como é o caso do Brasil. Fala-se então em garantia fundamental quando um direito, também fundamental, está inserido no texto constitucional. (PEDRA, 2012). A partir disso, é possível concluir que “[...] direitos fundamentais são essencialmente direitos do homem transformados em direito positivo.” (ALEXY, 1999, p. 73)

No entanto, é relativamente moderna a concepção de direitos fundamentais. Historicamente, é possível segregar esses direitos em, pelo menos, quatro dimensões. Na primeira dimensão, datada dos séculos XVII e XVIII, encontram-se os direitos civis, “[...] de não sermos molestados pelo Estado, direito de termos nossa integridade, nossa propriedade, além de nossa liberdade, a salvo das investidas arbitrárias do Poder Público. Esse grupo de direitos demarcaria os limites de ação do Estado Liberal.” (VIEIRA, 2006, p. 39). Frise-se que a liberdade é o primeiro direito fundamental a ser garantido através de uma constituição.

Os direitos fundamentais da segunda dimensão, que nasceram durante a primeira guerra mundial, nos anos de 1914 a 1918, tratam-se de direitos sociais. É o chamado Estado Social. Aqui, as constituições tiveram como objeto, as relações de trabalho, as relações econômicas, a educação, a cultura, a saúde e a previdência (PEDRA, 2012). Outro ponto predominante no Estado Social é a noção de

coletividade, momento em que surgem vários movimentos de classes, como de mulheres, negros, dentre outros.

Na terceira dimensão, encontram-se os direitos de solidariedade ou fraternidade, que surgem a partir do século XX. Eles versam sobre o desenvolvimento, o meio ambiente, o patrimônio comum da humanidade, dentre outros. A finalidade dos direitos aqui protegidos é a segurança do próprio gênero humano.

Alguns autores sustentam a existência de uma quarta dimensão, como afirma Paulo Bonavides (2003, p. 570-572), que estaria relacionada ao fenômeno da globalização política. São os direitos relativos à democracia, à informação e ao pluralismo, porém, em amplitude internacional.

Outra corrente que também versa sobre a quarta dimensão dos direitos fundamentais afirma ser esta a dimensão da bioética ou do biodireito. Foi durante a Segunda Guerra Mundial, que se observaram experimentos genéticos usando os prisioneiros dos campos de concentração. Logo, nasceu a preocupação com a ética nesses procedimentos “[...] médicos e biológicos, preocupação que deveria redundar na proteção da pessoa humana, quer de forma física, quer em sua dignidade, ocasionando, por sua vez, uma humanização do progresso científico.” (FURTADO e MENDES, 2008)

Além das quatro dimensões supramencionadas, vale destacar aquela que, *a priori*, demonstra profunda relação com a pesquisa aqui desenvolvida. Se trata da quinta dimensão dos direitos fundamentais, que afirma os direitos da era da informação, ou, melhor dizendo, afirma os direitos “[...] que envolvem a cibernética e a informática”. (FURTADO e MENDES, 2008). Como já foi dito, essas dimensões reconhecem determinados direitos considerados, a partir daí, como fundamentais. Em detrimento disso, é preciso se questionar: quais seriam os direitos da era da informação que devem ser considerados como fundamentais? É possível que os direitos fundamentais versem sobre determinados recursos tecnológicos garantidos ao indivíduo? Seriam os recursos tecnológicos um caminho para se efetivar direitos e garantias fundamentais? Muito embora tenham sido elaboradas aqui, é preciso

que se possua um conjunto mínimo de conhecimento sobre a tecnologia para que seja possível responder essas perguntas. Portanto, esses pontos voltarão a ser abordados no terceiro capítulo deste trabalho.

De como complementar, sobreleva ressaltar a importância de se reconhecer um direito como fundamental. No momento em que ele alcança essa categoria, o Estado atrai para si as obrigações de respeitar e garantir esses direitos fundamentais. De igual modo, vale lembrar que os demais indivíduos também deverão respeitar esses direitos, sem o mesmo ônus de garanti-los, mas tão somente, observá-los.

Após a abordagem sobre o que são direitos fundamentais, e, por demonstrar que a liberdade se prefaz num direito dessa categoria, especificamente de primeira dimensão, cumpre agora, analisar algumas questões, tais como: antes do Estado Liberal, o indivíduo não era livre para pensar o que desejasse? Somente após a garantia do direito de liberdade é que pôde o indivíduo agir livremente dentro do domínio privado? Nas questões do domínio privado, a liberdade é um direito ou uma característica ontológica do ser?

Para que seja possível responder a esses questionamentos, faz-se necessário diferenciar a liberdade sob a ótica dos autores Robert Alexy[13] e Jean-Paul Sartre.

No entanto, sobreleva ressaltar qual o tipo de liberdade que se pretende verificar, pois as formas de se enxergá-la podem variar "[...] (como modo de autodeterminação, como possibilidade de escolha, como ato voluntário, como espontaneidade, como ausência de interferência etc.), bem como situá-la em sua esfera de ação ou alcance (liberdade pública, privada, pessoal, coletiva, política, moral, etc.)." (CUNHA, 2011, p. 66). Diante disso, impende compreender se uma liberdade positivada é suficiente para se garantir o espaço necessário para os assuntos do domínio privado ou se essa liberdade transcende a uma previsão legal, demonstrando pertencer a própria natureza da pessoa humana, se localizando no

13 Sobreleva ressaltar que o presente trabalho não possui a intenção de analisar um caso concreto utilizando a metodologia de decisão judicial de Robert Alexy, mas tão somente, valer-se de seu conceito sobre a liberdade, porquanto o referido autor a define sob a ótica dos direitos fundamentais.

âmago do ser, inalcançável pelo direito. Sendo assim, fala-se da liberdade do ser consigo e do ser com o outro.

Para Alexy (2008, p. 218), “o conceito de liberdade é, ao mesmo tempo, um dos conceitos práticos mais fundamentais e menos claros. Seu âmbito de aplicação parece ser quase ilimitado.” Por esse motivo, o referido autor restringe sua análise ao conceito de liberdade jurídica, que depende de uma norma inserida no ordenamento jurídico que a reconheça como um direito fundamental.

Uma liberdade jurídica deve ser construída sobre outro instituto, pois trata-se de um direito oriundo do reconhecimento de um Estado como seu autorizador. Isso quer dizer aqui, que essa liberdade jurídica é fundamentada por uma permissão jurídica. Numa afirmação emblemática, Montesquieu (1993) conclui então que “liberdade é o direito de fazer tudo o que a lei permite.” A partir desse pensamento, depreende-se que “quem diz que uma pessoa é livre, pressupõe que, para essa pessoa, não existem embaraços, restrições ou resistências de qualquer espécie.” (ALEXY, 2008, p. 219)

Observa-se, então, na estrutura do conceito de liberdade, três características, que são: um sujeito, um obstáculo e um objeto. O sujeito, até o momento, não é livre. O obstáculo se traduz na situação a que o sujeito terá que enfrentar. E o objeto se refere àquilo que o obstáculo inibe. Isso permite dizer que “a base do conceito de liberdade é constituída, portanto, por uma relação triádica entre um titular de uma liberdade (ou de uma não-liberdade), um obstáculo à liberdade e um objeto da liberdade.” (ALEXY, 2008, p. 220).

A análise da liberdade a partir de uma relação triádica se justifica, pois um indivíduo é livre, juridicamente, mas sua liberdade sofre influência da liberdade de outrem. Logo, a análise desses três componentes permite que a liberdade seja atribuída a determinada pessoa sem que esta entre em conflito com a liberdade do próximo. Do mesmo modo, sem prejuízo da liberdade jurídica, é possível analisar também as liberdades de ação e vontade, pois estas também se traduzem em liberdades de pessoas.

Dentro da relação triádica, a ação repousa sobre o objeto da liberdade, ou seja, através de sua análise, é possível verificar se existe apenas uma ação possível ou se existe uma alternativa de ação.

Se houver uma liberdade de ação, estar-se-á diante de uma liberdade negativa. “Uma pessoa é livre em sentido negativo na medida em que a ela não são vedadas alternativas de ação.” (ALEXY, 2008, p. 222). De forma oposta, se existir apenas uma opção de ação, trata-se de uma liberdade positiva.

Ainda sobre as liberdades jurídicas, é possível classificá-las como liberdades protegidas e não-protegidas. Da mesma forma que a liberdade negativa, a liberdade não-protegida se ampara na opção entre um fazer e um não fazer correspondente ao fazer (abstenção). Já a liberdade protegida nasce de uma norma constitucional permissiva. Vale lembrar o que já foi dito acima, de que também se caracteriza uma liberdade a inexistência de norma proibitiva. Aqui, a única diferença residirá numa permissão explícita ou implícita. Entretanto, conforme dito alhures, por se tratar de um direito fundamental, a liberdade, necessariamente, deve estar prevista em uma norma constitucional, que, nesse caso, será permissiva de forma explícita.

Ao finalizar sua análise sobre o conceito de liberdade, Alexy (2008, p. 234) conclui que

> toda liberdade fundamental é uma liberdade que existe ao menos em relação ao Estado. Toda liberdade fundamental que existe em relação ao Estado é protegida, no mínimo, por um direito, garantido direta e subjetivamente, a que o Estado não embarace o titular da liberdade no fazer aquilo para o qual ele é constitucionalmente livre.

Ora, afirmar que o indivíduo é constitucionalmente livre, significa reduzir a liberdade do ser ao texto da Constituição de seu Estado. Rememorando os questionamentos feitos acima, como se aqui transcritos estivessem, a liberdade trazida por Robert Alexy não é suficiente para fundamentar a resolução das referidas perguntas. Isso porque, a liberdade em Alexy é uma liberdade oriunda de um contrato social.

De acordo com Vieira (2006, p. 32),

> como destaca Habermas, os direitos básicos não são uma dádiva transcendente, mas uma consequência da decisão recíproca dos cidadãos iguais e livres de “legitimamente regular suas vidas em comum por intermédio do direito positivo”. O contrato social é uma metáfora dessa decisão, assim como os momentos constituintes em que se declaram direitos são tentativas de dar concretude aos ideais de autonomia; do livre estabelecimento das leis sob as quais a comunidade pretende viver.

Isso ocorre, porque o domínio público é o lugar de igualdade. Sendo assim, o estabelecimento da liberdade se constitui numa “decisão recíproca dos cidadãos”. Entretanto, o domínio privado é o lar das diferenças. O que, *de per si*, comprova a inaplicabilidade de uma liberdade jurídica, ou seja, contratual, às esferas pertencentes ao ser. Portanto, pende-se encontrar a liberdade pertencente ao ser que assegura a sua existência no domínio privado.

Analisando a proposta de Jean-Paul Sartre, percebe-se que esta se aproxima mais da liberdade ontológica do ser do que a de Robert Alexy. Isso porque traz a subjetividade do indivíduo como ponto de partida (SARTRE, 2010, p. 46), pois, segundo o próprio Sartre (2010, p. 46), “[...] queremos uma doutrina embasada na verdade e não em um conjunto de belas teorias, cheias de esperança mas sem fundamentos reais.” Por subjetividade, deve-se entender, então, como a incapacidade do ser humano de transgredi-la. Isso significa dizer que o homem não é nada além daquilo do que pode vir a ser enquanto ser humano.

Sartre, como existencialista, entende que a “existência precede a essência”. Isso significa que o homem primeiro existe para, só então, se definir. Toda essa filosofia parte da verdade de Descartes (2001, p. 38-39), conhecida como *cogito*, ou seja, “penso, logo existo”. Para Sartre, o correto é: existo, logo penso.

É preciso esclarecer que não é o foco do presente trabalho discutir as bases do existencialismo. O que se pretende com essa análise é ressaltar o caráter laico do estudo, pois, conforme se verificará a seguir, dentro da esfera da privacidade, existem as esferas da vida privada e da intimidade. E, nesta última, apenas a crença de um ser ou uma força onipresente é que pode adentrá-la. Contudo, o existencialismo também respeita, sobretudo, a opinião laica de que ninguém, sem que seja o próprio ser, pode vir a tomar conhecimento do que ocorre na intimidade.

Portanto, para que a “existência preceda a essência” é preciso entender a ideia do desamparo, que preconiza a inexistência, conforme abordado por Sartre (2010, p. 35), de um deus. Sendo assim, sem uma força superior que reja o ser humano, bem como, seus atos, ele está desamparado. Por esse motivo é que a angústia anda junto com o desamparo (SARTRE, 2010, p. 39). Fatalmente, tem-se ainda o desespero, que é a obrigação de se tomar decisões conforme os próprios entendimentos, ou seja, conforme as próprias dúvidas e certezas.

Nesse sentido, deve o homem pautar seus atos numa moral que observe os outros. No entanto, não existe uma moral geral. “E quando dizemos que o homem é responsável por si mesmo, não queremos dizer que ele é responsável estritamente por sua individualidade, mas que é responsável por todos os homens.” (SARTRE, 2010, p. 26). Isso quer dizer que o homem se torna responsável por aquilo que é percebido como consequência de seus atos, devendo ele evitar o que vier a causar prejuízo para si e para todos. “Assim, nossa responsabilidade é muito maior do que poderíamos supor, pois ela envolve a humanidade como um todo.” (SARTRE, 2010, p. 27).

A partir desse entendimento é que se observa a liberdade inerente ao ser humano, pois ele é livre para fazer aquilo que entender necessário, segundo seus próprios juízos de valor, “[...] dizendo de outro modo, não existe determinismo, o homem é livre, o homem é liberdade.” (SARTRE, 2010, p. 33). Diante disso, é possível concluir que o “[...] homem está condenado a ser livre.” (SARTRE, 2010, p. 33). Dessa forma, tem-se que, a partir de sua existência o homem é livre. Isso porque não existem embaraços, impedimentos ou regras que o precedam. O homem é o seu próprio legislador.

Cumpre salientar que quando se afirma que o homem é livre, isso não quer dizer que o ordenamento jurídico não se aplique a ele, mas tão somente que ele é livre ainda que suas ações resultem numa sanção legal. Contudo, como já foi dito, se o homem se orientar por aquilo que é melhor para todos, consequentemente, ele não desobedecerá nenhuma previsão legislativa. “Quando declaro que a liberdade, em cada circunstância concreta, não pode ter outro fim que procurar a si mesma, se o

homem reconheceu, a certa altura, que estabeleceu valores no desamparo, ele não pode querer outra coisa senão a liberdade como fundamento de todos os valores." (SARTRE, 2010, p. 55). Portanto, como lugar de diferença, é certo que a liberdade seja própria do indivíduo no domínio privado, devendo ele observar como a exercerá.

É por esse motivo que a liberdade jurídica de Robert Alexy não é capaz de fundamentar a liberdade ontológica do ser, pois deriva da abstração de um contrato social. Para Almeida (2015, p. 62),

> noutras palavras, a concepção contratualista de liberdade natural no sentido de que ninguém se sujeita à outro por motivo de nascença e liberdade civil, em que se deve participar do corpo político para ser livre proprietário de todas as posses conquistadas, não é suficiente para traduzir o amplo significado do termo.

A liberdade possui uma estreita ligação com o domínio privado, pois, após o limite até onde a esfera do social conseguiu invadir, o ser é livre para decidir quem terá acesso as informações de sua privacidade, sua vida privada ou sua intimidade. No momento em que o se perde a liberdade de decidir sobre quem terá acesso, o que será acessado, e, por quanto tempo será acessado, o indivíduo perde, consequentemente, sua autonomia, ou seja, sua liberdade.

Portanto, aceitar que a liberdade que protege as esferas da privacidade, da vida privada e da intimidade advém de uma liberdade positivada, é afirmar que nenhum ser humano é livre até que uma norma jurídica, no caso, uma constituição, a reconheça como um direito. Por esse motivo, a liberdade para as referidas esferas pertence, essencialmente, ao próprio ser humano, ou seja, como afirmou Sartre (2010, p. 33) "[...] homem está condenado a ser livre", pois ainda que não exista nenhum Estado instituído ou nenhum direito reconhecido, o ser humano permanecerá livre para permitir quem terá acesso as informações de sua privacidade, vida privada e intimidade.

Ainda sobre a intimidade, esta demonstra ser inalcançável para outro indivíduo, mesmo que sua liberdade de escolha seja cerceada. Contudo, caso a pessoa confie

sua intimidade a um diário, por exemplo, quem tiver acesso a ele, poderá alcançar esse recôndito do ser. Logo, a intimidade se torna vulnerável a partir do momento em que o indivíduo confia em um dispositivo que, no seu entendimento, teria o condão de garantir a segurança de suas informações íntimas.

Sendo assim, como já foi dito, a liberdade do ser extrapola os limites do Estado, ultrapassando a sua Constituição por estar acima dela, ou seja, por pertencer a própria Constituição do ser.

Ninguém é obrigado a pensar aquilo que não deseja e nem mesmo dizer o que não tem vontade, ainda que sejam empregadas técnicas de persuasão ou, até mesmo, de tortura. A liberdade é, para a privacidade, sua pedra angular, onde sem aquela, esta não existe.

Além disso, mesmo que ao ser humano seja possível se opor a outro que deseje obter suas informações íntimas, constitui-se um risco se confiar na tecnologia, uma vez que, é através dela, que se torna possível acessar o conteúdo mais profundo da esfera do ser.

Ainda sobre a liberdade, é o indivíduo que possui a autonomia para afirmar onde determinada informação sua se localiza, se na privacidade, na vida privada ou na intimidade. A título de exemplificação, a preferência sexual de uma pessoa pode se localizar na esfera de sua vida privada, pois, para ela, não existem restrições que a fazem manter sob sigilo essa informação. Contudo, para outra pessoa, a preferência sexual é por demais vexatória para ser vista e ouvida, se localizando, portanto, em sua intimidade.

Isso permite afirmar que toda ação judicial que verse sobre os direitos à privacidade, à vida privada e à intimidade é considerada um caso difícil[14], nos termos de Ronald Dworkin (2002).

14 Um caso difícil ocorre “[...] quando uma ação judicial específica não pode ser submetida a uma regra de direito clara, estabelecida de antemão por alguma instituição.” (DWORKIN, 2002, p.127)

Conforme dito acima, a esfera da privacidade, objeto de estudo do presente trabalho, consiste ainda, em mais duas esferas, a da vida privada e a da intimidade da pessoa humana. Cada uma dessas esferas é abordada no tópico a seguir.

1.4. A MORADA ONTOLÓGICA DO SER: AS INFORMAÇÕES PESSOAIS E AS DELIMITAÇÕES NAS ESFERAS DA PRIVACIDADE, DA VIDA PRIVADA E DA INTIMIDADE

Ao se tratar de informações pessoais, é preciso abordar o significado de alguns termos utilizados ao longo deste trabalho. Diante disso, faz-se aqui outro acordo semântico para a correta compreensão textual. A partir daí, é preciso diferenciar os significados de termos, tanto no singular quanto no plural, como: dados, dados pessoais, dados sensíveis, dados anônimos, metadados, conteúdo, informações, informações pessoais, informações privadas e informações íntimas.

Tem-se que dado é “[...] qualquer elemento identificado em sua forma bruta que, por si só, não conduz a uma compreensão de determinado fato ou situação.” (OLIVEIRA, 2002). Sendo assim, um dado é a menor partícula de uma informação, ou seja, quando vários dados são reunidos, tem-se uma informação.

A título de exemplificação, obtendo-se dados como roda, pneu e volante, pode-se deduzir estar-se diante de uma informação sobre um veículo. O que se deve perceber é que não são quaisquer dados que, aglomerados, representam uma informação, mas sim, aqueles dados que se referem ao mesmo objeto, pois, somente a imaginação é que pode relacionar dados distintos, como, por exemplo: pneu, asa e água. Estes, por si só, não transmitem segurança para um correto juízo de valor.

Logo, os dados pessoais são dados relacionados “[...] à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos.” (PENSANDO O DIREITO, 2015). Já os dados sensíveis

recebem esse nome, pois revelam “[...] a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, como dados genéticos.” (PENSANDO O DIREITO, 2015). Os dados anônimos são aqueles “[...] relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular.” (PENSANDO O DIREITO, 2015). Frise-se que, não raro, a palavra dados no plural, denota informação pela própria definição desta.

O termo metadado refere-se ao título de um dado, auxiliando a organizar as informações sobre determinado objeto ou pessoa. Tomando-se um livro como exemplo, tem-se que seu título é “Livro sobre trabalhos acadêmicos”. Extrai-se daí que título é o nome do metadado do livro, enquanto que “Livro sobre trabalhos acadêmicos” é o metadado em si. Assim, metadado são as informações acessórias, ou seja, que se referem a classificação de um objeto ou pessoa. Com relação ao conteúdo, este se difere do metadado por significar a essência do objeto ou pessoa. Desse modo, toda a temática tratada dentro da obra “Livro sobre trabalhos acadêmicos” refere-se ao seu conteúdo.

Por fim, diferenciando-se as informações em pessoais, privadas e íntimas, estas residem, cada uma, em suas respectivas esferas, ou seja, na privacidade, na vida privada e na intimidade. Cabe aqui ressaltar a dificuldade de se classificar a informação dessa forma por se tratar de um direito subjetivo fundamental. Por esse motivo, o termo que é largamente utilizado a fim de representar todas as esferas do domínio privado é “informações pessoais”. Além disso, é comum notar a utilização de todos esses termos em forma de sinônimo, pois dados sensíveis podem, perfeitamente, representar informações privadas ou íntimas.

Assim, feito mais esse acordo semântico pertinente ao presente trabalho, segue-se com outra diferenciação importante para a compreensão deste estudo. É inevitável que isto leve a formação de mais um acordo semiótico. Desta vez, a fim de possibilitar a identificação das esferas existentes dentro do domínio privado, pois é

comum referir-se a privacidade querendo que esta signifique a vida privada ou a intimidade, pois ambas estão inseridas na privacidade. Logo, sempre que for necessário diferenciar as esferas, estas serão mencionadas individualmente. Mas, quando o texto se referir tão somente o termo privacidade, esta deve ser entendida em seu sentido mais amplo, ou seja, se reportando também as outras duas esferas.

Sobre a esfera da privacidade, como já foi dito, esta encontra-se dentro do domínio privado, que ora, foi invadido pela esfera do social, tornando os assuntos daquele de interesse desta. Some-se a isso as questões atinentes a era da informação, que tornam todas as informações contidas na esfera da privacidade, da vida privada e da intimidade de interesse dos governos e do mercado também, conforme a presente pesquisa comprova no próximo capítulo. Por esse motivo, é preciso ressaltar a importância da privacidade, da vida privada e da intimidade como lugar próprio do ser, e de cuja existência, depende a própria existência humana (ARENDT, 2014, p. 87).

É necessário tratar cada esfera existente dentro do domínio privado de forma a evidenciar até onde consegue chegar o poder invasivo da tecnologia.

Tanto a privacidade, quanto a vida privada e a intimidade, se tratam de direitos subjetivos fundamentais (FERRAZ JÚNIOR, 1993). O caráter subjetivo dessas esferas merece atenção, pois aquilo que para um indivíduo é privado ou íntimo, para outro pode não ser. Diante desse cenário, verifica-se a dificuldade do legislador e do julgador para, corretamente, estabelecer os limites de uma norma jurídica ou os ditames de uma sentença, por exemplo. Ainda sobre isso, com base nesse subjetivismo, as violações que ocorrem a essas esferas não são enxergadas nitidamente por outro indivíduo, pois não há uma clara identificação de que determinada situação que expôs uma intimidade, de igual modo, será considerada também como violadora da própria intimidade. Entretanto, é preciso abordar cada esfera isoladamente para que seja possível medir as suas abrangências.

Iniciando-se, pois, pela privacidade, tem-se que a mesma, como dito, se trata de um direito subjetivo que se constrói sobre uma estrutura básica “[...] cujos elementos

são o *sujeito*, o *conteúdo* e o *objeto*.” (FERRAZ JÚNIOR, 1993, grifos no original). De forma a visualizar melhor esse ponto, tem-se a figura 1 abaixo.

Figura 1 – Elementos de um Direito Subjetivo Fundamental.

O titular desse direito é o sujeito, que pode ser “[...] toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente (ou transeunte cf. Mello Filho, p. 20) no País (art. 5º, *caput*)” (FERRAZ JÚNIOR, 1993). Já o conteúdo, é a “[...] faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão.” (FERRAZ JÚNIOR, 1993). Por fim, o objeto se traduz naquilo que é protegido, que, no caso da privacidade, se trata da “[…] integridade moral do sujeito.” (FERRAZ JÚNIOR, 1993).

A privacidade rege-se pelo princípio da exclusividade, cujos três principais atributos são: “[...] a solidão (donde o desejo de estar só), o segredo (donde a exigência de sigilo) e a autonomia (donde a liberdade de decidir sobre si mesmo como centro emanador de informações).” (FERRAZ JÚNIOR, 1993). De igual modo, tem-se aqui mais uma relação triádica, como se demonstra na figura 2 a seguir.

Figura 2 – Atributos do Princípio da Exclusividade.

Contudo, é preciso ressaltar que a privacidade comporta certo grau de publicidade, pois algumas informações podem ir a domínio público sem prejuízo para o sujeito, mas lembrando sempre que deve ocorrer oriundo de um ato de sua vontade. É o caso do nome, da imagem (características) e da reputação (informações básicas sobre como é o seu comportamento, onde trabalha, onde vive, dentre outros), por exemplo.

Utilizando-se de dados hipotéticos, supondo ser o Gustavo um indivíduo humano, sua privacidade se digna a responder a seguinte questão: **Quem é ele?**

A resposta a essa pergunta se faz com dados de sua privacidade, com por exemplo, respondendo àquela indagação: seu nome é Gustavo. Ele é alto, magro, cabelo castanho, olhos azuis, sem nenhuma necessidade especial aparente, dentre outros. Ele mora no bairro Centro, no Edifício Solar da Praça, no apartamento 201.

Sendo assim, pode-se dizer que esses dados são oponíveis a terceiros, ou que eles "[...] demarcam a individualidade *em face* dos outros. Ninguém tem um nome, uma imagem, uma reputação só para si mesmo, mas como condição de comunicação." (FERRAZ JÚNIOR, 1993, grifos no original)

Como se verifica, mesmo que alguns dados tenham sido vistos e ouvidos, isso não representou uma grande exposição gerando prejuízos para o indivíduo. Relacionando-se essa questão com a problemática da era da informação, tem-se que, em vários momentos, a divulgação dessas informações independem de ato de vontade do sujeito, desrespeitando assim, sua liberdade de decisão, demonstrando que, nem sempre "[...] as quatro paredes da propriedade privada de uma pessoa oferecem o único refúgio seguro contra o mundo público comum, não só contra tudo o que nele ocorre, mas também contra a sua publicidade, contra o fato de ser visto e ouvido." (ARENDT, 2014, p. 87)

Cumpre esclarecer aquilo que Ferraz Júnior (1993) afirma, pois, "embora os comentadores não vejam diferença entre a vida privada e intimidade (cf. Ferreira Filho, p. 35, Cretella Júnior, p. 257), pode-se vislumbrar um diferente grau de

exclusividade entre ambas.” Assim, a vida privada se localiza fora da esfera da intimidade, mas parcialmente dentro da esfera da privacidade.

A vida privada também possui os mesmos três atributos informados acima, quais sejam: a solidão, o segredo e a autonomia. Entretanto, para a vida privada, a solidão é um estar-só entre os seus (familiares, colegas de trabalho, amizades, entre outros), ou seja, não sem encontram terceiros nessa relação. “Numa forma abstrata, o terceiro compõe a sociedade, dentro da qual a vida privada se desenvolve, mas que com esta não se confunde (cf. Luhmann).” (FERRAZ JÚNIOR, 1993). Aqui também existem dados que podem vir a público, por exemplo, a quantidade de filhos de um casal pode ser exigida quando da aquisição de um novo imóvel. Nesse momento, o dado se tornará público. Por esse motivo, na vida privada cabe a pergunta: **Como o Gustavo se relaciona com os seus?**

Como resposta a esse quesito, e a título de exemplificação, poderiam ser obtidas as seguintes informações: Gustavo é uma pessoa extrovertida, ou então, Gustavo é uma pessoa tímida que costuma ir na Igreja aos domingos para depois ir ao shopping center com os amigos. É casado com Ciclana, mas, sem filhos. Possui uma relação estreita com seu amigo Fulano. Logo, Isso permite concluir que a vida privada de um indivíduo tem uma forte relação com os seus hábitos. Muito embora ela não se limite apenas a isso.

Já a intimidade, de igual forma, também possui aqueles mesmos três atributos, quer sejam: a solidão, o segredo e a autonomia. Todavia, a solidão aqui é um estar-só num espaço reservado para si mesmo, sem qualquer alcance para a esfera social. Sendo assim, a intimidade se perfaz num local, intangível e imaterial, onde também se localiza a figura do ser, mas de uma forma que somente ele próprio é capaz de reconhecer. “O primeiro eloquente explorador da intimidade e, até certo ponto, o seu teórico foi Jean-Jacques Rousseau [...]” (ARENDT, 2014, p.47). O fato mais interessante sobre isso foi a forma como ele chegou a conclusão de que existia mais um lugar que necessitava de proteção especial “[...] contra a insuportável perversão do coração humano pela sociedade, contra a intrusão desta última em uma região recôndita do homem […]” (ARENDT, 2014, p.47).

Arendt (2014, p. 47-48) ensina ainda que “para Rousseau, tanto o íntimo quanto o social eram, antes, formas subjetivas da existência humana, e em seu caso era como se Jean-Jacques se rebelasse contra um homem chamado Rousseau.” Posteriormente, a intimidade se mostrou como um lugar seguro, tido como “[...] fuga do mundo exterior [...]” (ARENDT, 2014, p. 85), para um outro *locus*, aquele que é interior ao indivíduo.

Aqui, tem-se uma pergunta que se remete ao próprio ser, qual seja: **Como é o Gustavo?** As possíveis respostas para essas questões seriam, então, a opinião política, a crença, a preferência sexual, os gostos, as fobias, dentre inúmeros outros.

O reconhecimento da existência da intimidade mudou a forma como alguns filósofos contratualistas enxergavam a intervenção estatal. O caso mais notório sobre isso encontra-se no Leviatã de Thomas Hobbes. Para Krohling e Martinelli (2014),

> em sua comparação entre Hobbes, filósofo que não permite resistência ao poder do soberano[15], Locke, que entende haver um estado de natureza e uma lei natural onde, por consequência, se verificam direitos, e Schmitt, que encontrou uma contradição no pensamento de Hobbes afirmando que isso “[...] destruiu de dentro para fora o poderoso Leviatã [...]” conclui que, até mesmo Hobbes “[...] diante do foro interno, fazia distinção entre o privado e o público, e seu Leviatã chegava até o limite do privado, mas não penetrava nele. Deste modo, deixava a salvo a liberdade de consciência religiosa das pessoas.” Zaffaroni (2007 p. 134-135). Logo, até mesmo quem defende o poder absoluto do soberano, em determinado momento lhe impõe resistência. Dessa forma, fica claro que é preciso impor limites para a atuação do Estado. Contudo, como seria possível estabelecer esses limites?

Verifica-se assim, que até mesmo Hobbes, um contratualista que não aceita que o soberano desconheça uma informação necessária a garantia dos direitos instituídos, seja do domínio público ou do domínio privado, concorda que um limite seja estabelecido quando o Leviatã tenta saber qualquer assunto relacionado a sua consciência religiosa. Isso, *de per si*, demonstra que, absolutamente ninguém, deseja que todas as suas informações venham a ser vistas e ouvidas por quem quer que seja. Comprova-se, então, que o indivíduo é dotado de liberdade para negar o acesso a essas informações.

---

15 O termo Soberano deve ser entendido aqui como Estado.

De forma a esclarecer essa questão, é preciso revisitar a passagem que deu origem a esse entendimento por parte de Schmitt. Nela, Hobbes (2012, p. 353) afirma que

> um homem particular tem sempre a liberdade (**visto que o pensamento é livre**) de acreditar ou não, **intimamente**, nos fatos que lhe forem apresentados como milagres, considerando que benefícios poderão derivar da crença dos homens para aqueles que o defendem ou combatem e conjeturar, com esse fundamento, se são milagres ou mentiras. Porém, quando chegamos à confissão dessa fé, a razão privada deve submeter-se à pública, isto é, ao representante de Deus e ao chefe da Igreja, e sobre isso teceremos comentários mais adiante. (grifo nosso)

Zaffaroni (2007, p. 135) conclui que, "deste modo, embora se reconheça ao soberano – como chefe da Igreja – o poder de decidir em que milagres se deve crer, isso se dá apenas em referência ao culto público, mas não ao foro interno." Isso realça o caráter íntimo que a crença religiosa possui, uma vez que, se é livre para pensar o que bem se pretender. Portanto, entende-se que a "fé é uma questão íntima, sua profissão é pública; em questões íntimas o Leviatã não entra. (ZAFFARONI, 2007 p. 135)

Rüthers (2004, p. 110)[16], em seu estudo sobre as ideias de Carl Schmitt, notadamente, em sua crítica a Hobbes, afirma que "[...] se o soberano não pode intrometer-se no foro interno, quando o fizer não resta outra alternativa senão reconhecer que nasce aí um direito de resistência do súdito". Entretanto, insta discordar, especificamente, que esse impasse faça surgir um "direito" de resistência, como se toda e qualquer vontade ou escolha do ser se pautasse num direito reconhecido, pois, como já foi dito alhures, a esfera da intimidade se pauta pela liberdade essencial do ser, e não pelo direito à liberdade, muito menos, por um direito de resistência.

Sobreleva ressaltar que, pelo menos um dos fundamentos que pode ser encontrado para se justificar a garantia da intimidade está no pensamento da filosofia cristã. Quem bem explica esse ponto, numa crítica contundente, é Arendt (2014, p. 91), pois a única atividade que Jesus veio pregar foi a bondade. E a bondade, essencialmente, evita ser vista e ouvida, caso contrário, deixa de ser bondade. Essa afirmativa encontra razão, pois, se um cristão realiza algo que almeja o

16 O estudo de Carl Schmitt sobre o Leviatã de Thomas Hobbes encontra-se em seu texto *Der Leviatán in der Staatslehre des Thomas Hobbes*, 1938.

reconhecimento do domínio público, este não realizou a bondade em si, mas sim, um ato de caridade ou de solidariedade. “Só a bondade deve esconder-se de modo absoluto e evitar toda aparição, pois do contrário é destruída. […] Daí: “Que a tua mão esquerda não saiba o que faz a tua mão direita.”” (ARENDT, 2014, p. 92-93)

Esse entendimento obtido dentro do cristianismo tem sua origem na premissa de que somente Deus “vê em segredo” (ARENDT, 2014, p. 92). Na Bíblia, no livro do Evangelho Segundo Mateus, capítulo 6, versículo de 1 a 18, cujo título é “Fazer as boas obras em segredo”, muitas são as passagens que convalidam o pensamento da autora, pois é dito que “guardai-vos de fazer vossas boas obras diante dos homens, para serdes visto por eles. Do contrário, não tereis recompensa junto de vosso Pai que está no céu.” De igual modo, tem-se que “assim, a tua esmola se fará em segredo; e teu Pai, que vê o escondido, recompensar-te-á.” De forma a reforçar o caráter da onipresença de Deus, inclusive, dentro do recanto da intimidade, Mateus (6,18) afirma que, “assim, não parecerá aos homens que jejuas, mas somente a teu Pai, que está presente ao oculto; e teu Pai, que vê num lugar oculto, recompensar-te-á.”

Portanto, a liberdade de negação[17] para o acesso à esfera da intimidade, encontra-se, inclusive, contra a onipresença e a onipotência de um deus, onde ele apenas consegue obter as informações graças a seus poderes divinos. De outra forma, não lhe seria possível alcançar àquilo que se encontrasse na intimidade.

Após ter-se enfrentado a distinção entre os domínios público e privado, bem como, das esferas da política, do social, da privacidade, da vida privada e da intimidade, de forma a permitir uma melhor visualização dos entendimentos acima, colaciona-se uma representação gráfica, proposta pelo autor da presente pesquisa, idealizada durante a sua realização, que se encontra no diagrama de Euler da Figura 3.

17 Por liberdade de negação entende-se a liberdade que a pessoa possui de impedir quem quer que seja, inclusive a própria tecnologia, de adentrar as suas esferas da privacidade, da vida privada e da intimidade.

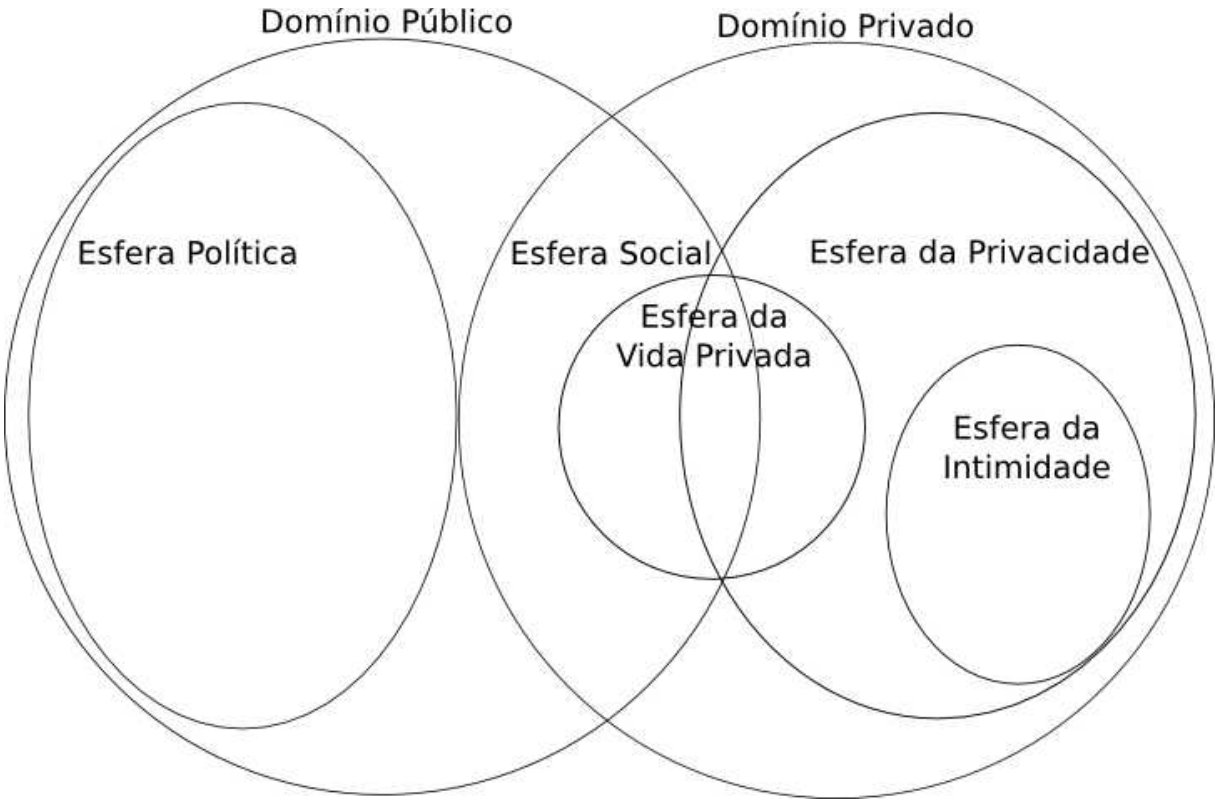

Figura 3 – Domínios e esferas relacionadas com a privacidade.

Também aqui, não é o objetivo da imagem acima, precisar os limites entre os domínios e as esferas, mas tão somente, demonstrar a sua existência e localização. Sobreleva ressaltar que o indivíduo se desloca entre os domínios e as esferas de acordo com a sua vontade.

Por fim, é preciso fazer agora um levantamento das principais previsões legislativas que trazem a luz a proteção à privacidade, à vida privada e à intimidade.

1.5. AS NORMAS DE PROTEÇÃO PARA AS ESFERAS DA PRIVACIDADE, DA VIDA PRIVADA E DA INTIMIDADE

Para Sanden (2014, p. 26-27), “as práticas sociais para obtenção e o uso da informação relativa à pessoa são tão antigas quanto a própria humanidade, assim como a necessidade de se subtrair do olhar alheio.” Ela se remete, então, a um conto sumério chamado Gilgamesh que foi feito há mais de quatro mil anos. Um dos

personagens é Utnapishtim, um eremita que faz questão de não revelar seu nome a Gilgamesh sem que ele justifique os motivos que o trouxeram até ali. Isso reforça o que já foi dito acima, que ninguém deseja que suas informações se tornem, involuntariamente, do conhecimento de terceiros.

Além disso, a coleta de dados pessoais, ainda que em arquivos manuais, já serviu a propósitos diversos, como ocorreu com o nazismo (SANDEN, 2014, p. 27), acelerando e acrescentando nomes às execuções.

Antes de se adentrar no estudo sobre as previsões legais que tratam o tema, é preciso observar que os direitos à privacidade, à vida privada e à intimidade estão ligados as garantias da casa enquanto asilo inviolável[18] e do sigilo de dados[19].

Sobre a inviolabilidade da casa, conforme já tratado no segundo subtópico deste capítulo, o homem necessita de um lugar que é seu, considerado como propriedade privada, onde se estabelece o próprio domínio privado. Logo, é natural que não se permita a intromissão em seu lar sem que, para isso, sejam atendidas algumas exigências legais.

De igual entendimento, os Estados Unidos da América também asseguram esse direito aos seus cidadãos, pois, de acordo com Greenwald (2014, p.12),

> [...] a oposição à invasão da privacidade pelo governo foi um fator decisivo para a fundação dos próprios Estados Unidos, quando colonos norte-americanos protestaram contra leis que permitiam aos agentes do governo britânico saquear qualquer casa que quisessem. Os colonos concordavam que fosse legítimo o Estado obter mandados específicos para revistar pessoas quando os indícios estabelecessem uma causa provável para suas infrações. Mas os mandados genéricos – a prática de submeter a população inteira a revistas indiscriminadas – eram fundamentalmente ilegítimos.
> A Quarta Emenda constitucional entronizou essa ideia no direito norte-americano. Seus termos são claros e sucintos: "O direito dos cidadãos à segurança de sua pessoa, de suas casas, de seus documentos e de seus bens contra revistas e confiscos não fundamentados não será violado, e só

18 O inciso XI do art. 5º da Constituição Federal da República Federativa do Brasil de 1988 – CF/88 afirma que "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;"

19 O inciso XII do art. 5º da CF/88 afirma que "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"

> serão emitidos mandados mediante causa provável, sustentados por juramento ou declaração, e que descrevam em pormenores o local a ser revistado e as pessoas ou coisas a serem confiscadas."

É em função disso que a privacidade sempre entende haver um recanto único que significa o lugar onde o indivíduo pode estar-só.

Para uma melhor segmentação, as principais normas internacionais que versam sobre a privacidade serão trabalhadas. Após isso, é realizado um estudo sobre esse direito no Brasil.

Portanto, a primeira proteção legal sobre a privacidade de nível internacional que se conhece é a Declaração Americana dos Direitos de Deveres do Homem, aprovada na IX Conferência Internacional Americana, que ocorreu na cidade de Bogotá, na Colômbia, no ano de 1948. Seu texto garante, em seus arts. V[20] e X[21], a toda pessoa o direito "à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar, e, à inviolabilidade e circulação da sua correspondência." (CIDH, 1948).

No mesmo ano, a já conhecida Declaração Universal dos Direitos Humanos preconizou em seu art. 12[22] que "ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques." (DHNET, 1948)

Vale citar que o termo "correspondência", previsto em ambas as declarações, sob a égide da era da informação, não se limita ao entendimento de uma carta que se recebe em determinada residência. É preciso, de forma hermenêutica, ampliar essa expressão para toda e qualquer comunicação que também ocorre no mundo digital.

---

20 Artigo V. Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar.

21 Artigo X. Toda pessoa tem o direito à inviolabilidade e circulação da sua correspondência.

22 Artigo 12 – Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques.

O próximo tratado que também enfrentou esse tema foi a Convenção Europeia dos Direitos do Homem, elaborada pelo Conselho da Europa[23], em 1950, que traz em seu art. 8º, §1º[24] que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência." (GDDC, 1950).

O Pacto Internacional dos Direitos Civis e Políticos de 1966, também trouxe em seu art. 17, §1º[25] a previsão de que "ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação." (OAS, 1966)

O respeito a privacidade continuou sendo protegido por várias outras convenções e tratados, a saber: a Convenção Americana sobre Direitos Humanos (PGE, 1969), também conhecida para Pacto de São José da Costa Rica, de 1969, a Resolução número 428 da Assembleia Parlamentar do Conselho da Europa de 1970 (PACE, 1970).

Contudo, após verificar-se que os meios digitais estavam se alastrando e propiciando uma melhor gestão dos níveis de serviços e produtos, entendeu-se que também era necessário, além de proteger a privacidade, proteger os dados pessoais. A partir daí, verifica-se o surgimento de convenções mais elaboradas que trouxeram, também, a exigência legal de implementação de medidas referentes a segurança da informação. Como é o caso da Lei de proteção de dados pessoais do Estado de Hessen na Alemanha (HDSG, 1999), em 1970, que é a **primeira lei de proteção de dados do mundo**. Sua inovação se deu com a proteção do indivíduo e

23 "Não se confunde o Conselho da Europa (organização internacional com sede em Estrasburgo) com o Conselho Europeu (órgão da União Europeia composto pelos chefes de Estado ou de governo dos países-membros). São objetivos do Conselho da Europa: proteger os direitos humanos, o pluralismo democrático e a observância do Estado de direito (*rule of law*); promover a consciência e encorajar o desenvolvimento da identidade e a diversidade cultural da Europa; encontrar soluções comuns envolvendo os desafios relativos à sociedade europeia; consolidar a estabilidade democrática na Europa mediante a construção de reformas políticas e legislativas. A organização internacional Conselho da Europa é atualmente composta por 47 países, sendo que todos os Estados-Membros da União Europeia a integram." (SANDEN, 2014, p. 27)

24 Artigo 8º – 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

25 Artigo 17 – §1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação.

de sua vida privada frente aos bancos de dados eletrônicos do setor privado (SANDEN, 2014, p. 187).

Seguindo essa necessidade, a Organização para Cooperação e Desenvolvimento Econômico editou, em 1980, as Diretrizes sobre Proteção da Privacidade e Fluxo de Dados Pessoais entre Fronteiras (OECD, 2013), sendo seguida, em 1981, pela Convenção para a Proteção dos Indivíduos com Relação ao Processamento Automatizado de Dados Pessoais do Conselho da Europa (COUNCIL OF EUROPE, 1981).

Já em 1990, a Organização das Nações Unidas – ONU editou as Diretrizes sobre Arquivos de Dados Eletrônicos Computadorizados. Em 2000, a Carta de Direitos Fundamentais da União Europeia previu, expressamente, a proteção de dados de caráter pessoal. Por fim, em 2010 e 2013, a União Europeia realizou a Reforma do arcabouço da proteção de dados pessoais (SANDEN, 2014, p. 188-189).

Em 2011, após o evento que ficou conhecido como Primavera Árabe[26], a ONU elaborou um relatório informando que retirar o acesso à Internet do cidadão é um desrespeito aos direitos humanos (PORTAL FÓRUM, 2011). O documento pede ainda que os países garantam o acesso à rede mundial de computadores como um direito fundamental. Ou seja, o objeto de um direito fundamental se trata de uma tecnologia.

Em seguida, devido as denúncias feitas por Edward Snowden, tema tratado no próximo capítulo, Brasil e Alemanha, no mês de novembro de 2014, conseguiram aprovar uma resolução na ONU a fim de proteger o "[...] direito à privacidade em comunicações digitais, assim como a oferta de soluções em casos de quebra da privacidade de seus cidadãos." (O GLOBO, 2014). Sem que fosse preciso haver votação no plenário, esse documento foi aprovado no comitê de Direitos Humanos da Assembleia Geral da ONU.

26 Primavera Árabe é o nome dado a uma onda de protestos que ocorreu em vários países do Oriente Médico e do norte da África a partir de 2011, culminando na queda de quatro ditaduras e na morte de milhares de pessoas. O que se destaca nesse movimento é o fato dele ter se organizado e propagado pela Internet. Em função disso, ficou claro que a grande rede teria se transformado num meio de luta por direitos, em especial, pelos direitos humanos (ESTADÃO, 2015).

Com relação as previsões da legislação brasileira[27], a Constituição Política do Império do Brazil, de 25 de março de 1824, continha apenas o direito a inviolabilidade da propriedade assegurado em seu art. 179, *caput*[28]. Já a Constituição da República dos Estados Unidos do Brasil, de 24 de fevereiro de 1891, também estabeleceu a casa como asilo inviolável no §11, e acrescentou a inviolabilidade do sigilo da correspondência no §18, ambos do art. 72[29]. Na Constituição da República dos Estados Unidos do Brasil, de 16 de julho de 1934, nos itens 8 e 16 do art. 113[30], são garantidos o sigilo da correspondência e a inviolabilidade do lar, respectivamente.

A Constituição dos Estados Unidos do Brasil, de 10 de novembro de 1937, em seu art. 122, no item 6º)[31], previu "a inviolabilidade do domicílio e de correspondência, salvas as exceções expressas em lei." Entretanto, apesar de se encontrar inserida na seção dos direitos e garantias individuais, ela foi suspensa pelo Decreto número 10.358, de 31 de agosto de 1942, que declarou o estado de guerra no Brasil.

---

27 É mister informar que os Atos Institucionais criados durante período correspondente a Ditadura Militar, qual seja, de 1964 a 1985 não foram objeto de análise no presente trabalho.

28 Art. 179. A inviolabilidade dos Direitos Civis, e Politicos dos Cidadãos Brazileiros, que tem por base a liberdade, a segurança individual, e a propriedade, é garantida pela Constituição do Imperio, pela maneira seguinte.

[...]

29 Art.72 – A Constituição assegura a brasileiros e a estrangeiros residentes no paiz a inviolabilidade dos direitos concernentes á liberdade, á segurança individual e á propriedade, nos termos seguintes:

[...]

§11. A casa é o asylo inviolavel do individuo; ninguem póde ahi penetrar, de noite, sem consentimento do morador, senão para acudir a victimas de crimes, ou desastres, nem de dia, senão nos casos e pela fórma prescriptos na lei.

[...]

§18. É inviolavekl o sigillo da correspondencia.

30 Art 113 - A Constituição assegura a brasileiros e a estrangeiros residentes no País a inviolabilidade dos direitos concernentes à liberdade, à subsistência, à segurança individual e à propriedade, nos termos seguintes:

[...]

8) É inviolável o sigilo da correspondência.

[…]

16) A casa é o asilo inviolável do indivíduo. Nela ninguém poderá penetrar, de noite, sem consentimento do morador, senão para acudir a vítimas de crimes ou desastres, nem de dia, senão nos casos e pela forma prescritos na lei.

31 Art 122 – A Constituição assegura aos brasileiros e estrangeiros residentes no País o direito à liberdade, à segurança individual e à propriedade, nos termos seguintes:

[...]

6º) a inviolabilidade do domicílio e de correspondência, salvas as exceções expressas em lei;

A suspensão desse direito apenas cessou com a Constituição dos Estados Unidos do Brasil, de 18 de setembro de 1946, que trouxe em seus §§ 6º e 15 do art. 141[32], novamente, o sigilo da correspondência e a casa como asilo inviolável, respectivamente.

O direito fundamental à privacidade aparece com mais clareza na Constituição da República Federativa do Brasil, de 24 de janeiro de 1967, quando em seus §§ 9º e 10 do art. 150[33] preleciona que "são invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas", além de assegurar a inviolabilidade do lar, respectivamente. Nota-se assim, um aumento das garantias, que agora englobam formas mais modernas de comunicação, por onde, consequentemente, transitam informações pessoais.

Ainda que a Constituição da República Federativa do Brasil de 1967 tenha sofrido uma Emenda Constitucional, a de número 1, de 17 de outubro de 1969, as garantias de inviolabilidade da correspondência e das comunicações telegráficas e telefônicas continuaram sendo mantidas, bem como, a casa enquanto asilo inviolável, apenas tendo sido deslocadas para os §§ 9º e 10 do art. 153[34].

---

32 Art 141 – A Constituição assegura aos brasileiros e aos estrangeiros residentes no País a inviolabilidade dos direitos concernentes à vida, à liberdade, a segurança individual e à propriedade, nos termos seguintes:
[...]
§6º – É inviolável o sigilo da correspondência.
[…]
§15 – A casa é o asilo inviolável do indivíduo. Ninguém, poderá nela penetrar à noite, sem consentimento do morador, a não ser para acudir a vitimas de crime ou desastre, nem durante o dia, fora dos casos e pela forma que a lei estabelecer.

33 Art 150 – A Constituição assegura aos brasileiros e aos estrangeiros residentes no Pais a inviolabilidade dos direitos concernentes à vida, à liberdade, à segurança e à propriedade, nos termos seguintes:
[...]
§9º – São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas.
[…]
§10 – A casa é o asilo inviolável. do indivíduo. Ninguém pode penetrar nela, à noite, sem consentimento do morador, a não ser em caso de crime ou desastre, nem durante o dia, fora dos casos e na forma que a lei estabelecer.

34 Art. 153. A Constituição assegura aos brasileiros e aos estrangeiros residentes no País a inviolabilidade dos direitos concernentes à vida, à liberdade, à segurança e à propriedade, nos têrmos seguintes:
[...]
§9º É inviolável o sigilo da correspondência e das comunicações telegráficas e telefônicas.

É apenas na Constituição da República Federativa do Brasil, de 05 de outubro de 1988, que várias garantias relacionadas com o direito fundamental à privacidade são percebidas. Na verdade, foram precisos três incisos para cercar a privacidade das garantias necessárias. É somente nessa Carta Magna que se encontram os termos intimidade, vida privada, honra e imagem das pessoas. Aqui também se encontram as proteções de sigilo da correspondência, das comunicações telegráficas e telefônicas. A grande inovação que essa constituição realizou foi inserir, expressamente, o **sigilo de dados**. Todas essas previsões, acrescidas da inviolabilidade do lar, estão previstas nos incisos X, XI e XII de seu art. 5º.[35]

Segundo Pedra (2012), todo esse garantismo erigiu do receio de uma volta à ditadura militar no Brasil, que fez com que tivéssemos um extenso rol de cláusulas pétreas[36] na atual constituição, "[...] haja vista que o legislador constituinte de 1987-1988 estava embalado por seus sonhos nos pós-regime autoritário de 1964-1984."

A Constituição Federal de 1988 previu também um remédio útil ao direito fundamental à privacidade. É o *habeas data*, que está previsto no inciso LXIX de seu art. 5º[37], tendo sido regulamentado pela Lei número 9.507, de 12 de novembro de 1997. Esse dispositivo tem por finalidade, conforme o art. 7º da referida lei, assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; para a retificação de dados, quando não se prefira fazê-lo por

35 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
[...]
X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

36 As cláusulas pétreas são previsões legais que não podem ser abolidas em hipótese alguma, nos termos do inciso IV, do §4º do art. 60 da Constituição Federal de 1988.

37 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
LXIX – conceder-se-á mandado de segurança para proteger direito líquido e certo, não amparado por *habeas corpus* ou ***habeas data***, quando o responsável pela ilegalidade ou abuso de poder for autoridade pública ou agente de pessoa jurídica no exercício de atribuições do Poder Público;

processo sigiloso, judicial ou administrativo; e, para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável. Logo, permite o controle de informações pessoais por parte de qualquer indivíduo.

Sobre o sigilo de dados, novamente aqui, nota-se que uma evolução tecnológica obrigou o Direito a acrescentar essa nova modalidade de comunicação em sua garantia fundamental, pois como Bastos e Grandra (1989, p. 73) afirmam, "[...] a expressão "dados" manifesta uma certa improbidade", pois ela não é o "[...] objeto de comunicação, mas uma modalidade tecnológica de comunicação." Mas antes que se adentre a esse debate, é preciso trazer ao presente trabalho as exceções que compreendem na violação do direito fundamental à privacidade.

A primeira delas é a possibilidade de interceptação das comunicações telefônicas, conforme a própria Lei número 9.296, de 24 de julho de 1996, que a regulamenta para fins de "investigação criminal ou instrução processual penal". Contudo, a ordem judicial somente poderá ser conferida se houverem "indícios razoáveis da autoria ou participação em infração penal, ou se a prova não puder ser feita por outros meios disponíveis, ou ainda, se o fato investigado não constituir infração penal punida, no máximo, com pena de detenção". Entretanto, mesmo que a interceptação telefônica seja deferida, a ação principal deve correr "sob segredo de justiça", conforme o *caput* do art. 1º[38] da referida lei. Isso, por si só, reafirma a importância do direito à privacidade, pois ainda que um crime esteja sendo investigado, mesmo assim, o número de pessoas que terá acesso a essa intromissão na vida privada do indivíduo será reduzido àqueles com acesso aos autos da ação principal.

Por último, mas não menos importante, frisa-se que as interceptações telefônicas deverão durar pelo período de quinze dias, renováveis, justificadamente, por, apenas e tão somente, mas quinze dias, de acordo com o art. 5°[39] da lei supramencionada. A

38 Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, **sob segredo de justiça**.
39 Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova.

única exceção a essa regra se encontra no art. 136[40] da Constituição Federal de 1988, que decreta o Estado de Defesa, onde esse período é prorrogado pelo prazo de trinta dias renováveis por igual período. Além disso, o Estado de Defesa impõe, expressamente, restrições ao sigilo da correspondência e da comunicação telegráfica e telefônica[41].

Entretanto, o prazo de duração das interceptações telefônicas está sendo debatido de forma acirrada pelo Supremo Tribunal Federal – STF através do Recurso Extraordinário número 625263, interposto pelo Ministério Público Federal, que assim procedeu no momento em que o Superior Tribunal de Justiça – STJ concedeu *habeas corpus* anulando as escutas telefônicas que teriam durado mais de dois anos, ininterruptamente, durante uma investigação criminal ocorrida no Estado do Paraná.

Para o Ministério Público Federal, aceitar o posicionamento do STJ é abrir um precedente para todos os casos onde essa situação se verificou, ou seja, vários casos onde as interceptações telefônicas duraram um período acima daquele permitido por lei.

---

40 Art. 136. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, decretar estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções na natureza.
§ 1º - O decreto que instituir o estado de defesa determinará o tempo de sua duração, especificará as áreas a serem abrangidas e indicará, nos termos e limites da lei, as medidas coercitivas a vigorarem, dentre as seguintes:
I - restrições aos direitos de:
a) reunião, ainda que exercida no seio das associações;
b) sigilo de correspondência;
c) sigilo de comunicação telegráfica e telefônica;
II - ocupação e uso temporário de bens e serviços públicos, na hipótese de calamidade pública, respondendo a União pelos danos e custos decorrentes.
§ 2º - O tempo de duração do estado de defesa não será superior a **trinta dias**, podendo ser prorrogado uma vez, por igual período, se persistirem as razões que justificaram a sua decretação.
[...]
41 Vide nota de rodapé número 39.

O STF reconheceu a existência de repercussão geral[42] para o tema[43], momento em que recebeu do recurso. Atualmente, este aguarda julgamento. Contudo, insta salientar que o Ministro Gilmar Mendes já informou que a jurisprudência do STF “tem se manifestado sobre o assunto, admitindo, em algumas hipóteses, a possibilidade de renovação do prazo das interceptações telefônicas.” (STF, 2013)

Não é o objetivo aqui debater a questão suscitada, porém, é preciso observar ao que já se referiu, de que o processo onde as escutas são realizadas deve correr sob segredo de justiça, ou seja, ainda assim, resguardando o direito à privacidade do(s) indivíduo(s) envolvido(s). Ao mesmo tempo, utilizar-se da interceptação telefônica por período superior a dois anos pode se mostrar descabido, devendo ser aceito somente se demonstradas fundadas razões para isso. Todavia, em que pese a observância da Constituição e da Lei para que o Estado Democrático de Direito não se valha de justificações genéricas, tais como a segurança nacional, de forma a convalidar ações, aparentemente, perniciosas.

Sobre a inserção feita pela Constituição Federal de 1988 no direito à privacidade, qual tenha sido, a sigilo de dados, Ferraz Júnior (1993) informa que essa inovação “[...] trouxe com ela dúvidas interpretativas que merecem, por isso mesmo, uma reflexão mais detida.” Segundo ele, “sigilo não é o bem protegido, não é o objeto do direito fundamental. Essa garantia diz respeito à faculdade de agir (manter sigilo,

---

42 A Repercussão Geral é um instrumento processual inserido na Constituição Federal de 1988, por meio da Emenda Constitucional 45, conhecida como a “Reforma do Judiciário”. O objetivo desta ferramenta é possibilitar que o Supremo Tribunal Federal selecione os Recursos Extraordinários que irá analisar, de acordo com critérios de relevância jurídica, política, social ou econômica. O uso desse filtro recursal resulta numa diminuição do número de processos encaminhados à Suprema Corte. Uma vez constatada a existência de repercussão geral, o STF analisa o mérito da questão e a decisão proveniente dessa análise será aplicada posteriormente pelas instâncias inferiores, em casos idênticos. A preliminar de Repercussão Geral é analisada pelo Plenário do STF, através de um sistema informatizado, com votação eletrônica, ou seja, sem necessidade de reunião física dos membros do Tribunal. Para recusar a análise de um RE são necessários pelo menos 8 votos, caso contrário, o tema deverá ser julgado pela Corte. Após o relator do recurso lançar no sistema sua manifestação sobre a relevância do tema, os demais ministros têm 20 dias para votar. As abstenções nessa votação são consideradas como favoráveis à ocorrência de repercussão geral na matéria. (STF, 2015)

43 PROCESSO PENAL. INTERCEPTAÇÃO TELEFÔNICA. ALEGAÇÃO DE VIOLAÇÃO AOS ARTIGOS 5º; 93, INCISO IX; E 136, § 2º DA CF. ARTIGO 5º DA LEI N. 9.296/96. DISCUSSÃO SOBRE A CONSTITUCIONALIDADE DE SUCESSIVAS RENOVAÇÕES DA MEDIDA. ALEGAÇÃO DE COMPLEXIDADE DA INVESTIGAÇÃO. PRINCÍPIO DA RAZOABILIDADE. RELEVÂNCIA SOCIAL, ECONÔMICA E JURÍDICA DA MATÉRIA. REPERCUSSÃO GERAL RECONHECIDA.
(RE 625263 RG, Relator(a): Min. GILMAR MENDES, julgado em 13/06/2013, ACÓRDÃO ELETRÔNICO DJe-176 DIVULG 06-09-2013 PUBLIC 09-09-2013)

resistir ao devassamento), conteúdo estrutural do direito. (FERRAZ JÚNIOR, 1993). Entretanto, quando se trata de dados digitais, manter sigilo ou resistir ao devassamento se torna precário como forma de proteger informações pessoais.

Ainda sobre isso, o fato da redação do inciso XII do art. 5º da CF/88 não se referir, expressamente às comunicações de dados, causa dúvida, permitindo várias interpretações. Observando o trecho atacado, verifica-se que "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas." Nota-se, então, que a única modalidade transmissão de informações que não possui a palavra "comunicações" a antecedendo, é a de dados.

Isso pode levar a interpretação de que apenas os dados estáticos, ou seja, armazenados, é que são objeto de proteção estatal. Entretanto, com a rede ou a comunicação de dados, esse entendimento deve ser realizado de forma teleológica[44] a fim que abarcar todo o tipo de processamento que o dado venha a sofrer. Logo, uma garantia constitucional que se preze a proteger o dado, mas não a comunicação do dado, é uma garantia sem qualquer finalidade em si.

Esse tipo de comportamento aparece, por exemplo, no art. 8º da Constituição do Estado do Espírito Santo quando ela afirma que:

> Art. 8º – Não poderão constar de registro, ou de bancos de dados de entidades governamentais ou de caráter público, as informações referentes a convicção política, filosófica ou religiosa nem as que se reportem a filiação partidária ou sindical, nem as que digam respeito à vida privada e à intimidade pessoal, salvo quando se tratar de processamento estatístico e não-individualizado.

Em nenhum momento a comunicação de dados se mostra assegurada por essa previsão, mas tão somente, o dado que está na qualidade de armazenado, o que não deixa de ser uma garantia, mas, incompleta, pois, conforme se verificará no capítulo a seguir, durante a transmissão, o dado pode ser interceptado, processado

---

44 Segundo Violante (2000, p. 123-124), "[...] busca-se descobrir qual o sentido atribuído ao texto, pela vontade do legislador. Confundia-se, assim, a pesquisa do sentido de uma lei com o sentido que a ela desejou atribuir a vontade do legislador. A reação da doutrina contra tal orientação alcançou grande êxito, por mostrar o erro que consistia em procurar, na lei, apenas a *vontade do legislador*. […] A busca da vontade do legislador deve ser entendida sempre no sentido da compreensão da *finalidade da lei*."

e sequer chegar a ser armazenado, somente aplicando-se essa proteção legal através da hermenêutica.

O que se pretende afirmar é a incompletude dessas previsões legais. Em momento nenhum se pretendeu excluir as restrições no armazenamento de dados, mas sim, ampliar essa previsão a fim de que também proteja os dados enquanto transmitidos, e não somente armazenados. Essa preocupação se verifica quando Sanden (2014, p. 21) informa que "com a brutal queda nos custos de armazenagem, transmissão e processamento da informação, a minimização da coleta de dados pessoais não encontra estímulo econômico nem técnico."

De gradação infraconstitucional, as normas relativas a proteção de dados encontram-se nos crimes de violação, sonegação ou destruição de correspondência; de violação de comunicação telegráfica, radioelétrica ou telefônica[45]; de violação da correspondência comercial[46]; da divulgação de segredo[47]; da violação de segredo

45 Violação de correspondência
Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
Pena - detenção, de um a seis meses, ou multa.
Sonegação ou destruição de correspondência
§1º - Na mesma pena incorre:
I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;
Violação de comunicação telegráfica, radioelétrica ou telefônica
II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;
III - quem impede a comunicação ou a conversação referidas no número anterior;
IV - quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal.
§2º - As penas aumentam-se de metade, se há dano para outrem.
§3º - Se o agente comete o crime, com abuso de função em serviço postal, telegráfico, radioelétrico ou telefônico:
Pena - detenção, de um a três anos.
§4º - Somente se procede mediante representação, salvo nos casos do §1º, IV, e do §3º.
46 Correspondência comercial
Art. 152 - Abusar da condição de sócio ou empregado de estabelecimento comercial ou industrial para, no todo ou em parte, desviar, sonegar, subtrair ou suprimir correspondência, ou revelar a estranho seu conteúdo:
Pena - detenção, de três meses a dois anos.
Parágrafo único - Somente se procede mediante representação.
47 Divulgação de segredo
Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
Pena - detenção, de um a seis meses, ou multa.
§ 1º Somente se procede mediante representação.
§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.
§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

profissional[48] e da invasão de dispositivo informático[49], todos do código penal brasileiro.

A Lei número 8.078, de 11 de setembro de 1990, que instituiu o Código de Defesa do Consumidor, em sua Seção VI, arts. 43 e 44[50], também confere direitos aos consumidores de acessarem suas informações constantes de cadastros e outros registros pessoais. Não obstante, ainda se observam normas, no mesmo código,

---

48Violação do segredo profissional
Art. 154 – Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
Pena – detenção, de três meses a um ano, ou multa.
Parágrafo único – Somente se procede mediante representação.

49 Art. 154-A. 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:
Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I – Presidente da República, governadores e prefeitos;
II – Presidente do Supremo Tribunal Federal;
III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

50 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, 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.
§1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.

nos arts. 72 e 73[51] que prevêem crimes para aqueles que impedirem, dificultarem e deixarem de corrigir as informações sobre o consumidor que constarem de seus cadastros ou registros.

A problemática da transmissão e do armazenamento de dados é melhor tratada na Lei 12.965, de 23 de abril de 2014, também conhecida como Marco Civil da Internet, que "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". Aqui, são afirmados alguns direitos e garantias fundamentais, em especial, a proteção da privacidade.

Em seu art. 7º são assegurados alguns direitos, em especial, os dos incisos VIII, IX e X, que seguem transcritos abaixo.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> [...]
> VIII – informações claras e completas sobre **coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais**, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX – **consentimento expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X – **exclusão definitiva dos dados pessoais** que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> [...]

Depreende-se daí o cuidado que o legislador teve com a privacidade do indivíduo. Entretanto, a realidade se mostra muito diferente, pois a tecnologia não respeita e não observa normas, tão-pouco sofre influência de seu poder coercitivo.

---

§1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado.
§2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código.

51 Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
Pena Detenção de seis meses a um ano ou multa.
Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
Pena Detenção de um a seis meses ou multa.

Ainda sobre o Marco Civil da Internet, extrai-se outra inteligência trazida por ele. Salienta-se, no entanto, a diferença entre o provedor de conexão com a Internet do provedor de aplicações de Internet. O primeiro é responsável pela interconexão de um usuário com a grande rede. Já o segundo, diz respeito as empresas que prestam algum tipo de serviço na rede mundial, como um e-mail gratuito ou uma rede social.

Ambos os provedores têm a obrigação de manter os *logs*, ou seja, arquivos que contenham as informações necessárias para identificar o usuário, como a data, a hora e o endereço IP, que é um número que o usuário recebe ao se conectar na rede mundial. Esse número é único no mundo no momento em que um usuário o está utilizando. O endereço IP será melhor tratado no capítulo a seguir.

A identificação do usuário pode se dar em dois momentos distintos. O primeiro é quando ele se conecta com a Internet, sendo essa informação de responsabilidade do provedor de conexão com a Internet. Já o segundo, identifica que aplicação de Internet um usuário acessou e em que data e hora.

Todavia, de forma que nenhuma empresa detenha todas as informações pessoais de um usuário, o art. 14[52] veda que o provedor de conexão com a Internet guarde também as informações de acesso às aplicações de Internet. Aqui se constata uma grande atenção e inteligência do legislador[53], muito embora, esse comando também não esteja sendo observado por empresas que atuam na grande rede.

Assim, verifica-se que o direito fundamental à privacidade, além de ser uma garantia fundamental, também está previsto em várias outras normas jurídicas. Contudo, sem que seja necessário atacar a validade, eficácia e eficiência de toda a legislação, pende demonstrar que a tecnologia vem sendo empregada no sentido da não observância de todas as previsões legislativas.

---

52 Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

53 Sobreleva ressaltar que a elaboração do texto do projeto de lei do Marco Civil da Internet foi fruto da parceira entre a Escola de Direito da FGV-Rio e do Ministério da Justiça, e ocorreu em duas fases de quarenta e cinco dias cada, onde qualquer internauta pôde participar diretamente sugerindo alterações no texto do projeto. Sendo assim, ao se falar em legislador, tem-se que levar em consideração que o próprio povo também participou da criação dessa lei. Sobre isso, de forma catedrática, ensina Teixeira (2012).

Se nas esferas da privacidade, da vida privada e da intimidade não é possível “entrar no indivíduo”, a única forma de se alcançá-las encontra-se no momento em que a pessoa deposita as informações relativas àquelas esferas dentro de um dispositivo computacional.

Por se tratar de uma coisa, notadamente, de um bem imóvel[54], a propriedade privada cerca e protege aqueles que se localizam dentro de seu espaço físico, servindo de limite. Mas isso não garante que, em nenhum momento, os assuntos que lhe são pertinentes não extrapolem suas fronteiras contra a vontade de seus conviventes. É aqui que os recursos tecnológicos agem, pois se a casa é asilo inviolável, e possui como fronteiras, a terra, o ar e/ou o mar, a tecnologia abre uma nova frente, imaterial, imperceptível e ilimitável, que é o virtual.

A conclusão é que, embora o ordenamento jurídico assente toda uma sistemática de proteção para a privacidade, esta não é suficiente para impor limites ao virtual. Portanto, não basta assegurar a privacidade e a liberdade se, mesmo assim, a tecnologia desrespeita a norma. Se o direito positivado não garante a privacidade e a liberdade necessária, é preciso saber contra-utilizar[55] a tecnologia como forma de se alcançar esses direitos. Para comprovar o que aqui é alegado, todas as infrações perpetradas pela tecnologia são demonstradas no capítulo a seguir.

54 Por não se incluir no objeto de estudo, as questões atinentes aos moradores de rua e aos movimentos daqueles que não possuem uma propriedade imóvel não são tratados pelo presente trabalho.

55 A ideia de se aplicar a contra-utilização da tecnologia é a mesma empregada na inteligência e contrainteligência militar.

2. A FRAGILIZAÇÃO DO DIREITO FUNDAMENTAL A PRIVACIDADE EM DECORRÊNCIA DO AVANÇO TECNOLÓGICO: IMPACTOS DA ERA DA INFORMAÇÃO.

Verificada a evolução do direito fundamental à privacidade, ainda que esse se segregue em privacidade, vida privada e intimidade, faz-se necessário observar a norma que o assegura correlacionando-a com as tecnologias existentes, notadamente, a tecnologia da informação.

Mas para que isso seja possível, é preciso que se detenha um conjunto mínimo de saberes, de forma que estes proporcionarão um melhor entendimento sobre o funcionamento dos principais dispositivos que ganharam lugar no cotidiano das pessoas. Inicialmente, são analisadas literaturas que retratam uma realidade desprovida de privacidade para o indivíduo. Após isso, são abordados, de forma objetiva, o histórico e o funcionamento das principais tecnologias encontradas em uso atualmente.

Não obstante, também serão tratados os impactos que essas tecnologias provocam no direito fundamental à privacidade, demonstrando que é preciso repensar a forma de sua utilização ou, então, a implementação de mecanismos capazes de reestabelecer a privacidade.

Contudo, cumpre salientar que não é o foco do presente estudo, abordar questões como as câmeras de monitoramento em estabelecimentos privados ou em locais públicos. Da mesma forma, outros mecanismos tecnológicos não foram abordados, como a presença de etiquetas RFID[56], dentre outros recursos, que são inseridos em alguns documentos, como o passaporte. Sobre isso, ver Aton Edwards (2014).

56 RFID é o acrônimo para Radio-Frequency IDentification. Essas etiquetas permitem uma identificação automática por meio de sinais de rádio frequência.

2.1. A IMPORTÂNCIA DA PROTEÇÃO A PRIVACIDADE: DE 1984 À ATUALIDADE

O tema privacidade demonstra ser objeto de preocupação de vários autores, porém, alguns deles traduziram de forma pormenorizada e com perfeição o que seria viver em uma sociedade sem privacidade.

No romance de George Orwell, intitulado 1984, é observado um relato detalhado da ideia do autor sobre uma sociedade vivendo em completa ausência de privacidade. Os posfácios frisam que o autor foi influenciado pelo pós Segunda Guerra Mundial, porém, seu livro condiz com a realidade atual, sendo, inclusive, citado por Edward Snowden[57] como um alerta para a sociedade. Vale ressaltar que a referida obra se vale da seguinte premissa: a informação é o bem mais preciso. Quem a detém, detém o poder, principalmente, sobre o indivíduo.

Em 1984, Orwell recria o mundo dividido em três grandes países, são eles: Oceânia, Eurásia e Lestásia. Oceânia era governada pelo Grande Irmão (*Big Brother*) líder do Partido. O governo era organizado em quatro ministérios: o Ministério da Paz, que cuidava dos assuntos de guerra; o Ministério da Verdade, que tratava as mentiras; o Ministério do Amor, que praticava a tortura; e o Ministério da Pujança, que lidava com a escassez de alimentos. Na hierarquia social, tinha-se o Grande Irmão, o Núcleo do Partido, o Partido Exterior e, finalmente, os Proletas.

A vítima dessa história se chama Winston Smith, cidadão de Oceânia, que trabalhava para o Ministério da Verdade, onde sua função era recriar o passado alterando a verdade dos fatos, sempre em benefício do Partido. Contudo, ele percebe que o que o Partido fazia era manipular as informações sempre com o intuito de manter o domínio sobre a população. O controle sobre a informação permitia ao Partido recriar o passado.

---

57 Edward Snowden denunciou o programa de monitoramento global criado pelo governo dos Estados Unidos da América. Esse tópico é tratado no subtítulo 2.4.7.

Mas essa não era a única estratégia, pois até mesmo os filhos eram ensinados nas escolas a identificar e denunciar comportamentos suspeitos de seus pais dentro de casa. Da mesma forma, deveriam proceder colegas de trabalho e amigos pessoais. Tecnologicamente, a cidade possuía escutas instaladas com a finalidade de gravar toda e qualquer conversa que conseguisse captar.

No entanto, um dispositivo chamado Teletela era o que se demonstrava como sendo o mais invasivo, pois estava presente em todo e qualquer cômodo existente, fosse uma residência ou um local de trabalho. A Teletela tinha a capacidade de exibir informações enviadas pelo Partido, assim como, a função de transmitir tudo o que acontecia no cômodo onde se encontrasse instalada.

Diante desse cenário, não existia um lugar comum oriundo do princípio da exclusividade onde se poderia "ficar só". Isso se verifica, uma vez que, com já foi dito, a Teletela estava presente em todo e qualquer cômodo, sempre captando e transmitindo as informações do interior destes. Isso quer dizer que mesmo que Winston estivesse em seu quarto, deitado em sua cama para dormir, lá estaria uma Teletela[58]. O intuito do Partido era saber tudo, inclusive, "o que o indivíduo estaria pensando".

Mesmo correndo um risco muito grande, Winston decide comprar um diário e passa a preenchê-lo diariamente, sempre tomando o cuidado para que a Teletela não captasse essa ação, pois, certamente, ele seria preso ou condenado a morte. Tamanha era a ausência de privacidade que os membros de Oceânia aceitavam correr esses riscos para terem um momento sem que o Grande Irmão os estivesse observando. No momento em que Winston escuta os avisos transmitidos por esse peculiar dispositivo, ele escreve em seu diário a frase: "abaixo o grande irmão" (ORWELL, 2009, p. 29). Nesse momento, ele acabara de cometer um Pensamento-Crime, ou seja, o simples fato de pensar ou agir de forma contrária a filosofia do Partido, conhecida como *socing*, transformava o indivíduo em suspeito. Segundo Orwell (2009, p. 29-30) "o pensamento-crime não era uma coisa que se pudesse disfarçar para sempre. Você até conseguia se esquivar durante algum tempo, às

58 Apesar de não ser objeto do presente trabalho, insta citar que esse livro foi o que inspirou o programa de *reality show* conhecido como *Big Brother*, exibido no Brasil pela Rede Globo.

vezes durante anos, só que mais cedo ou mais tarde, com toda a certeza, eles o agarrariam.” O procedimento de vigiar e agir era feito pelo Polícia das Ideias, uma força estatal que se valia de todos os recursos disponíveis para se investigar uma pessoa.

Para Winston, a privacidade “[...] era uma coisa muito valiosa. Todo mundo queria ter um lugar em que pudesse estar a sós de vez em quando.” (ORWELL, 2009, p. 166). Foi a ausência de privacidade que o levou a lutar contra o sistema instaurado.

Orwell se vale de uma invenção já existente a época, no caso, a televisão, para abordar os riscos existentes em se ter um aparelho dentro das casas, ou seja, muito próximo a privacidade das pessoas. A televisão é inofensiva, pois não tem a capacidade de transmitir o conteúdo de dentro para fora das casas, entretanto, é justamente nesse ponto que o autor cria a Teletela. Em sua história, a privacidade deixou de ser um direito fundamental, garantida pelo Estado, por ter sido invadida pelo avanço tecnológico. O autor afirma que,

> Com o desenvolvimento da televisão e o avanço técnico que possibilitou a recepção e a transmissão simultâneas por intermédio do mesmo aparelho, a vida privada chegou ao fim. Todo os cidadãos, ou pelo menos todos os cidadãos suficientemente importantes para justificar a vigilância, podiam ser mantidos vinte e quatro horas por dia sob os olhos da polícia, ouvindo a propaganda oficial, como todos os outros canais de comunicação fechados. A possibilidade de obrigar a todos os cidadãos a observar a estrita obediência às determinações do Estado e completa uniformidade de opinião sobre todos os assuntos existia pela primeira vez. (ORWELL, 2009, p.242-243)

Sobreleva ressaltar que a evolução tecnológica narrada no livro foi utilizada para realizar o monitoramento de cidadãos suspeitos, e esse era o argumento que justificava esse tipo de vigilância. Ainda que esse pensamento derive de um romance, isso se verifica na realidade contemporânea, onde países se valem do mesmo discurso de forma a justificar todo tipo de controle do cidadão em nome da segurança nacional. Para Krohling, Tessarolo e Pertel (2013, p.15 e 17) "em nome da nova panaceia da segurança nacional se aceitam excessos impensáveis antes contra a liberdade individual.”

Depreendem-se desse cenário, as inquestionáveis e pertinentes semelhanças existentes entre uma Teletela e um computador. Note-se que ambos possibilitam o recebimento de informações, assim como, também, a transmissão destas. Numa análise sumária, a única diferença se encontra na questão onde a Teletela serve as vontades do Estado, que a controla, e, o computador, serviria as vontades de seus usuários.

Cumpre salientar que o conhecimento acerca dos dados privados e íntimos do indivíduo permite a sua manipulação, como é o caso em que Winston é torturado com o uso de ratos, onde o Partido veio a saber que este era o maior pavor dele. Esse ponto do romance é fundamental, pois o personagem chega ao seu limite após essa sessão de tortura.

De toda forma, dada a virtualização das informações, é possível concluir que o computador é o repositório mais consistente acerca dos dados de seu usuário. Além disso, quando se conecta esse mesmo dispositivo com a rede mundial de computadores, tem-se a possibilidade de coleta de várias informações. Isso, *de per si*, constata as possibilidades de transgressões contra a privacidade.

De forma a propiciar um melhor entendimento sobre os caminhos pelos quais a privacidade do indivíduo vem sendo dilapidada, é preciso compreender, minimamente, o conhecimento sobre como a tecnologia funciona, notadamente, o computador e a Internet, conforme será feito a seguir.

2.2. A PESSOALIDADE DO COMPUTADOR: DO CÁLCULO A GUARDA DOS DADOS PESSOAIS

Inicialmente, insta salientar que, etimologicamente, a palavra computador originou-se da palavra em latim *computare*, que significa calcular (DECHILE, 2014). Logo, foi a necessidade de se realizar operações matemáticas com mais eficiência que deu origem a invenção desse dispositivo.

Como exemplo dessa necessidade, pode-se citar o ábaco, instrumento mecânico utilizado para realização de cálculos matemáticos de adição e subtração, criado na mesopotâmia há 3.500 a.C. (UFF, 2012). Séculos mais tarde, em 1642, Blaise Pascal criaria uma calculadora que desempenharia o mesmo papel. Essa é a chamada geração zero de computadores, conhecidos por serem mecânicos, ou seja, dependiam diretamente da intervenção humana para a realização de suas operações. Posteriormente, em 1972, Babbage cria as máquinas diferencial e analítica, que trouxeram avanços significativos para a computação.

Com o início da Segunda Guerra Mundial, os recursos empregados fizeram os computadores evoluir para a primeira geração, datada de 1945 a 1955, onde suas operações eram realizadas por válvulas, que dispensava a intervenção humana. Esses dispositivos chegavam a ocupar vários andares de um edifício. Considerado o primeiro computador digital, o *Eletronic Numerical Integrator And Computer*, comumente conhecido como ENIAC, pesava 30 toneladas e ocupava uma área de 180 m^2 (TECNOBLOG, 2011), conforme mostra a figura 4.

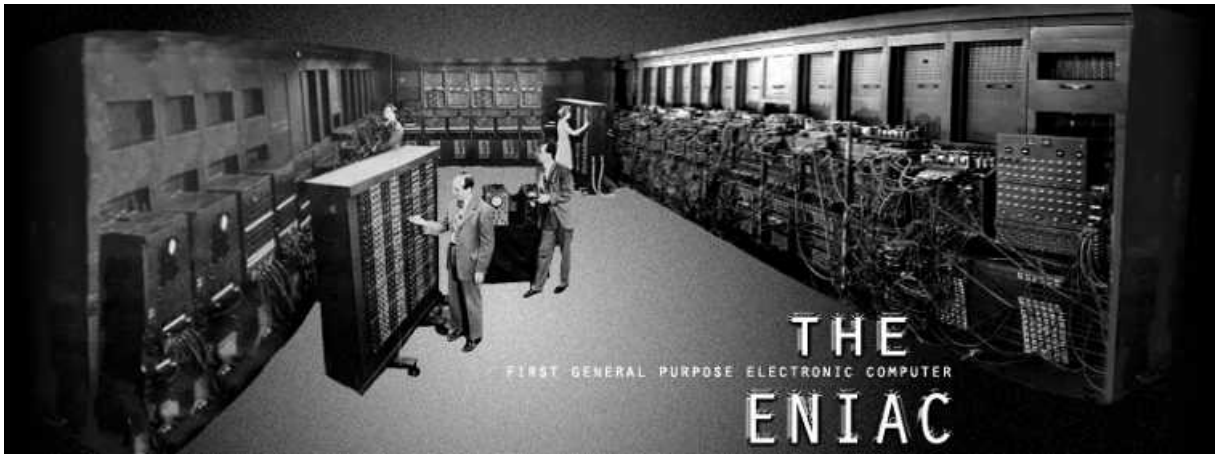

Figura 4 – ENIAC – O primeiro computador eletrônico.
Fonte: http://the-eniac.com/wp-content/uploads/2011/01/eniaclogo_755x281.jpg

Ainda sobre essa geração de computadores, foi durante a Segunda Guerra Mundial que eles desempenharam um papel fundamental para a vitória dos Aliados. Alan Turing, matemático inglês, idealizou uma máquina, que ficou conhecida como COLOSSUS, que foi desenvolvida com a finalidade de quebrar a criptografia utilizada pelo exército alemão (VEJA, 2015, p. 89), cujas mensagens eram codificadas por uma máquina chamada ENIGMA. Todas as mensagens eram

interceptadas pelos ingleses, que não conseguiam decifrá-las com o trabalho humano, pois o número de combinações possíveis chegava a 159.000.000.000.000.000.000. E, para agravar a situação, as combinações eram mudadas diariamente. Ou seja, todo o trabalho desempenhado em um dia era inutilizado no dia seguinte. Apenas quando a equipe de Alan Turing identificou que determinadas partes das mensagens se repetiam, foi possível identificar o padrão de cifragem. Então, os ingleses começaram a decifrar as mensagens nazistas em tempo real com a COLOSSUS, permitindo o estabelecimento de uma estratégia com rápidas tomadas de decisão. Por causa desse fato, o matemático John von Neumann, que também participou do desenvolvimento da máquina inglesa, criou uma arquitetura que é a base da computação moderna, a chamada máquina de von Neumann.

Sobreleva ressaltar a utilização da criptografia pelo exército alemão para a mantença do sigilo das comunicações e informações contendo dados sensíveis sobre as investidas durante a Segunda Grande Guerra.

Após a primeira geração, o computador evoluiu para a sua segunda (1955), terceira (1965) e quarta (1980) gerações, sendo as válvulas substituídas por transístores e, posteriormente, por circuitos integrados, o que elevou demasiadamente seu poder de processamento. Apenas para exemplificar, o ENIAC possuía a capacidade de realizar cinco mil operações por segundo, onde, atualmente, um processador[59] de mercado chega a realizar três bilhões de operações por segundo (UFF, 2012).

Esse crescimento exponencial se deve a Lei de Moore. Gordon Moore, um dos fundadores da empresa fabricante de processadores Intel, observou que o número de transístores numa pastilha de silício – matéria-prima para os processadores modernos – dobrava a cada 18 meses. Com isso, é possível estimar o poder de processamento de máquinas futuras[60].

59 O processador é um componente presente nos dispositivos computacionais responsável por realizar todos os cálculos requisitados, além de administrar os demais recursos do equipamento.

60 A Lei de Moore se convalida, uma vez que, o crescimento estimado por ela se dá com a redução do tamanho do transístor, fazendo com que mais transístores caibam numa mesma patilha de silício. O efeito colateral dessa manobra se dá justamente por isso. O transístor vem sendo reduzido de tal forma que, atualmente, seu tamanho já está próximo ao do átomo de silício. Sendo esse um limite natural. Já existem estudos que apontam como o processador será desenvolvido quando essa limitação for alcançada, como, por exemplo, a computação quântica, os nanotubos de carbono,

Verificando-se que o computador aumentava a sua capacidade de processamento enquanto reduzia o seu tamanho, assim como, seu custo, e, apesar das apostas contra essa tendência[61], foi inevitável que ele se tornasse acessível a quem o desejasse. Esses dispositivos receberam o nome de *Personal Computers* – PC ou Computadores Pessoais, também chamados de Microcomputadores, mais comumente encontrados, atualmente, em sua versão portátil, ou seja, como *notebook*, também chamados de *netbooks* ou *laptops*.

O aspecto da pessoalidade que se confere as essas máquinas é constatado no contexto anterior ao da rede mundial de computadores, pois estes ficavam isolados, sendo apenas possível a troca ou o acesso aos dados pessoais por meio dos chamados disquetes[62], o que exigia o acesso físico ao local onde se encontrasse o dispositivo informático. Por permanecer inacessível a terceiros e dentro das residências de seus proprietários, o computador se tornou um local onde são armazenadas todo tipo de informação, inclusive, as privadas e íntimas de seus usuários.

Vale mencionar que os *smartphones*, também desenvolvidos sob a arquitetura de von Neumann, são pequenos computadores que possuem uma alta capacidade de armazenamento de informação. E a concepção de pessoalidade faz com que eles também sejam tratados da mesma forma que um computador pessoal, ou seja, a cada momento, a confiança sobre o sigilo das informações depositadas na tecnologia aumenta.

Essa situação se agrava com a quinta geração de computadores. Segundo Tanenbaum (2007, p.15) ela será composta de computadores invisíveis.

> No futuro, computadores estarão por toda parte e embutidos em tudo – na verdade, invisíveis. Eles serão parte da estrutura da vida diária, abrindo portas, acendendo luzes, distribuindo dinheiro e milhares de outras coisas. dentre outros.

61 Essa afirmação se refere a declaração de Ken Olson, presidente e fundador da Digital Equipment Corp., fabricante de computadores de larga escala, conhecidos como Mainframe, que afirmou, categoricamente: “Não há razão para que alguém queira ter um computador em casa.” (UFF, 2012) Da mesma forma, T. J. Watson, antigo presidente da IBM, disse que o mercado mundial de computadores correspondia a 4 ou 5 unidades (TANENBAUM, 2007, p. 11)

62 O disquete é um dispositivo móvel de armazenamento utilizado nos primeiros anos dos computadores pessoais.

> Esse modelo, arquitetado pelo Falecido Mark Weiser, foi denominado originalmente **computação ubíqua**, mas o termo **computação pervasiva** também é usado agora com frequência (Weiser, 2002). Ele mudará o mundo com tanta profundidade quanto a Revolução Industrial. (negritos no original)

Essa evolução computacional vai de encontro a outro avanço tecnológico, no caso, a Internet das Coisas, que será abordada mais a frente.

Por esse motivo, de forma a compreender a fragilização da privacidade pela tecnologia da informação, faz-se necessário trazer um conhecimento mínimo sobre o surgimento e o funcionamento da Internet, essencial para que os operadores do direito possam verificar os impactos dela advindos. É o que se faz no tópico a seguir.

2.3. DA ORIGEM E FUNCIONAMENTO DA INTERNET

Em 1950, durante o período da Guerra Fria nos Estados Unidos da América, uma rede de comunicação foi idealizada com o intuito de possuir dois atributos fundamentais para a sua utilização: a redundância e a resiliência das informações trafegadas. Tudo porque, caso alguma base militar sofresse um ataque nuclear, as suas informações não poderiam ser perdidas. (TANENBAUM, 2007).

Pensando nisso, foi criada, em 1958, a *Advanced Research Projects Agency* – ARPA. Após isso, o Departamento de Defesa dos Estados Unidos solicitou a uma empresa, RAND Corporation, que encontrasse uma solução. No entanto, somente em 1960 foi que Paul Baran, um dos funcionários daquela empresa, propôs a utilização de um modelo amplamente distribuído. Seus diagramas são exibidos na figura 5 que traz três formas de interação em rede, são elas: a centralizada, a descentralizada e a distribuída.

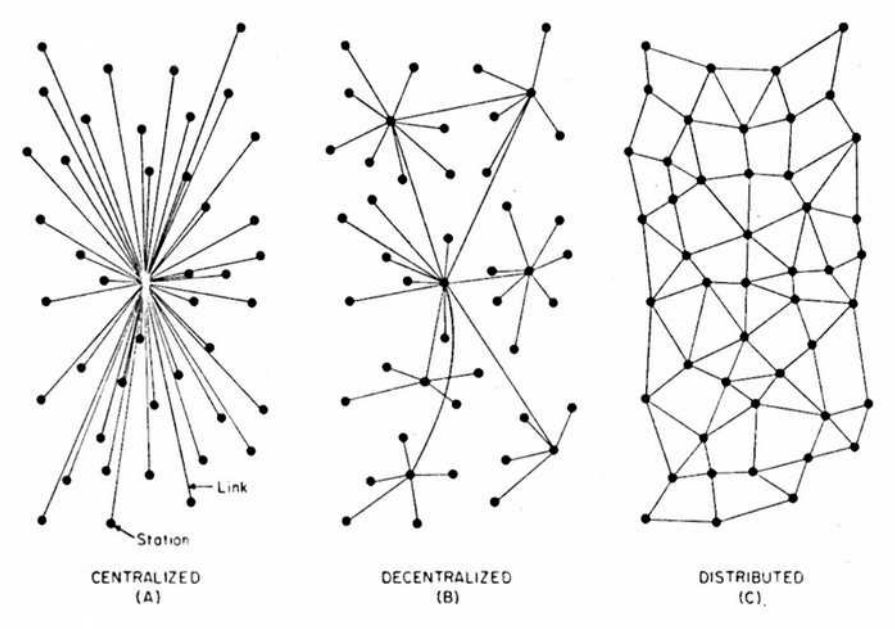

Figura 5 – Diagrama de comunicação em rede.
Fonte: Nêposts.

Os pontos da figura 5 são chamados de nó e as linhas de links ou conexões. Numa análise sumária, as desvantagens do modelo centralizado são a existência da interconexão por apenas um nó, ou seja, sem ele, não há rede, e o alto poder de controle sobre a informação trafegada. Já o modelo descentralizado, ainda que possua vários nós para interligação, ainda assim, possui a fragilidade caso um nó específico venha a ser neutralizado. Por fim, o sistema distribuído impede um controle sobre a informação trafegada e, além disso, disponibiliza vários caminhos por seus nós, propiciando, assim, uma grande interação entre eles.

Uma vez escolhido o modelo distribuído, a *Advanced Research Projects Agency* – ARPA criou, em 1967, a ARPANET, que já utilizava o modelo TCP/IP (*Transmission Control Protocol* / *Internet Protocol*), que será explicado adiante. Durante as pesquisas, essa rede chegou a interligar até quatro universidades[63], entretanto, somente as instituições que possuíssem um contrato com o Departamento de Defesa americano é que estariam autorizadas a se conectar a essa malha. Diante desse obstáculo a *National Science Foundation* – NSF desenvolveu uma rede nos mesmos parâmetros que foi conhecida como NSFNET. Tamanho foi o sucesso dessa iniciativa que o governo se viu impelido a entregar a operação da rede à

63 As universidades interligadas foram as Universidades da Califórnica, Los Angeles e Santa Barbara; *Stanford Research Institute* – SRI; e a Universidade do Utah.

indústria (TANENBAUM, 2007, p.60). Após isso, o número de redes que utilizam a mesma arquitetura e o mesmo modelo foram aumentando, momento em que vários continentes se interligaram. Analisando esse cenário é possível compreender porque a Internet é uma “rede de redes.” (TEIXEIRA, 2012, p. 44).

A parte física das redes é composta por cabos e dispositivos[64], tais como *hubs*, *switches*, roteadores, *gateways*, dentre outros, que as interconectam. Atualmente, existem também as chamadas redes Wi-Fi[65], comumente conhecidas como redes sem fio, onde os acessos são realizados, geralmente, por frequências de rádio. Insta evidenciar que toda e qualquer informação que trafega numa rede, obrigatoriamente, passa por vários desses dispositivos.

Com relação a comunicação interna, ou seja, a parte lógica da rede, Sudré Filho e Martinelli (2014, p. 205-206) explicam que uma rede de computadores se interconecta por meio de protocolos. “Basicamente, um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação”. (TANENBAUM, 2003: p.29).

Assim, qualquer programa[66], de acordo com a sua finalidade, deve utilizar um determinado protocolo para realizar essa comunicação. Pensando nisso, foi necessário delimitar um conjunto mínimo de protocolos para que qualquer dispositivo interligado a Internet conseguisse enviar e receber informações. Como dito acima o modelo utilizado é o TCP/IP (*Transmission Control Protocol / Internet Protocol*), comumente chamado também de Pilha de Protocolos TCP/IP.

Muito embora esse modelo carregue apenas as siglas de dois de seus protocolos mais importantes, o primeiro corresponde ao conjunto que se encarrega de transmitir os dados de forma confiável através da grande rede, e o segundo de identificar, através de um endereço único, o computador que se conectou a rede, pois é necessário saber tanto a origem quanto o destino de uma informação. No momento

64 O presente estudo não possui o condão de analisar, especificamente, cada equipamento utilizado para o funcionamento de uma rede.
65 O termo Wi-Fi é de propriedade da Wi-Fi Alliance e significa *Wireless Fidelity*, que em português quer dizer Fidelidade Sem Fio.
66 A palavra programa também significa aplicação, *software*, aplicativo ou sistema que quer dizer um conjunto de funcionalidades instaladas num computador.

em que um computador, *smartphone* ou qualquer dispositivo se conecta a Internet este recebe um endereço IP – *Internet Protocol*, único em todo o mundo e que permanece o mesmo até o final de sua conexão. Assim, de posse do endereço IP, data e hora de sua utilização, é possível identificar a origem do acesso.

Alinhado com os constantes avanços tecnológicos, notadamente, com a Internet das Coisas, que será tratada posteriormente, o endereço IP, em sua versão atual, a 4.0 ou IPv4, encontrou o seu limite de utilização. Devido ao esgotamento dos endereços disponíveis da versão 4.0 do IP (IPv4) desde junho de 2012, a Internet vem utilizando, conjuntamente com o IPv4, a versão 6.0 ou IPv6, do protocolo IP. O IPv6 proporcionará a conexão de "5,6 x 10^{28}" (cinco vírgula seis vezes dez elevado a vinte e oito) endereços IP por ser humano (IPv6.br, 2012). Isso significa dizer que, atualmente, já é possível que, além dos computadores e *smartphones*, também fogões, geladeiras, televisores, condicionadores de ar, chuveiros, interruptores de energia elétrica, automóveis, dentre outros, podem se conectar a Internet. Vale mencionar que o IPv4 permanecerá ativo até que a migração para o IPv6 seja realizada.

Já a primeira sigla do modelo TCP/IP, a do Protocolo de Controle de Transmissão – TCP, além de se fazer constar, ela também representa o conjunto de vários outros protocolos que fornecem os recursos necessários para que o envio e recebimento de dados pela Internet seja possível. Cada protocolo fornece um tipo diferente de serviço. A tabela 1 relaciona os principais e mais utilizados protocolos com os tipos de serviço providos por cada um.

Protocolo	Tipo de serviço
HTTP – *HyperText Transfer Protocol*	Envio e Recebimento de Páginas Web
HTTPS – *HyperText Transfer Protocol Secure*	Envio e Recebimento Seguro de Páginas Web
POP3 – *Post Office Protocol 3*	Recebimento de E-mail
SMTP – *Simple Mail Transfer Protocol*	Envio de E-mail
IMAP – *Internet Message Access Protocol*	Envio e Recebimento de E-mail
FTP – *File Transfer Protocol*	Transferência de arquivos

Tabela 2 – Principais protocolos utilizados na Internet.
Fonte: Tanenbaum (2003)

Os protocolos realizam a comunicação através da Internet utilizando-se de mensagens. E como se sabe, uma mensagem pode ter diversos tamanhos. Assim, caso ela exceda o tamanho estabelecido pelo protocolo, ela será dividida em tantos pacotes quantos forem necessários. Cada pacote de informação recebe um cabeçalho contendo os endereços de origem e destino e podem seguir um caminho diferente até o objetivo final. Segundo Tanenbaum (2003), os pacotes são mensagens curtas que fazem parte da mensagem original. Para exemplificar, deve-se observar a figura 6 que ilustra uma rede de computadores.

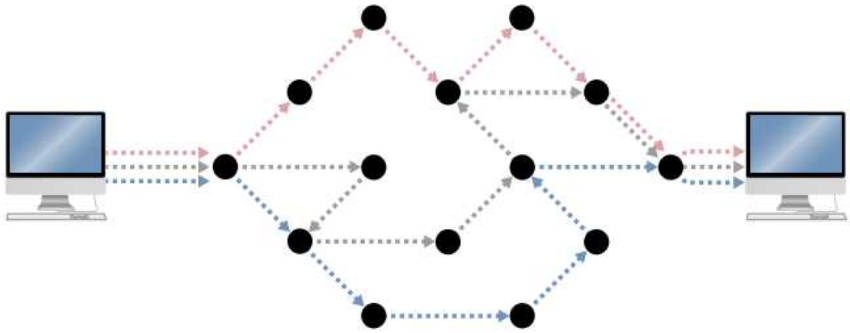

Figura 6 – Uma rede de redes de computadores.
Fonte: European Digital Rights[67].

Observando a figura 6, nota-se a existência de três caminhos distintos, uma rosa, um cinza e um azul. Cada ponto significa um equipamento de interconexão existente ao longo da rede. Logo, caso um computador envie uma mensagem para o outro e esta possua um tamanho maior do que o permitido por pacote pelo protocolo, ela será dividida em vários outros pacotes. Cada pacote poderá percorrer um caminho diferente, e eles não precisam chegar na mesma ordem em que foram enviados. O computador que emitiu a mensagem envia também a quantidade e a ordem correta dos pacotes para que o computador de destino possa reorganizá-los de forma que a mensagem consiga ser lida.

Mesmo que a Internet tenha sido entregue a indústria, “os padrões da arquitetura Internet TCP/IP não são elaborados por órgãos internacionais de padronização, como a ISO ou o IEEE.” Quem coordena esse desenvolvimento é um comitê denominado IETF – *Internet Engineering Task Force*[68], “[...] formado pela

67 O link para o documento que contém a imagem é: http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf
68 Antes da coordenação passar para a IETF, ela pertencia ao IAB – *Internet Activity Board*.

comunidade internacional de designers de rede, operadores, fornecedores, e pesquisadores preocupados com a evolução da arquitetura da Internet.[69]" (IETF, 2015). Por esse motivo, "qualquer pessoa pode projetar, documentar, implementar e testar um protocolo para ser usado na Internet." No entanto, para que um protocolo se transforme num padrão para a Internet, é preciso "[...] documentá-lo através de uma RFC – *Request for Comments*." Após isso, são realizados testes, e, se o protocolo se tornar estável, um membro do IETF pode propôr ao comitê que ele seja incorporado a pilha de protocolos. Se isso ocorrer, a RFC será publicada indicando que o protocolo se tornará um padrão. Se em seis meses não houver nada em desfavor, o IETF incorpora o protocolo declarando-o um Internet *Standard*. (SOARES, LEMOS, COLCHER, 1995, p.142-143).

Por conseguinte, cada protocolo listado na tabela 1 possui uma RFC que regulamenta, com precisão, o seu funcionamento. Para se pesquisar uma RFC, deve-se acessar o link do IETF – *Internet Engineering Task Force*, clicar no link RFC *Pages* e, após isso, clicar em RFC *Search Page*[70]. A pesquisa pode ser realizada diretamente pelo número da RFC ou por alguma palavra-chave.

Uma RFC em especial deve ser analisada, pois representa o formato utilizado para o envio e recebimento das mensagens pela Internet, notadamente, o conteúdo da informação enviada. É a RFC 822 – *Internet Message Format*[71], ou Formato de Mensagem da Internet.

Em sua seção 2.3, a RFC 822 informa que o corpo das mensagens na grande rede são composto, simplesmente, "[...] de linhas e caracteres US-ASCII[72]." O que equivale a dizer que toda mensagem que trafega na Internet, o faz em texto claro, ou seja, se algum desses pacotes for interceptado, será possível ler o seu conteúdo. De forma análoga, podemos citar um exemplo onde se envia, pelos correios, um segredo escrito num cartão-postal a outra pessoa. Ao final do percurso deste cartão,

69 No original: *The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.*
70 O link direto para acesso a essa sessão é: http://www.rfc-editor.org/search/rfc_search.php
71 Link para a RFC 822: http://www.rfc-editor.org/rfc/rfc2822.txt
72 ASCII é o acrônimo de *American Standard Code for Information Interchange*, e corresponde a uma tabela de caracteres alfanuméricos e especiais.

todos os funcionários dos correios que tiveram contato com ele, potencialmente, saberão o segredo.

Esse padrão permite que todas as ações de um internauta sejam monitoradas, relavando-se um grande risco para a privacidade do indivíduo. Os principais efeitos dessa arquitetura são analisados no tópico a seguir.

2.4. USAR, OU NÃO USAR, EIS A QUESTÃO: A TECNOLOGIA COMO FERRAMENTA DE ACESSO AOS DADOS PESSOAIS

Ante a todo o exposto, cumpre esclarecer agora, como a tecnologia, devido a sua forma de funcionamento, não observa a privacidade do indivíduo, cabendo então, ao Direito, a tarefa de rever esse ponto de modo a conferir validade à norma vigente, pois as ferramentas abordadas coletam informações a revelia do usuário.

Logo quando a Internet começou a ser utilizada, por ser um "lugar" desconhecido, onde muitos internautas[73] sequer tinham o correto entendimento do que estavam realizando enquanto navegavam[74], havia uma preocupação quanto ao fornecimento dos dados pessoais, onde muitos desconfiavam de *websites*[75] que exigiam informações como nome, sobrenome, e-mail, dentre algumas outras. Um dos motivos que levaram os internautas a temer o envio de dados pessoais se deve aos notórios crimes que ocorriam com informações financeiras, especificamente, com cartões de crédito que eram utilizados na *web*[76].

Ainda assim, a grande rede se mostrou propicia ao comércio, se iniciando então, a era do comércio eletrônico. De forma a aumentar a confiança dos usuários para a utilização da Internet como ambiente de compras, as empresas investiram na

73 Internauta, assim como, usuário, são termos utilizados para se referir aos usuários de Internet no momento em que a utilizam.
74 Navegar é o termo utilizado para a utilização da Internet por um Internauta.
75 *Website*, *site*, sítio, página são nomes que designam um lugar de hipertexto na Internet.
76 *Web*, Grande Rede, Rede Mundial, Rede Mundial de Computadores ou Mundo Virtual são termos utilizados que se referem a Internet.

criptografia como meio de se aumentar a segurança e a confiabilidade nas transações realizadas. Ressalte-se a utilização da criptografia como solução para o sigilo das informações.

Tamanho foi o sucesso dessa iniciativa que a confiança na *web*, ainda que precária, se estabeleceu, pois os usuários proviam suas informações às empresas ou outras partes com as quais já se mantinha algum tipo de contato. Posteriormente, foram desenvolvidos mecanismos com a finalidade de monitorar e armazenar dados pessoais. Cumpre destacar que foi em função do comércio eletrônico que a Internet implementou certa segurança de forma a tornar a grande rede um lugar de transações financeiras. Desse ponto em diante, a tecnologia ganhou cadas vez mais a confiança de seus usuários de modo que, atualmente, determinadas informações que antes eram consultadas e fornecidas diretamente pelo indivíduo, ficam sob a responsabilidade da tecnologia.

Segundo Radfahrer (2013), os usuários terceirizaram suas consciências para as máquinas, onde, atualmente, já se verificam esses efeitos quando não se é possível recordar um número de telefone, seja de um parente próximo, por exemplo, sem que a agenda telefônica seja consultada. Da mesma forma, não se recordam mais endereços, pois é possível simplesmente procurar por eles utilizando-se palavras-chaves em *sites* de busca. Em outras palavras, confiamos demais na tecnologia, delegando para ela o que antes era uma atribuição pessoal.

De acordo com o estudo de McLuhan (2009, p. 129-130) “[...] o cérebro é extremamente plástico. Ele tem a capacidade de esticar, de estender o mundo para os objetos que você usa.” Isso quer dizer que o cérebro enxerga os dispositivos eletrônicos como uma extensão do próprio corpo. Pragmaticamente, isso significa que a confiança na tecnologia aumenta naturalmente a medida em que ela se integra ao cotidiano do indivíduo. Infere-se então, que essa é a causa de uma demasiada utilização da tecnologia, enquanto que não lembrar o número do telefone da própria residência é a consequência.

Some-se a isso a falta de conhecimento acerca do funcionamento da tecnologia, ou seja, da entrega massiva dos dados pessoais sem a compreensão do que pode ocorrer, reafirmando-se aqui, o que já foi dito nos subtítulos 2.2 e 2.3, que o computador possui um caráter de pessoalidade transformando-se num dispositivo pessoal de armazenamento de informações privadas e íntimas totalmente acessíveis através da Internet.

Para corroborar esse ponto, os principais recursos empregados na utilização da rede mundial são abordados a seguir.

2.4.1. *Cookies*: arquivos armazenadores e fornecedores de informações pessoais

Conforme já mencionado, a maioria dos sites requer o fornecimento de dados comuns, como nome, sobrenome, e-mail, dentre outros. Ocorre que, um problema sempre era verificado quando se tentava acessar o mesmo *website*, pois era necessário proceder com o preenchimento dos mesmos dados repetidas vezes. Foi pensando nesse problema que essa técnica foi desenvolvida.

Cookies são pequenos arquivos, em geral, no formato de texto claro, que residem na máquina do usuário, cuja finalidade é armazenar o máximo de informação reutilizável sobre ele de forma que, no momento em que este retornar ao *site*, será identificado sem a necessidade de responder as mesmas informações. Sua implementação pode ocorrer de duas formas: *cookies* de sessão, que somente armazenam dados enquanto o usuário está utilizando o sítio; ou, *cookies* permanentes, que persistem na máquina do usuário até que sejam excluídos ou até o final de sua duração – quando já pré-configurada pelo *site*.

Cookies são uma realidade largamente aplicada na Internet, de modo que, é improvável que um usuário esteja navegando sem que essa técnica seja utilizada. Mas é de se observar que os navegadores possuem a opção de desabilitar esse

funcionamento quando esta for a expressa manifestação de vontade do usuário, devendo ele se dirigir as preferências do referido programa para desabilitá-la.

Mas como meio para forçar o usuário a manter esse recurso habilitado, alguns *websites* exigem que o *cookie* esteja ativado para que se possa usufruir de seus serviços.

Muito embora possuam uma utilização favorável ao internauta, esse recurso passou a ser largamente empregado para, além de armazenar, monitorar o seu comportamento durante a navegação na página. Não demorou muito para que outra vantagem também fosse percebida, a de que sites parceiros ou concorrentes pudessem pesquisar informações em diferentes *cookies* armazenados. Isso faz com que os dados pessoais do indivíduo sejam fornecidos sem o seu prévio conhecimento. Além disso, o usuário passa a ser alvo de uma vigilância constante enquanto se encontra conectado a rede mundial. Vigilância essa, feita por todo tipo de página, tais como: redes sociais, lojas, mídia, sites de governo, dentre outros.

Além da utilização dos *cookies*, essas informações também são compartilhadas em tempo real com sites parceiros, enquanto se está em uma página. De forma a demonstrar essa ocorrência, exibe-se uma imagem que traz a aplicação de um *plug-in*[77] chamado *Lightbeam*[78]. A função dessa ferramenta é informar ao internauta quais *sites* o estão monitorando e/ou compartilhando os seus dados, conforme a figura 7.

77 *Plug-in* são pequenos programas que são instalados para serem utilizados junto a um navegador.
78 O *plug-in Lightbeam* está disponível para o navegador Firefox. Para obter maiores informações, acesse: https://addons.mozilla.org/En-uS/firefox/addon/lightbeam/

Figura 7 – Gráfico do Lightbeam.
Fonte: http://lwn.net/images/2013/10-lightbeam-graph.png

A Figura 7 exibe os *websites* que estão monitorando o usuário no momento em que ele está navegando pela rede mundial. Destaque-se a diversidade de seguimentos que realizam esse tipo de monitoramento. Para Bauman(2013), o intuito desse constante controle é criar um perfil ou padrão para o indivíduo.

Além disso, esse tipo de fiscalização gera como resultado, o conhecimento sobre vários aspectos da vida pessoal e privada do indivíduo, tais como:

- sua religião;
- sua opinião política;
- suas preferências sexuais;
- doenças que porventura possua;
- seu círculo de relacionamentos; e
- seus interesses em serviços ou produtos específicos;

Toda essa coleta influencia na utilização da Internet. Pariser (2012) esclarece que a grande rede aprende tanto sobre o Internauta e armazena essas informações em

sua máquina de forma que se ele pesquisar pela palavra “felicidade” utilizando seu computador obterá um resultado, ao passo que, se realizar a mesma pesquisa através de outro computador, obterá um retorno completamente diverso do primeiro.

Isso, *de per si*, traduz os motivos pelos quais existe o interesse de empresas em coletar todo e qualquer tipo de informação sobre um usuário. Contudo, muito embora o motivo alegado seja o de construir um perfil de consumo do usuário, essas informações são apenas uma pequena parte de tudo o que é rastreado do usuário.

2.4.1.1. O caso do programa Navegador da Oi

Sobreleva ressaltar o caso do programa conhecido como Navegador, que era fornecido pela empresa de telecomunicações Oi.

Fruto da parceria entre a Oi e a empresa britânica Phorm, o *software*[79] Navegador “[...] mapeava o tráfego de dados do consumidor na Internet de modo a compor seu perfil de navegação. Tais perfis eram comercializados com anunciantes, agências de publicidade e portais da web, para ofertar publicidade e conteúdo personalizados.” (INTERNET LEGAL, 2014). Essas ações ocorreram sem o conhecimento do usuário que utilizava o referido programa. Por esse motivo, eles sequer foram alertados sobre a segurança dos seus dados pessoais.

As funcionalidades implementadas pelo programa Navegador faziam com que o tráfego de dados do usuário fosse filtrado de modo a permitir a construção do seu perfil de navegação.

Essa ocorrência foi denunciada e apurada pelo Departamento de Proteção e Defesa do Consumidor (DPDC) da Secretaria Nacional do Consumidor, que multou a empresa Oi em R$ 3,5 milhões por violar várias previsões legais, inclusive, constitucionais.

79 Os termos *software*, aplicativo e programa designam construções feitas em linguagem de máquina para sua utilização por usuários de computador.

Demonstrado que um simples programa instalado na máquina do usuário tem o poder de reunir todas as informações que julgar pertinente, e sem a sua prévia autorização, é de se analisar o comportamento de outros produtos que também fazem uso da grande rede, como é o caso das Smart TVs.

2.4.2. Smart TV: o perigo bem diante de seus olhos

Uma Smart TV é uma televisão que oferece "[...] vários níveis de conectividade, seja por meio da Internet ou convergindo com outros aparelhos multimídia[80] disponíveis no mercado [...]" (ZOOM, 2014). Aparentemente, esse produto não ofereceria risco quanto a coleta de dados de seus usuários, mas o fazia sem que estes fossem informados.

Essa fato ocorreu com os consumidores da Smart TV da empresa LG. O primeiro caso aconteceu quando o usuário Doctor Beet descobriu que sua Smart TV estava coletando dados referentes ao seu comportamento durante a sua utilização mesmo com a função de compartilhamento desligada. Segundo ele, os nomes de arquivos que estivessem em HDs externos[81] também eram enviados para a fabricante.

Num primeiro pronunciamento, a LG não reconheceu esse tipo de monitoramento. Foi quando então, mais um usuário informou que esse comportamento ocorria, fornecendo, inclusive, detalhes sobre o seu funcionamento. Segundo ele,

> […] o nível de monitoramento é mais profundo do que se pensava: a Smart TV envia um log de autorização à LG toda a vez que é ligada e outro de desautorização quando é desligada. Trocando em miúdos, a empresa sabe quanto tempo seus usuários ficam na frente na TV, além de enviar informações não só de drives externos mas também de pastas compartilhadas com PCs através do recurso Smart Share: ele confirmou o lance ao mover os arquivos para outra pasta […] (MEIOBIT, 2013)

80 Recursos Multimídia são aqueles que trabalham com textos, gráficos, áudios, vídeos e animações, indo além do simples cálculo feito pelo computador. Atualmente, a maioria dos computadores possuem recursos multimídia.
81 HD externo é um dispositivo de armazenamento computacional utilizado para se realizar cópias de segurança (*backup*), transportar dados e manter arquivos que poderão ser compartilhados.

A partir daí, a empresa reconheceu a realização da vigilância quantos aos hábitos e preferências do usuário, admitindo que os faz sem a autorização de seus clientes por considerar que esses dados são “públicos”.

Com isso, sua principal concorrente nesse seguimento, a empresa Samsung, informou que não coletaria dados de HDs externos e nem de pastas compartilhadas, mas se silenciou sobre monitorar os hábitos de seus usuários.

Dessa forma, fica claro que, além do computador, outros recursos também são utilizados para o acúmulo de dados pessoais. Outro exemplo disso, são os *smartphones*[82], pequenos aparelhos que substituíram o já obsoleto aparelho celular.

2.4.3. *Smartphones*: a onipresença da violação da privacidade

A notória evolução tecnológica da telefonia móvel obrigou a todos a possuírem um aparelho *smartphone*. Isso porque, atualmente, é impossível viver sem programas de mensagem como o Whatsapp[83], ou sem as Mídias Sociais, como o Facebook, Twitter[84], dentre outros.

Na verdade, os *smartphones* mostraram que eles podem ser utilizados para várias outras funções além de chamadas de telefonia móvel. Isso porque, também são construídos sobre o modelo já abordado no subtítulo 2.2 supra, qual seja, a Máquina de von Neumann. Por esse motivo, pode-se dizer que esses aparelhos são pequenos computadores que são carregados, em média, na quantidade de 01 (hum) aparelho por indivíduo.

---

82 *Smartphone* são aparelhos que acumulam as funções de um telefone celular e de um computador (WEBOPEDIA, 2015, tradução nossa).
83 Whatsapp é um aplicativo para *smartphones* que permite a troca de mensagens e arquivos de forma instantânea. O link para acesso ao site do fabricante é http://www.whatsapp.com/
84 O Twitter pode ser acessado através do link https://twitter.com/

Muito embora existam vários modelos de *smartphone*, o mercado é dominado pelos sistemas operacionais[85] de três grandes marcas, Google, Apple e Microsoft, respectivamente, são eles: Android, iOS e Windows Phone. O número de usuário ativos no mundo chega a 1 bilhão para o Android, 800 milhões para o iOS e 60 milhões para o Windows Phone (TECMUNDO, 2013).

Igualmente ao computador, esses dispositivos carregam consigo uma grande quantidade de dados pessoais, como, por exemplo: contatos, mensagens privadas e do correio eletrônico enviadas e recebidas, documentos, imagens, vídeos, a geolocalização do usuário, dentre outros.

Malte Spitz (TED.COM, 2012), um cidadão alemão, se utilizou de um remédio constitucional similar ao *habeas data* previsto no inciso LXIX do art. 5º da Constituição Federal de 1988, para que sua operadora de telefonia móvel, a empresa Deutsche Telekom, entregasse todas as informações que possuísse no período de seis meses, os quais foi seu usuário. O resultado foi espantoso, pois os dados de todos os lugares em que esteve, mapeados através de suas informações de geolocalização, durante esse período foram entregues, especificando, inclusive, a data, a hora, e, consequentemente, a sua permanência no local. Não fosse o suficiente, ainda foi possível identificar mais de trinta e cinco mil atividades que ele realizou, incluindo *posts*[86] em suas redes sociais, blogs e *sites* privados. Isso revelou o poder que as operadoras de telefonia celular possuem com relação a coleta e o monitoramento de seus clientes. Não se sabe, até então, se esses dados teriam sido compartilhados com parceiros da empresa ou com terceiros.

Mas o fato é que os *smartphones* podem se transformar em verdadeiras escutas telefônicas, além de possibilitarem o acesso as informações pessoais mencionadas acima.

---

85 Sistema operacional é o sistema que executa o *smartphone*, fazendo a ponte entre o *hardware* e os *softwares* instalados no aparelho.

86 *Post* é um jargão que se traduz no ato de publicar um conteúdo na Internet, especialmente, em Redes Sociais ou Blogs.

2.4.4. Mídias Sociais

Outra grande ferramenta que fragiliza o direito fundamental a privacidade são as mídias sociais, tais como: Facebook, Twitter, Instagram, LindedIn, dentre outras. Todos eles focam seus serviços no provimento de uma rede de relacionamentos, pois é dessa forma que seus usuários entregam, voluntariamente, seus dados pessoais. Muito embora um indivíduo não se relacione, efetivamente, com todos os seus contatos, é comum e notório ele possuir centenas deles. Isso potencializa a sua exposição.

O que se quer dizer, é que quando um usuário posta uma informação, este não o faz no intuito de, diretamente, publicizá-la, mas sim, porque está se relacionando com outra pessoa. Isso se confirma, por exemplo, pela existência de *chats* privados, onde o conteúdo das comunicações não é violado, mas tão somente, visualizado pelas partes envolvidas. Entretanto, este se torna de ciência também da mídia social.

Com o intuito de coletar o máximo de dados possível, essas mídias manipulam seus usuários procedendo com experiências para analisar suas reações. Recentemente, o Facebook manipulou o *feed* – página onde são exibidas os *posts* dos usuários para os seus contatos, também conhecida como mural – de seiscentos mil internautas para fazer um experimento social (CANALTECH, 2014). O experimento se deu com a inclusão de conteúdos positivos e negativos para os usuários, onde se media a influência disso em suas futuras publicações. A conclusão foi a de que os internautas são “[...] sim influenciados pelo que aparece no nosso feed, uma vez que ele é capaz de manipular o que sentimos, positiva ou negativamente.” (CANALTECH, 2014). Isso implica dizer que o Facebook tem o poder de manipular as emoções daqueles que estão inseridos em sua rede de relacionamentos.

Cumpre mencionar que esses testes foram feitos sem o consentimento dos participantes escolhidos. O Facebook chegou a ser acusado de tratar seus usuários como “ratos de laboratório”, pois, para Adam Kramer, cientista encarregado por essa

pesquisa “[...] afirmou gostar de ter trabalhado no Facebook porque era o maior banco de dados sobre o comportamento humano no mundo.” (CANALTECH, 2014)

Sobreleva ressaltar que as informações coletadas foram oriundas de *posts* que se faziam em seus murais, necessitando-se recordar que os internautas possuem vários informações privadas depositadas no Facebook. Sendo assim, constata-se que o poder dessa mídia social extrapola os limites da esfera privada.

Novamente, verifica-se a finalidade perniciosa de se criar um perfil do usuário para que este seja fornecido, a título gratuito ou oneroso, às empresas de publicidade ou parceiras. Na realidade, cada mídia social tem a capacidade de identificar o perfil de seu usuário, cada um, dentro de sua esfera atuação. Mas o ponto de contato entre todas elas é o de que o internauta é produtor de conteúdo.

Apenas para exemplificar, o Twitter exige a interação por meio da postagem de imagens, ou de mensagens no limite de cento e quarenta caracteres. O que lhe rendeu o apelido de microblog. Já o Instagram, é uma mídia social de relacionamentos com base em imagens que são enviadas por seus usuários. O LinkedIn se perfaz numa rede de contato corporativa que possui o foco na carreira profissional do indivíduo.

O fato do usuário ser o provedor de todo o conteúdo e interação das mídias sociais revela agressivamente várias informações pessoais, além das que já foram mencionadas alhures.

A maior controvérsia relacionada a privacidade que se pode encontrar aqui, diz respeito aos termos de uso, pois estes desrespeitam qualquer legislação existente que proteja o direito fundamental à privacidade. Isso revela o caráter intrusivo que a tecnologia possui.

Conforme o documentário americano intitulado “*Terms and conditions may apply*” (2013), esses termos são, propositalmente escritos com textos longos para

desestimular a sua leitura. Aliado a isso, a escolha da fonte e de seu tamanho também visam coibir a leitura atenta e completa desses documentos.

Questionada a validade jurídica desses termos, tem-se que os tribunais americanos reconhecem a sua validade e os aplicam quando as relações entre usuários e a mídia social são questionadas. O reflexo disso é que esse mesmo comportamento é replicado aos demais países onde a rede social possui usuários, como é o caso do Brasil. Até o presente momento, não se tem conhecimento de nenhum caso que tenha sido enfrentado tendo como cerne a aplicabilidade ou não dos termos de uso dessa natureza.

Estima-se que os internautas despenderiam de 180 horas por ano para a leitura de todos os termos de uso a que deveriam ler antes de aceitar utilizar um produto[87] ou serviço. Isso corresponde a 7,5 dias de leitura ininterrupta.

Muito além das características já mencionadas, esses termos prevêem que suas cláusulas poderão ser alteradas sem prévio aviso ou sem a necessidade de nova aceitação. Um exemplo claro dessa condição foi a alteração feita pelo Facebook sobre as conversas pessoais privadas que já estavam armazenadas por ele, onde essas informações vieram a público sem qualquer restrição, podendo ser acessadas livremente. Logo após essa manutenção, imediatamente, milhares de conversas privadas se tornaram públicas e visíveis a, absolutamente, todos os usuários dessa rede. Era necessário que o internauta fosse nas mensagens e as tornasse, novamente, privadas. Ocorre que, até que isso fosse feito, as conversas estavam em domínio público.

Por fim, não existem quaisquer garantias de que as informações coletadas pelo Facebook não serão compartilhadas com terceiros, parceiros e com o governo. Isso porque, as mídias sociais se tornaram um verdadeiro centro de coleta de dados sobre qualquer indivíduo que se torne seu usuário.

---

87 Atualmente, é preciso aceitar termos de uso para se utilizar, inclusive, *smartphones*, como é o caso do Android, que exige a criação de um e-mail no Gmail para se poder utilizar o referido aparelho de forma correta.

2.4.5. Computação em Nuvem: a inversão do posse direta dos dados pessoais

Outro recurso tecnológico tem sido largamente utilizado através da Internet, pois possibilita o armazenamento de muitas informações geradas pelo próprio usuário. É a computação em nuvem, ou *cloud*, termo em inglês que significa nuvem pelo qual também é conhecida no Brasil.

O termo nuvem se refere ao fato das informações não estarem armazenadas nos dispositivos pessoais do internauta, mas sim, em servidores espalhados pela Internet. Geralmente, esse serviço é oferecido a título gratuito e se presta ao armazenamento de arquivos, sejam eles documentos, imagens, vídeos e outros conteúdos. Além disso, também é possível utilizar a nuvem para deixar anotações de acesso rápido, como é o caso da empresa Evernote[88].

Basicamente, a nuvem permite que o indivíduo se desloque para qualquer localidade e consiga, mesmo que não esteja portando o seu computador, acessar suas informações através de qualquer outro dispositivo informático. Em outras palavras, a nuvem pode ser entendida como um disco rígido[89] virtual acessível de qualquer lugar do mundo.

Com relação a privacidade, o usuário precisa ter ciência de que a utilização desse serviços implica na possibilidade do acesso de terceiros aos documentos enviados para ele. Um provedor muito conhecido desse serviço é o Dropbox[90], que, de forma transparente, informa em sua política de privacidade (DROPBOX, 2015) que as informações sobre o usuário, ou seja, todos os arquivos armazenados, e sobre os seus dispositivos são coletadas. A referida política informa ainda que esses dados serão compartilhados com empresas terceirizadas, outros usuários, outros aplicativos e para fins legais, ressaltando ainda que os funcionários da empresa que possuam função de administradores poderão acessar qualquer conteúdo.

88 O site da empresa Evernote é: https://evernote.com/
89 Do inglês *Hard Drive* – HD, discos rígidos são os dispositivos responsáveis pelo armazenamento dos arquivos de um computador.
90 O site da empresa Dropbox é: https://www.dropbox.com/

Isso confirma a utilização de dados pessoais para fins diversos do que o previsto na finalidade do serviço em si, que é o de mero armazenamento da informação. Some-se a isso o fato de que esses dados podem estar relacionados a profissões das quais a lei exige o sigilo profissional, como a advocacia, psicologia, medicina, dentre outras.

Cumpre salientar que outros serviços também são providos na modalidade de nuvem. A título de exemplo, cita-se o e-mail. Há muito tempo não é mais necessário utilizar o próprio computador para se acessar as mensagens eletrônicas. Logo, é possível afirmar que todo seu histórico e conteúdo permanecem em servidores alheios a propriedade do usuário. Da mesma forma, as políticas de privacidade informam o uso e fornecimento de informações privadas, inclusive, para terceiros, como é o caso do Gmail, oferecido pela empresa Google, quando aduz que “[...] fornecemos informações pessoais as nossas afiliadas ou outras empresas ou pessoas confiáveis para processá-las para nós, com base em nossas instruções [...]” (GOOGLE, 2015).

Para agravar essa situação, Radfahrer(2013) conclui de forma clara afirmando: “o que está na nuvem, não é seu.” Isso porque, sem ela, os dados permanecerão inacessíveis. Ou seja, se em algum momento o Dropbox ou o Gmail se tornarem indisponíveis ou, simplesmente, desativarem os seus serviços, nenhum dado poderá ser acessado por seu proprietário.

2.4.6. Big Data

É preciso notar uma característica predominante na prestação de serviços através da tecnologia, notadamente, por meio da Internet. Isso porque, atualmente, é possível encontrar gratuidade em todos os serviços que se deseja utilizar. Mas essa particularidade, na verdade, não ocorre de forma transparente, pois os dados são “[...] o novo combustível dos negócios” (TAURION, 2013, p.5).

Depreende-se então, as razões pelas quais os serviços não auferem um ganho direto, pois objetivam acessar os dados pessoais de seus consumidores, processá-los e vendê-los, conforme já abordado no subtítulo anterior, que alguns termos de uso e privacidade prevêem.

É preciso esclarecer que não é o foco deste trabalho questionar a validade jurídica ou os aspectos éticos e morais desses termos, mas tão somente referenciá-los, por serem constantemente citados quando a privacidade na prestação desses serviços é questionada. É, justamente, quando se aborda o tema do Big Data que a privacidade se mostra mais fragilizada.

Big Data, ou Grandes Dados, se refere a "[...] um conjunto de tecnologias, processos e práticas que permitem às empresas analisarem dados a que não tinham acesso e tomar decisões ou mesmo gerenciar atividades de forma muito mais eficiente." (TAURION, 2013, p. 28)

Mitchell Kapor afirmou que "obter uma informação da Internet é como tentar encher um copo de água em um hidrante." (SUDRÉ FILHO, 2010). Essa afirmação corresponde a velocidade e o volume de informação que a Internet permite gerar. Frise-se que todas as técnicas e dispositivos supramencionados nos subtítulos anteriores também são fornecedores desses dados para a grande rede. Quando o assunto é mídia social, por exemplo, tem-se que

> […] o Facebook, divulgou o blog TechCrunchque, processa 2.5 bilhões de conteúdo e mais de quinhentos terabytes de dados por dia. Com 2,7 bilhões de "curtidas" (termo adaptado para o português que se refere ao botão "curtir", específico da rede) e trezentos milhões de fotos por dia. Isso garante uma taxa de 105 terabytes a cada meia hora, permitindo que se tenha uma noção da quantidade de informações armazenadas pela rede.
> Estima-se que dos 1,8 zetabytes (10^{21} bytes) gerados em 2012 pularemos para 7,9 zetabytes em 2015.

Insta destacar que a quantidade de informação dita acima condiz somente a uma espécie de mídia social. Resta claro que se as várias fontes de dados que a Internet possui servirem de fornecedores de informação, ter-se-á um volume incomensurável que servirá de alimento para as já mencionadas técnicas de processamento existentes dentro o conceito de Big Data.

Mas o maior risco disso não reside somente na coleta e análise desses dados. Mas também, num recurso conhecido como algoritmo preditivo.

Esses algoritmos tornam possível a "[...] análise preditiva para se resolver […] problemas difíceis. Ela ajuda a descobrir padrões no passado que podem sinalizar o que está por vir." (IBM, 2012). Isso significa que um algoritmo preditivo encontra padrões de comportamento e "tenta" prever o futuro.

O fato de criar padrões se refere a categorização humana, que será analisada mais a frente. Entretanto, questiona-se não apenas a criação e associação de padrões as idiossincrasias de um indivíduo com base em seus dados pessoais, mas também, a efetividade desses métodos que se pautam por lógicas matemáticas não possuindo qualquer julgamento moral ou ético em sua tomada de decisões. (BAUMAN, 2013)

Alguns casos práticos se encarregam de demonstrar essa preocupação, como o da loja americana Target (RAOPO!, 2013), onde o pai de uma adolescente, que ainda cursava o ensino médio, percebeu que vários anúncios contendo produtos relacionados a mulheres grávidas estavam sendo enviados para o e-mail de sua filha, momento em que, ele decidiu procurar a loja para registrar a sua reclamação e exigir que esses envios fossem interrompidos. Segundo ele, a Target estava induzindo sua filha a ficar grávida. O gerente da loja não soube explicar o ocorrido e se desculpou. No retorno para a sua residência, sua esposa lhe contou que a filha realmente estava grávida.

As fontes utilizadas pela Target não foram divulgadas, mas sabe-se que toda as informações que a adolescente, mencionada no caso acima, procurava na Internet estavam relacionadas com o tema gravidez.

Sendo assim, pode-se concluir que a Target, através de técnicas de Big Data, ficou sabendo da gravidez da adolescente antes mesmo que seu pai.

Esses são os riscos de se tratar e analisar, ou, conforme o termo técnico se refere, minerar dados[91] de forma isolada e fora de contexto. Logo, para questões

91 O termo minerar dados se refere a expressão *Data Mining*.

mercadológicas, que são analisadas de forma numérica, esse método pode ser útil, mas estabelecer padrões sem que haja uma validação dessa informação pode, conforme demonstrado, expôr o indivíduo a várias situações inesperadas.

2.4.7. A tecnologia a serviço do Estado: o aparelhamento estatal para o monitoramento global.

Muito além do monitoramento que o mercado realiza para vender mais, também o Estado viu na tecnologia, principalmente, na Internet, a possibilidade de manter o maior número de pessoas em vigilância, fundamentando essa ação sob o argumento da segurança nacional.

Em meados de junho do ano de 2013, um jovem de 29 anos chamado Edward Snowden denunciou para o mundo o programa de monitoramento global realizado pela Agência Nacional de Segurança – NSA dos Estados Unidos da América. Ele decidiu se reunir com dois jornalistas, Glenn Greenwald e Laura Poitras, na cidade de Hong Kong, a fim de explicar todo o planejamento e entregar a documentação que comprovaria a existência de tudo o que seria relatado. “Considerado em sua totalidade, o acervo de Snowden levava, em última instância, a uma conclusão bem simples: o governo dos Estados Unidos construíra um sistema cujo objetivo é a completa eliminação da privacidade eletrônica no mundo inteiro.[92]” (GREENWALD, 2014, p. 101)

O pan-óptico da vigilância global se estende para além dos Estados Unidos. Segundo Greenwald (2014, p. 97-98), os documentos fornecidos por Snowden eram classificados como ultrassecretos, assinalados “[...] pelo acrônimo “FVEY”, ou seja, só tinha aprovação para circular entre os quatro aliados de vigilância mais próximos da NSA, a aliança dos Cinco Olhos (*Five Eyes*), formada com os países de língua inglesa Grã-Bretanha, Canadá, Austrália e Nova Zelândia.”

92 Cumpre salientar que a China também possui um programa de monitoramento local e global chamado de *Golden Shield* (RADFAHRER, 2013).

Quando em contatos com os jornalistas, Snowden solicitava a ambos que retirassem a bateria de seus *smartphones* ou que os colocassem no congelador do frigobar, pois a NSA possui o poder de transformá-los em escutas de ambiente, capturando tudo o que for dito próximo ao aparelho.

Em seus relatos Snowden demonstrou ter feito a denúncia de forma motivada de acordo com as ações da agência. Segundo Greenwald (2014, p. 52),

> - as coisas que vi começaram a me perturbar de verdade – declarou. - Eu podia assistir em tempo real as imagens, geradas por drones, de pessoas que eles talvez fossem matar. Era possível observar aldeias inteiras e ver o que todo mundo estava fazendo. Vi a NSA monitorar as atividades das pessoas na internet enquanto elas digitavam. Fui percebendo quanto as capacidades de vigilância dos Estados Unidos tinham se tornado invasivas, e me dei conta do verdadeiro escopo desse sistema. E quase ninguém sabia que isso estava acontecendo.

A NSA possuía vários programas internos, cada um com uma finalidade específica. Por exemplo, o Informante Sem Limites (BOUNDLESS INFORMANT) tinha a finalidade de "[...] quantificar, com exatidão matemática, a atividades diárias de vigilância da agência. […] Uma unidade da NSA havia coletado mais de três bilhões de itens apenas nos sistemas de comunicações dentro dos Estados Unidos." (Greenwald, 2014, p. 39). Já o Projeto Corrida dos Touros (PROJECT BULLRUN) focava em burlar os meios mais utilizados de criptografia na Internet. A Girafa Egomaníaca (EGOTISTICAL GIRAFFE) se incumbia do navegador Tor, utilizado para navegação anônima e para se entrar na Internet Profunda, também conhecida por *Deep Web*. Outro projeto, chamado de Musculoso (MUSCULAR), permite a invasão das redes pessoais do Google e do Yahoo!.

Se valendo de uma vantagem oriunda do fato de a Internet ter surgido em solo estadunidense, o governo americano também mantinha o programa STORMBREW, executado pela NSA em parceria com o FBI – *Federal Bureau of Investigation*. Esse projeto

> […] proporciona à NSA acesso ao tráfego de internet e telefonia que entra nos Estados Unidos por vários "gargalos" situados em território norte-americano. O programa explora o fato de que a grande maioria do tráfego de internet do mundo passa em algum momento pela infraestrutura de comunicação dos Estados Unidos, subproduto residual do papel central

> desempenhado pelo país no desenvolvimento da rede. (GREENWALD, 2014, p. 113)

E mesmo que as transmissões não atravessem o continente norte-americano, também é realizada a chamada coleta *upstream*, que consiste na conexão de equipamentos da agência em cabos de fibra ótica, inclusive cabos submarinos, de forma a ser possível capturar todo e qualquer tráfego de dados existente.

Entretanto, o programa conhecido como PRISM – *Planning Tool for Resource Integration, Syncronization, and Management* se mostrou o maior violador dos direitos e garantias fundamentais. Isso porque, ele obriga que várias empresas americanas, provedoras de aplicações de Internet para o mundo, forneçam mecanismos de captura de dados sem que seja necessário requisitá-las judicialmente ou, inclusive, diretamente para a própria empresa.

> De suas estações de trabalho em qualquer lugar do mundo, funcionários do governo credenciados com acesso ao PRISM podem solicitar uma 'tarefa' ao sistema" - ou seja, fazer uma busca - "e receber resultados de uma empresa de internet sem qualquer outra interação com seus funcionários. (GREENWALD, 2014, p. 116, aspas no original)

Fazem parte do PRISM, as empresas Google, com acesso direto também ao Gmail, Facebook, Hotmail, Yahoo!, Apple, Skype, Paltalk.com, YouTube, AOL Mail, Microsoft (SkyDrive e Outlook.com).

Ainda que já se esteja operando uma verdadeira engrenagem de coleta de dados, a NSA realiza também a Exploração de Rede Computacional "[...] inserindo *malwares*[93] em computadores específicos para vigiar seus usuários. Quando se consegue inserir *malwares* desse tipo, a NSA torna-se, no jargão da agência, "dona" do computador: passa a ver cada tecla digitada e cada tela visualizada." (GREENWALD, 2014, p. 124)

> Embora o *malware* em geral seja instalado por meio da "obtenção de acesso a redes de computador, a NSA cada vez mais vem lançando mão de uma tecnologia secreta que lhe permite acessar e alterar dados em

93 *Malware* é um programa malicioso criado para causar danos ou alguma outra ação inesperada no sistema do computador, como, por exemplo, espionar enviando dados contidos nessa máquina. (TECHTERMS.COM, 2015)

> computadores mesmo quando não conectados à internet.” (GREENWALD, 2014, p. 125)

Segundo o relatório da NSA, Brasília está infectada pela Exploração de Rede Computacional. (GREENWALD, 2014, p. 125)

Outra técnica que é utilizada pela NSA consiste na interceptação de produtos que serão enviados para clientes fora dos Estados Unidos de forma que estes carreguem consigo verdadeiros grampos, permitindo o acesso a redes estrangeiras, bem como, a seus usuários. Segundo Greenwald (2014, p. 156),

> a agência recebe ou intercepta, de forma rotineira, roteadores, servidores, e outros equipamentos de rede que serão exportados pelos Estados Unidos antes que sejam despachados para os clientes internacionais. Ela então implanta ferramentas de vigilância do tipo porta dos fundos, reembala os produtos com um selo de fábrica e os despacha. Assim, a NSA consegue acesso a redes inteiras e aos seus usuários.

Mas o principal programa utilizado pela NSA é o X-KEYSCORE. Em operação desde 2007, ele

> [...] permite um salto radical no escopo dos poderes de vigilância da agência. A NSA qualifica o X-KEYSCORE de seu sistema “de maior alcance” para a coleta de dados eletrônicos, e não é para menos. Um documento preparado para o treinamento de analistas alega que o programa capta “praticamente tudo o que um usuário típico faz na internet”, incluindo texto contido em e-mails, buscas no Google e o nome dos sites visitados. O X-KEYSCORE proporciona até o monitoramento “em tempo real” das atividades de navegação na hora em que acontecem.
> […]
> O programa também possibilita pesquisar e recuperar documentos e imagens embutidas que foram criados, enviados e recebidos. (GREENWALD, 2014, p. 162-163)

O X-KEYSCORE tem a capacidade de interceptar os pacotes das mensagens que trafegam na grande rede. Conforme já abordado no subtítulo 2.3, o protocolo HTTP é responsável pela transmissão de páginas Web, o que corresponde a maior parte de informações que trafegam na Internet. Esse protocolo, em especial, interessa a NSA, “porque quase tudo o que um usuário típico faz na internet usa HTTP.” (GREENWALD, 2014, p.164)

Nesse mesmo sentido, praticamente toda informação que trafega na rede mundial de computadores o faz em texto claro, a menos que se trate de um protocolo de transmissão criptografado, como é o HTTPS, ou de uma Rede Privada Virtual – VPN, ou ainda, aplicações que implementem a criptografia. Frise-se que a criptografia já é empregada na Internet quando se deseja a segurança e o sigilo das comunicações.

Pragmaticamente, quando uma mensagem trafega em texto claro, quer dizer que é possível capturar um ou mais pacotes que estejam trafegando na Web de forma que a mensagem transportada será lida. Essa interceptação pode ser feita de várias formas, sendo a mais comum utilizar-se de um programa conhecido como *sniffer*[94]. Por trafegarem em texto claro, assim que se seleciona, ou clica, em cima de um pacote capturado, é possível ler a mensagem nele contida. A Figura 5 exibe um pacote retido e aberto por um programa desse tipo.

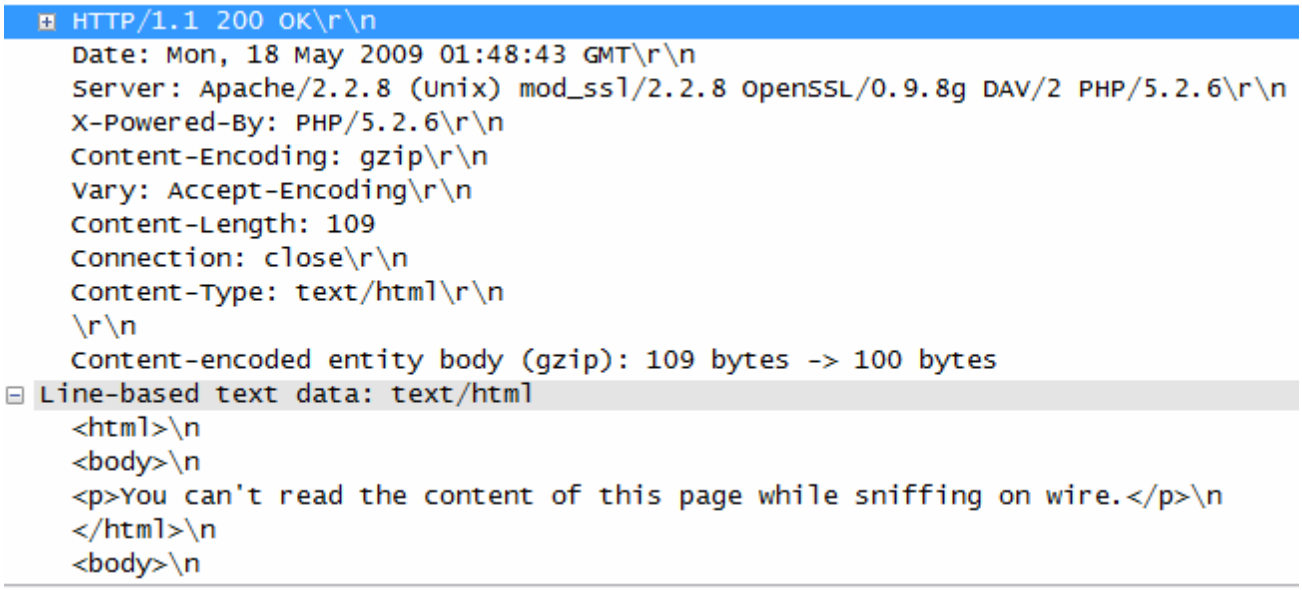

Figura 8 – Pacote HTTP aberto por um programa *Sniffer*
Fonte: https://blogs.sans.org/appsecstreetfighter/files/2009/06/09-05-21-wireshark-full.png

Observando-se a Figura 5, verifica-se que o pacote capturado pertence ao protocolo HTTP. Na terceira linha de baixo para cima, é possível constatar que, embora esteja na língua inglesa, a mensagem transmitida está em texto claro, ou seja, completamente legível, destaque-se: "*You can't read the content of this page while sniffing on wire*".

94 *Sniffer*: programa capaz de interceptar pacotes de uma rede e exibi-los.

Independente do significado da mensagem, insta ressaltar o que já foi dito alhures. De que a maior quantidade das informações que estão na Internet são transmitidas em texto claro. Isso permite que o X-KEYSCORE veja “[...] todo o tráfego de determinado endereço (ou endereços) de IP para um site específico.” (GREENWALD, 2014, p. 165). O que quer dizer que se a NSA desejar acompanhar em tempo real todas as ações de um internauta, basta utilizar o X-KEYSCORE.

Com um programa tão bem-sucedido com o implementado pela NSA, os Estados Unidos não tiveram outra opção a não ser utilizá-lo também para a espionagem econômica e diplomática, comprovando que a justificativa da segurança nacional não passa de um mero discurso.

Sobre a espionagem econômica, o Brasil foi um de seus alvos por meio do programa específico para esse fim conhecido como OLYMPIA, destinado a vigiar o Ministério das Minas e Energia brasileiro.

> O Canadá também é um parceiro muito ativo da NSA e, por si só, uma enérgica força de vigilância. Na conferência de Desenvolvimento de Sinais de 2012, a CSEC (Organização de Serviços de Comunicações do Canadá) gabou-se de ter tido como alvo o Ministério das Minas e Energia do Brasil, agência responsável por regulamentar o setor de maior interesse para as empresas canadenses. (GREENWALD, 2014, p. 127)

Além desse ministério, também a Petrobras foi alvo da espionagem econômica dos Estados Unidos.

> Os motivos para a espionagem econômica são bem claros. Quando os Estados Unidos usam a NSA para espionar as estratégias de planejamento de outros países durante discussões sobre comércio e economia, podem obter enorme vantagem para a indústria norte-americana. (GREENWALD, 2014, p. 147)

Já relativo a espionagem diplomática, o Brasil foi, novamente, alvo dos Estados Unidos, em especial, a Presidente Dilma Rousseff. Também o México sofreu esses efeitos, sendo o atual Presidente mexicano Enrique Peña Nieto monitorado enquanto ainda candidato àquele cargo. Inclusive suas mensagens de celular, conhecidas comumente como torpedos, foram capturadas e lidas pela NSA.

Os motivos que levaram os norte-americanos a espionar tanto o Brasil quanto o México pode ser entendido pelo fato de ambos serem “[...] ricos em recursos petrolíferos [...]” e por serem “[...] forte influente em suas regiões.” (GREENWALD, 2014, p.149)

Os países escolhidos para serem monitorados são classificados de acordo com três categorias diferentes segundo a sua relação com os Estados Unidos da América.

A primeira delas é com o grupo dos Cinco Olhos: os Estados Unidos espionam junto com esses países, mas raramente os espiona, a menos que solicitados pelas autoridades dos próprios países parceiros. O segundo grupo é formado por países com os quais a NSA trabalha em projetos de vigilância específicos ao mesmo tempo que os espiona de forma ampla. O terceiro é formado por países que os Estados Unidos espionam de forma rotineira, mas com os quais nunca coopera. (GREENWALD, 2014, p. 126). Brasil e México são classificados pelos Estudos Unidos da América como “Amigos, inimigos ou problemas?” (GREENWALD, 2014, p. 150).

Nem mesmo a Organização das Nações Unidas – ONU escapou da espionagem diplomática. A NSA “[...] usou seus programas para obter os principais tópicos a serem abordados pelo secretário-geral da ONU antes de seu encontro com o presidente Obama.” (GREENWALD, 2014, p. 150)

Ainda que criado sobre o argumento de proteção à Segurança Nacional, o programa de Monitoramento Global foi notoriamente utilizado para diversos fins. De forma análoga a uma criança que não sabe mais o que fazer com um brinquedo, a NSA apontou seu aspirador de informações pessoais e sigilosas para várias localidades e indivíduos no mundo. E o que tornou o programa absolutamente viável foi a infraestrutura atual da Internet, somadas com as possibilidades de interceptação e infecção já tratadas.

Num cenário futuro, esse monitoramento pode aumentar e ser mais intrusivo com o surgimento da Internet das Coisas, abordada no subtítulo a seguir.

2.4.8. A conexão universal com a Internet das Coisas: quando não será possível se desligar da grande rede

De acordo com o que foi explanado no subtítulo 2.3, o IPv6 permite que todo e qualquer indivíduo ou objeto se conecte com a rede mundial de computadores, que se tornará também a rede mundial de coisas, pois a partir desse ponto, fogões, geladeiras, interruptores, carros, caminhões, embarcações, relógios, sapatos, brincos, canetas, anéis, dentre outros objetos estarão conectados a grande rede. É a chamada Internet das Coisas.

Segundo o ex-diretor executivo do Google, Eric Schmidt, “a Internet como conhecemos vai desaparecer”, pois "haverá tantos endereços IP, tantos dispositivos, sensores, itens que você vestirá, coisas que você interagirá, que você nem vai mais notá-la. Ela será parte de sua vida o tempo todo". (INFO, 2015)

Dessa forma, fica claro que se não forem adotadas medidas legais e pragmáticas, a privacidade estará perto de se tornar um fato histórico. De forma a corroborar com essa ideia, é preciso que os efeitos do monitoramento global sejam analisados, propondo-se medidas que assegurem o direito fundamental à privacidade na era da informação. É o que será feito no capítulo a seguir.

3. REAFIRMANDO UM DIREITO FUNDAMENTAL: COMO A CRIPTOGRAFIA E AS TECNOLOGIAS LIVRES PODEM SER UTILIZADAS PARA ASSEGURAR O DIREITO FUNDAMENTAL À PRIVACIDADE

Após analisar como a tecnologia funciona e vem sendo empregada, verifica-se que é preciso proteger a informação, pois é impossível mensurar a extensão dos danos que a perda da privacidade e o monitoramento do indivíduo, ou da população, podem alcançar. A percepção mais clara que se tem, é tida no já abordado romance de George Orwell (2009), intitulado 1984.

Além disso, uma questão correlata a privacidade se nota quando este tema é tratado socialmente. Não raro, é comum encontrar aqueles que alegam não possuir nada para esconder, momento em que, segundo suas alegações, a perda da privacidade não teria nenhum efeito. Mas até mesmo os que se dizem imunes ao devassamento da privacidade, em determinado momento, se contradizem quando manifestam atitudes que visam a proteção do espaço necessário para se estar-só.

Tudo porque, viver sob a mira constante do monitoramento tira do indivíduo sua liberdade, além de forçar o regramento de suas ações. O prejuízo da vigilância constante é, fatalmente, que a pessoa deixe de ser quem ela, realmente, é. Em linhas gerais, é alcançar um nível de comportamento social padronizado, sem eventos anormais, pois, caso estes ocorram, a conduta do indivíduo será considerada ilegal. Isso porque, com o controle absoluto da população, o Estado torna-se pleno a fim de neutralizar qualquer ato de desobediência civil.

Dessa forma, a análise dessas questões se tornam necessárias para que, então, seja reforçada fragilidade da privacidade para que se aborde como a criptografia e as tecnologias livres podem ser utilizadas como uma forma de impedir a invasão, cada vez maior, que a tecnologia vem proporcionando nas esferas na privacidade, da vida privada e da intimidade.

Portanto, passa-se agora a averiguar os danos percebidos com a vigilância exacerbada que foi demonstrada no capítulo anterior.

Entretanto, cumpre esclarecer que na solução proposta por este trabalho não foram analisados os riscos relacionados a segurança da informação oriundos da infecção de equipamentos e/ou programas por vírus[95], cavalos de Troia[96], *worms*[97], *back orifice*[98], dentre outros. Portanto, tem-se a premissa de que o ambiente computacional está hermeticamente seguro, livre de ameaças como as supramencionadas.

3.1. SORRIA! VOCÊ ESTÁ SENDO FILMADO: QUANDO O MONITORAMENTO DO INDIVÍDUO ANIQUILA A ESSÊNCIA DO SER

Quando se fala em vigilância, é normal suscitar a ideia de um filósofo inglês, conhecido como Jeremy Bentham. Ele, como um bom utilitarista, elaborou um conceito incomum na construção civil. Isso porque, sua criação permite o controle absoluto sobre todos os que nessa edificação se encontrarem. É o chamado Panóptico[99], ou Casa de Inspeção, ou ainda, Elaboratório. Frise-se também que, além de objetivar esse tipo de eficiência, ele o faz prevendo que ocorra com o menor custo possível.

---

95 Vírus "são programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador. Eles têm comportamento semelhante ao do vírus biológico: multiplicam-se, precisam de um hospedeiro, esperam o momento certo para o ataque e tentam esconder-se para não serem exterminados" (UOL, 2015).

96 Cavalo de Troia, também chamado de Trojan, "é um programa que se oculta dentro de outro, legítimo, com a finalidade de abrir uma porta para que o hacker mal intencionado tenha acesso ao computador infectado" (TECHTUDO, 2014). Ista salientar que o termo hacker mal intencionado é conhecido como *cracker – criminal hacker*.

97 Worms são programas que se replicam, mas não alteram nenhum arquivo do computador da máquina do usuário. Entretanto, eles realizam uma sobrecarga, pois se multiplicam preenchendo a quantidade de memória livre e o espaço disponível no disco rígido (TECHTERMS.COM, 2015).

98 Back Orifice é uma ferramenta que consiste em duas peças principais, uma aplicação cliente e uma aplicação servidora. A aplicação cliente, executando na máquina no invasor, pode ser utilizada para monitorar e controlar a máquina de um usuário que esteja infectada com a aplicação servidora (SYMANTEC, 2007).

99 Bauman (2013, p. 18) informa que a palavra panóptico vem do grego "pan-óptico", e significa "lugar de onde tudo se vê".

É comum associar-se a ideia do monitoramento de Bentham às questões ligadas ao sistema prisional. Entretanto, em sua obra, ele aplicou o mesmo conceito também às casas de trabalho, ou de correção, espécie de local para o desenvolvimento do indivíduo, casas de manufaturas, hospícios, hospitais e escolas. Segundo Bentham (2008, p. 19), sua ideia é aplicável, "[...] sem exceção, a todos e quaisquer estabelecimentos, nos quais, num espaço não demasiadamente grande para que possa ser controlado e dirigido a partir de edifícios, queira-se manter sob inspeção um certo número de pessoas."

Toda a sua capacidade de fiscalização baseava-se na arquitetura que fora desenvolvida. Basicamente, utilizando-se o modelo adotado para as prisões, trata-se de uma estrutura circular externa onde se localizariam as celas dos prisioneiros, desenvolvidas de forma a permitir que a iluminação exterior adentrasse cada partição do edifício. No entanto, não havia a possibilidade de comunicação entre os prisioneiros. A face interior dessa estrutura receberia grades para permitir que a vigilância ocorresse. No centro dessa armação estaria uma torre de mesma grandeza preparada para proporcionar que **um inspetor observe sem ser visto**.

Embora a teoria de Bentham não tenha sido, efetivamente, utilizada, ela chegou a ser testada, onde algumas construções ainda resistem ao tempo, como a da Figura 8, que representa a Penitenciária de Stateville no Estado de Illinois, nos Estados Unidos da América (TARINGA, 2012).

Figura 9 – Penitenciária de Stateville no Estado de Illinois, nos Estados Unidos da América.
Fonte: http://upload.wikimedia.org/wikipedia/commons/a/ac/Presidio-modelo2.JPG

O intuito dessa filosofia de Bentham era permitir tanto ao Estado quanto ao proprietário de um estabelecimento o controle pleno daqueles que estivessem dentro dessa estrutura. “É óbvio que, em todos esses casos, quanto mais constantemente as pessoas a serem inspecionadas estiverem sob a vista das pessoas que devem inspecioná-las, mais perfeitamente o propósito do estabelecimento terá sido alcançado.” (BENTHAM, 2008, p. 20).

A finalidade disso era introduzir a sensação de observância constante de forma que qualquer ação de um prisioneiro ou indivíduo, contrária aos interesses daquele que estivesse observando, estariam passíveis de sofrer uma intervenção imediata. “A perfeição ideal, se esse fosse o objetivo, exigiria que cada pessoa estivesse realmente nessa condição, durante cada momento do tempo.” (BENTHAM, 2008, p. 20)

Introduzir o monitoramento constante é fazer com que o indivíduo meça cada atitude sua de modo que a regra geral, ou seja, a norma de conduta, se torne válida, contudo, **involuntariamente**. Mas vigiar um grande número de pessoas o tempo todo custaria o mesmo número de pessoas, só que, na função de inspetor. Foi pensando assim que Bentham aprimorou sua construção para que “sendo isso impossível, a próxima coisa a ser desejada é que, em todo momento, ao ver razão para acreditar nisso e ao não ver a possibilidade contrária […]” o indivíduo “[...] deveria pensar que está nesta condição. (BENTHAM, 2008, p. 20). “Como as instituições – qualquer instituição – não eram capazes de observar todo mundo o tempo todo, a solução de Bentham foi criar “a aparente onipresença do inspetor” na mente dos ocupantes.” (GREENWALD, 2014, p. 188)

Ainda que essa vigilância constante tolha o indivíduo de sua naturalidade, ou seja, de sua essência, mesmo assim, ele permanece com sua liberdade para decidir que tipo de comportamento adotará, independente das consequências disso. Mas como já foi abordado no capítulo anterior, o poder invasivo da tecnologia retira das pessoas essa liberdade de negação. Isso porque, a esmagadora maioria dos indivíduos não possuem a correta noção da amplitude desse poder invasivo das capacidades tecnológicas. Logo, é comum e rotineiro que todos os indivíduos

confiem e depositem em seus dispositivos computacionais suas informações pessoais. Some-se a isso as várias técnicas empregadas pelo mercado e pelo governo americano para acessar os dados pessoais armazenados em todo e qualquer aparelho. O que, por si só, implica na violação das esferas da privacidade, da vida privada e da intimidade da pessoa, pois se o acesso a um dispositivo contendo essas informações é realizado, não há como mensurar a profundidade da obtenção de informações pessoais. Devendo-se entender, portanto, que todas as esferas foram violadas.

Michel Foucault (2007, p. 167), filósofo que analisou os escritos de Bentham, afirma que “o Panóptico é uma máquina maravilhosa que, a partir dos desejos mais diversos, fabrica efeitos homogêneos de poder.”

Em suas obras, Foucault analisa o poder e sua visibilidade dentro das sociedades de soberania e disciplinar. Segundo ele, “o poder não existe” (FOUCAULT, 2001, p. 248), mas sim sua prática, ou seja, relações de poder. Nas sociedades de soberania, período do séc. XVII até a Revolução Industrial, o poder era visível, sendo que a força desse poder dependia de sua visibilidade. Como exemplo, o poder de um rei possuía mais força que o poder de um súdito, ou o poder de um empresário, mais força que o de um empregado.

Já nas sociedades disciplinares, o poder torna-se menos visível, pois agora, existem vários espaços de confinamento dos sujeitos (DELEUZE, 1992), quer seja, a família, a escola, a empresa, o exército, o hospital, a prisão, dentre outros. Esses espaços seriam as disciplinas do sujeito. Daí o nome de sociedades disciplinares. O poder permeia cada uma das disciplinas do sujeito. É dentro da questão da visibilidade do poder que Foucault (2007) analisa o Panóptico, chamando-o de Panoptismo.

Para Foucault (2007, p. 166), o panoptismo faz com que o indivíduo seja visto, mas não veja, se tornando “[...] objeto de uma informação, nunca sujeito numa comunicação.” Pode-se concluir que esse constante monitoramento retira do ser suas reações naturais. “Daí o efeito mais importante do Panóptico: induzir no

detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder.” (FOUCAULT, 2007, p. 166)

O próprio Greenwald também se concentra nos estudos de Foucault para analisar os danos causados pela vigilância global. Segue ele,

> [...] Michel Foucault observou que o princípio do Panopticon de Bentham era um dos mecanismos fundadores do Estado moderno. Em *Vigiar e punir*, ele afirma que o panopticonismo é “um tipo de poder aplicado aos indivíduos na forma de uma supervisão individual contínua, ou seja, a moldagem e transformação dos indivíduos segundo determinadas normas. (GREENWALD, 2014, p.188)

É nesse sentido que Foucault (2007, p. 169) conclui que

> o Panóptico funciona como uma espécie de laboratório de poder. Graças a seus mecanismos de observação, ganha em eficácia e em capacidade de penetração no comportamento dos homens; um aumento de saber vem se implantar em todas as frentes do poder, descobrindo objetos que devem ser conhecidos em todas as superfícies onde este se exerça.

Infere-se daí que o monitoramento global extrapola a simples coleta de informações para se transformar numa ferramenta para o exercício do poder, para o controle.

Em contrapartida, é comum notar um discurso presente em alguns indivíduos de que eles não possuem nada para esconder, logo, seus dados pessoais podem ser vasculhados e monitorados. Contudo, como bem frisou Greenwald (TED.COM, 2014) em sua apresentação sobre a privacidade, todas as pessoas que fizeram essa alegação para ele tiveram suas senhas de e-mail requeridas. Qual não foi a surpresa, nenhuma delas a revelou. Logo, esse tipo de argumento não prospera contra seu próprio emissor, uma vez que, ele mesmo se nega a abrir a porta de sua privacidade. Depreende-se daí, que o indivíduo deseja a proteção de sua privacidade, e não o contrário.

A verdade é que o discurso de que a privacidade não é mais valorizada beneficia o mercado, pois a moeda hoje são os dados pessoais. Essas informações possuem um valor agregado que as tornam bens de consumo mercadológicos.

Por esse motivo, é comum se verificar o discurso de que se a pessoa não deseja que alguém venha a saber o que ela está fazendo, ela, então, não deve fazer. Ora, foi exatamente isso que Eric Schmidt, CEO[100] do Google, afirmou ao ser entrevistado pela CNBC em 2009, pois ele disse que "[...] se você tiver alguma coisa que não quer que ninguém saiba, talvez não a devesse estar fazendo, para começo de conversa." (GREENWALD, 2014, p.183). Fica claro aqui, que a observância panóptica anula a liberdade do ser humano.

Ocorre que, a empresa CNET notou que Eric Schmidt evitava divulgar suas informações pessoais através de seu site pessoal. Foi então, para a surpresa das empresas de Tecnologia da Informação, que a CNET conseguiu explorar a privacidade do CEO do Google utilizando as suas próprias ferramentas, valendo-se do tempo de trinta minutos para isso (CNET, 2005). Essa fato demonstrou o quanto o Google é invasivo quando o assunto é a coleta de dados pessoais. Mas, além disso, mostrou que o autor do discurso do "pense duas vezes antes de fazer alguma coisa", foi violado em sua privacidade quando, de fato, desejava protegê-la.

De igual modo, o fundador e atual CEO do Facebook, Mark Zuckerberg, é tão contraditório quanto Eric Schmidt, pois, sem qualquer base sociológica, afirma que "a privacidade na era digital não é mais uma "norma social"" (GREENWALD, 2014, p. 183). Entretanto, quando decidiu adquirir a sua residência na cidade de Palo Alto, na Califórnia, nos Estados Unidos da América, comprou também as quatro casas adjacentes à sua (GREENWALD, 2014, p. 184) para ter mais privacidade.

> A privacidade é um conceito relacional; depende do seu público. Você não quer que seu patrão saiba que está procurando outro emprego. Não conta tudo sobre a sua vida amorosa a sua mãe ou a seus filhos. Não revela segredos profissionais a seus concorrentes. Nós não nos expomos de forma indiscriminada, e damos importância suficiente à exposição para mentir sem hesitação. Entre cidadãos respeitadores das leis, pesquisadores já mostraram muitas vezes que mentir é "uma interação social diária" (duas vezes ao dia entre estudantes universitários, uma vez por dia no "mundo real"). A transparência total é um pesadelo. Todo mundo tem algo a esconder. (GREENWALD, 2014, p. 194)

100 CEO é o acrônimo de *Chief Executive Officer*, que significa Diretor Executivo.

Portanto, o discurso do fim da privacidade é uma tentativa inócua de fazer com que as pessoas creiam ser interessante não resistir ao devassamento de seu domínio privado. Conforme Greenwald observou (2014, p. 184),

> a mesma contradição é expressada pelos muitos cidadãos comuns que desdenham o valor da privacidade, mas mesmo assim protegem com senhas suas contas de e-mail ou de mídias sociais. Essas pessoas põem trinco na porta de seus banheiros e lacram os envelopes nos quais enviam suas cartas. Quando ninguém está olhando, fazem coisas que jamais cogitariam fazer quando totalmente expostas. Dizem coisas aos amigos, psicólogos e advogados que não querem que ninguém mais saiba. Expressam opiniões on-line que não desejam ver associadas ao seu nome.
> Os muitos defensores da vigilância com quem conversei desde que Snowden fez suas revelações logo repetiram a opinião de Eric Schmidt: a privacidade é para quem tem algo a esconder. Só que nenhum deles se mostrou disposto a me informar a senha de seu e-mail ou permitir câmeras de vídeo dentro de suas casas.

Acerca do monitoramento global empregado pelos Estados Unidos da América, a presidente do Comitê de Inteligência do Senado, Dianne Feinsteinn, alegou que a Agência Nacional de Segurança – NSA coletava metadados, e que isso não mostraria, em momento nenhum, uma vigilância. Mas, ora, os metadados a que ela se refere são, na verdade, dados que dizem muitos sobre a privacidade, a vida privada e, até mesmo, a intimidade da pessoa.

Após essa declaração, Dianne Feinsteinn foi questionada se, ela mesma, divulgaria essas informações pessoais, como: os contatos recentes de e-mails e telefonemas, a duração dessas conversas e a geolocalização desses indivíduos. E qual não foi a surpresa, ela se negou a fazê-lo.

A reação tida por todas as pessoas informadas acima é natural e chega a ser óbvia.

> O fato é que o desejo de privacidade é compartilhado por todos nós como parte essencial, e não secundária, do que significa ser humano. Nós todos compreendemos de forma instintiva que a esfera privada é onde podemos agir, pensar, falar, escrever, experimentar e decidir como ser longe do olhar avaliador dos outros. A privacidade é uma das condições centrais para ser livre. (GREENWALD, 2014, p. 185)

Além do contraditório discurso do fim da privacidade, nota-se também que o próprio Estado, destaque-se, o governo estadunidense, está tomando todas as precauções necessárias para garantir a privacidade de suas operações, omitindo do povo muitas

de suas ações. “Esse mundo de sombras é tão secreto, “tão grande e impenetrável”, como descreveu o *Washington Post*, “que ninguém sabe quanto ele custa, quantas pessoas emprega, quantos programas engloba ou exatamente quantas agências fazem o mesmo trabalho.”” (GREENWALD, 2014, p. 184)

Na verdade, o que se percebe com o discurso de que a privacidade está acabando e de que o governo sequer presta conta de suas ações, assemelha-se a ideia de uma violência simbólica no sentido de ser um “poder que chega a impor significações como legítimas, dissimulando as relações de força que estão na base de sua força” (BORDIEU e PASSERON, 1996). A finalidade dessa violência simbólica é criar uma ação pedagógica para que esta seja inculcada na população. Isso se confirma, pois “o trabalho pedagógico é, justamente, a inculcação de um *habitus*, ou seja, de um produto de interiorização de um arbítrio cultural capaz de se perpetuar mesmo quando a ação pedagógica cessa”, cuja capacidade é “perpetuar uma atitude de forma mais eficiente do que qualquer coerção política” (BORDIEU e PASSERON, 1996).

Como meio de se corroborar com essa argumentação, cumpre mencionar um estudo do Professor de mídia, artes e ciências do Instituto de Tecnologia de Massachusetts – MIT, Alex Pentland, chamado a “realidade de mineração de comunicações móveis: em direção a um novo acordo sobre dados”[101] (MIT, 2009). Esse trabalho foi apresentado no Fórum Mundial de Economia.

A teoria de Pentland é a de que a privacidade deve deixar de ser um direito, no caso, fundamental, para ser tornar uma espécie de bem móvel, onde o indivíduo seria munido dos direitos que versam sobre a propriedade móvel, tais como: o direito de possuir seus dados, o direito sobre o controle do uso de seu dado, e o direito de dispor e distribuir seus dados.

Essas premissas causam estranheza, pois permitem o entendimento de que a posse dos dados está sempre em poder de terceiros. Não que isso não seja verdade nessa era tecnológica, mas não deve ser o ponto basilar. De igual modo, Pentland omite-se quanto a uma característica inerente ao bem móvel, qual seja, o de reavê-lo de

101 No original: *Reality Mining of Mobile Communications: Toward a New Deal on Data*.

quem injustamente o possua. E, na era da informação, como garantir que um dado foi integralmente excluído?

Nesse mesmo sentido, se um ser humano tomar conhecimento acerca de um fato sobre a privacidade, vida privada ou intimidade de terceiro, como no caso da manipulação desses dados pelas empresas provedoras de aplicações de Internet, ou de sua obtenção ilícita ou irregular, como já demonstrado com os dispositivos computacionais abordados no segundo capítulo, como será possível reaver uma informação que se localiza num órgão vital de um ser humano, o cérebro, e que, até o presente momento, desconhece meios de editar as informações que lá se localizam? Essa fragilidade comprova a importância da garantia da privacidade na era da informação, mantendo a liberdade de negação do ser como forma de decidir quem poderá ter acesso aos dados sobre sua privacidade. Sem a tecnologia, um indivíduo somente saberá acerca de outro se este, voluntariamente, o disser.

Respeitosamente, argumenta-se que Pentland errou ao comparar um direito inerente ao ser humano com um direito de propriedade, bastando essa afirmação para demonstrar que a teoria da privacidade enquanto um bem móvel não pode prosperar. Sobre isso, Warren e Brandeis (UNIVERSITY OF ILLINOIS, 1890, tradução nossa) afirmam que “o princípio que protege os escritos pessoais e outras produções individuais não contra o roubo e a apropriação física, mas contra a publicação em qualquer formato, na verdade não é o princípio da propriedade privada, mas sim o de uma personalidade inviolável.”[102]

Quando um indivíduo age ciente de que é observado, essa fato altera drasticamente o seu comportamento. “[...] se você acredita que está sendo sempre vigiado e julgado, na realidade não é um indivíduo livre.” (GREENWALD, 2014, p. 186).

Conforme já tratado no primeiro capítulo dessa pesquisa, o domínio público é o lugar de igualdade. Dentre outras características, isso se dá pela observância de práticas sociais estabelecidas como forma de se permitir uma convivência harmônica. Logo,

---

102 No original: “*The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.*”

desvios de conduta poderão ser considerados como comportamentos indesejados. Isso se deve ao fato das pessoas estarem sendo observadas por outras. Portanto, ao adentrar-se no domínio privado, lar de desigualdade, o ser desvela-se como é. Por esse motivo, “[...] o leque de escolhas que elas consideram quando acham que estão sendo observadas é bem mais estreito do que as suas possíveis ações em âmbito privado. A negação da privacidade tem por efeito uma severa restrição da liberdade de escolha.” (GREENWALD, 2014, p. 186)

Assim, ainda que na segurança de uma propriedade privada, tornando-se, num primeiro momento, invisível aos demais, um ser pode se ver limitado em suas ações pelo poder invasivo da tecnologia, pois ela é um canal de acesso existente entre os domínios público e privado, uma vez que, “o que torna um sistema de vigilância eficaz no controle do comportamento humano é a consciência de que as palavras e ações das pessoas são passíveis de monitoramento” (GREENWALD, 2014, p.188), conforme já demonstrado.

A questão mais preocupante que se extrai da invasão dos meios tecnológicos pode se encontrar na ignorância das pessoas, pois desconhecem a forma de funcionamento desses dispositivos, não compreendendo como a sua privacidade, vida privada e intimidade vêm sendo devassadas. Apenas quando ocorre um vazamento de informações pessoais é que se pode medir o quão profunda foi a intrusão da tecnologia. Some-se a isso o que já foi dito no capítulo anterior, que o indivíduo confia nesses recursos para armazenar toda a sua privacidade. Um adágio pertinente, conhecido dos profissionais da área de segurança da informação afirma que: “pior do que a ausência de segurança é a falsa sensação de segurança.” E é, justamente, essa falsa sensação de segurança que permite a pessoa depositar tantas informações pessoais quantas consiga ter ciência de ter gerado nos dispositivos computacionais que, comprovadamente, repassam esses dados sem que o emissor tome ciência ou, quando venha a saber, entenda o fim para que a coleta desses dados foi feita.

O efeito colateral disso é que quando, então, as pessoas tomarem conhecimento de que sua privacidade está numa nuvem de empresas ou de governos, talvez seja

tarde demais para uma contra ação. É preciso agir preventivamente de forma a proteger os dados e informações pessoais, não se justificando, em hipótese alguma, o monitoramento global e o armazenamento generalizado de informações sobre o indivíduo.

Caso nenhuma ação seja efetivada, pois o direito fundamental à privacidade é flagrantemente violado, estar-se-á diante de um possível estado panóptico, onde já não adiantará resistir ao monitoramento que vem sendo empregado. “O que torna um sistema de vigilância eficaz no controle do comportamento humano é a consciência de que as palavras e ações das pessoas são passíveis de monitoramento.” (GREENWALD, 2014, p. 188). Portanto, conforme abordado acima, esse cenário poderia se traduzir no fim da essência do ser, onde este se tornaria obrigado a observar as normas de conduta do domínio público dentro do domínio privado, perdendo assim, a sua liberdade.

Portanto, na era da informação, a sociedade de controle de Deleuze (1992)[103] justifica seu nome, uma vez que, a tecnologia permite que o poder foucaultiano se granule adentrando ao domínio privado perpassando as esferas da privacidade, da vida privada e da intimidade, pois a intrusão dos recursos tecnológicos retira da pessoa sua liberdade de negação de forma que, cada vez mais, se torna impossível impedir o acesso às informações que residem nessas esferas. Isso faz com que o Panóptico de Bentham se torne possível e que o Estado e/ou as empresas observem sem serem vistos, exercendo o controle da forma que melhor servir aos seus interesses. A observância constante sem que existam mecanismos hábeis a controlar o acesso as informações pessoais induz a pessoa a observar-se constantemente, criando um padrão de comportamento, alterando a essência do seu ser. Ocorre que, o ser pode alterar sua essência de forma a anulá-la caso essa invasão não seja impedida ou ao menos reduzida.

Uma prova da consequência do monitoramento pode ser verificada quando um indivíduo adentra um recinto e observa a placa com o seguinte comunicado: Sorria! Você está sendo filmado. Imediatamente, o comportamento espontâneo dessa pessoa é tolhido, sendo que ela mesma se observará antes de agir de forma a não

103 A sociedade de controle de Deleuze (1992) é tratada no tópico 3.2.

deixar nada registrado contra a sua vontade. De igual modo, no momento em que uma pessoa souber que suas informações ou suas mensagens são monitoradas, como já se demonstrou no capítulo anterior, um simples *post* numa rede social, que já o torna público, ou um segredo enviado pelo Whatsapp receberá especial atenção do seu emissor antes de ser transmitido.

3.2. A SEGURANÇA NACIONAL COMO JUSTIFICATIVA DO MONITORAMENTO GLOBAL

Como já demonstrado no capítulo anterior, a forma como a Internet foi desenvolvida permite a captura de uma grande quantidade de informação. É a partir dessa possibilidade que alguns países desenvolveram seus programas de vigilância, como os Estados Unidos da América e a China. Porém, ao devassar a privacidade dos indivíduos, é preciso criar uma justificativa aceitável para isso. Foi assim que se desenhou o discurso da segurança nacional[104].

> A segurança – palavra com a qual frequentemente se deseja designar alguma ideia mal definida de segurança "nacional" – é hoje prioridade política em muitos países e através deles, e constitui uma poderosa motivação no mundo da vigilância.
> Os principais meios de obter segurança, ao que parece, são as novas técnicas e tecnologias de vigilância, que supostamente nos protegem, não de perigos distintos, mas de riscos nebulosos e informes. (BAUMAN, 2013, p. 95)

Há que se ressaltar que, conforme Khroling e Martinelli (2014), o programa de monitoramento global dos Estados Unidos da América "[...] nasceu com a publicação, em 2001, durante o governo do Presidente George Bush, de uma lei americana conhecida como Ato Patriota (JUSTICE.GOV, 2001), cujo objetivo era adotar medidas contra o terrorismo em nome da segurança nacional." Essa lei empoderou o presidente de tal forma que ele pôde demandar programas, como o de monitoramento global, sem prévia aprovação do congresso.

---

104 Para uma leitura mais profunda sobre a denúncia realizada por Snowden ver Khroling e Martinelli (2014).

Entretanto, é preciso analisar de forma mais contundente os impactos causados por esses programas, ainda que seu fundamento, *a priori*, implique numa forma de prevenção de riscos à nação. Isso porque, capturar todas as informações de vários indivíduos, indiscriminadamente, acaba por torná-los, "suspeitos em potencial" (KHROLING e MARTINELLI, 2014).

Naturalmente, quando se obtém dados sobre um indivíduo, é possível tomar conhecimento sobre o seu perfil, construído a partir daquela fonte, seja esse um perfil social, de consumo ou familiar, dentre outros. Dependendo da origem dos dados e da qualidade das informações, chega-se, inclusive, as opiniões políticas e religiosas, por exemplo. Bauman (2013, p. 11-12) recorda que "Gilles Deleuze introduziu a expressão "sociedade de controle", na qual a vigilância cresce menos como uma árvore – relativamente rígida, num plano vertical, como o pan-óptico – e mais como ervas daninhas. […] Assim, o que é seguro, estruturado e estável se liquefaz."

Deleuze (1992) tem como ponto de partida as teorias de Michel Foucault sobre o poder e sua visibilidade dentro das sociedades de soberania e disciplinar, criando então o termo sociedades de controle.

Comparando as sociedades de controle com as sociedades disciplinares, Deleuze (1992, p. 5) ensina que

> nas sociedades disciplinares, sempre se está reiniciando (da escola para o quartel, do quartel para a fábrica), enquanto nas sociedades de controle nunca se finaliza o ciclo – a corporação, o sistema educacional, as forças armadas são estados metaestáveis coexistindo numa mesma modulação, como um sistema universal de deformação.[105]

Isso convalida o que Bauman afirmou acima, pois na sociedade de controle, há uma onipresença dessa vigilância, não importando em que espaço de confinamento o sujeito se encontre.

---

105 No original: *In the disciplinary societies one was always starting again (from school to the barracks, from the barracks to the factory), while in the societies of control one is never finished with anything – the corporation, the educational system, the armed services being metastable states coexisting in one and the same modulation, like a universal system of deformation.*

> Nas sociedades de controle, por outro lado, o que é importante não é tanto uma assinatura ou um número, mas um código: o código é uma senha, enquanto que, por outro lado, as sociedades disciplinares são regulados por palavras de ordem (tanto a partir do ponto de vista da integração quanto como da resistência).[106] (DELEUZE, 1992, p. 5)

Por conseguinte, essa situação se agrava no momento em que os recursos já discutidos anteriormente manipulam esses dados no intuito de tentar, também, prever o futuro através das técnicas de *Big Data*, *Data Mining* e dos algoritmos preditivos, abordados no capítulo anterior. “A segurança transformou-se num empreendimento orientado para o futuro – agora nitidamente descrito no filme e no romance intitulados *Minority Report* (2002) – e funciona por meio da vigilância, tentando monitorar o que vai acontecer pelo emprego de técnicas digitais e raciocínio estatístico.” (BAUMAN, 2013, p. 13)

Além disso, em função da atual velocidade da comunicação, foi preciso reinterpretar o Panóptico de Bentham, onde, para Bauman (2013, p.19), a fluidez da informação se perfaz num momento pós-pan-óptico. “Se naquela época era possível presumir que o inspetor pan-óptico estava presente (em algum lugar), nas atuais relações de poder, os que controlam suas alavancas “têm a possibilidade de, a qualquer tempo, fugir para algum lugar inalcançável – para a pura e simples inacessibilidade.”” (BAUMAN, 2013, p.19)

A questão a que Bauman (2013) chama atenção é definida por ele como “categorização social”. É justamente nesse momento, o de tentar identificar as ameaças para a segurança nacional que se pode gerar uma insegurança.

> em termos simples, Bigo propõe o “ban-óptico” para indicar de que modo tecnologias de elaboração de perfis são usadas para determinar quem será colocado sob vigilância específica. Mas ele emerge de uma análise teórica completa a respeito de como surge uma nova “insegurança global” a partir das atividades crescentemente combinadas dos “gerentes da inquietação” internacionais, como policiais, agentes de fronteira e companhia aéreas. Burocracias transnacionais de vigilância e controle, tanto empresariais quanto políticas, agora trabalham a distância para monitorar e controlar, pela vigilância, os movimentos da população. (BAUMAN, 2013, p. 62-63)

---

106 No original: *In the societies of control, on the other hand, what is important is no longer either a signature or a number, but a code: the code is a password, while on the other hand the disciplinary societies are regulated by watchwords (as much from the point of view of integration as from that of resistance).*

Ainda assim, Zaffaroni (2007, p.117) adverte sobre o risco dessa categorização social baseada na vigilância global, uma vez que torna todos suspeitos, pois ela tende a violar os direitos de todos os indivíduos em detrimento da busca de ameaças à segurança nacional, uma vez que,

> […] quando os destinatários do tratamento diferenciado (os inimigos) são seres humanos não claramente identificáveis *ab initio* (um grupo com características físicas, étnicas ou culturais bem diferentes), e sim pessoas misturadas ao e confundidas com o resto da população e que só uma investigação policial ou judicial pode identificar, perguntar por um tratamento diferenciado para eles importa interrogar-se acerca da possibilidade de que o Estado de direito possa limitar as garantias e as liberdades de todos os cidadãos com objetivo de identificar e conter os inimigos.
> Isso é assim porque, por exemplo, ao se permitir a investigação das comunicações privadas para individualizar os inimigos, a intimidade de todos os habitantes será afetada, pois esta investigação incluirá as comunicações de milhares de pessoas que não são inimigos.

Portanto, mesmo que num primeiro momento, a segurança nacional se mostre como uma justificativa autorizadora dos programas de monitoramento, é preciso observar o que afirmou Greenwald (2014, p. 214, grifo nosso), pois,

> […] ficou provado que o argumento de que a vigilância em massa impediu complôs terroristas – alegação feita por Obama e por uma série de autoridades de segurança nacional – **é falso**. Como observou o *Washington Post* em dezembro de 2013 em artigo intitulado “Defesa do programa telefônico da NSA por autoridades pode estar desmoronando”, um juiz federal declarou o programa de coleta de metadados de telefonia “quase certamente” inconstitucional, **dizendo também que o Departamento de Justiça foi incapaz de “citar um só caso em que a análise da coleta em massa de metadados pela NSA tenha de fato impedido um atentado terrorista iminente”.**

Ora, então, o único produto resultante de um programa de monitoramento global é um Estado de Exceção permanente, pois, suspende direitos e garantias individuais em detrimento de uma falácia conhecida como “segurança nacional”.

> Quando um país monitora todas os seus meios de comunicação, e vigia também, outras nações, como foi o caso revelado por Snowden sobre o governo brasileiro, tem-se um Estado de Exceção permanente que não garante direito algum, pois “o estado de exceção não é um direito especial (como o direito de guerra), mas, enquanto suspensão da própria ordem jurídica, define seu patamar ou seu conceito limite.” (AGAMBEN, 2007, p. 15) (KHROLING e MARTINELLI, 2014)

Quando o representante do Poder Executivo, legalmente, recebe todos os poderes entendidos como necessários para a garantia da segurança nacional por meio de disposições feitas pelo legislativo, acaba por retirar a harmonia da tripartição de poderes, fragilizando, inclusive, qualquer forma de fiscalização de sua utilização. “Sendo assim, aquilo que deveria ser um poder constitucional a ser utilizado em casos excepcionais se torna regra e não a exceção. (AGAMBEN, 2007, p. 21) E isso se opõe ao Estado Democrático de Direito.” (KROHLING e MARTINELLI, 2014).

É preciso, pois, fortalecer o direito fundamental à privacidade como forma de reafirmá-lo. No entanto, a questão que se põe é: como fazê-lo diante dos impactos tecnológicos?

Outro ponto que merece destaque se encontra na utilização das informações pessoais como forma de munir o mercado de produtos e serviços, permitindo que eles alcancem, personificadamente, seus clientes e potenciais clientes. É o que se faz no item a seguir.

3.3. A UTILIZAÇÃO INDEFINIDA PELO MERCADO DA COLETA DE DADOS PESSOAIS

Além dos Estados, outras entidades possuem interesse em informações pessoais, mas também o mercado de bens e serviços. De certa forma, entrar na privacidade dos indivíduos é, como já foi dito alhures, descobrir suas opiniões, gostos, preferências, dentre outros.

Muito embora as empresas, até onde se possui conhecimento, não tenham desenvolvido um programa de monitoramento, a forma como a tecnologia vem sendo empregada desempenha perfeitamente esse papel. Rememorando-se o que foi explanado no capítulo anterior, pode-se comprovar que as empresas realizam a coleta de dados pessoais para analisá-los e se chegar a “melhor” forma de se oferecer um tipo de produto ou serviço.

A exemplo disso, citam-se os *cookies*, as Smart TVs, os *Smartphones*, as Mídias Sociais, a Computação em Nuvem, a Internet das Coisas e a própria Internet como fontes de informações pessoais sobre os Internautas. Após isso, são empregadas as técnicas também já mencionadas de *Big Data* e *Data Mining* e algoritmos preditivos, cujo objetivo é encontrar um perfil de consumo de um cliente ou potencial cliente.

Outro ponto sensível dessa questão, encontra-se nos termos de uso dos provedores de aplicação de Internet, onde informam que os dados coletados poderão ser compartilhados com empresas parceiras.

Imaginando um cenário hipotético, onde as empresas de telefonia e telefonia celular, as de cartões de crédito, os bancos, e as demais empresas do comércio em geral compartilhem, entre si, as informações pessoais coletadas, ter-se-ia um perfil que, além daqueles que já foram mencionados, conseguiria traçar o de consumo e o de condição financeira. Diante disso, seria o mercado capaz de evitar a discriminação do consumidor por ele não possuir, segundo suas análises de dados, condições para consumir os seus produtos ou serviços?

Essa categorização de consumidores poderia inverter o poder de decisão para o consumo, fazendo com que os fornecedores invistam recursos apenas numa determinada categoria de consumidores que, potencialmente, consumirão seus produtos ou serviços. “Um paradoxo aqui é que, enquanto o consumo exige a sedução prazerosa dos consumidores, essa sedução também é resultado da vigilância sistemática numa escala de massa.” (BAUMAN, 2014, p. 23). Isso geraria uma exclusão de uma parcela de consumidores que não se encontrariam dentro do perfil necessário para determinado consumo, o que segrega ainda mais os espaços sociais. Não se fala aqui de exclusão digital, onde o usuário está impedido do acesso aos recursos tecnológicos que o conduzem ao mundo virtual, mas sim, a exclusão da possibilidade de consumo, ainda que seja esse o desejo do consumidor. Para exemplificar, no momento da aquisição de um determinado produto ou serviço, uma empresa verificaria os dados minerados do usuário que revelariam que ele não possuiria condições de adquirir o referido produto ou serviço. Nesse momento, ele seria cientificado da negação da venda sem que, para isso, fosse justificado o

motivo. Isso porque, se a própria coleta de dados não está determinada e regrada pelo ordenamento jurídico, tampouco o uso desses dados está. Logo, a negação sem justificativa se tornaria legítima. De igual modo, esses dados poderiam ser utilizados na construção de perfis de saúde, limitando, assim, "[...] a cobertura dos planos de alguns pacientes." (BAUMAN, 2014, p. 23)

Oscar Gandy (1996, p. 133) realizou um estudo especificamente sobre esse ponto, conhecido como *The Panoptic Sort*. Nessa obra, verifica-se a realização de uma classificação geral oriunda de um marketing fundado em bases de dados ao qual Gandy chama de "geodemografia".

> O *panoptic sort* é uma tecnologia discriminatória complexa. É o panóptico que considera toda a informação sobre o status e o comportamento de um indivíduo para ser potencialmente útil na produção de inteligência sobre o valor econômico de uma pessoa. É uma tecnologia discriminatória porque é utilizada para classificar pessoas dentro de categorias baseadas nestas estimativas.[107](GANDY , 1996, p. 133, tradução nossa)

Nele, "as pessoas se agrupam em segmentos populacionais incipientes, de modo que os marqueteiros possam tratá-las de forma diferente, dependendo de seu comportamento de consumo." (BAUMAN, 2014, p. 68)

A consequência dessa análise de dados, realizada por softwares estatísticos, é conhecida como "discriminação racional". Isso quer dizer que "[...] a classificação organizacional de usuários, clientes, pacientes, consumidores, e assim por diante, é uma parte cada vez mais significativa da vida moderna." (BAUMAN, 2014, p. 69)

Ocorre que, a discriminação racional também possui sua característica negativa de exclusão, pois "[...] também define as possibilidades de ação dos grupos afetados. Gandy vai adiante, e insiste que a "discriminação racional" nas economias de informação muitas vezes se baseia em perfis raciais e provoca uma desvantagem cumulativa para aqueles negativamente identificados." (BAUMAN, 2014, p. 69)

---

107 No original: *The panoptic sort is a complex discriminatory technology. It is panoptic in that it considers all information about individual status and behavior to be potentially useful in the production of intelligence about a person's economic value. It is a discriminatory technology because it is used to sort people into cetogories based upon these estimates.*

Portanto, a proteção da privacidade do indivíduo, além de prevenir o surgimento de um Estado de Exceção permanente, também possui o condão de evitar discriminações injustificadas e desnecessárias, pois se basearão num espaço amostral de dados finito, onde, porventura, poderão chegar a conclusões equivocadas por não possuírem todas as informações necessárias para uma eficiente tomada de decisão.

É possível identificar a ocorrência desse tipo de discriminação de dados utilizando-se o filtro invisível de Pariser (2012), pois ao se navegar pela Internet, caso se realize uma busca, fatalmente, o resultado dessa pesquisa será exibido de forma diferente se dois internautas o fizerem em seus, respectivos, computadores, ainda que o termo seja o mesmo. Sendo assim, um produto ou serviço pode não ser exibido para um usuário, mas o será para o outro. Entretanto, isso não quer dizer que ambos os internautas não possuam condições de adquirir ou usufruir daquele produto ou serviço.

Logo, isso reforça o que vem sendo afirmado ao longo deste trabalho, de que a privacidade do indivíduo deve ser assegurada. No entanto, como realizar essa ação se a tecnologia não observa e, além disso, desrespeita a norma sem perceber, inclusive, uma sanção?

Nesse sentido, reafirma-se o que já foi dito anteriormente, de que é preciso contra-utilizar a tecnologia como forma de reafirmar o direito à privacidade. Essa contra-utilização se distancia da contrainformação, pois não tem o condão de trabalhar com o tema da ludibriação ou da sabotagem como formas de se assegurar a privacidade. Silva Neto (2001, p. 118-120) argumenta que

> assim nos parece que uma boa alternativa a ser utilizada para a preservação de nossa privacidade é a contrainformação, a disseminação de dados falsos. Se desvalorizarmos o resultado do produto, desvalorizaremos, de modo igual, sua importância para aqueles que estão interessados em sua utilização. Afinal... ¿que governos ou corporações se interessariam por um banco de dados falsos, viciados? Enfim, revertendo o caminho dos ponteiros do relógio e compactuando com os pervasivos ideais de todos os governos de todos os tempos, é chegado o momento de mentir. Não apenas como ideal, mas como ideologia, como tática.
> [...]

> Portanto, toda vez que se cadastrar em qualquer site, seja para que fim o for, necessariamente informações suas lhe serão solicitadas, MINTA. com todas as letras: ¡MINTA! Seus dados são a matéria prima que é buscada. Em vez de ouro, dê cassiterita, o ouro do tolo.
> Cremos que é oportuno que ludibriemos o sistema que nos espiona. Toda e qualquer informação falsa que puder ser fornecida deve ser fornecida; todos os métodos que puderem ser usados para confundir devem ser utilizados contra aqueles que pretendem degustar nossa intimidade.

Entretanto, esse método se mostra custoso ao indivíduo, pois terá sempre que gerar diferentes informações acerca do mesmo dado requerido, bem como, ineficaz, pois, ao contrário da contrainformação utilizada contra seres humanos, as máquinas possuem vários dados armazenados e um alto poder de processamento, o que poderia, singularmente, permitir que as máquinas adivinhassem a fonte das informações pelas próprias contrainformações geradas, minando todo o processo da contrainteligência. Além disso, essa prática pode levar as pessoas a cometer inúmeros ilícitos civis ou até mesmo crimes.

Por esse motivo, serão estudadas tecnologias que também manipulam e tratam a informação de forma que o emissor mantém o controle sobre elas, bem como, de quem terá acesso a elas. Desse modo, serão tratadas a criptografia e as tecnologias livres, que são o software e o hardware livre. Esta tríade da segurança da informação permite que a privacidade seja reafirmada e garantida no cenário atual de coleta e monitoramento dos dados pessoais dos indivíduos. Elas serão abordadas a seguir, iniciando-se pela criptografia.

3.4. A UTILIZAÇÃO DA CRIPTOGRAFIA PARA SE CRIAR UM LUGAR VIRTUAL PARA ESTAR SÓ

A palavra criptografia se origina do grego *kriptós* + *grápho*. O termo *kriptós* se traduz em escondido ou oculto. Já *grápho* quer dizer grafia (ABSOLUTA, 1999). Logo, criptografia significa escrita oculta.

Embora seja muito difundida no ambiente tecnológico, a criptografia é uma técnica antiga, utilizada há muito tempo, sendo considerada “[...] tão antiga quanto a própria escrita, visto que já estava presente no sistema de escrita hieroglífica dos egípcios” (MORENO, PEREIRA e CHIARAMONTE, 2005, p. 22). Sua primeira utilização registrada, data do ano de 1.900 a.C., “[...] quando o escriba de Khnumhotep II teve a ideia de substituir algumas palavras ou trecho de texto. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro e morreria de fome perdido nas catacumbas da pirâmide” (MORENO, PEREIRA e CHIARAMONTE, 2005, p. 22).

A criptografia tem sido utilizada para fins variados, desde uma adolescente que escreve seu diário em códigos para que seus pais não saibam de suas aventuras, bem como, de uma confissão de um segredo entre amigos feito por meio de cartas, e, obviamente, o sigilo nas comunicações durante uma batalha ou guerra. “A criptologia faz parte da história humana porque sempre houve fórmulas secretas e informações confidenciais que não deveriam cair no domínio público ou na mão de inimigos.” (MORENO, PEREIRA e CHIARAMONTE, 2005, p. 22).

Portanto, a criptografia demonstra ser um meio confiável para se depositar ou fazer trafegar informações sobre a privacidade, a vida privada ou a intimidade de um indivíduo, pois não revela o conteúdo de sua mensagem, logo, não exibindo o conhecimento sobre a essência do ser.

De forma a permitir o correto entendimento sobre as explicações a seguir, acerca da criptografia, é preciso fixar o conhecimento de alguns termos, tais como: texto claro, que é a mensagem antes de ser criptografada ou cifrada; algoritmo de criptografia, que é a rotina que manipula o texto claro, aplicando sobre ele a chave secreta; chave secreta, que é a chave com a qual o texto claro será cifrado ou criptografado; texto cifrado, que é o texto claro criptografado; e o algoritmo de decriptografia, responsável pela transformação do texto cifrado em texto claro.

Basicamente, a criptografia é utilizada através de algumas técnicas, sendo as principais a da chave simétrica e a da chave assimétrica[108]. No caso da chave simétrica, seu funcionamento é relativamente simples, pois consiste na elaboração de uma chave secreta que será responsável por esconder a mensagem original, e, somente com essa mesma chave secreta é que será possível tornar o conteúdo original compreensível.

O Império Romano, em 50 a.C., fez uso de uma criptografia que ficou conhecida como Cifra de César (STALLINGS, 2008, p. 22). A ideia de César era relativamente simples. Ele escrevia uma mensagem que era reescrita, criptografada, alterando o alfabeto de forma que sua primeira letra era pré-fixada por outra da seguinte forma:

alfabeto: a b c d e f g h i j k l m n o p q r s t u v w x y z
cifra: d e f g h i j k l m n o p q r s t u v w x y z a b c

Assim, caso fosse escrita a palavra "*ataque*" em texto claro, com base na Cifra de César acima, o texto cifrado seria "*dwdsxh*". E somente quem soubesse a pré-fixação do alfabeto, ou seja, a cifra, é que conseguiria descobrir a mensagem original.

Texto claro: ataque
Texto cifrado: dwdsxh

A Cifra de César é uma das modalidades de criptografia simétrica. "A criptografia simétrica é uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando a mesma chave secreta. Ela também é conhecida como criptografia convencional" (STALLINGS, 2008, p. 17). Logo, tanto o emissor quanto o destinatário de uma mensagem conhecem, previamente, a chave secreta.

De forma a aprofundar a exemplificação, caso a mensagem "O código secreto é sigilo-fdv" fosse transmitida utilizando a Cifra de César, com base na mesma cifra acima, o conteúdo que trafegaria na Internet seria: "R frgmkr vhfuhwr h vmkmor-igy". Isso deixa claro que qualquer informação armazenada ou transmitida utilizando a criptografia, permanece protegida. Por conseguinte, caso o conteúdo da frase fosse

108 O foco da presente pequisa não é estudar a criptografia com profundidade, logo, são abordadas apenas as principais técnicas.

uma informação pessoal localizada na esfera da privacidade, da vida privada ou da intimidade de um indivíduo, e, ainda assim, ela fosse interceptada por alguma das técnicas que já foram vistas no capítulo anterior, o direito fundamental à privacidade estaria assegurado, pois o conteúdo da mensagem seria ininteligível. De forma a ilustrar esse entendimento, a Figura 10 exibe o procedimento de criptografia com chave simétrica.

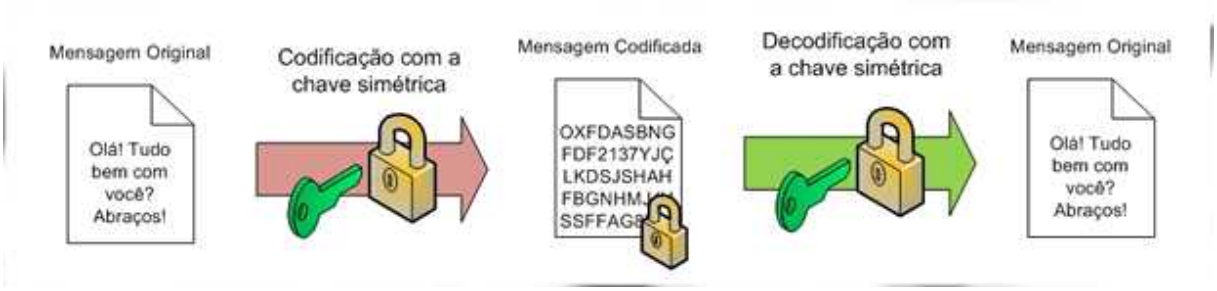

Figura 10 – Procedimento de criptografia de chave simétrica.
Fonte: http://s.glbimg.com/po/tt/f/original/2012/06/21/simetrica.png

A Figura 10 mostra a utilização da criptografia simétrica. Um emissor possui uma mensagem original que é cifrada com uma chave secreta. Então, como resultado dessa operação, é gerada uma mensagem codificada. O destinatário aplica a mesma chave secreta para decodificar a mensagem cifrada que, assim, volta a ser a mensagem original.

Mas se a Cifra de César for analisada, sua chave secreta possui 26 posições possíveis, que são as combinações alfabéticas em si. A técnica conhecida para se “quebrar” uma criptografia é chamada de criptoanálise. Uma das criptoanálises mais conhecidas é a de força bruta, que testa uma a uma as combinações possíveis até que a mensagem seja decifrada. Assim, bastam 26 testes, no pior caso, para se descobrir a mensagem original. E com o auxílio do computador, por exemplo, quebrar a criptografia romana ocorreria em questão de segundos.

Por esse motivo é que a criptografia ganhou tanta notoriedade na era da informação, pois, com a utilização do poder de processamento dos computadores são criadas técnicas criptográficas impossíveis de serem descobertas ou quebradas pelo ser humano. Na verdade, até mesmo para os computadores, dependendo da criptografia, quebrá-la representa anos de processamento.

Com base nessa premissa, da utilização dos computadores, é que surgiu outro tipo de criptografia, considerada uma revolução nessa ciência (STALLINGS, 2008, p. 182), que é a criptografia assimétrica. Essa técnica "[...] é uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando diferentes chaves – uma chave pública e uma chave privada. Ela também é conhecida como criptografia de chave pública." (STALLINGS, 2008, p. 181).

Enquanto a criptografia simétrica aplica a cifra realizando operações de permuta e substituição, a criptografia assimétrica realiza operações com funções matemáticas, geralmente, baseadas em números primos[109] (STALLINGS, 2008, p. 182).

Por possuir duas chaves, uma privada e uma pública, seu funcionamento é, relativamente, diferente. O texto claro é cifrado utilizando-se a chave pública do destinatário, que pode ser de conhecimento de qualquer pessoa, muitas vezes, divulgada abertamente pelo proprietário. Já a decriptografia ocorre com a aplicação da chave privada, que fica em poder e conhecimento do destinatário somente. Sendo assim, essa técnica pode ser utilizada para "[...] confidencialidade, autenticação[110] ou ambos." (STALLINGS, 2008, p. 181).

Frise-se que a chave privada, como já mencionado, deve ser de conhecimento apenas do destinatário. Já a chave pública deste, pode ser divulgada para quem quer que seja, porquanto apenas a chave privada de determinada chave pública é capaz de decifrar a mensagem que foi por esta encriptada. Por esse motivo, é correto dizer que essas chaves somente funcionam em pares. De igual modo, ilustra-se a utilização da criptografia assimétrica com a Figura 11.

---

109 Números primos são números pertencentes ao conjunto dos números inteiros divisíveis pelo número inteiro 1 (hum) e por eles mesmos. Para a criptografia, quanto maior o número primo, mais forte será a criptografia desenvolvida.

110 Cumpre esclarecer que essa é a técnica utilizada para a assinatura digital dos certificados digitais brasileiros exigidos pela Medida Provisória 2.200-2, de 24 de agosto de 2001, em prática na operação do Processo Judicial Eletrônico no Brasil.

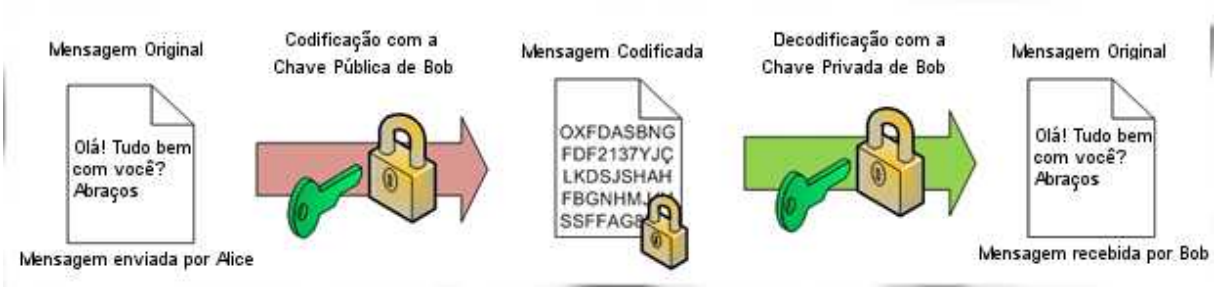

Figura 11 – Procedimento de criptografia de chave assimétrica.
Fonte: http://s.glbimg.com/po/tt/f/original/2012/06/21/simetrica.png

No exemplo da Figura 11, Alice quer enviar com privacidade uma mensagem para Bob. Para isso, ela criptografará a mensagem utilizando a chave pública de Bob. Quando Bob então receber a mensagem, ele descriptografará a mesma utilizando a sua chave privada. Essa forma de utilização da criptografia assimétrica garante a confidencialidade da comunicação, ou seja, o sigilo tão necessário à privacidade, à vida privada e à intimidade.

Já Bob possui duas opções para responder Alice, são elas: utilizar a chave pública de Alice ou respondê-la valendo-se de sua própria chave privada. Como Bob, necessariamente, precisa que Alice tenha a certeza de que ele é o emissor da mensagem, ele aplicará sua chave privada, que somente ele conhece. No momento em que Alice receber a mensagem, ela a decifrará com a chave pública de Bob. Assim, Alice terá certeza da autenticidade da mensagem, ou seja, de que ela, sem sombra de dúvidas, partiu de Bob. Esse cenário é ilustrado pela Figura 12.

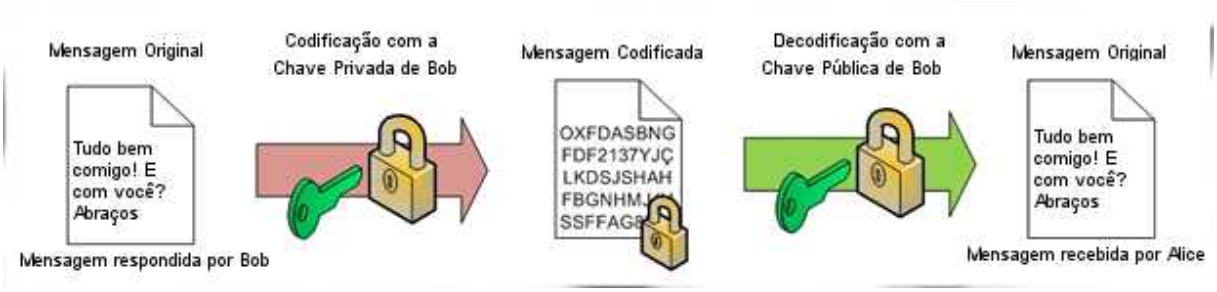

Figura 12 – Procedimento de criptografia com chave assimétrica.
Fonte: http://s.glbimg.com/po/tt/f/original/2012/06/21/simetrica.png

Cite-se que o método acima garante apenas a autenticidade da mensagem, uma vez que, como a chave pública de Bob pode ser de conhecimento de muitos, aquele que interceptar a mensagem e também possuir a chave pública de Bob poderá decifrá-la.

A única forma de se garantir a autenticidade e a confidencialidade da mensagem na criptografia assimétrica é realizando o procedimento de cifragem em duas etapas. Supondo que Bob enviará uma mensagem para Alice de forma que ela terá certeza da autoria e do sigilo, a primeira etapa consiste em Bob criptografar o texto utilizando sua chave privada. Em segundo lugar, com o texto, resultado da primeira etapa de criptografia, Bob encriptará essa mensagem com a chave pública de Alice. Após isso, Alice receberá o texto que descriptografará com a sua chave privada, comprovando o sigilo da transmissão. Ato contínuo, descriptografará a mensagem com a chave pública de Bob, entretanto, isso somente foi possível após utilizar sua própria chave privada. Sendo assim, esse procedimento garante tanto a autenticidade quanto o sigilo das comunicações.

Cumpre salientar o que adverte Stallings (2008, p. 182) sobre as criptografias simétricas e assimétricas, pois ele afirma que é um erro pensar que uma é superior a outra. Da mesma forma, a criptografia assimétrica não tornou obsoleta a criptografia simétrica. Portanto, ambas as formas de criptografia são igualmente seguras, se diferenciando apenas quanto a finalidade de sua aplicação.

No entanto, a criptografia não garante apenas a privacidade nas comunicações, mas também, a privacidade dos dados e informações pessoais que tenham sido armazenadas em dispositivos computacionais. Logo, também é possível que dados sejam salvos em computadores, pendrives[111] e *smartphones* de forma criptografada, onde somente quem souber a chave secreta conseguirá acessá-los.

Alguns programas acessíveis a população, principalmente, aos usuários de *smartphone*, garantem o sigilo das comunicações e dos dados de seus usuários. Como exemplo, tem-se o OTR[112], o TextSecure[113] e o RedPhone[114]. O Off-the-Record – OTR é um *plug-in* para mensagens instantâneas que criptografa a mensagem para o seu envio. Assim, o simples fato de se conversar pela Internet já se torna mais

111 Pendrive é um dispositivo de armazenamento portátil que é ligado no computador, geralmente, por uma porta conhecida como porta USB (Universal Serial Bus)
112 O OTR pode ser acessado pelo link: https://otr.cypherpunks.ca/
113 O TextSecure pode ser acessado pelo link: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en
114 O RedPhone pode ser acessado pelo link: https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone&hl=en

seguro. Inclusive o Snowden utilizou o OTR para se comunicar com Greenwald antes de conhecê-lo pessoalmente (GREENWALD, 2014). O TextSecure é um programa que criptografa mensagens *Short Message Service* – SMS ou o *Multimedia Message Service* – MMS, comumente conhecidos como torpedos. Dessa forma, as mensagens enviadas entre aparelhos celulares ou *smartphones* que utilizarem essa técnica, garantirão o sigilo das comunicações. Por fim, o RedPhone é um programa de Voz sobre IP – VoIP[115], ou *Voice over Internet Protocol*, que criptografa as ligações telefônicas, desde que, ambos os usuários possuam o referido programa instalado. Isso garante, especialmente, o sigilo das comunicações telefônicas. As aplicações TextSecure e RedPhone fazem parte do projeto *Open Whisper Systems*[116].

Outra técnica de criptografia largamente utilizada pelas empresas é a *Virtual Private Network* – VPN ou Rede Privada Virtual, que permite, inclusive, que os funcionários trabalhem à distância, mas, com acesso à rede local da empresa.

Sobreleva ressaltar agora, uma característica muito importante acerca da criptografia, que é considerada sua fragilidade, que ocorre quando se compreende como ela é utilizada e, assim, torna-se possível então, produzir ataques com o intuito de decifrar a mensagem chegando-se ao seu real conteúdo.

Rememorando-se o que foi dito no item 2.2 do presente trabalho, o exército alemão utilizava uma criptografia simétrica cuja cifra era alterada toda manhã. Ou seja, todo o trabalho do dia anterior dos ingleses era inútil, pois a cifra utilizada no dia seguinte era diferente. Diante dessa dificuldade, o matemático inglês, Alan Turing desenvolveu uma máquina chamada COLOSSUS capaz de analisar o texto cifrado procurando por combinações de palavras que revelassem a chave secreta. Quando então conseguiu esse feito, os ingleses recobraram a vantagem durante a Segunda Guerra Mundial. Estima-se que o tempo de duração da guerra seria de mais de três anos caso a criptografia alemã não tivesse sido “quebrada”. Esse ponto da história

115 Voz sobre IP – VoIP é uma técnica que realiza transmissões de voz através de pacotes de dados utilizando os protocolos disponíveis na Internet.
116 O Projeto *Open Whisper Systems* pode ser acessado através do link: https://whispersystems.org/#page-top

revela que a criptografia não é absoluta e pode ser violada, e o método para isso, que já foi descrito acima, é a criptoanálise.

A criptoanálise consiste no entendimento acerca do funcionamento de determinado algoritmo de criptografia com a finalidade de se encontrar alguma brecha para se introduzir um ataque. Entretanto, quanto mais criptoanálise é feita sobre um algoritmo de criptografia, mas eficiente e seguro ele se torna, pois esses algoritmos, normalmente, são públicos e possuem o seu código-fonte divulgado. Logo, recebem estudos e contribuições de várias pessoas ao redor do mundo. Isso que dizer que os algoritmos que são utilizados há mais tempo são mais seguros que os demais. Frise-se que o segredo da criptografia encontra-se na chave secreta criada pelo usuário. É ela que permitirá decifrar a mensagem cifrada.

Para ilustrar o que foi dito, vale-se de um caso que ocorreu no Brasil, que foi a Operação Satiagraha, depreendida pela Polícia Federal no ano de 2008 (G1, 2010). Durante a operação, cinco discos rígidos, uma peça do computador onde são armazenadas todas as informações que ele contém, do banqueiro Daniel Dantas foram apreendidos. Ocorre que, esses dispositivos estavam criptografados pelos *softwares* TrueCrypt[117] e PGP[118], que utilizaram o algoritmo de criptografia AES 256 bits. Após o Instituto Nacional de Criminalística – INC, durante cinco meses, não ter conseguido quebrar a segurança aplicada, os discos rígidos foram enviados para o *Federal Bureau of Investigation* – FBI nos Estados Unidos da América, que depois de doze meses, também não conseguiu quebrar a criptografia utilizada. Os discos rígidos permanecem sob custódia do INC. “Os peritos do INC esperam que novos dados da investigação, ou que uma nova tecnologia, os ajudem a quebrar as chaves de segurança.” (GGN, 2012). Isso demonstra, *de per si*, que a criptografia é uma técnica confiável para se manter informações pessoais, inclusive as relativas à privacidade, à vida privada e à intimidade, sob proteção, devolvendo para ao

117 O programa TrueCrypt pode ser acessado através do link http://truecrypt.sourceforge.net/ . Entretanto, o próprio site exibe a informação de que esse aplicativo não é seguro e possui falhas sem correção. Suspeita-se de que o governo americano tenha requerido a implementação de falhas que fossem exploradas apenas pelos EUA, momento em que a TrueCrypt optou por encerrar o desenvolvimento e manutenção do programa (TECNOBLOG, 2014).
118 PGP é o acrônimo para *Pretty Good Privacy*. É um dos softwares mais populares de criptografia. Ele pode ser acessado pelo link http://www.openpgp.org/ .

indivíduo, a liberdade de negação. Da mesma forma, pode-se dizer que a criptografia empodera o indivíduo na luta pela privacidade.

O liame entre a criptografia e o presente trabalho se verifica em dois pontos distintos. O primeiro foi demonstrado no parágrafo anterior, que é a proteção às informações pessoais. O segundo diz respeito a problemática da coleta e guarda indiscriminada de dados pessoais que é feita por governos e por empresas, que tornam o indivíduo vulnerável, além de transformar a todos, em suspeitos em potencial. Dentro desse tema, não há, na atualidade, uma tecnologia capaz de quebrar várias criptografias ao mesmo tempo. Logo, se todo indivíduo utilizar a criptografia como forma de proteção dos dados pessoais, o Estado teria que selecionar com base em algum critério uma pessoa que desejasse investigar para, então, utilizar os meios tecnológicos necessários para quebrar a criptografia e revelar as informações sobre essa pessoa. Esse cenário faz com que a ideia da suspeita prévia seja mais adequada do que todos como suspeitos em potencial.

Por esse motivo é que a presente pesquisa se fundamenta e justifica na declaração feita pelo Presidente norte-americano Barack Obama após o atentado ocorrido contra o jornal *Charlie Hebdo* (EXAME, 2015), pois segundo sua declaração, ele é contrário a utilização da criptografia, especialmente, em *smartphones*.

A intenção estadunidense surpreende pois pretende criar uma falha de segurança conhecida como *backdoor*[119], ou porta dos fundos, onde a polícia, mediante uma ordem judicial, poderia acessar todo o conteúdo criptografado em questão de segundos. Ocorre que, toda a população do planeta saberia da existência dessa falha, logo, tornando-se ela, explorável por qualquer indivíduo que manifeste interesse.

Ocorre que, essa se mostra uma tendência entre governos, pois, recentemente, à revelia de empresas, juízes e jornalistas, a França aprovou uma lei de segurança que se assemelha ao Ato Patriota americano (PUBLICO, 2015). Essa lei abriu "[...] a

119 *Backdoor* ou porta dos fundos é uma brecha propositalmente inserida no sistema de forma a permitir que seu autor possa acessar tanto o programa quanto as informações deste através dela.

porta à invasão da privacidade de cidadãos que não têm nenhuma relação com o terrorismo ou qualquer outra actividade criminosa.” (PUBLICO, 2015).

Segundo o texto da própria lei, “[...] a polícia e os serviços secretos franceses podem implantar aparelhos de vigilância em habitações, tirar fotografias ou interceptar conversas telefónicas no âmbito de uma investigação a um suspeito **sem que seja necessário pedir autorização a um juiz.**” (PUBLICO, 2015, grifo nosso).

Além disso, a polícia e os serviços secretos também terão autorização para “aceder aos servidores das empresas que fornecem acesso à Internet, através de um algoritmo secreto preparado para filtrar as palavras-chave definidas pelas autoridades.” (PUBLICO, 2015). Isso é violar qualquer previsão legal existente sobre privacidade.

Contudo, a criptografia consegue, mesmo diante desse cenário, garantir o sigilo das comunicações e das informações pessoais armazenadas em dispositivos computacionais.

Além disso, a criptografia tem sido a pedra angular de vários movimentos pela Internet, possibilitando, inclusive, denúncias baseadas em informações provindas do mais alto escalão do poder. Dentre diversos movimentos, citam-se os Cypherpunks, o Wikileaks e a Deep Web.

Os Cypherpunks estão espalhados pela Internet e, geralmente, são especialistas em criptografia. Eles “[...] defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas.” (ASSANGE *et al*, 2013, p. 06). Embora os adeptos da utilização da criptografia sempre tenham existido, o movimento cypherpunk “[...] atingiu seu auge durante as “criptoguerras” e após a censura da internet em 2011, na Primavera Árabe.” (ASSANGE *et al*, 2013, p. 06)

Foi com base na criptografia que surgiu o Wikileaks, um canal mundial de denúncias, principalmente, de violações contra os Direitos Humanos.

O Wikileaks[120] é uma organização sem fins lucrativos cujo objetivo é trazer informações importantes para o público (WIKILEAKS, 2011). Foi através dele que vários abusos contra os Direitos Humanos foram divulgados. Dentre inúmeras denúncias, destaca-se aquela feita em 2010, onde vídeos oficiais das forças armadas americanas foram exibidos mostrando o ataque a civis e o assassinato de um jornalista da imprensa Reuters (OBSERVATÓRIO DA IMPRENSA, 2010).

A questão que se põe diante de um site como o Wikileaks, é descobrir como tantas pessoas confiam nessa instituição de forma que enviam todo o tipo de documento secreto, arriscando-se em ser processado e condenado a uma prisão, por exemplo. A resposta é simples: criptografia.

Julian Assange, um dos fundadores do Wikileaks, é também o criador de um sistema de criptografia conhecido como *rubberhose*, "[...] desenvolvido para que defensores de direitos humanos consigam manter em segredo parte dos dados criptografados mesmo se pressionados sob tortura por regimes autoritários." (ASSANGE *et al*, 2013, p. 12).

O *rubberhose* implementa o conceito de criptografia de negação. Ele é o "[...] primeiro bem-sucedido, distribuído gratuitamente, programa prático de criptografia de negação do mundo.[121]" (DEVIANTART, 2013). O que o torna tão atraente para ativistas captarem documentos secretos é o fato de ser possível criptografar um dispositivo de armazenamento de forma que o conteúdo secreto se localize numa área onde somente quem a colocou lá é que sabe a sua localização.

Assim, se um ativista for torturado para entregar seus equipamentos e dispositivos computacionais, ele poderá fazê-lo sem nenhum temor, ainda que sob tortura, pois mesmo que possuam acesso ao seu disco rígido, por exemplo, não saberão onde se localiza, exatamente, o material criptografado.

---

120 O link para acesso ao Wikileaks é https://wikileaks.org/index.en.html .
121 No original: *Rubberhose is the first successful, freely available, practical program of deniable cryptography in the world.*

Outro grande ponto que propicia o envio de documentos para o Wikileaks é a omissão das fontes, ou seja, os documentos podem ser enviados anonimamente, ou, ainda que o Wikileaks conheça a fonte, ele não mantém qualquer registro que possa ser analisado pelo governo.

Por fim, outra tecnologia que se vale da criptografia como engrenagem motora, é a *Deep Web* ou Internet Profunda. Ao contrário do que se pensa, a *Deep Web* não é outra Internet, mas sim, uma Internet dentro da Internet.

O principal ponto que liga a *Deep Web* com a criptografia é o fato dela ter surgido como um movimento contra-hegemônico cujo objetivo é aumentar a privacidade e a segurança na Internet. Sua infraestrutura é constituída, basicamente, de servidores independentes e voluntários[122] (TOR, 2015).

A única forma de acessá-la é através de um programa chamado Tor[123]. Tor é o acrônimo para *The Onion Router*, ou, em tradução livre, o roteador cebola. Isso porque, a Internet Profunda está organizada em camadas, onde, desde a primeira, somente é possível realizar o acesso com a criptografia disponibilizada pelo aplicativo Tor. Estima-se que existam até sete camadas acessíveis na *Deep Web*. A complexidade da criptografia evolui a medida que se progride nessas camadas (ANONYMOUSBR4SIL.NET, 2013).

Insta ressaltar que os sites da superfície são acessíveis através da Deep Web, mas o contrário não se verifica caso o site na Internet Profunda esteja utilizando o *hidden service protocol*.

O *hidden service protocol*, ou protocolo de serviços ocultos em tradução livre “[...] possibilita aos usuários esconder sua localização enquanto oferece vários tipos de serviços, como uma publicação na Web ou um servidor de mensagem instantânea. Usando o Tor "*rendezvous points*", outros usuários podem conectar com esses

122 No origirnal: *The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet.*
123 O programa Tor pode ser “baixado” do link https://www.torproject.org .

serviços ocultos, cada um sem saber a identidade de rede do outro[124].” (TOR, 2015). Os servidores disponibilizados através desse protocolo possuem o sufixo .onion no lugar de .com.br , por exemplo.

Assim, por se fundar em criptografia, a Internet Profunda consegue se tornar invisível para o que se convencionou chamar de superfície, que é a Internet convencional, onde a maioria dos usuários do mundo acessa. Outro ponto favorável aos internautas é que a *Deep Web* preza pelo anonimato e pela privacidade. Insta salientar, que o programa Tor, utilizado sem o auxílio de outras técnicas, não garante o anonimato na Internet Profunda.

E não é outra a razão da *Deep Web* ser tão popular, senão pela privacidade e anonimato garantidos pela criptografia, que ela representa a maior parte da Internet. Estima-se que 70 a 75% de toda a rede mundial esteja na Internet Profunda (PORTAL TIC, 2015).

Cumpre salientar também que, muito provavelmente pela falsa sensação de anonimato, muitos prefiram acessar a *Deep Web* na ilusão de não serem identificados quando da execução de uma conduta ilícita ou criminosa. Por esse motivo, é possível encontrar nela sites que vendam drogas, ofereçam serviços como matadores de aluguel, assim como, conteúdo relacionado a pedofilia. Mas para desmistificar a impressão de que na Internet Profunda se pode ter qualquer conduta, vale lembrar a Operação Darknet, deflagrada pela Polícia Federal em 2014, que prendeu 51 pessoas em 18 Estados e no Distrito Federal (ESTADAO, 2014). A atuação da Polícia Federal fez parte de uma ação em conjunto com mais cinco países, sendo eles Portugal, Itália, Colômbia, México e Venezuela, cujo objetivo era prender os membros de uma rede internacional de pedofilia. Logo, fica claro que a *Deep Web* não se propõe como um ambiente de anonimato, mas sim, um ambiente mais seguro para o tráfego de dados, inclusive, os relativos a informações pessoais, pois a base de sua comunicação é a criptografia. Sudré Filho (2015) salienta que “[...] o vazamento de informações do Hacked Team mostrou que eles desenvolveram

124 No original: *Tor makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server. Using Tor "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity.*

uma ferramenta que, em tese, permite identificar o usuário do Tor. A ferramenta, inclusive, estava sendo negociada com o *Federal Bureau of Investigation* – FBI."

Portanto, após comprovar-se que a criptografia assegura tanto o sigilo quanto a autenticidade da mensagem durante sua transmissão ou armazenamento, é possível afirmar que as informações pessoais das esferas da privacidade, da vida privada e da intimidade podem ser protegidas contra o conhecimento de terceiros. Conclui-se, assim, nos dizeres de Hannah Arendt (2014, p. 87), que a criptografia oferece o "[...] refúgio seguro contra o mundo público comum, não só contra tudo o que nele ocorre, mas também contra a sua publicidade, contra o fato de ser visto e ouvido." Logo, a criptografia empodera o indivíduo, novamente, com a sua liberdade essencial de negação, além de possibilitar que um segredo seja armazenado de forma segura e sigilosa, onde outras pessoas sequer saberão onde ele se encontra, muito menos, qual é o seu conteúdo. Desta feita, pode-se afirmar que a criptografia é a técnica capaz de criar um lugar virtual para se estar só.

Demonstrada a importância da criptografia para a mantença da privacidade na era da informação, é preciso abordar outro ponto que também reafirma e garante esse direito fundamental. Fala-se do Software Livre.

3.5. SOFTWARE LIVRE: QUANDO A TECNOLOGIA DEVOLVE A LIBERDADE ONTOLÓGICA DO SER

Precipuamente, é preciso salientar que, em meados do ano de 1971, a maioria dos desenvolvedores de software frequentemente trocava ou distribuíam o seu código-fonte[125] com o intuito de aprender e compartilhar diferentes programas. "Já na década de 1980, quase todo o software era proprietário, o que significa que ele possuía donos que proibiam e evitavam a cooperação dos usuários." (GNU, 2014)

125 Código-fonte é a forma como o programa está escrito, ou seja, codificado, porém, numa linguagem compreensível ao homem.

Isso fez com que um grupo de hackers[126] se reunisse e criasse o Projeto GNU. A sigla GNU significa *GNU is Not Unix*, o que, em tradução livre, representa GNU não é Unix[127], onde Unix é um Sistema Operacional[128]. A partir daí, o Projeto GNU criou um Sistema Operacional que precisava de um *kernel*[129]. Foi quando, em 1991, Linus Torvalds criou o Linux, que se tornou um Software Livre em 1992 (GNU, 2014). Assim nasceu o GNU/Linux, um Sistema Operacional integralmente feito com Software Livre. Atualmente, é a *Free Software Foundation* – FSF[130], uma fundação sem fins lucrativos, promove e defende os direitos dos usuários de software livre.

Nota-se, então, que o Software Livre é um movimento contra-hegemônico, porquanto foi contrário a tendência estatal e mercadológica de fechar o código-fonte das aplicações.

A motivação para isso é clara, como permitir que um programa execute em um computador, que é um repositório de dados pessoais, porta de entrada para a privacidade do indivíduo, sem que se saiba o que esse software fará? Infelizmente, essa é uma realidade hoje. Todos os usuários dos Sistemas Operacionais Windows, OS X (MacBook), iOS (iPhone e iPad), Android[131] (*smartphones*), dentre outros, não possui condição ou noção do que programa faz com a máquina ou com as informações que ela contém. O jargão da informática para designar esse comportamento é caixa-preta, pois não se sabe como o programa funciona “por dentro”.

---

126 Hackers são entusiastas da tecnologia, e, geralmente, a utilizam como forma de ajudar a sociedade. Portanto, é um erro chamar aqueles que utilizam a tecnologia de forma ilícita ou criminosa de hacker, sendo correto chamar de cracker – *criminal* hacker.

127 Unix é um Sistema Operacional criado no ano de 1970 no laboratório da AT&T. Por ter o código-fonte acessível, a partir de seu lançamento, foram surgindo várias versões do mesmo sistema operacional. Isso o popularizou e fez com que servisse de base para vários outros sistemas operacionais. (UNIX, 2012)

128 Sistemas Operacionais são responsáveis por fazerem a interface entre os softwares e o hardware dos computadores. São exemplos de sistemas operacionais o Windows, o Linux, o OS X, dentre outros.

129 *Kernel* é o núcleo do Sistema Operacional. Ele é quem centraliza e administra todas as requisições feitas pelo computador.

130 A *Free Software Foundation*, ou Fundação de Software Livre em tradução livre, pode ser acessada através do link http://www.fsf.org .

131 Muito embora o Google levante a bandeira de que o Android é um sistema operacional de código aberto, uma pesquisa revelou que ele não possibilita o acesso ao código-fonte do modo que informa. (TUDOCELULAR.COM, 2011)

Para que um software seja considerado livre é preciso que ele obedeça a quatro liberdades (GNU, 2014), são elas:

> • A liberdade de executar o programa como você desejar, para qualquer propósito (liberdade 0);
> • A liberdade de estudar como o programa funciona, e adaptá-lo às suas necessidades (liberdade 1). Para tanto, acesso ao código-fonte é um pré-requisito;
> • A liberdade de redistribuir cópias de modo que você possa ajudar ao próximo (liberdade 2);
> • A liberdade de distribuir cópias de suas versões modificadas a outros (liberdade 3). Desta forma, você pode dar a toda comunidade a chance de beneficiar de suas mudanças. Para tanto, acesso ao código-fonte é um pré-requisito.

Frise-se que se constata nas quatro liberdades, que o acesso ao código-fonte é um pré-requisito. Além disso, é preciso a liberdade de redistribuir o programa. Sendo assim,

> por “software livre” devemos entender aquele software que respeita a liberdade e senso de comunidade dos usuários. Grosso modo, os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software. Assim sendo, “software livre” é uma questão de liberdade, não de preço. Para entender o conceito, pense em “liberdade de expressão”, não em “cerveja grátis”. (GNU, 2014)

Cumpre ressaltar algumas dúvidas que ocorrem, muito comum quando se trata a temática do software livre. O primeiro ponto é esclarecer que software livre não é software gratuito. Existem softwares livres que são pagos, e, inclusive possuem contrato de suporte. Portanto, não há o que se falar sobre o software livre atrapalhar a iniciativa privada. O segundo ponto é que o software livre também não se confunde com softwares do tipo *open source*, ou código-aberto. Alguns softwares *open source* não permitem a modificação da aplicação, o que desrespeita a liberdade 1, e impede a sua classificação como software livre.

O Software Livre se relaciona com o direito fundamental à privacidade quando permite ao usuário entender como determinada aplicação funciona, devolvendo para ele a liberdade de escolha entre usar ou não usar um programa. Ora, se uma pessoa, antes de adquirir um dispositivo computacional, acessa o código-fonte do sistema e descobre que ele monitora as suas ações e envia seus dados pessoais para o fabricante, ele tem o poder de decidir se adquirirá o produto ou não.

No caso das Smart TVs, mencionado no capítulo anterior, subtítulo 2.4.2, caso a LG ou a Samsung utilizassem em suas TVs o software livre, seria possível a comunidade alertar os clientes sobre a coleta e envio dos dados pessoais. Mas, obviamente, essa atitude não se mostra de interesse dos fabricantes.

Após Snowden denunciar o programa de monitoramento global, bem como, a espionagem realizada contra o Brasil, notadamente, contra a Presidente Dilma Rousseff, a Petrobras e o Ministério de Minas e Energia, conforme narrado no capítulo anterior, subtítulo 2.4.7, a Presidente expediu o decreto número 8.135, de 04 de novembro de 2013, que "dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional."

A inteligência desse decreto encontra-se no momento em que ele exige que programas e equipamentos permitam a realização de "[...] auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações", conforme o que dispõe o §3º do art. 1º do referido decreto, que segue:

> Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.
> [...]
> § 3º Os programas e equipamentos destinados às atividades de que trata o caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.

Contudo, a única forma de se realizar uma auditoria no sistema utilizado é possuir acesso ao código-fonte.

Porém, a auditoria do código-fonte não garante que este representa o verdadeiro código do programa que se encontra em execução. Se assim o fosse, uma aplicação *open source* atenderia essa exigência legal. Mas para que se possua essa certeza, é preciso, além de ter o código-fonte, ter o poder de compilá-lo[132], ou melhor

132 Compilar um programa significa transformar o código-fonte, compreensível para o ser humano, em linguagem de máquina, compreensível apenas para a máquina.

dizendo, transformá-lo em linguagem de máquina[133] a partir do código-fonte em questão. E isso só se mostra possível respeitando a liberdade 0 já referenciada acima. Portanto, é somente utilizando Softwares Livres que o decreto número 8.135/2013 consegue ser cumprido em sua integralidade.

A importância do acesso ao código-fonte é asseverada, por exemplo, no caso dos sistemas do Processo Judicial Eletrônico brasileiro, pois "[...] não é facultado a sociedade o acesso ao seu código-fonte, instruções que definem como o sistema irá se comportar. Este acesso é necessário para proporcionar total transparência quanto aos serviços disponibilizados pelo sistema PJe." (SUDRÉ e MARTINELLI, 2014, p. 299)

O argumento das empresas para não permitirem o acesso ao código-fonte é o de que isso pode representar um problema de segurança para o sistema. Entretanto, Sudré Filho e Martinelli (2014, p. 299-300) advertem que "acreditar que parte da segurança está em manter sigilo sobre o código-fonte é um conceito antigo e ineficaz e que pode gerar em seus desenvolvedores e usuários uma falsa sensação de segurança."

A questão da utilização de Software Livre pelo Poder Público foi melhor enfrentada pelo Estado do Rio Grande do Sul, que publicou a Lei Estadual número 11.871, de 19 de dezembro de 2002, que "dispõe sobre a utilização de programas de computador no Estado do Rio Grande do Sul". O art. 1º da referida lei é claro quanto a adoção de sistemas construídos sob a premissa do Software Livre, de acordo com o que se verifica a seguir:

> Art. 1º - A administração pública direta, indireta, autárquica e fundacional do Estado do Rio Grande do Sul, assim como os órgãos autônomos e empresas sob o controle do Estado utilizarão preferencialmente em seus sistemas e equipamentos de informática **programas abertos, livres de restrições proprietárias quanto a sua cessão, alteração e distribuição.**
> § 1º - Entende-se por programa aberto aquele cuja licença de propriedade industrial ou intelectual não restrinja sob nenhum aspecto a sua cessão, distribuição, utilização ou alteração de suas características originais, assegurando ao usuário acesso irrestrito e sem custos adicionais ao seu

133 As particularidades atinentes as linguagens de programação compiladas ou interpretadas não influenciam na questão do acesso ao código-fonte. Por esse motivo é que elas não são tratadas no presente trabalho.

> código fonte, permitindo a alteração parcial ou total do programa para seu aperfeiçoamento ou adequação.
> § 2º - Para fins de caracterização do programa aberto, o código fonte deve ser o recurso preferencial utilizado pelo programador para modificar o programa, não sendo permitido ofuscar sua acessibilidade, nem tampouco introduzir qualquer forma intermediária como saída de um pré-processador ou tradutor.
> § 3º - Quando da aquisição de softwares proprietários, será dada preferência para aqueles que operem em ambiente multiplataforma, permitindo sua execução sem restrições em sistemas operacionais baseados em software livre. (grifo nosso)
> § 4º - A implantação da preferência prevista nesta Lei será feita de forma paulatina, baseada em estudos técnicos e de forma a não gerar perda de qualidade nos serviços prestados pelo Estado.

Essa lei foi alvo da Ação Direto de Inconstitucionalidade – ADI número 3.059 ajuizada no Supremo Tribunal Federal – STF, que foi julgada em 09 de abril desse ano, pugnando pela improcedência do pedido de declaração de inconstitucionalidade. Segundo o STF, a preferência por Software Livre não se traduz na obtenção de vantagem sobre determinado produto. A ementa reforça a importância da adoção de software livre para o Poder Público, conforme segue.

> AÇÃO DIRETA DE INCONSTITUCIONALIDADE. DIREITO ADMINISTRATIVO E CONSTITUCIONAL. LEI No 11.871/02, DO ESTADO DO RIO GRANDE DO SUL, QUE INSTITUI, NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA REGIONAL, PREFERÊNCIA ABSTRATA PELA AQUISIÇÃO DE SOFTWARES LIVRES OU SEM RESTRIÇÕES PROPRIETÁRIAS. EXERCÍCIO REGULAR DE COMPETÊNCIA LEGISLATIVA PELO ESTADO-MEMBRO. INEXISTÊNCIA DE USURPAÇÃO DE COMPETÊNCIA LEGIFERANTE RESERVADA À UNIÃO PARA PRODUZIR NORMAS GERAIS EM TEMA DE LICITAÇÃO. LEGISLAÇÃO COMPATÍVEL COM OS PRINCÍPIOS CONSTITUCIONAIS DA SEPARAÇÃO DOS PODERES, DA IMPESSOALIDADE, DA EFICIÊNCIA E DA ECONOMICIDADE. PEDIDO JULGADO IMPROCEDENTE.
> 1. A competência legislativa do Estado-membro para dispor sobre licitações e contratos administrativos respalda a fixação por lei de preferência para a aquisição de softwares livres pela Administração Pública regional, sem que se configure usurpação da competência legislativa da União para fixar normas gerais sobre o tema (CRFB, art. 22, XXVII).
> 2. A matéria atinente às licitações e aos contratos administrativos não foi expressamente incluída no rol submetido à iniciativa legislativa exclusiva do Chefe do Poder Executivo (CRFB, art. 61, §1o, II), sendo, portanto, plenamente suscetível de regramento por lei oriunda de projeto iniciado por qualquer dos membros do Poder Legislativo.
> 3. A Lei no 11.871/2002 do Estado do Rio Grande do Sul não engessou a Administração Pública regional, revelando-se compatível com o princípio da Separação dos Poderes (CRFB, art. 2o), uma vez que a regra de precedência abstrata em favor dos softwares livres pode ser afastada sempre que presentes razões tecnicamente justificadas.
> 4. A Lei no 11.871/2002 do Estado do Rio Grande do Sul não exclui do universo de possíveis contratantes pelo Poder Público nenhum sujeito, sendo certo que todo fabricante de programas de computador poderá participar do certame, independentemente do seu produto, bastando que

> esteja disposto a celebrar licenciamento amplo desejado pela Administração.
> 5. Os postulados constitucionais da eficiência e da economicidade (CRFB, arts. 37, caput e 70, caput) justificam a iniciativa do legislador estadual em estabelecer a preferência em favor de softwares livres a serem adquiridos pela Administração Pública.
> 6. Pedido de declaração de inconstitucionalidade julgado improcedente.

Portanto, visto que o Software Livre permite saber, previamente, o que ocorrerá com os dados e informações pessoais confiados aos dispositivos tecnológicos, é nítida a sua relação com a privacidade, e, no mesmo sentido, com o poder de reafirmá-la frente ao devassamento que este direito fundamental vem sofrendo.

De forma análoga, o ser humano possui a faculdade de permitir que determinada pessoa venha a saber uma informação pessoal oriunda das esferas da privacidade, da vida privada e da intimidade. Essa é a liberdade essencial do ser a que Sartre sentencia ao afirmar que o “[...] homem está condenado a ser livre.” (SARTRE, 2010, p. 33). Isso porque, como dito alhures, ele possui a liberdade de decisão sobre o acesso a determinada informação pessoal. Ocorre que, sob o paradigma da era da informação, o Software Livre devolve essa liberdade para o indivíduo de forma que ele sabia o que determinado programa está fazendo com seus dados, com sua privacidade. Portanto, conclui-se que a filosofia do Software Livre respeita o direito fundamental à privacidade, conforme exige a Constituição da República Federativa do Brasil de 1988.

Agora, faz-se necessário analisar o terceiro item dessa tríade tecnológica de garantia e manutenção do direito fundamental à privacidade, que é o hardware livre. Abordado no subtítulo a seguir.

3.6. HARDWARE LIVRE: A PROTEÇÃO DA PRIVACIDADE DO INDIVÍDUO COMO PROCESSO NATURAL DA CONSTRUÇÃO DO COMPUTADOR

Muito embora o hardware signifique a parte física de um dispositivo eletrônico, é preciso acrescentar a esse entendimento, a noção de que é necessário, ainda que minimamente, um software que saiba como operar esse equipamento. Por isso, é errado entender o hardware como sendo apenas a parte material de uma máquina, por exemplo. Mesmo a peça de um microcomputador pode conter um *chip*[134], onde se localizará um programa que foi desenvolvido para fazer funcionar o mecanismo.

Geralmente, esse programa se localiza num *microchip* chamado de *Electrically-Erasable Programmable Read-Only Memory* – EEPROM, que, em tradução livre quer dizer memória programável eletricamente apagável somente leitura. Isso significa que somente é possível executar o programa, sem qualquer perspectiva de alteração.

Ocorre que, também aqui, esse sistema se mostra como um caixa-preta, ou seja, não se sabe o que ele está, exatamente, executando. Diante disso, com base no Software Livre, nasceu outro movimento, dessa vez, com foco no hardware dos equipamentos, que é o Hardware Livre[135] ou Hardware Aberto. Existem duas organizações que amparam essa iniciativa, é a *Free Software Foundation* – FSF, já mencionada acima, e a *Open Source Hardware Association* – OSHWA[136].

A finalidade do movimento Hardware Livre é ter acesso a dispositivos eletrônicos que não são protegidos por nenhuma patente, além de ter acesso ao código-fonte dos programas que ficam armazenados na EEPROM.

---

134 Também chamado de *microchip*. Consiste num circuito integrado que possui, também, uma região de armazenamento, onde são instalados os programas que executarão o hardware.
135 Em inglês *Open Source Hardware*.
136 O link para acessar a *Open Source Hardware Association* – OSHWA é http://www.oshwa.org/ .

O primeiro ponto consiste na possibilidade de se encontrar desenhos técnicos de dispositivos para a montagem autônoma, ou seja, para a "fabricação" em casa, por exemplo. Apesar de causar estranheza, essa prática é comum no meio dos profissionais de tecnologia da informação. Os desenhos técnicos não exigem a fabricação de todos os componentes, mas tão somente a aquisição das peças e a montagem. Logo, é relativamente simples a proposta.

Além disso, dispositivos que não permitem a edição ou a substituição dos programas que operam o hardware, como a EEPROM, estão sendo substituído por *chips* programáveis. Isso permite que, além de montar o próprio hardware, seja possível inserir ou auditar o programa que fará o hardware funcionar, tendo, assim, a ciência sobre quais operações, exatamente, ele realizará. O dispositivo programável mais comum no mercado é o Arduino[137]. Essa plataforma tem permitido que pessoas comuns desenvolvam os mais variados usos, como, por exemplo: "automações residenciais em geral; aplicações na robótica; aplicações e soluções de [...]" rede; dentre outros (TARGETTRUST, 2014).

Outro grande exemplo é o notebook *open source* conhecido como Projeto Novena (INFO, 2014). Esse computador possui todos os seus esquemas divulgados na Internet[138]. A partir daí, qualquer pessoa pode comprar as peças e montá-lo como achar melhor. Seu diferencial consiste naquilo que se almeja aqui, que é o domínio sobre o que o hardware executará e fará com as informações pessoais de seu usuário.

A *Free Software Foundation* – FSF desenvolveu um selo de garantia que atesta que o software utilizado em determinado hardware possui os mesmos padrões da FSF, ou seja, que observa e respeita as quatro liberdades abordadas no subtópico anterior (FSF, 2012). É a certificação RYF – *Respect Your Freedom*, que em tradução livre quer dizer "respeite sua liberdade". Os fabricantes de equipamentos que desejarem possuir esse selo, devem, conforme já informado, respeitar os padrões da Fundação do Software Livre.

137 O link para acessar o site sobre Arduino é http://www.arduino.cc/ .
138 Para acessar os esquemas do Projeto Novena, acesse: http://www.kosagi.com/w/index.php?title=Novena_PVT_Design_Source

Novamente aqui, a preocupação com a privacidade se localiza na problemática sobre o que o hardware está executando quando acessa as informações pessoais armazenadas nos dispositivos.

Nas denúncias realizadas por Snowden, conforme o subtítulo 2.4.7, a infecção do hardware antes que ele chegue ao seu destino é uma das técnicas executadas para o monitoramento global ou para a espionagem. Entretanto, não se pretende aqui, aniquilar as fábricas e a venda de equipamentos, mas sim, que o usuário possua o poder de auditar o software instalado na máquina adquirida. Somente assim é que se possuirá a certeza sobre o uso que é feito com as informações confiadas e armazenadas nos dispositivos computacionais.

De forma semelhante ao Software Livre, o Hardware Livre também permite que a pessoa saiba o que é feito com as suas informações pessoais. Sendo assim, de igual modo, a liberdade essencial do ser é devolvida para ele permitindo que decida se determinado hardware receberá suas informações pessoais ou não. Dizendo “[...] de outro modo, não existe determinismo, o homem é livre, o homem é liberdade.” (SARTRE, 2010, p. 33). De igual modo, conclui-se que a filosofia do Hardware Livre também respeita o direito fundamental à privacidade, conforme exige a Constituição da República Federativa do Brasil de 1988.

Finalmente, após esclarecer-se como a criptografia, o software livre e o hardware livre são meios efetivos de se reafirmar o direito fundamental à privacidade, é preciso, agora, abordar alguns temas relacionados também a privacidade e ao sigilo das comunicações.

3.7. A ELABORAÇÃO DO DIREITO PELA TECNOLOGIA: O CÓDIGO É A LEI

Uma das possíveis críticas a esse trabalho pode surgir em relação a solução proposta, pois ela não é um problema necessariamente jurídico, mas sim,

pragmático. Trata-se de parar o vazamento de informações pessoais que ocorre atualmente por meio da tecnologia impedindo a sua penetração nas esferas da privacidade, da vida privada e da intimidade, utilizando ela própria para isso. Um fenômeno parecido é investigado pelo ciberfilósofo Lawrence Lessig.

Nas páginas anteriores, pode-se observar que a Internet alavancou o avanço tecnológico interconectando incontáveis máquinas de inúmeras nações pelo mundo. Esse acontecimento fez surgir o chamado ciberespaço, “uma representação física e multidimensional do universo abstrato da “informação”. Um lugar para onde se vai com a mente, catapultada pela tecnologia, enquanto o corpo fica para trás.” (GIBSON, 2003, p. 5-6). Insta advertir que o ciberespaço não se confunde com a Internet, pois aquele se constata em algo mais valorativo do que a rede mundial, onde os internautas acreditam encontrarem-se conectados uns com os outros como se numa comunidade estivessem.

Devido a impressão de que a grande rede era uma terra sem lei, vários autores propuseram teorias sobre como se poderia regular esse espaço abstrato da informação. “Vernor Vinge falou sobre a “aplicação onipresente da lei” possibilitada por “refinados sistemas distribuídos”, nos quais a tecnologia que possibilitará nosso estilo de vida futuro também se alimenta de dados para, e aceita comandos de, o governo.[139]” (LESSIG, 2006, p. 41). Para Tom Maddox, “o poder do governo não viria apenas a partir de fragmentos [...]. Em vez disso, seria reforçado por uma aliança entre o governo e o comércio.[140]” (LESSIG, 2006, p. 51). Ambas as teorias nortearam os entendimentos que tentavam, sem sucesso, compreender como o ciberespaço seria regulado.

Para Lessig (2006), o código é a lei[141]. Para entender essa afirmação, distingui-se a acepção da palavra código enquanto uma construção cultural oriunda da própria história humana, onde as normas jurídicas dos ordenamentos são compiladas em códigos, e, a outra significação que se refere ao código do programa, seja ele o

139 No original: *Vernor Vinge spoke about “ubiquitous law enforcement” made possible by “fine-grained distributed systems,” in which the technology that will enable our future way of life also feeds data to, and accepts commands from, the government.*
140 No original: *The government’s power would not come just from chips, he argued. Instead, it would be reinforced by an alliance between government and commerce.*
141 No original: *code is law.*

código-fonte ou o código complicado para ser executado pelo computador. É aqui que Lessig (2006) ensina que ambas as acepções coincidem por possuírem o mesmo significado. O "ciberespaço demanda um novo entendimento sobre como a regulamentação funciona. Ele nos compele a olhar além do telescópico tradicional do advogado – além das leis, ou mesmo das normas.[142]" (LESSIG, 2006, p. 5)

O que Lessig quer dizer é que mesmo que o ciberespaço não possua nenhuma lei o regulando, ele possui uma força reguladora igual ao da própria lei. Ou seja, softwares e hardwares compõem a arquitetura do ciberespaço, e, ao mesmo tempo, o regulam se tornando normas de conduta dentro dele.

Portanto, a ideia de se utilizar a própria tecnologia como forma de regular o seu comportamento encontra amparo na teoria ensinada por Lawrence Lessig. Isso porque, embora a criptografia, o software livre e o hardware livre não sejam regrados por nenhuma legislação, eles mesmos impõem normas de conduta para que sejam utilizados, possibilitando, assim, a reafirmação do direito fundamental à privacidade.

3.8. SOBERANIA COMPUTACIONAL: O SURGIMENTO DE UM NOVO PARADIGMA PARA O ESTADO CONTEMPORÂNEO

Embora não seja o foco da presente pesquisa, é preciso salientar que a utilização da tríade criptografia, software livre e hardware livre não possui apenas o condão de assegurar o direito fundamental à privacidade do indivíduo, mas também, a Soberania Computacional de um país.

Após a denúncia do Snowden, subtítulo 2.4.7 supra, restou configurado que o programa de monitoramento global dos Estados Unidos da América não foi utilizado somente para buscar evidências de possíveis ataques terroristas, mas sim, para a espionagem de vários países, incluindo o Brasil, e de órgãos internacionais como a

142 No original: *Cyberspace demands a new understanding of how regulation works. It compels us to look beyond the traditional lawyer's scope—beyond laws, or even norms.*

ONU. Esses fatos demonstram que o virtual se tornou a nova fronteira que precisa ser protegida, evitando-se, assim, invasões como as que foram demonstradas.

Diante desse cenário e sob a ótica da segurança da informação, a criptografia serve para assegurar o sigilo, a autenticidade, a integridade e a proveniência das informações governamentais. Já o software livre garantirá a certeza do tipo de utilização que os dados estatais sofrerão. O hardware livre, por sua vez, mostra-se como mais uma forma de proteção e como uma oportunidade econômica, pois em vez de se adquirir e utilizar máquinas de fabricantes de outros países, consideradas verdadeiras caixas-pretas, o Brasil pode iniciar investimentos nesse setor construindo uma economia que abastecerá o Poder Público e a própria nação de equipamentos confiáveis que não permitam, tão facilmente, atentados a privacidade a aos segredos de Estado. Quando se fala em Soberania Computacional, quer dizer a não dependência tecnológica de empresas ou países estrangeiros, de forma que, o Brasil seja autossuficiente na produção e utilização de seus recursos tecnológicos. Portanto, a partir daí, é necessário que o Brasil inicie um plano de ação que objetive assegurar a Soberania Computacional do país.

4. CONSIDERAÇÕES FINAIS

No momento em que se assume a realização de um mestrado em direito, convergindo os conhecimentos das graduações em Ciência da Computação e em Direito, o resultado não poderia ter sido outro senão um somatório de sentimentos e sensações.

O caminho percorrido para se chegar ao fim desta dissertação foi desafiador, doloroso, instigante e libertador. O desafio se encontrou em problematizar corretamente a relação entre o direito fundamental à privacidade e a tecnologia, pois, em nenhum momento o objetivo foi trazer ao bojo do presente trabalho um ponto sem a relevância necessária que justificasse a pesquisa. Já a dor se subdividiu em duas vertentes, a da dor física, inerente a horas de detidas leituras e buscas ininterruptas sobre o tema abordado, e, a outra dor que está ligada a dura tomada de decisão para se delimitar o ponto central do estudo, pois muitos foram os caminhos que poderiam ter sido seguidos, mas, talvez, sem a devida motivação.

A força eletromotriz que instigou todo o esforço empregado nas atividades nasceu do conhecimento sobre a arquitetura e o funcionamento da tecnologia, sendo possível observar as constantes utilizações que ferem o direito fundamental à privacidade feitas por empresas e governos com as mais diversas finalidades. Por esse motivo, percebeu-se que não era o caso de se buscar a criação de novas leis ou garantias constitucionais, mas sim de se propor uma solução pragmática, imediata. Foi pensando assim que formulou-se a hipótese de que a própria tecnologia pode ser utilizada para reafirmar o direito fundamental à privacidade.

Contudo, dentro do universo tecnológico era preciso selecionar qual ou quais recursos seriam capazes de assegurar o controle e o sigilo sobre as informações pessoais. Outro grande desafio foi analisar a própria utilização dos mecanismos disponíveis pelos usuários para que fosse possível pensar em algo mais próximo de sua efetiva implementação. Então, após inúmeros estudos, e aplicando a máxima que afirma que a segurança da informação não consiste numa medida, mas num conjunto de medidas, foi elaborada a pergunta que norteou toda a pesquisa, que

consiste em saber se: com o advento da era da informação, a contra-utilização de tecnologias como a criptografia, o software livre e o hardware livre servem como elementos garantidores para se reafirmar o direito fundamental à privacidade?

A justificativa para essa pergunta encontrou amparo no discurso que alguns governos vêm adotando no sentido de criar mecanismos para se burlar a utilização da criptografia, principalmente, em aparelhos como o *smartphone*, tópico já tratado durante o trabalho.

Mas antes de se entrar na seara da tecnologia, foi preciso identificar o surgimento da esfera da privacidade dentro da própria convivência humana, que, segundo os estudos da Hannah Arendt, é uma das esferas mais importantes para o ser humano. Além disso, a referida autora conclui que sem o domínio privado é impossível a existência do próprio domínio público. Logo, era preciso encontrar um meio de permitir a mantença da privacidade. Além disso, foi proposta a criação de mais duas esferas, a da vida privada e a da intimidade.

Essa tripartição se mostrou necessária, pois ficou claro que existe uma segregação para as informações pessoais, onde algumas, além de poderem vir ao domínio público, são oponíveis a terceiros, como os dados da privacidade. Já a vida privada, deriva das relações interpessoais. E, a intimidade, foi a esfera que se mostrou mais delicada para o ser, pois é onde ele deseja permanecer só para que ninguém mais venha a saber o que ele nela mantém. Diante disso, uma análise sobre a liberdade também foi feita para que ficasse evidente qual é a liberdade necessária para o domínio privado.

De forma a demonstrar a preocupação que foi tida com a privacidade, especialmente, com o sigilo dos dados, as principais leis internacionais e nacionais foram abordadas. A partir desse ponto, ficou claro que o Estado Democrático de Direito possui a previsão legal assegura a privacidade.

Foi então, que no segundo capítulo a forma como a tecnologia desrespeita o direito fundamental à privacidade foi evidenciada, demonstrando os riscos em se utilizar

dispositivos informáticos e programas que não deixam claro o que eles fazem quando são executados.

Entretanto, para se compreender corretamente como essa intrusão ocorre, o funcionamento dos principais recursos tecnológicos foram tratados, inclusive, o próprio funcionamento da Internet. Além disso, também foi demonstrado como o ser humano confia e deposita suas informações em seus dispositivos tecnológicos.

Frise-se que esse conhecimento se faz necessário à qualquer operador do direito, pois, diferente de qualquer outra área do saber, é preciso que advogados, magistrados, legisladores, dentre outros, pensem tecnologia para que desempenhem suas funções de forma eficaz.

Mas, principalmente, a denúncia realizada por Snowden se mostrou incomensurável, pois comprovou o que foi afirmado em vários pontos desta dissertação, que a tecnologia pode ser utilizada para se acessar o espaço mais íntimo do ser humano. É preciso esclarecer a identificação que se teve com a preocupação que Snowden demonstrou ao sacrificar todo o seu futuro no auge de seus vinte e noves anos, ou seja, que mesmo sabendo de toda a intrusão que os recursos tecnológicos vêm desempenhando, ninguém desse a mínima para isso e continuasse a não se preocupar com a privacidade a partir da era da informação (GREENWALD, 2014).

Além da ausência de privacidade em si, outros riscos foram identificados, como a anulação da essência do ser humano por ser monitorado a todo momento. Outro ponto importante é a possibilidade do surgimento de um Estado de Exceção Permanente, onde a privacidade seria exceção e não a regra. De igual modo, a coleta indiscriminada de dados pessoais feita pelo mercado também foi analisada concluindo-se sobre o risco da exclusão de pessoas que não sejam classificadas com efetivas consumidoras de determinado bem ou serviço, por exemplo.

Com isso, pensando em devolver ao ser humano a proteção sobre os dados e as informações pessoais, e o poder de decisão sobre quem pode acessá-la, a proposta da criptografia e das tecnologias livres foi apresentada.

Dentro da criptografia, após explanar brevemente o seu funcionamento e suas principais técnicas, sendo elas a criptografia simétrica e assimétrica, ficou evidenciado como ela pode ser utilizada para se proteger não só o armazenamento das informações pessoais em si, mas também, a sua transmissão. Esse tipo de desempenho possibilita criar um espaço virtual para se estar só.

Esse foi o primeiro elemento da tríade recomendada neste trabalho. Tudo porque, de nada adiantaria confiar na criptografia se o programa que a executasse estivesse maculado por algum comportamento malicioso inserido propositalmente para que alguém, então, fosse capaz de acessar os dados que estivessem criptografados, sem que, para isso, possuía a chave secreta. De igual forma, existem aplicativos que agem ativamente para a obtenção de informações pessoais e são utilizados em larga escala. Portanto, é preciso que um software seja livre para que se possa confiar em sua utilização.

Pensamento nisso é que a utilização do software livre foi adotada, pois através dele se tem a certeza sobre o que determinado aplicativo está executado dentro do computador ou o que ele está fazendo com as informações pessoais dos usuários. Esse entendimento se convalida pelo acesso ao código-fonte que permite entender todo o funcionamento do programa utilizado, além de se garantir, pela possibilidade de reutilização do mesmo código, de que são exatamente aquelas ações que são trabalhadas. O software livre corresponde ao segundo elemento da tríade em comento.

Contudo, para se convalidar que a segurança da informação se realiza através de um conjunto de medidas, ainda era necessário garantir que o hardware onde são executados os softwares de criptografia e demais programas era seguro e não possuía nenhum risco para o seu usuário. De igual modo como se verificou com o software livre, também o hardware livre requer que a pequena parte de software que o faz funcionar também proveja o acesso ao seu código-fonte para que de igual modo se saiba como determinado equipamento se comporta quando a fonte de sua execução são os dados pessoais do usuário.

Entretanto, salienta-se que a presente dissertação não possui o condão de esgotar essa temática, mas sim, demonstrar que existem possibilidades para se contra-utilizar a tecnologia com a finalidade de se assegurar o devido sigilo às informações pessoais.

Romper com o paradigma de se aguardar uma proteção legal para conter o devassamento feito pela tecnologia faz parte da democracia. É imprescindível verificar que todas as medidas adotadas nas páginas precedentes convergem para um movimento contra-hegemônico por se caracterizar como uma iniciativa popular. Faz-se necessário questionar sobre a ciência que a pessoa deve possuir ao fazer uso de determinado dispositivo informático. Somente com o conhecimento das ações tecnológicas é que se poderá garantir que direitos fundamentais, como a privacidade, não serão desrespeitados.

> “A transparência total é um pesadelo. Todo mundo tem algo a esconder.”
>
> (Glenn Greenwald, 2014, p. 194)

5. REFERÊNCIAS

ABSOLUTA. **História e Aplicações da Criptografia.** 1999. Disponível em: <http://www.absoluta.org/cripty/cripty_h.htm>. Acesso em: 01 mai. 2015.

ADD-ONS. **Lightbeam for Firefox.** 2015. Disponível em: <https://addons.mozilla.org/En-uS/firefox/addon/lightbeam/>. Acesso em: 22 fev. 2015.

AGAMBEN, G. **Estado de Exceção.** 2 ed. São Paulo: Boitempo, 2004.

ALEXY, R. Colisão de direitos fundamentais e realização de direitos fundamentais no Estado de Direito Democrático. **Revista de Direito Administrativo.** Rio de Janeiro: Renovar, n. 217, jul-set 1999.

_____. **Teoria dos Direitos Fundamentais.** São Paulo: Malheiros. 2008.

ALMEIDA, L. A. A. **O sistema de cotas eleitorais de gênero e o princípio da igualdade:** uma análise da busca brasileira pela representação política feminina. 186 fls. Dissertação. Faculdade de Direito de Vitória. Vitória, 2015.

ANONYMOUSBR4SIL.NET. **Deep Web: Entenda.** 2013. Disponível em: <http://www.anonymousbr4sil.net/2013/04/deep-web-entenda-e-acesse.html>. Acesso em: 18 jul. 2015.

ARENDT, H. **A condição humana.** 12 ed. Rio de Janeiro: Forense Universitária, 2014.

ASSANGE, J., APPELBAUM, J., MÜLLER-MAGUHN, A., *et al*. **Cypherpunks:** liberdade e o futuro da internet. São Paulo: Boitempo, 2013. 166 p.

ASSEMBLÉIA LEGISLATIVA DO ESTADO DO ESPÍRITO SANTO. **Constituição do Estado do Espírito Santo.** Disponível em: <http://www.dhnet.org.br/dados /lex/a_pdf/constituicao_es.pdf>. Acesso em: 10 mar. 2014.

BASTOS, C., MARTINS, I. G. **Comentários à Constituição do Brasil.** São Paulo: Saraiva, 1989.

BAUMAN, Z. **Vigilância líquida.** Rio de Janeiro: Zahar, 2013.

BENHTAM, J. **O Panóptico.** Belo Horizonte: Autêntica Editora, 2008.

BONAVIDES, P. **Curso de direito constitucional.** 13 ed. rev. e atual. São Paulo: Malheiros, 2003.

BORDIEU, P., PASSERON, J. **La reproduccíon:** elementos para una teoría del sistema de enseñanza. 2 ed. Editorial Laia: México D.F. 1996.

CANALTECH. **Facebook manipulou feed de 600 mil usuários para fazer experimento social. 2014.** Disponível em: <http://canaltech.com.br/noticia/facebook/Facebook-manipulou-feed-de-600-mil-usuarios-para-fazer-experimento-social/>. Acesso em: 25 fev. 2015.

CIDH. **Declaração americana dos direitos e deveres do homem.** 1948. Disponível em: <http://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm>. Acesso em 15 jan. 2015.

CNET. **Google balances privacy, reach.** 2005. Disponível em: <http://news.cnet.com/Google-balances-privacy,-reach/2100-1032_3-5787483.html>. Acesso 28 abr. 2015.

COULANGES, F. de. **A Cidade Antiga.** São Paulo: Martin Claret, 2004.

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.** 1981. Disponível em: <http://conventions.coe.int/treaty/en/treaties/html/108.htm>. Acesso em 15 jan. 2015.

CUNHA, R. A. V. **Segurança jurídica e crise no direito.** Belo Horizonte: Arraes Editores, 2011.

DECHILE. **Etimología de CALCULAR.** 2014. Disponível em: <http://etimologias.dechile.net/?calcular>. Acesso em: 27 fev. 2015.

DELEUZE, G. **Postscript on the societies of control.** vol. 59. Massachusetts: MIT Press, 1992.

DESCARTES, R. **Discurso do método.** 2 ed. São Paulo: Martins Fontes, 2001.

DEVIANTART. **The Idiot Savants' Guide to Rubberhose.** 2013. Disponível em: <http://fc04.deviantart.net/fs71/f/2013/121/3/8/rubber_hose_cryptographically_deniable_file_system_by_l33tn3rdz-d63qcd2.pdf>. Acesso em: 03 mai. 2015.

DHNET. **Declaração Universal do Direitos Humanos.** 1948. Disponível em: <http://www.dhnet.org.br/direitos/deconu/textos/integra.htm>. Acesso em: 15 jan. 2015.

DROPBOX. **Política de Privacidade.** 2015. Disponível em: <https://www.dropbox.com/privacy#privacy>. Acesso em: 25 fev. 2015.

DWORKIN, R. **Levando os direitos a sério.** São Paulo: Martins Fontes, 2002.

EDWARDS, A. **Aton Edwards.** 2014. Disponível em: <https://www.youtube.com/user/IADO4u/videos>. Acesso em: 25 fev. 2015.

ESTADÃO. **Um ano de Primavera Árabe, a primavera inacabada.** 2015. Disponível em: <http://topicos.estadao.com.br/primavera-arabe>. Acesso em 21 abr. 2015.

_____. **PF prende 51 em operação contra pedofilia na Deep Web.** 2014. Disponível em: <http://www.estadao.com.br/noticias/geral,pf-prende-51-em-operacao-contra-pedofilia-na-deep-web,1577365>. Acesso em: 03 mai. 2015.

EXAME. **Obama diz ser contrário ao uso de criptografia em smartphone.** 2015. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/obama-diz-ser-contrario-ao-uso-de-criptografia-em-smartphone>. Acesso em: 25 jan. 2015.

FABRIZ, D. C. **Bioética e direitos fundamentais.** Belo Horizonte: Mandamentos, 2003.

FOUCAULT, Michel. Sobre a história da sexualidade. In: _____. **Microfísica do Poder.** Organização e tradução de Roberto Machado. Rio de Janeiro: Edições Graal, 2001.

_____. **Vigiar e punir**: nascimento da prisão. 34 ed. Petrópolis: Vozes, 2007.

FSF. **A bit about free hardware.** 2012. Disponível em: <https://www.fsf.org/bulletin/2012/fall/a-bit-about-free-hardware>. Acesso em: 03 mai. 2015.

FURTADO, E. T., MENDES, A. S. V. Os direitos humanos de 5ª geração enquanto direito à paz e seus reflexos no mundo do trabalho - inércias, avanços e retrocessos na Constituição Federal e na legislação. In: XVII CONGRESSO NACIONAL DO CONPEDI, 2008, Brasília, Distrito Federal. **Anais do XVII Congresso Nacional do CONPEDI.** Brasília: CONPEDI, 2008, p. 6970-6989.

G1. **Nem FBI consegue decifrar arquivos de Daniel Dantas, diz jornal.** 2010. Disponível em: <http://g1.globo.com/politica/noticia/2010/06/nem-fbi-consegue-decifrar-arquivos-de-daniel-dantas-diz-jornal.html>. Acesso em: 02 mai. 2015.

GDDC. **Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais.** 1950. Disponível em: <http://direitoshumanos.gddc.pt/3_1/IIIPAG3_1_13.htm>. Acesso em 15 jan. 2015.

GGN. **Os dados indecifráveis e o software livre.** 2012. Disponível em: <http://jornalggn.com.br/blog/luisnassif/os-dados-indecifraveis-e-o-software-livre>. Acesso em: 02 mai. 2015.

GIBSON, W. **Neuromancer.** São Paulo: Aleph, 2003.

GNU. **O que é o software livre?**. 2014. Disponível em: <https://gnu.org/philosophy/free-sw.html>. Acesso em: 03 mai. 2015.

_____. **Visão Geral do Sistema GNU.** 2014. Disponível em: <https://gnu.org/gnu/gnu-history.html>. Acesso em: 03 mai. 2015.

GOOGLE. **Política de Privacidade.** 2015. Disponível em: <http://www.google.com/intl/pt-BR/policies/privacy/#access>. Acesso em: 25 fev. 2015.

GREENWALD, G. **Sem lugar para se esconder.** Rio de Janeiro: Sextante, 2014.

HDSG. **Hessisches Datenschutzgesetz.** 1999. Disponível em: <https://www.datenschutz.hessen.de/hdsg99.htm>. Acesso em 15 jan. 2015.

HEIDEGGER, M. **Ser e tempo.** 8 ed. Petrópolis: Vozes, 2013.

HOBBES, T. **Leviatã.** 2 ed. São Paulo: Martin Claret, 2012.

IBM. **Prevendo o futuro, Parte 1: O Que é a Análise Preditiva?** 2012. Disponível em: <http://www.ibm.com/developerworks/br/industry/library/ba-predictive-analytics1/>. Acesso em: 26 fev. 2015.

IETF. **About the IETF.** 2015. Disponível em: <https://www.ietf.org/about/>. Acesso em: 25 fev. 2015.

INFO. **Novena: um notebook open source para hackers.** 2014. Disponível em: <http://info.abril.com.br/noticias/blogs/gadgets/notebooks/novena-um-notebook-open-source-para-hackers/>. Acesso em: 18 jul. 2015.

_____. **"Internet como conhecemos vai desaparecer", diz Eric Schmidt.** 2015. Disponível em: <http://info.abril.com.br/noticias/it-solutions/2015/01/a-internet-como-conhecemos-vai-desaparecer-diz-eric-schmidt.shtml>. Acesso em: 26 fev. 2015.

INTERNET LEGAL. **Ministério da Justiça multa Oi por monitorar navegação de consumidores na internet.** 2014. Disponível em: <http://www.internetlegal.com.br/2014/07/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet/>. Acesso em: 24 fev. 2015.

IPV6.BR. **Quantos endereços Internet existem no IPv4? O que muda com o IPv6?** 2012. Disponível em: <http://ipv6.br/faq/#Quantos_endere_os_Internet_exist>. Acesso em: 20 de jun. 2013.

KROHLING, A. **Dialética e direitos humanos:** múltiplo dialético – da Grécia à contemporaneidade. Curitiba: Juruá, 2014.

KROHLING, A., MARTINELLI, G. G. **A violação de normas pátrias em nome dos direitos humanos: uma leitura do caso Edward Snowden.** 2014. Disponível em: <https://sites.google.com/a/criticadodireito.com.br/revista-critica-do-direito/todas-as-edicoes/numero-4-volume-63/aloisio>. Acesso em 01 abr. 2015.

KROHLING, A., TESSAROLO, E. M., PERTEL, A. M. dos S.. A utopia da cidadania ecológica: desafios à consolidação da ética da responsabilidade na sociedade de risco. In: revista **Veredas do Direito: Direito Ambiental e Desenvolvimento Sustentável.** Escola Superior Dom Helder Câmara, Belo Horizonte, v, 10, n. 19, p. 1-21, 2013.

LESSIG, L. **Code version 2.0.** New York: Basic Books. 2006. Ebook. Disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em 01 jul. 2015.

LYON, D., ZUREIK, E. **Computers, surveillance, and privacy.** Minnesota: University of Minnesota, 1996.

MCLUHAN, M. **Understanding Media:** the extensions of man. 2009. Disponível em: <https://cultphoto.files.wordpress.com/2009/09/marshall-mcluhan-undertanding-media-the-extensions-of-man.pdf>. Acesso em 15 fev. 2015.

MEIOBIT. **LG admite: nossas Smart TVs estão realmente coletando dados.** 2013. Disponível em: <http://meiobit.com/272095/lg-smart-tv-coleta-dados-empresa-admite/>. Acesso em: 24 fev. 2015.

MIT. **The Global Information Technology Report 2008-2009. 2009.** Disponível em: <http://hd.media.mit.edu/wef_globalit.pdf>. Acesso em: 01 mai. 2015.

MONTESQUIEU, C. S. **O Espírito das Leis.** São Paulo: Martins Fontes, 1993.

MORENO, E. D., PEREIRA, F. D., CHIARAMONTE, R. B. **Criptografia em software e hardware.** Rio de Janeiro: Novatec, 2005.

NEPÔSTS. **As revoluções cognitivas e as mudanças nas topologias das redes.** 2011. Disponível em: <http://nepo.com.br/2011/08/16/ultimo-nepost-as-revolucoes-cognitivas-e-as-mudancas-nas-topologias-das-redes/>. Acesso em: 03 de Fev. 2014.

OAS. **Pacto internacional dos direitos civis e políticos.** 1966. Disponível em: <http://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20Direitos%20Civis%20e%20Pol%C3%ADticos.pdf>. Acesso em 15 jan. 2015.

OBSERVATÓRIO DA IMPRENSA. **Site divulga ataque americano a fotógrafo da Reuters.** 2010. Disponível em: <http://observatoriodaimprensa.com.br/monitor-da-

imprensa/site_divulga_ataque_americano_a_fotografo_da_reuters/>. Acesso em: 03 mai. 2015.

OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em 15 jan. 2015.

O GLOBO. **ONU aprova resolução proposta por Brasil e Alemanha sobre privacidade on-line.** 2014. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/onu-aprova-resolucao-proposta-por-brasil-alemanha-sobre-privacidade-on-line-14678862>. Acesso em 21 abr. 2015.

OLIVEIRA, D. P. R. de. **Sistema de informações gerenciais.** 8 ed. São Paulo: Atlas, 2002.

ORWELL, G. **1984.** São Paulo: Companhia das Letras, 2009.

OSHWA. **Open source hardware association.** 2014. Disponível em: <http://www.oshwa.org/>. Acesso em: 03 mai. 2015.

PACE. **Declaration on mass communication media and Human Rights.** 1970. Disponível em: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en>. Acesso em 15 jan. 2015.

PARISER, E. **O filtro invisível:** o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PAULA, R. F. **Liberdade e discriminação no domínio privado:** reflexões sobre as escolhas de tratamento discriminatórias nas relações privadas. 160 fls. Dissertação. Faculdade de Direito de Vitória. Vitória, 2010.

PEDRA, A. S. **A constituição viva:** poder constituinte permanente e cláusulas pétreas na democracia participativa. Rio de Janeiro: Lumen Juris, 2012.

PGE. **Convenção Americana de Direitos Humanos.** 1969. Disponível em: <http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm>. Acesso em 15 jan. 2015.

PENSANDO O DIREITO. **Proteção de dados pessoais.** 2015. Disponível em: <http://participacao.mj.gov.br/dadospessoais/>. Acesso em: 26 abr. 2015.

PORTAL FÓRUM. **Ter acesso à internet é direito humano básico de acordo com a ONU.** 2011. Disponível em: <http://www.revistaforum.com.br/mariafro/2011/06/13/ter-acesso-a-internet-e-direito-humano-basico-de-acordo-com-a-onu/>. Acesso em 21 abr. 2015.

PORTAL TIC. **Deep Web:** O que é isso?. 2015. Disponível em: <http://portaltic.com/84-alcyon-junior/338-deep-web-o-que-e-isso.html>. Acesso em: 03 mai de 2015.

PUBLICO. **França aprova lei de segurança comparada ao Patriot Act americano.** 2015. Disponível em: <http://www.publico.pt/mundo/noticia/franca-da-passo-importante-para-ter-o-seu-patriot-act-1694611>. Acesso em: 05 mai. 2015.

RADFAHRER, L. **O Invisível - "The hole is underer".** 2013. Disponível em: <http://youtu.be/168jsIqMjs0>. Acesso em: 15 fev. 2015.

RAOPO!. **Computadores descobrem antes do pai a gravidez da filha. 2013.** Disponível em: <http://raopo.com.br/2013/09/computadores-descobrem-que-a-filha-esta-gravida-antes-do-pai/>. Acesso em: 26 fev. 2015.

RÜTHERS, B. **Carl Schmitt en el tecer reich.** Bogotá: Fundacion FES, 2004.

SANDEN, A. F. M. de S. **A proteção de dados pessoais do empregado no direito brasileiro:** um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado. São Paulo: LTr, 2014.

SANTOS, R. **Dado, informação e conhecimento.** 2009. Disponível em: <http://pt.slideshare.net/robssantoss/dados-informao-e-conhecimento>. Acesso em: 13 jan. 2015.

SARTRE, J. P. **O existencialismo é um humanismo.** Petrópolis: Vozes, 2010.

SILVA NETO, A. M. **Privacidade na internet:** um enfoque jurídico. Edipro: São Paulo, 2001.

SOARES, L. F. G., LEMOS, G., COLCHER, S. **Redes de Computadores:** das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Elsevier, 1995.

STALLINGS, W. **Criptografia e segurança de redes.** 4 ed. São Paulo: Pearson Prentice Hall, 2008.

STF. **Prazo de escutas telefônicas é matéria com repercussão geral reconhecida.** 2013. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=242810>. Acesso em: 20 abr. 2015.

_____. **Repercussão Geral.** 2015. Disponível em: <http://www.stf.jus.br/portal/glossario/verVerbete.asp?letra=R&id=451>. Acesso 20 abr. 2015.

SUDRÉ FILHO, G. N., MARTINELLI, G. G. O princípio da natureza participativa no Marco Civil da Internet: uma abordagem sobra a sua importância. In: LEITE, G. S., LEMOS, R. (Org.). **Marco Civil da Internet.** São Paulo: Atlas, 2014, p. 202-215.

_____. Processo Judicial Eletrônico: aspectos tecnológicos e da segurança da informação. In: COÊLHO, M. V. F., ALLEMAND, L. C. (Org.). **Processo Judicial Eletrônico.** Brasília: OAB, 2014, p. 297-306.

SUDRÉ FILHO. **Fique por dentro das notícias.** 2010. Disponível em: <http://gilberto.sudre.com.br/fique-por-dentro-das-noticias/>. Acesso em: 26 fev. 2015.

SYMANTEC. **Information on Back Orifice and NetBus.** 2007. Disponível em: <http://www.symantec.com/avcenter/warn/backorifice.html>. Acesso em: 18 jul. 2015.

TANENBAUM, A. S. **Redes de computadores.** Rio de Janeiro: Elsevier, 2003.

_____. **Organização estruturada de computadores.** São Paulo: Pearson Prentice Hall, 2007.

TARGETTRUST. **Arduino - Potencialidades de desenvolvimento utilizando a plataforma. 2014.** Disponível em: <http://targettrust.com.br/evento/workshop-arduino-potencialidades-de-desenvolvimento-utilizando-a-plataforma>. Acesso em: 20 abr. 2015.

TARINGA. **El Panoptico, tambien llamado el Ojo Del Poder.** 2012. Disponível em: <http://www.taringa.net/posts/ciencia-educacion/15075192/El-Panoptico-tambien-llamado-el-Ojo-Del-Poder.html>. Acesso em: 20 abr. 2015.

TAURION, C. **Big Data.** Rio de Janeiro: Brasport, 2013.

TC. **Google's Cerf Says "Privacy May Be An Anomaly".** Historically, He's Right. 2013. Disponível em: <http://techcrunch.com/2013/11/20/googles-cerf-says-privacy-may-be-an-anomaly-historically-hes-right/>. Acesso em: 16 jul. 2014.

TECHTERMS.COM. **Malware.** 2015. Disponível em: <http://techterms.com/definition/malware>. Acesso em: 26 fev. 2015.

_____. **Worm.** 2015. Disponível em: <http://techterms.com/definition/worm>. Acesso em: 18 jul. 2015.

TECHTUDO. **O que é um Trojan ou Cavalo de Troia?** 2014. Disponível em <http://www.techtudo.com.br/noticias/noticia/2014/06/o-que-e-um-trojan-ou-cavalo-de-troia.html>. Acesso em: 18 jul. 2015.

TECMUNDO. **iOS, Android e Windows Phone: números dos gigantes comparados [infográfico].** 2013. Disponível em: <http://www.tecmundo.com.br/sistema-operacional/60596-ios-android-windows-phone-numeros-gigantes-comparados-infografico.htm>. Acesso em: 24 fev. 2015.

TECNOBLOG. **ENIAC, primeiro computador do mundo, completa 65 anos.** 2011. Disponível em : <https://tecnoblog.net/56910/eniac-primeiro-computador-do-mundo-completa-65-anos/>. Acesso em: 03 fev. 2015.

_____. **TrueCrypt aparentemente morreu e de maneira bastante misteriosa.** 2014. Disponível em: <https://tecnoblog.net/157446/truecrypt-descontinuado-inseguro/>. Acesso em: 02 mai. 2015.

TED.COM. **Your phone company is watching.** 2012. Disponível em: <https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching>. Acesso em: 24 fev. 2015.

_____. **Why privacy matters.** 2014. Disponível em: <http://www.ted.com/talks/glenn_greenwald_why_privacy_matters>. Acesso em: 30 mar. 2015.

TEIXEIRA, B. C. **Cidadania em Rede:** A Inteligência coletiva enquanto potência recriadora da democracia participativa. 129 fls. Dissertação. Faculdade de Direito de Vitória. Vitória, 2012.

Terms and Conditions May Apply. Direção: Cullen Hoback. Intérpretes: Max Schrems; Moby; Mark Zuckerberg e outros. Hyrax Films; 2013. 1 filme (79min).

TOR. **Tor: Overview.** 2015. Disponível em: <https://www.torproject.org/about/overview.html.en>. Acesso em: 18 jul. 2015.

_____. **Tor: Hidden Service Protocol.** 2015. Disponível em: <https://www.torproject.org/docs/hidden-services.html.en>. Acesso em: 18 jul. 2015.

TUDOCELULAR.COM. **O Android é um sistema aberto, mas nem tanto.** 2011. Disponível em: <http://www.tudocelular.com/software/noticias/n24562/android-aberto-fechado.html>. Acesso em: 03 mai. 2015.

UFF. **Histórico da Computação.** 2012. Disponível em: <www.professores.uff.br/asilva/fac/historico.pptx>. Acesso em: 03 fev. 2015.

UFPA. **História do computador e da internet.** 2015. Disponível em: <http://www.ufpa.br/dicas/net1/int-h190.htm>. Acesso em: 10 dez. 2014.

UNIVERSITY OF ILLINOIS. **The right to privacy.** 1890. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>. Acesso em 01 mai. 2015.

UNIX. **History and Timeline.** 2012. Disponível em: <http://www.unix.org/what_is_unix/history_timeline.html>. Acesso em: 03 mai. 2015.

UOL. **O que são vírus de computador?** 2015. Disponível em: <http://seguranca.uol.com.br/antivirus/duvidas/o-que-sao-virus-de-computador.html#rmcl>. Acesso em: 07 mai. 2015.

VIEIRA, O. V. **Direitos Fundamentais:** uma leitura da jurisprudência do STF. São Paulo: Malheiros, 2006.

VIOLANTE, C. A. M. S. M. **Lei de introdução ao código civil.** Campinas: Copola, 2000.

WEBOPEDIA. **Smartphone.** 2015. Disponível em: <http://www.webopedia.com/TERM/S/smartphone.html>. Acesso em: 24 fev. 2015.

WHATIS.COM. **Plug-in.** 2015. Disponível em: <http://whatis.techtarget.com/definition/plug-in>. Acesso em: 22 fev. 2015.

WIKILEAKS. **About:** what is Wikileaks?. 2011. Disponível em: <https://wikileaks.org/About.html>. Acesso em: 03 mai. 2015.

Veja, São Paulo, ed. 2411, ano 48, n 5, p. 86-90. 2015.

ZAFFARONI, E. R. **O inimigo do direito penal.** 2 ed. Rio de Janeiro: Revan, 2007.

ZOOM. **O que é Smart TV?** 2014. Disponível em: <http://www.zoom.com.br/tv/deumzoom/o-que-e-smart-tv>. Acesso em: 25 fev. 2015.