João Pedro Seefeldt Pessoa

O EFEITO ORWELL NA SOCIEDADE EM REDE

Cibersegurança, regime global de vigilância social e direito à privacidade no século XXI

Fi

Na sociedade em rede, as tecnologias de informação e comunicação criaram novos desafios relacionados à livre circulação de dados, o que torna necessário repensar o direito à privacidade. Esta obra estuda a vigilância e o direito à privacidade na sociedade em rede, problematizando em que medida o regime global de vigilância social de dados pessoais pode afetar o direito à privacidade em tempo de cibersegurança no século XXI. O livro é dividido em dois blocos, sendo o primeiro grande capítulo sobre a vigilância perpetrada pelas redes de poder e o segundo grande capítulo sobre a alteração de paradigma do direito à privacidade para um regime coletivo de proteção. Dessa forma, a obra reflete como o direito à privacidade passou por transformações desde uma concepção clássica, possuindo novas dimensões na sociedade em rede, como o direito à autodeterminação informativa e à proteção de dados pessoais, de modo que, em relação à sociedade de vigilância, o direito à privacidade pode ser usado como contravigilância, exigindo uma atuação transparente, controlada e vigiada dos responsáveis e encarregados do tratamento de dados pessoais.

9 786559 170739

editora fi.org

O efeito Orwell na sociedade em rede

O efeito Orwell na sociedade em rede

Cibersegurança, regime global de vigilância social e direito à privacidade no século XXI

João Pedro Seefeldt Pessoa

Diagramação: Marcelo A. S. Alves
Capa: Lucas Margoni

O padrão ortográfico e o sistema de citações e referências bibliográficas são prerrogativas de cada autor. Da mesma forma, o conteúdo de cada capítulo é de inteira e exclusiva responsabilidade de seu respectivo autor.

Dados Internacionais de Catalogação na Publicação (CIP)

PESSOA, João Pedro Seefeldt

O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI [recurso eletrônico] / João Pedro Seefeldt Pessoa -- Porto Alegre, RS: Editora Fi, 2020.

214 p.

ISBN - 978-65-5917-073-9
DOI - 10.22350/9786559170739

Disponível em: http://www.editorafi.org

1. Cibersegurança; 2. Privacidade; 3. Orwell; 4. Sociedade em rede; 5. Estado; I. Título.

CDD: 340

Índices para catálogo sistemático:
1. Direito 340

Aos que aceitaram os termos e condições

You have zero privacy anyway. Get over it.

Scoot McNealy, ex CEO de Sun Microsystems.
SPRENGER, Polly. *Sun of privacy:* 'get over it'. [Wired, 26/01/1999] Disponível em: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/. Acesso em: 05 jul. 2019.

Sumário

Parte II

El efecto Orwell en la sociedad en red: ciberseguridad, régimen global de vigilancia social y derecho a la privacidad en el siglo XXI

Prefácio

Cristiane Penning Pauli de Menezes [1]

A sociedade em rede garantiu uma nova roupagem para o velho Direito. Conceitos já estáveis foram revisitados em razão da explosão tecnológica do século XXI.

O direito à privacidade, assim, renasceu.

Os nossos dados pessoais, em escalas cada vez mais agressivas, são exigidos para que possamos fazer parte de comunidades digitais e, até mesmo, reais, sem as quais nos tornamos *outsiders*. Assim, ora somos expostos e nossos direitos violados contra nossa vontade, ora temos nossos dados desnudados por uma autoexposição, ora nossas informações pessoais são monitoradas e compartilhadas sem que sequer saibamos.

O olhar de João Pedro Seefeldt Pessoa é atento a questões sensíveis sobre a privacidade, partindo da análise de um regime global de vigilância social, que chama de onipresente, uma vez que de forma institucional e silenciosa permite que sejamos observados o tempo todo, em condições que nem George Orwell imaginou quando escreveu a obra "1984", história esta que, oportunamente, serve de inspiração para o presente estudo.

Ao compreendermos que essa vigilância é institucionalizada, devemos concluir que em todas as esferas de poder - escolar, familiar, laboral, prisional etc. -, somos vigiados, de modo que podemos ser manipulados, controlados e até mesmo punidos. Na virada tecnológica da sociedade em

[1] Doutora em Processos e Manifestações Culturais pela Universidade Feevale (FEEVALE). Mestre em Direito pela Universidade Federal de Santa Maria (UFSM). Especialista em Direito Empresarial pela Faculdade de Direito de Santa Maria (FADISMA). Bacharel em Direito pela Faculdade de Direito de Santa Maria (FADISMA). Graduada na Formação Especial de Professores pela Universidade Federal de Santa Maria (UFSM). Professora na Faculdade de Direito de Santa Maria (FADISMA), Universidade Franciscana (UFN) e FN e CEISC Cursos Preparatórios. E-mail: cristianepaulidemenezes@gmail.com; Currículo: http://lattes.cnpq.br/5370634318308124

rede, essa estrutura vigilante apenas foi remodelada, já que a vigilância também é vertiginosamente digital, uma vez que o poder, segundo o marco teórico adotado nesta obra, está em toda a parte e fundamenta todas as relações sociais.

A super vigilância vivenciada, com grande inspiração nas ideias do panoptismo, porém, agora, dentro do contexto da sociedade em rede, é justificada em *n* circunstâncias: no combate ao terror, na manutenção da segurança nacional, na preservação da ordem pública, entre tantas outras referências perspicazmente exploradas por Seefeldt ao longo de sua obra. Por outro lado, contribuímos com esse regime de vigilância, quando fornecemos nossos próprios dados pessoais para acesso a produtos e serviços, sem os quais não nos sentimos parte da sociedade em rede.

A verdade é que, na sociedade informacional, nossos dados são também uma mercadoria à disposição do capital. Com isso, os algoritmos fazem uma leitura minuciosa de nossas preferências e somos bombardeados de forma exponencial por anúncios e vibrações que nos levam ao consumo de conteúdo, serviços e mercadorias, produzindo cada vez mais dados, numa retroalimentação dessa rede.

Temos, ainda, uma falsa sensação de que podemos vigiar o outro, mas esquecemos que estamos sendo vigiados, não só também pelo outro, como também pelas agências governamentais e pelas grandes corporações tecnológicas. Falar, na modernidade, em *right to be alone* é, pois, uma falácia, já que para fazer jus a este direito, como dito, precisamos nos assumir *outsiders,* o que representa outro grande gargalo. Daí, porque a necessidade de se repensar e reestruturar o direito à privacidade na sociedade em rede.

Uma das questões que atestam e endossam a importância das reflexões de Seefeldt é justamente a recente entrada em vigor do Regulamento Geral de Proteção de Dados Pessoais (RGPD ou GPDR, na sigla em inglês) e da Lei Geral de Proteção de Dados no Brasil (LGPD), que inauguram um regime jurídico de proteção dos dados pessoais. A temática é tão sensível que índices criados pela Associação Brasileira das Empresas de Software

(ABES) e pela EY[2] apontam que apenas em torno de 40% (quarenta por cento) das sociedades empresárias no Brasil estão aptas a atuarem sob a égide dos preceitos trazidos pelo recente texto legal.

João Pedro Seefeldt Pessoa, com muita propriedade, nos guia com um olhar que só pode ser dado por alguém que estudou de forma comparada o regime europeu e brasileiro. Essa importante obra traduz as convicções de um autor que há anos dedica seu espaço acadêmico para reflexões oriundas da sociedade em rede.

Posso falar, como professora e como Coordenadora do Núcleo de Estudos de Direito Internacional da Faculdade de Direito de Santa Maria, que Seefeldt traz nessa obra as inquietudes de um pesquisador destacado em toda sua trajetória acadêmica.

Os pontos aqui explorados são frutos dos estudos que realizou com afinco desde a graduação e que foram solidificados em sua experiência no Mestrado junto à Universidad de León, na Espanha, bem como no Mestrado junto à Universidade Federal de Santa Maria, cujas linhas de pesquisa ganham guarida justamente nos estudos sobre esses novos direitos.

Ao concluir que o direito à privacidade pode supor um regime global de contravigilância social, o autor nos rememora que as mudanças sociais identitárias advindas da sociedade em rede podem permitir que utilizemos das novas tecnologias de informação e comunicação para assumirmos protagonismos, valermos nossos direitos e vigiarmos quem nos vigia.

A leitura é um convite para repensarmos nosso papel frente aos novos paradigmas.

---

[2] Informações disponibilizadas pela Valor Econômico. Disponível em: https://valor.globo.com/publicacoes/suplementos/noticia/2020/10/23/implementacao-da-lgpd-requer-esforco-adicional.ghtml. Acesso em: 23 dez. 2020.

Parte I

O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI

Introdução

Na sociedade em rede, novos atores sociais e novas relações sociais são inseridas, de modo transversal e multidirecional, proporcionando um maior fluxo de comunicação e uma distribuição nodal de interações, inclusive no que se refere às relações de poder. As redes, formadas por nós, arestas e *clusters*, competem ou cooperam entre si, marcadas pelo uso de novas tecnologias da informação e comunicação, numa horizontalização da comunicação em grande escala, à medida em que as novas plataformas permitem uma interação expansiva sem a necessária intervenção de canais de comunicação ou lideranças.

A evolução tecnológica e a globalização criaram novos desafios relacionados à privacidade e à proteção de dados pessoais, já que, no horizonte da *Internet of Things* e da *Internet of Everything,* a coleta, o tratamento e o compartilhamento de dados registaram um aumento significativo, permitindo que as corporações privadas e as instituições públicas utilizem os dados pessoais numa escala sem precedentes durante o exercício das atividades do cotidiano. Por outro lado, as pessoas fornecem, cada vez mais, as suas informações, de maneira pública e global, tendo em vista que a disponibilização dos dados pessoais é condição para acesso de produtos e serviços na sociedade em rede.

No século XX, com a profusão das tecnologias de informação e comunicação, os mecanismos de controle e vigilância, especialmente estatais, aperfeiçoaram-se e se converteram em ferramentas úteis para uma vigilância geral e espalhada, de forma institucional. Na sociedade em rede, a vigilância é líquida, onipresente e, por vezes, passa desapercebida pelos vigiados, exercendo sobre estes um controle sobre as formas de viver. E, em sentido inverso, os sujeitos acabam renunciando direitos e garantias fundamentais, em particular a privacidade, quando do fornecimento de

informações pessoais para acessar produtos e serviços, contribuindo para uma economia de vigilância e circulação de dados, muitas vezes sem verdadeira consciência das implicações e dos impactos dessa subjetivação tecnológica.

A presente pesquisa tem por objeto o estudo sobre a vigilância social e privacidade na sociedade em rede. E, de forma delimitada, trata-se, então, do estudo de uma ressignificação do direito à privacidade afetado pelo regime global de vigilância social de dados pessoais no contexto da cibersegurança do século XXI, em razão da alteração de paradigma produzida pelo avanço das tecnologias de informação e comunicação. Portanto, indaga-se em que medida e em que pressupostos o regime global de vigilância social de dados pessoais pode afetar o direito à privacidade em tempo de cibersegurança no século XXI.

O objetivo geral desta obra é analisar os impactos das tecnologias de informação e comunicação e do regime global de vigilância social no direito à privacidade, no contexto da cibersegurança do século XXI. No que tange aos objetivos específicos, pretende-se: a) investigar o panorama revelado do regime de monitoramento social global e os impactos na sociedade do século XXI; b) identificar a contribuição das pessoas nesse regime global de vigilância social a partir do fornecimento de dados para acesso a produtos e serviços; c) estabelecer a estrutura normativa global e regional do direito à privacidade, mudança e abordagens do conceito ao longo do tempo; e, por fim, d) discutir a ressignificação do direito à privacidade, baseada em novos conceitos, novos espaços, novos limites e novas possibilidades no contexto da cibersegurança.

A atualidade do tema está presente, porque o livro aborda discussões da pós-modernidade e da sociedade em rede, panorama sociopolítico atual, marcado pelo fluxo contínuo de informações entre sujeitos e multidões digitalmente conectadas, especialmente considerando os impactos das novas tecnologias de informação e comunicação sobre os direitos e garantias fundamentais, que são melhoradas e aperfeiçoadas a cada dia. Ainda, percebe-se que o direito à privacidade, um dos pilares dos direitos

fundamentais, está passando por mudanças, inclusive de paradigma, em razão da produção e fornecimento de dados pessoais na rede.

Ademais, a pesquisa trata detalhadamente do direito à privacidade e outras dimensões daí derivadas, cujo bem jurídico protegido foi recentemente tutelado pelo Regulamento Geral de Proteção de Dados da União Europeia, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, com aplicação obrigatória a partir de maio de 2018, em atenção aos novos avanços das tecnologias de informação e comunicação. No caso brasileiro, a Lei nº 13.709, de 14 de agosto de 2018, estabeleceu a Lei Geral de Proteção de Dados Pessoais (LGPD), que inaugura esse novo regime jurídico no Brasil.

Ainda, a pesquisa revela importância à sociedade e à academia, tendo em vista que o próprio Regulamento põe relevância no fato de que os princípios e as regras em matéria de proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais, independentemente da nacionalidade ou do local de residência dessas pessoas, devem respeitar os direitos e liberdades fundamentais. Assim, cada vez mais se faz necessário abordar a problemática do direito à privacidade frente aos avanços das tecnologias de informação e comunicação, formando profissionais capazes de refletir criticamente sobre a matéria.

Registra-se que a presente obra é fruto das pesquisas realizadas pelo autor nos anos de 2018 e 2019, bem como da dissertação apresentada, no âmbito do Mestrado Universitário em Direito da Cibersegurança e Entorno Digital da Universidade de León, em León, Espanha, sob orientação do Prof. Dr. Salvador Tarodo Soria. Dentro do programa espanhol, uma competência a ser desenvolvida pelos estudantes é justamente conhecer o sistema de fontes, direitos e liberdades fundamentais e os princípios básicos do Direito da Cibersegurança e do Ambiente Digital, sabendo integrar conceitos multidisciplinares para poder analisar, interpretar e resolver

problemas e conflitos jurídicos, políticos e sociais que surgem nesse campo.

Nessa mesma perspectiva, o curso de mestrado se enquadra no marco de cooperação entre Fundação Carolina e o Instituto Nacional de Cibersegurança da Espanha – INCIBE, já que um dos objetivos dessa instituição, para enfrentar os desafios colocados pelos avanços das tecnologias de informação e comunicação, é precisamente tentar satisfazer adequadamente a demanda social de profissionais altamente qualificados nas normativas sobre cibersegurança e ambiente digital, tanto que as pesquisas realizadas pelo autor foram subvencionadas por estas duas instituições.

O percurso metodológico do presente livro deve perpassar, em face dos objetivos a serem atendidos e do problema de pesquisa, por quatro momentos e nos seguintes pontos temáticos: a) investigação preliminar sobre a temática do regime global de vigilância social por parte das agências institucionais; b) investigação preliminar sobre a temática da vigilância, porém sob ponto de vista das pessoas físicas e multidões: c) revisão de conceitos e normativas relativas ao direito à privacidade e suas dimensões, especialmente tratados internacionais, regulamentos comunitários e leis específicas; e d) debate mais profundo sobre o direito à privacidade na sociedade de vigilância.

Quanto à metodologia de abordagem, utiliza-se o método dedutivo, porque se realiza uma conexão descendente entre os temas tratados, partindo-se de um plano geral e premissa geral para proceder à análise de panoramas específicos, a fim de obter uma conclusão a partir desse silogismo lógico. Em outras palavras, investiga-se, primeiramente, a ascensão de uma sociedade baseada numa economia de vigilância de dados, que permite a vigilância de atores sociais por parte de agências institucionais e por parte de grandes corporações, para, posteriormente, verificar como esse novo paradigma afeta o direito à privacidade.

Quanto à metodologia de procedimento, utiliza-se o método monográfico, com o objetivo de estudar a vigilância social, sob ponto de vista da

razão governamental dominante e também do tratamento de dados pessoais pelas grandes corporações, para analisar detalhadamente o direito à privacidade no século XXI. Para isso, através do estudo científico de atores sociais, processos comunicativos e fatores organizativos dessa nova sociedade em rede envolvendo a vigilância de dados, pretende-se obter conclusões em relação ao tema e investigar criticamente os efeitos no direito à privacidade.

Para tanto, pretende-se aplicar as técnicas de pesquisa de documentação indireta e documentação direta. Assim, utiliza-se da pesquisa documental e bibliográfica, considerando que grande parte da revisão bibliográfica realizada no presente estudo é oriunda da literatura especializada no tema, especialmente sobre direito à privacidade e os efeitos dos novos paradigmas sociais sobre direitos e garantias fundamentais; outra parte virá de normativas internacionais, comunitárias e nacionais, bem como de notícias e trabalhos científicos realizados sobre a temática, dentre outras.

A teoria de base adotada apresenta aportes teóricos trazidos por, principalmente, Michel Foucault (vigilância como panóptico de poder), Gilles Deleuze (dados e vigilância na sociedade de controle), Gleen Greenwald (regime de vigilância global), Zigmunt Bauman (vigilância na pós-modernidade e pós-panóptico), Manuel Castells (sociedade em rede), Stefano Rodotà (privacidade na sociedade de vigilância), dentre outros, já que tenta-se ponderar sobre o impacto do avanço das tecnologias de informação e comunicação na comunidade global, evidenciando-se as relações de vigilância características da sociedade em rede baseadas no tratamento de dados pessoais, bem como analisando-se o impacto desse novo paradigma no direito à privacidade

Em termos estruturais, a pesquisa está desenvolvida em dois grandes capítulos, demonstrando a relação de premissa geral e específica. O primeiro capítulo, por sua vez, está subdividido em dois grandes blocos: o primeiro tratando sobre o panóptico do século XXI e a vigilância perpetradas pelas agências de segurança nacionais; o segundo abordando a

contribuição dos usuários para fornecimento de dados para acesso a produtos e serviços. Por outro lado, o segundo capítulo também está subdividido em dois grandes blocos: o primeiro analisando a evolução do direito à privacidade até o direito à proteção de dados pessoais; o segundo ponderando sobre a alteração de paradigma do direito à privacidade a um regime coletivo de proteção.

1

"O Grande Irmão está de olho em você": a vigilância social e o processamento de dados na sociedade em rede do século XXI

O título do presente capítulo faz referência a uma das frases mais conhecidas da obra "1984", de George Orwell: "o Grande Irmão está de olho em você", significando a vigilância marcada da Oceania, cenário de fundo para as reflexões do personagem principal, Winston Smith. Na cidade em que passa a história, há pôsteres enormes, em diferentes lugares, com uma imagem do Grande Irmão, líder do Partido, para relembrar, a todo momento, que os cidadãos estão sendo vigiados e devem se comportar conforme determinado pelas fontes de poder.

A frase – e a própria história referenciada – é oportuna para o presente capítulo, uma vez que o avanço das tecnologias de informação e comunicação, especialmente da microeletrônica e da nanoeletrônica, possibilitaram a criação de mecanismos de vigilância dos cidadãos, a partir da interceptação de dados pessoais, que, a sua vez, podem ser entendidos como o ouro dessa nova arquitetura social surgida após o final da Segunda Guerra Mundial, já que o fornecimento das informações pessoais é condição para acesso e participação na sociedade em rede.

Considerando que o objetivo geral deste livro é analisar os impactos das tecnologias de informação e comunicação e do regime global de vigilância social no direito à privacidade, no contexto da cibersegurança do século XXI, este capítulo, como forma de introduzir premissas gerais sobre o tema, pretende: a) investigar o panorama revelado do regime de monitoramento social global e os impactos na sociedade do século XXI; e b)

identificar a contribuição dos indivíduos nesse regime global de vigilância social a partir do fornecimento de dados para acesso a produtos e serviços.

1.1 A procura do ouro do século XXI: o regime global de vigilância social

O poder pode ser entendido como uma prática social construída ao longo do tempo, de forma heterogênea e dinâmica, como resultado de uma relação de forças em uma determinada sociedade, em determinado momento, sendo dissolvida por todo o tecido social, sendo exercida por meios de dispositivos, isto é, caminhos, formas e meios de exercer poder, como punição, disciplina, sexualidade, loucura, exame[1]. A partir do século XVIII, a vigilância tornou-se um dos principais dispositivos para o exercício do poder, sendo, ao longo do tempo, ampliada e aperfeiçoada, com o objetivo de imprimir processos de coerção aos sujeitos sob vigilância[2].

1.1.1 Do panoptismo à vigilância como dispositivo de poder

Na sociedade disciplinar – ou ainda "momento das disciplinas"[3] –, os dispositivos de poder, dentre eles, utilizados nas instituições totais – família, escola, quartel, fábrica, hospital e prisão –, conseguiam vigiar e punir os indivíduos, na tentativa de docilizar e submeter os sujeitos a moldagens pré-definidas e utilitaristas, numa espécie de disciplinarização e controle sobre o corpo[4]. O panoptismo, inspirado no modelo de Jeremy Bentham, foi, então, o arquétipo arquitetural ideal do momento das disciplinas, uma vez que, através de técnicas ópticas e solares, especialmente em composições circulares, como prisões, fábricas e manicômios, era possível criar

[1] FOUCAULT, Michel. *Microfísica do poder*. 23 ed. São Paulo: Graal, 2004.

[2] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 196.

[3] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 196.

[4] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 197-198.

uma vigilância literalmente institucional[5]. Nesse modelo, o indivíduo sujeitado à disciplina entendia e propriamente visualizava que estava sendo permanentemente vigiado, embora nem sempre o estivesse de verdade, porém saber que poderia estar sendo vigiado por alguém já era suficiente para manter a disciplina e o controle, num "funcionamento automático do poder"[6].

Já na segunda metade do século XVIII, após a profusão das medidas disciplinares, o exercício do poder, que antes era limitado ao corpo-indivíduo num espaço-tempo definido, passou a ser endereçado a uma multiplicidade de corpos, por meio de procedimentos coletivos, numa biopolítica dirigida ao corpo-população enquanto massa modular[7]. Ou seja, a ideia não era mais somente moldar o indivíduo em si, mas modular uma coletividade, para maior controle, de forma que, para tanto, os dispositivos de poder deviam se adaptar, a vigilância devia acompanhar os novos desafios, inclusive como uma tática de guerra [8].

1.1.2 A revolução das TICs e o regime global de vigilância social

Com o fim da Segunda Guerra Mundial, um sem número de transformações ajudaram na mudança de paradigma social, já que que caíram os muros e as fronteiras, permitindo-se um fluxo de interações entre atores sociais em um campo aberto[9]. A vigilância sofre intensas mudanças e aperfeiçoa-se proporcionalmente à evolução das tecnologias de informação e comunicação, tornando-se, então, horizontalizada (não mais verticalizada), difundindo-se por inúmeros campos de captação e atuação

[5] BENTHAM, Jeremy. O panóptico ou a casa de inspeção. In: TADEU, Tomaz (Org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008, pp. 17-30.

[6] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 224-225.

[7] FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005, p. 285-289.

[8] FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005, p. 293-294.

[9] DELEUZE, Gilles. *Conversações:* 1972-1990. São Paulo: 34, 1992, p. 220.

(não mais somente instituições fechadas), para visualizar o maior número de corpos de interesse[10].

Durante o conflito internacional mencionado, agências estatais e organizações de diferentes países, notadamente Reino Unido e Estados Unidos, interceptaram, leram e analisaram diversas informações trocadas pelas tropas alemãs e japonesas, criando, desde o final da guerra, uma rede planetária de inteligência para escuta e captação de sinais, desenvolvida através do Tratado de Segurança *UK-USA* (também grafado *UKUSA*, remetendo-se às iniciais dos países envolvidos). Esse acordo e a conjectura daí desenvolvida contou com a ajuda dos Cinco Olhos, Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos, sendo somente revelado ao final do século XX e confirmado no início do século XXI[11].

Então, o marco de cooperação de inteligência secreta *UKUSA*, liderado substancialmente pela Agência de Segurança Nacional dos Estados Unidos (*National Security Agency*, em inglês), entidade também mantida em sigilo por décadas, fez criar um sistema de vigilância global, denominado Echelon, com capacidade para captar e analisar, virtualmente, informações advindas de chamadas telefônicas e mensagens de fax, telex, e-mail e outros dispositivos, enviadas de qualquer lugar do mundo[12]. Trata-se, pois, de uma rede de espionagem, que, por meio de interceptação, capta o tráfego de dados ocorrido por satélite, fibra ótica, frequência de rádio, micro-ondas, cabos submarinos, internet e outras formas de processamento de informação e comunicação, ainda que haja um avanço nas técnicas de criptografia.

---

[10] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192 f. Dissertação (Mestrado) - Curso de Direito, Departamento do Direito, Universidade Federal de Santa Maria, Santa Maria, 2018, p. 41.

[11] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014; NORTON-TAYLOR, Richard. *Not so secret: deal at the heart of UK-US intelligence*. [The Guardian, 25/06/2010]. Disponível em: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released. Acesso em: 16 abr. 2019.

[12] UNIÃO EUROPEIA. *Parlamento Europeu. Relatório de 11 de julho de 2001 sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON").* Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//PT. Acesso em: 16 abr. 2019.

Conforme uma investigação realizada pelo Parlamento Europeu, divulgado no Relatório de 11 de julho de 2011, no âmbito do sistema *Echelon*, dados brutos de comunicação captados pelas agências de inteligência, tanto de voz, telex, fax e internet, puderam ser interceptados, registrados, analisados, trocados, vendidos e classificados por meio de filtros, permitindo a elaboração fácil de perfis e outros relatórios pelas partes interessadas[13].

Os relatórios elaborados dão conta de que os programas de vigilância global em massa se aperfeiçoaram durante o século XX, imprimindo importantes avanços tecnológicos para o sistema de inteligência de sinais[14]. Em apertada síntese, pode-se dizer que, na década de 40, quando o acordo de cooperação fora estabelecido, o objetivo principal da vigilância era a espionagem militar e diplomática; na década de 60, era a espionagem comercial e industrial, passando por setores econômicos e científicos; já na década de 90, era o combate ao crime organizado, à lavagem dinheiro, ao tráfico de drogas, armas e pessoas e, mais ainda, como nos próximos anos, ao terrorismo[15].

Em 2006, Julian Assange, jornalista e ciberativista, constituiu a *WikiLeaks*, uma organização transnacional em favor da transparência, a fim de publicar informações e dados confidenciais, especialmente sensíveis, vazados ou hackeados de governos ou outras instituições para acesso e crítica públicos[16]. Assange defende a figura dos *cypherpunks*, os quais "defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas", de forma que "criado no início dos anos

---

[13] UNIÃO EUROPEIA. *Parlamento Europeu. Relatório de 11 de julho de 2001 sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON").* Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//PT. Acesso em: 16 abr. 2019.

[14] UNIÃO EUROPEIA. *Parlamento Europeu. Relatório de 11 de julho de 2001 sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON").* Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//PT. Acesso em: 16 abr. 2019.

[15] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

[16] WIKILEAKS. *What is WikiLeaks*. Disponível em: https://wikileaks.org/What-is-Wikileaks.html. Acesso em: 16 abr. 2019.

1990, o movimento atingiu seu auge durante as 'criptoguerras' e após a censura da internet em 2011, na Primavera Árabe"[17].

Em 2010, Chelsea Manning – à época, Bradley Manning –, forneceu ao *WikiLeaks* mais de 700 (setecentos) mil arquivos secretos, vídeos de confrontos e comunicações diplomáticas do Departamento de Estado dos Estados Unidos, sendo detida, em 2013, em uma penitenciária militar e submetida a técnicas de privação de sono, nudez forçada e tortura psicológica, detenção considerada desumana e ilegal pela Anistia Internacional[18]. A ativista foi levada a julgamento e condenada a 35 (trinta e cinco) anos de prisão, mas o ex-presidente estadunidense Barack Obama comutou sua sentença antes de deixar o cargo em 2017[19].

Em 2013, Edward Snowden, analista de sistemas até então funcionário do governo estadunidense, tornou público inúmeras informações confidenciais sobre a existência e atuação da Agência Nacional de Segurança, dos Estados Unidos, assim como sobre os programas que compõem um sistema de vigilância global americano, dentre eles o *PRISM*, referido antes[20]. Em detalhes, Snowden viajou até Hong Kong em maio de 2013, onde entregou documentos probatórios aos jornalistas Glenn Greenwald e Laura Poitras, os quais foram revelados pelos portais *The Guardian, The Washington Post* e *The Intercept*, gerando uma crise institucional e desconforto global, tanto que o ativista vive atualmente sob asilo político[21].

A partir de 2013, com o vazamento de documentos ultrassecretos, descobriu-se a existência de outros programas de vigilância global, quer no âmbito do sistema Echelon, isto é, vinculados a ele ou submetidos a ele,

---

[17] ASSANGE, Julian. *Cypherpunks*: liberdade e futuro da internet. São Paulo: Boitempo, 2013, p. 05.

[18] AYUSO, Silvia; PEREDA, Cristina. *Obama conmuta la pena de la soldado Chelsea Manning.* [El País, 18 jan. 2017] Disponível em: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html. Acesso em: 10 abr. 2019.

[19] AYUSO, Silvia; PEREDA, Cristina. *Obama conmuta la pena de la soldado Chelsea Manning.* [El País, 18 jan. 2017] Disponível em: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html. Acesso em: 10 abr. 2019..

[20] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

[21] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

ou não. Por exemplo, *PRISM*, dos Estados Unidos, Austrália, Reino Unido e Países Baixos; *XKeyscore*, dos Estados Unidos, Alemanha e Austrália e Nova Zelândia; *Project 6,* da Alemanha e Estados Unidos; *Stateroom,* dos Cinco Olhos; *Lustre,* dos Estados Unidos e França; *Optic Nerve*, dos Estados Unidos e Reino Unido; *Turbine*, dos Estados Unidos, Reino Unido e Japão; *Operation Socialist*, do Reino Unido; *Tempora, Muscular, Follow The Money, Marina, Dishfire, Mystic*, estes todos dos Estados Unidos, podendo haver ou não coordenação com outras agências parceiras[22].

Os Estados Unidos, no bojo da *National Security Agency,* admitiram haver dois programas, *PRISM* e *UPSTREAM*. Em resumo, o *PRISM* é um programa de inteligência que permite a obtenção de material de inteligência, desde que devidamente aprovado por uma corte de juízes, adquirido junto aos provedores de serviços, de maneira detalhada e direcionada, ainda que sem grande capacidade de *data mining,* estando regulado pelo *Foreign Intelligence Service Act (FISA)*[23]. Por sua vez, o *UPSTREAM* é um programa de inteligência que coleta dados oriundos de comunicação por cabos de fibra óptica e infraestrutura dos provedores de serviço, o qual permite acesso aos dados globais, inclusive de cidadãos não estadunidenses[24].

O Reino Unido, através da agência *Government Communications Headquarters,* com sigla *GCHQ,* confirmou operar o programa denominado *Tempora*, com o qual acessava e armazenava informações de dados de portadores.[25] O programa permitia, em apertada síntese, comparar o tráfico

---

[22] PIRES, Hindenburgo Francisco. Geografia das indústrias globais de vigilância em massa: limites à liberdade de expressão e organização na internet. *Ar@cne Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales*, Universidad de Barcelona, n.º 183, abr. 2014. Disponível em: http://www.ub.edu/geocrit/aracne/aracne-183.htm#_edn16. Acesso em: 20 abr. 2019.

[23] UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

[24] UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

[25] UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido:

de dados com um rol de seleções e buscas pré-determinadas de um objeto específico para realizar uma triagem da comunicação realizada[26]. A agência argumenta que o sistema é referendado pelo *Regulation of Investigatory Powers Act 2000 (RIPA),* legislação interna que possibilita com que o Secretário de Estado expeça mandados para interceptação de comunicações[27].

Importante tratar sobre outros três desses programas para compreender a magnitude do monitoramento de dados. O *XKeyscore*, um dos primeiros sistemas informáticos operados pela NSA e compartilhado com Alemanha, Austrália e Nova Zelândia, na forma de um motor de busca, permite, conforme Snowden que já teve autorização para acessá-lo, a recuperação de dados de todos os registros coletados diariamente em todo mundo, dispondo de ferramentas capazes de captar tudo o que os usuários fazem na rede[28].

Por outro lado, o programa *Lustre*, dirigido especialmente pela *Direction Générale de la Sécurité Extérieure – DGSE*, agência de segurança da França, com cooperação dos Cinco Olhos, especialmente da NSA, baseia-se na posição geoestratégica no tráfego de dados eletrônicos, posto que a maioria dos cabos submarinos de comunicações que conecta a África adentra ao continente europeu pelo território francês, de modo que o

Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

[26] UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

[27] UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

[28] GREENWALD, Glenn. *XKeyscore*: NSA tool collects 'nearly everything a user does on the internet'. [The Guardian, 31/07/2013] Disponível em: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Acesso em: 20 de abr. 2019

DGSE pode interceptar os dados transmitidos e repassar às suas parceiras[29]. Por fim, o programa *Stateroom*, criado pelas agências de segurança dos Estados Unidos, Canadá, Austrália e Reino Unido, é um projeto de interceptação global em massa com base de operação em cerca de oitenta embaixadas e consulados estadunidenses espalhados pelo globo, que, por meio de um *exploit,* gerado a partir da infecção de mais de 50.000 (cinquenta mil) redes de comunicações em todo mundo por um arquivo malicioso (*malwares*) de vigilância em massa, pode interceptar mensagens a qualquer tempo, independentemente do conhecimento do usuário[30].

Além de agências de segurança e de inteligência dos países referidos, verificou-se que importantes universidades também estiveram envolvidas no projeto para fornecimento de bases científicas, como, por exemplo, *University of California, Stanford University, Massachusetts Institute of Technology (MIT), University of California Berkeley, California Institute of Technology (Caltech) e Johns Hopkins University*. Ademais, documentos secretos mostraram a cooperação e fornecimento de informações por empresas e organizações de setores econômicos, como *Google, Facebook, Microsoft, Apple, Verizon, Vodafone, EDS, AT&T, Qwest, Motorola, Intel, IBM, Qualcomm, Cisco, H-P, Oracle*, dentre outras[31].

1.1.3 O regime global de vigilância social nos discursos de legitimação

Através das sistemáticas revelações, observa-se extensas e complexas redes de cooperação e de competição entre agências de segurança e de inteligência estatais, especialmente localizadas em países desenvolvidos,

---

[29] FOLLOUROU, Jacques. *Surveillance*: la DGSE a transmis des données à la NSA américaine. [Le Monde, 30/10/2013] Disponível em: https://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html. Acesso em: 20 abr. 2019.

[30] DERIX, Steven. MODDERKOLK, Huib. *50.000 pakketjes kwaardaardige software*. [NRC, 23/11/2013] Disponível em: https://www.nrc.nl/nieuws/2013/11/23/50000-pakketjes-kwaardaardige-software-13162666-a1157982. Acesso em: 24 abr. 2019.

[31] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014, p. 83.

com o objetivo de interceptar, analisar, armazenar e monitorar informações e comunicações entre indivíduos, grupos, instituições, corporações, empresas e governos ao redor do globo. A principal justificativa para criação de zonas de exceção para permitir o monitoramento de informações e comunicações da população de forma incomensurável é o combate ao terrorismo, uma vez que, com a vigilância eletrônica realizada, é possível identificar redes de cooperação, antever atos terroristas e prevenir crimes daí decorrentes.

A respeito disso, a "guerra ao terror" faz com que nações do mundo inteiro atuem buscando inimigos, especialmente a partir de 2001, logo após os atentados terroristas de 11 de setembro, nos Estados Unidos. Oportunamente, o governo norte-americano dispôs e, com o tempo, recrudesceu, uma política estratégica de antiterror, com a formação de alianças ou com o comando de iniciativas de outros países, no âmbito do Conselho de Segurança da Organização das Nações Unidas, da Organização do Tratado do Atlântico Norte e da Organização dos Estados Americanos, em desfavor daquele inimigo comum – o terror, mesmo que este inimigo, taticamente, mude ora para redes terroristas, ora países financiadores do terrorismo, ora governos paralelos terroristas[32].

Ocorre que documentos expostos pelos movimentos contravigilantes revelaram que o discurso do terrorismo parece ser muito mais uma justificativa para ações tomadas com fins escusos e uma tática governamental para infligir medo social. É dizer, "uma porcentagem importante dos programas nada tinha a ver com segurança nacional", visto que "os documentos não deixavam dúvidas de que a NSA praticava também espionagem econômica e diplomática, além da vigilância de populações inteiras sem qualquer base para suspeita"[33]. De todas as maneiras, em virtude desse medo ao terrorismo, a população, preocupada com segurança

[32] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014, p. 74.

[33] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014, p. 75

interna, chancela o ideal vigilante e, em que pese tais programas de vigilância tenham sido pensados a escala global, as inovações tecnológicas e o fluxo de pessoas permitiram o monitoramento doméstico de cidadãos, já que a ameaça também pode ser interna.

Deste modo, uma guerra justa encontra-se justificada por si mesma, embora banalize, por um lado, quem é o inimigo, posto que qualquer um pode ser objeto de vigilância, mas, também, por outro lado, absolutiza o inimigo, haja vista que a ameaça à ordem é permanente e deve ser constantemente combatida e aniquilada[34]. A guerra ao terror transforma-se, assim, num completo estado de exceção em tons de guerra global permanente como plano de fundo, exigindo das nações que estejam preparadas e combativas, antevendo, vigiando, agindo ante a qualquer movimento suspeito no jogo do poder[35].

Outrossim, jornalistas revelaram que as agências de segurança trabalham não apenas para quebrar os códigos das conversas privadas dos indivíduos, mas também para boicotar a própria segurança das informações para facilitar a vigilância das informações, como, por exemplo, o caso da NSA que tenta obrigar a que grandes companhias criem *backdoors* nos códigos de criptografia das redes sociais, para permitir o acesso e manipulação das informações deixadas pelos usuários, fato este que a agência alega tratar-se de medida de segurança contra ataques terroristas[36]. Visualiza-se, então, uma dicotomia de personagens públicos, à medida em que, por um lado, "Assanges", "Mannings" e "Snowdens", que revelam a existência de programas de vigilância, são considerados vilões, enquanto que "Gates", "Jobs" e "Zuckerbergs", que contribuem, com suas plataformas, para esses sistemas, são considerados heróis da tecnologia.

---

[34] HARDT, Michael; NEGRI, Antonio. *Império*. São Paulo: Record, 2012, p. 31.

[35] HARDT, Michael; NEGRI, Antonio. *Império*. São Paulo: Record, 2012, p. 34.

[36] McCARTHY, Tom. *NSA director defends plan to maintain 'backdoors' into technology companies.* [The Guardian, 23/02/2015] Disponível em: https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies. Acesso em: 06 jan. 2018.

1.1.4 A relevância do *big data* e a tomada de decisões baseadas em dados

Diante desse cenário, depara-se com a obtenção em larga escala de uma quantidade exorbitante de dados, a qual possui especial importância, uma vez que, a partir da coleta, do armazenamento, da manipulação e da transferência de tais dados, é possível criar padrões e vigiar indivíduos e massas. Nesse sentido, *big data* é uma grandeza informacional, produzida e fornecida pelos usuários das redes sociotécnicas, cuja manipulação permite, por parte de corporações e governos, "analisar, processar e gestionar conjunto de dados extremadamente grandes que podem ser analisados informaticamente para revelar padrões, tendências e associações, especialmente em relação à conduta humana e às interações dos usuários"[37].

Embora o conceito de *big data* seja relativamente novo e não tão difundido socialmente, já é possível identificar, pelo menos, cinco aspectos que envolvem essa grandeza, conhecidos como *cinco Vs*: volume, velocidade, variedade, veracidade e valor. O volume faz referência à quantidade de dados produzidos, estimando-se na casa de exabytes e zettabytes diariamente; a velocidade diz respeito a que a manipulação de tais dados se dá em tempo muito hábil e simultâneo; a variedade quer dizer sobre a diversidade de dados que são coletados; a veracidade assimila que o processamento desses dados deve garantir a confiabilidade e integridade deles; e, por fim, o valor refere-se aos benefícios significativos oriundos do processamento dos dados coletados[38].

De acordo com o estudo *The Economic Value of Data: discussion paper*, do Ministério de Finanças do Reino Unido, a exploração de dados,

---

[37] REAL ACADEMIA ESPAÑOLA. Diccionario del español jurídico. *Big data.* Disponível em: https://dej.rae.es/lema/big-data. Acesso em: 20 abr. 2019.

[38] FERNÁNDEZ, Déborah. *Las cinco V's del Big Data.* [DataHack, 27/08/2018] Disponível em: https://www.datahack.es/cinco-v-big-data/. Acesso em: 20 abr. 2019; TAURION, Cezar. *Volume, variedade, velocidade, veracidade e valor:* os cinco Vs do Big Data. Disponível em: http://computerworld.com.br/volume-variedade-velocidade-veracidade-e-valor-os-cinco-vs-do-big-data. Acesso em: 16 abr. 2019.

conforme previsto pela União Europeia e pela Organização para Cooperação e Desenvolvimento Econômico, vai, cada vez mais, gerar valor público e privado[39]. Isso, pois *data-driven decision,* ou seja, tomada de decisões baseada no processamento de dados, é capaz de melhorar o desempenho, a produtividade e a lucratividade das empresas, bem como capaz de incrementar a eficiência de produtos e serviços públicos, já que os dados possuem o potencial de agilizar e personalizar métodos e técnicas de negócios[40].

Nesse ínterim, diversos mecanismos contribuem com a coleta e armazenamento de dados informacionais de usuários na rede, destacando-se, dentre outros, os *cookies, web beacons, spywares, tagging* e *tracking*. Por meio de tecnologias de todos os tipos, inclusive de técnicas de *doxxing* e *hacking,* torna-se possível criar perfis de usuários, identificar quais e quantos usuários estão engajados em rede, mapear como ocorre o comportamento dessas pessoas. E, atualmente, esses mecanismos estão espalhados nos mais diversos ambientes e espaços, por meio dos dispositivos móveis pessoais inteligentes, utilizados ao redor do globo por bilhões de pessoas, como, por exemplo, celulares, *tablets*, *notebooks*, relógios, televisores, dentre outros.

Diante tudo isso, é possível deduzir que a sociedade atual vive sob um superpanóptico, que tem no panoptismo trazido por Jeremy Bentham e Michel Foucault um modelo de inspiração, um ponto de partida – já que aquelas ideias de docilização e disciplina do corpo ainda subsistem –, mas essa técnica de biopoder ultrapassa, progressivamente, todos os limites já pensados, à medida do aperfeiçoamento das tecnologias de informação e comunicação, já que "o que conta é que estamos no início de alguma coisa"[41].

---

[39] REINO UNIDO. *The economic value of data:* discussion paper. Londres: HM Treasury, 2018. p. 04-07. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf. Acesso em: 20 abr. 2019.

[40] REINO UNIDO. *The economic value of data:* discussion paper. Londres: HM Treasury, 2018. p. 04-07. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf. Acesso em: 20 abr. 2019.

[41] DELEUZE, Gilles. *Conversações:* 1972-1990. São Paulo: 34, 1992, p. 225

1.1.5 O Estado de vigilância: a vigilância social pública frente aos direitos humanos e garantias

Como é cediço na doutrina do direito administrativo, impõe-se a supremacia do interesse público sobre os interesses privados e particulares, como própria razão de existir da Administração Pública, que deve atuar voltada ao bem da coletividade. Sob o medo gerado pela guerra ao terror, os governos justificam esse vigilantismo em massa em expressões tais como "segurança nacional", "defesa nacional", "situações de emergência", "manutenção da paz", "garantia da lei e da ordem", "prevenção da prática de infrações", "garantia da integridade territorial", "defesa da soberania" e outros sinônimos, de tal maneira que, ainda que entendidos como limitação à potestade do Estado, direitos e garantias humanas e fundamentais são ressignificados.

No âmbito comunitário europeu, o direito à privacidade, previsto como um direito humano desde o fim da Segunda Guerra Mundial, possui limitações já definidas no próprio ordenamento, o que, por si só, constitui o fundamento dos programas de vigilância social, como visto acima[42]. Sobre o direito ao respeito à vida privada e familiar, a Convenção menciona que poderá haver ingerência de autoridade pública nos casos de "segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros"[43].

Porém, em setembro de 2018, em importante posicionamento judicial ainda passível de revisão recursal, a Corte Europeia de Direitos Humanos julgou o caso intitulado "Case of Big Brother Watch and Others v. The United Kingdom (*Applications nº. 58170/13, 62322/14 and*

[42] CONSELHO DA EUROPA. *Convênio Europeu de Direitos Humanos de 1950*, p. 11. Disponível em: https://www.echr.coe.int/Documents/Convention_SPA.pdf. Acesso em: 17 abr. 2019.

[43] CONSELHO DA EUROPA. *Convênio Europeu de Direitos Humanos de 1950*, p. 11. Disponível em: https://www.echr.coe.int/Documents/Convention_SPA.pdf. Acesso em: 17 abr. 2019.

24960/15)", proposto por diversas entidades, dentre elas "Big Brother Watch", em desfavor do Reino Unido, sede da GCHQ[44]. Na ocasião, o tribunal ponderou que, embora os programas de vigilância estejam dentro da margem de aplicação dos Estados e justificam-se nas exceções existentes, a forma com que foram e vem sendo desenvolvidos pelas agências de segurança pode violar os direitos fundamentais dos administrados, em razão da falta de supervisão pública do processo de interceptação, da falta de garantias adicionais a setores específicos que podem ser objeto de investigação e da falta de publicidade relacionada aos programas, nos seus limites, já que suas existências foram reveladas sob polêmicas internacionais[45].

Trata-se de um Estado de vigilância, característico da sociedade contemporânea a qual tende a incorporar-se nos mais vários dispositivos, ambientes, setores, refletindo diariamente na vida das pessoas, de forma invisível, desapercebida, não hierárquica, descentralizada, individualizada, personalizada[46]. Essa vigilância contínua e desmedida é, senão a principal, uma das características dessa nova arquitetura social iniciada a partir da Segunda Guerra Mundial e que se aperfeiçoa ao longo dos anos, cujo poder busca, por excelência, modular os indivíduos e as massas para, ao fim e ao cabo, controlar todas as formas de vida nessa sociedade em rede.

1.2 O homem-caramujo: os dados como login na sociedade em rede

Como antes mencionado, as relações de poder dependem das características da arquitetura social nas quais os atores sociais interagem entre

---

[44] UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

[45] UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

[46] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192 f. Dissertação (Mestrado) - Curso de Direito, Departamento do Direito, Universidade Federal de Santa Maria, Santa Maria, 2018, p. 47-60.

si em um determinado contexto histórico. O século XX é marcado por diferentes transformações sociais, culturais e econômicas, a partir das mudanças oriundas da velocidade das relações sociais e das complexidades de ser, especialmente com a proliferação da microeletrônica entremeio a Segunda Guerra Mundial e posteriormente da nanoeletrônica.

1.2.1 A sociedade em rede: novos caminhos na mundialização

Com o desenvolvimento das tecnologias de informação e comunicação, o conceito de rede foi ressignificado, possuindo importante relevância nas relações intersubjetivas, o que inaugurou, inicialmente nos Estados Unidos, porém logo após ao redor do globo, a Era da Informação, conforme Manuel Castells[47]. Todavia, a visualização dos processos por meio de redes não é única e exclusivas das sociedades do século XXI, porque "a rede é uma estrutura comum a qualquer vida; onde quer que vejamos, vemos redes"[48].

Na realidade, a ideia de rede vem sendo utilizada em diversas áreas do conhecimento, adquirindo ressignificação própria, na tentativa de explicar, visualizar e contestar estruturas e processos, sejam biológicos, físicos, espaciais, temporais e sociais. Isso, pois não há como perder de vista que "o novo paradigma pode ser chamado de uma visão de mundo holística que concebe o mundo como um todo integrado e não como uma coleção de partes dissociada"[49]. A evolução das tecnologias da informação e comunicação possibilitou a introdução e remoção de novos atores sociais e processos nas redes, outorgando autonomia e multidirecionalidade necessárias para proporcionar o maior fluxo de comunicação e autoconsciência.

Nessa nova arquitetura social, houve a refundação das fronteiras entre o mundo real-vivo e o mundo virtual-artificial, permitindo-se a

[47] CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura, vol. 3. 3. ed. São Paulo: Paz e Terra. 2002.

[48] CAPRA, Fritjof. *As conexões ocultas*. São Paulo: Cultrix, 2002.

[49] CAPRA, Fritjof. *A Teia da Vida:* uma nova compreensão científica dos sistemas vivos. São Paulo: Cultrix, 1996.

visualização das relações sociais a partir de nós e arestas, devido à horizontalização do processo comunicativo. Para Castells, a sociedade em rede "é aquela cuja estrutura social é composta de redes ativadas por tecnologias digitais de comunicação e informação baseadas em microeletrônica", de modo que "as redes digitais são globais pela sua capacidade para se autoconfigurarem de acordo com as instruções dos programadores, transcendendo os limites territoriais e institucionais através de redes de computadores ligados entre si"[50].

Nesse ínterim, novos atores sociais, novos espaços sociais e novos processos em rede foram desenvolvidos com as inovações trazidas pelas tecnologias de informação e comunicação, conferindo autonomia e multidirecionalidade às relações. Na sociedade em rede, as atividades básicas que configuram e controlam a vida humana em cada canto do planeta estão organizadas em redes globais, afetando todo o mundo, embora não necessariamente todas as pessoas participem nas redes, já que o processo de inclusão e exclusão das redes também faz parte dessa nova arquitetura social, o que, por sua vez, influencia a própria formação da identidade humana[51].

1.2.2 A construção de uma identidade pelo *big data*

Se nas configurações sociais anteriores, o sujeito era identificado, principalmente, por meio de uma assinatura e um número de matrícula ou registro geral; nas novas sociedades, importa a cifra, que é uma senha, uma linguagem numérica de informação e controle, que consegue transformar os indivíduos em dividuais divisíveis e as massas em amostras, mercados, porcentagens[52]. Assim, por meio da cifra, é permitido ou proibido o acesso a determinada informação e é permitida ou proibida determinada comunicação entre atores sociais, já que, por exemplo, pagamentos com cartões de crédito, envio de mensagens, acesso a perfis em

[50] CASTELLS, Manuel. *O poder da comunicação*. São Paulo: Paz e Terra, 2013, p. 59.

[51] CASTELLS, Manuel. *O poder da comunicação*. São Paulo: Paz e Terra, 2013, p. 59.

[52] DELEUZE, Gilles. *Conversações:* 1972-1990. São Paulo: 34, 1992, p. 222.

redes sociais, dentre outras ações, dependem, necessariamente, de uma senha, de um código, de uma identificação peculiar[53].

Importa notar que, para que o indivíduo acesse à informação desejada com base em uma cifra específica utilizada, uma máquina de processamento de dados, fundada em algoritmos, precisa determinar, permitindo ou rejeitando, o processo comunicacional[54]. Então, para além da barreira informacional criada pela própria necessidade de utilização de uma cifra específica para acessar determinados processos comunicacionais, percebe-se que, nesse sentido, as tecnologias de informação e comunicação identificam cada indivíduo, numa modulação universal e matematicamente conhecida, de forma autônoma e automática, fazendo com que a cifra seja relevante e não a pessoa que a utiliza[55].

1.2.3 Quem sou eu?: A criação de perfis através de algoritmos

Torna-se possível, por meio das cifras escolhidas e com base em critérios cartográficos, catalogar dados, manipular informações, rastrear padrões de comportamento, antever ações, reduzindo-se as massas em menores grupos para análise e controle[56]. Dessa forma, pode-se visualizar, por exemplo, grupos de pessoas com determinada condição financeira, específico nicho mercadológico, índice de propensão a alguma doença, gosto por atividade esportiva, orientação sexual, diagnóstico de crédito de algum grupo populacional, monitoramento de transferências de valores, acompanhamento de ligações e conexões entre pessoas e grupos e outros vários exemplos do cotidiano, características dessa nova sociedade, caracterizada pela grandeza do *big data*.

Pode-se dizer que a sociedade em rede cria os seus próprios dispositivos de poder, como, por exemplo, a substituição da assinatura, que, por

---

[53] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 222.

[54] BAUMAN, Zygmunt. *Vida para consumo*. A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 11.

[55] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 223.

[56] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 222.

muitos séculos, foi o principal signo de identidade pessoal pelo código informacional, objetivando-se maior segurança e unicidade[57]. Dessa forma, o indivíduo passa a ser identificado pelos códigos que os sistemas produzem, como nos casos do número da carteira de identidade no registro geral, do número de CPF, do número do passaporte, do número do cartão de correntista bancário, da chave PIX, ou da combinação de números, letras e signos num *username* em determinada rede social, dentre outros exemplos; mas também passa a ser monitorizado e catalogado pelos dados que, consciente ou inconscientemente, produz.

Por outro lado, as técnicas publicitárias, como dispositivos de controle, foram expandidas e aperfeiçoadas em virtude da profusão das tecnologias de informação e comunicação, já que puderam avançar no campo digital e puderam ser direcionadas a uma pluralidade de indivíduos, que a todo momento procuram consumir em diferentes nichos mercadológicos. A publicidade acaba por envolver os sujeitos numa nova lógica consumerista, baseada num mercado de informações e comportamentos, já que os dados pessoais coletados e monitorados pelas empresas com fins comerciais possibilitam uma mercadotécnica especial, direcional e colaborativa [58].

Ademais, através desse rastreamento de informações e cruzamento de dados, é factível modular grupos de controle e forjar identidades, determinando-se o que precisa, quanto precisa e como precisa ser consumido, em um verdadeiro processo de subjetivação contínua[59]. Esse consumismo, marcado pela insatisfação perpétua do consumidor, já que sempre há algo melhor e mais novo para consumir, e pela lógica da exclusão social, já que se não há o consumo de determinados bens e serviços não se participa da vida social, acaba afetando a dignidade do indivíduo e o escraviza, porque "aposta na irracionalidade dos consumidores, e não

---

[57] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 222.

[58] BAUMAN, Zygmunt. *Vida para consumo*. A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 20.

[59] BAUMAN, Zygmunt. *Vida para consumo*. A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 20.

'suas estimativas sóbrias e bem informadas; estimula emoções consumistas e não cultiva a razão"[60].

1.2.4 O panóptico está vivo: o pós-panóptico, o banóptico e o sinóptico

Denota-se, assim, um controle sobre a população, como um todo objeto, não mais somente caracterizado por pessoas singulares, mas por dados informacionais multiplicados e multiplicáveis, de tal modo que é possível sujeitar esse corpo social a um processo de subjetivação e modulação contínua da identidade na sociedade em rede. Vê-se que o poder é disseminado por todas as formas de vida num *sem-tempo* e num *sem-espaço*, em razão da ausência das barreiras e limites físicos, possibilitando a atuação de dispositivos específicos, dentre eles a vigilância dos dados pessoais, o que torna necessário repensar a própria noção do panóptico na nova arquitetura social.

Vive-se, pois, um pós-panóptico, com o prefixo sugerido por Bauman, considerando o melhoramento e recrudescimento das tecnologias de vigilância, de forma que o panoptismo "está vivo e bem de saúde, na verdade, armado de músculos (eletronicamente reforçados, ciborguizados) tão poderosos que Bentham, ou mesmo Foucault, não conseguiria nem tentaria imaginá-lo"[61]. O pós-panóptico, com novas formas de vigilância e de panoptismo possibilitadas pelas inovações tecnológicas, remete-se à uma vigilância líquida, fundamentada na fluidez das relações entre sujeitos e instituições, permitindo a volatilidade do olhar vigilante, microcapilarizado em diferentes dispositivos informáticos[62].

Aliado a isso, o banóptico, sugerido Didier Bigo, com base na ideia de segurança nacional, refere que as tecnologias de informação e comunicação ajudam na elaboração de perfis de indivíduos, definindo quem deve

---

[60] BAUMAN, Zygmunt. *Vida para consumo*. A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 65.

[61] BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 22.

[62] BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 22-23.

ser colocado sob vigilância pelos agentes de segurança e estabelecendo quem está do lado de dentro e quem está do lado de fora[63]. Tais dispositivos estão alocados nas entradas dos espaços comunitários, não apenas em termos internacionais, como fronteiras viárias ou aeroportos, mas também domésticos, em *shopping centers,* supermercados e outros departamentos constantemente vigiados, confinando quem está do lado de dentro e excluindo que está do lado de fora[64].

1.2.5 O homem-caramujo: a vigilância pessoal

Por fim, o sinóptico inverte o vetor de vigilância, fazendo com que muitos observem a poucos, a partir do fato que se espera que os próprios sujeitos e objetos de vigilância se autodisciplinem e paguem pelos custos materiais e psíquicos dessa disciplina, de forma a exercer sobre si mesmo e sobre os outros um controle contínuo[65]. Acontece, assim, uma distribuição de minipanópticos, representados pelo tipo *do it yourself,* onde, por meio de dispositivos móveis e portáteis, fornecidos comercialmente, os usuários, através de inúmeras ações, vigiam a todos a todo momento, numa servidão contemporânea desse regime de vigilância[66].

Diante desse cenário, Bauman traz a ideia do homem-caramujo, que carrega, em sua concha, um panoptismo pessoal, possibilitando uma autovigilância e a vigilância do outro, numa metodologia mais econômica e popular que o panoptismo clássico[67]. Cada sujeito, empreendedor de si mesmo, transporta, consigo, dispositivos de controle, sujeitando-se ao mesmo tempo em que sujeita os outros, numa retroalimentação de dados, de tal maneira que a vigilância não é imposta verticalmente por poderes

---

[63] BIGO, Didier; TSOUKALA, Anastassia. *Terror, insecurity and liberty:* illiberal practices of liberal regimes after 9/11. New York: Routledge, 2008.

[64] BIGO, Didier; TSOUKALA, Anastassia. *Terror, insecurity and liberty:* illiberal practices of liberal regimes after 9/11. New York: Routledge, 2008.

[65] BAUMAN, Zygmunt. *Vigilância líquida***:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 26.

[66] BAUMAN, Zygmunt. *Vigilância líquida***:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 26.

[67] BAUMAN, Zygmunt. *Vigilância líquida***:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 22-23.

hegemônicos, mas exsurge do próprio indivíduo, que, não necessariamente consciente, vê-se obrigado a consumir uma autovigilância e uma vigilância dos demais para poder pertencer à sociedade em rede e produz, novamente não necessariamente consciente, um infinito número de dados pessoais.

1.2.6 Os dados: da Internet das Coisas à Internet de Tudo

No século XXI, essa questão assume especial relevância se considerado o avanço das tecnologias de informação e comunicação, como o uso da identificação por radiofrequência (RFID), do *Quick Response Code* (QRCode) e da rede de sensores sem fio (RSSF), sendo revolucionada a comunicação máquina-a-máquina (*machine to machine,* em inglês, ou pelo acrônimo *M2M).* No estágio atual, na Internet das Coisas (*Internet of Things,* em inglês, ou pelo acrônimo *IoT),* é possível a interconexão digital dos objetos através da internet, formando uma rede inteligente de coisas à disposição dos usuários, de onde derivam conceitos como *smart things*, *smart home, smart cities,* dentre outros.

Nesse cenário, inúmeras coisas que circundam o usuário são configuradas e conectadas à internet, captando, monitorando e processando dados para um bom funcionamento. Dessa forma, o indivíduo pode, por meio da rede mundial de computadores e dispositivos inteligentes, controlar remotamente tais objetos ou permitir com que provedores de serviços utilizem tais objetos para uma determinada função, o que gera um leque de oportunidades e desafios no campo tecnossocial[68]. Verifica-se que a *IoT*, embora possa ser melhor expandida com o advento de melhores protocolos de internet, já é uma realidade social, inscrita, inclusive, como técnica de publicidade para consumo de dispositivos[69].

---

[68] BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything: A $4.6 trillion public-sector opportunity.* San Jose: Cisco. 2013. Disponível em: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf. Acesso em: 21 abr. 2019.

[69] BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything: A $4.6 trillion public-sector opportunity.* San Jose: Cisco. 2013. Disponível em: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf. Acesso em: 21 abr. 2019.

Avançando nesse panorama, segundo alguns especialistas na área, chegar-se-á à Internet de Tudo (*Internet of Everything,* em inglês, ou pelo acrônimo *IoE*), onde haverá um fluxo contínuo e inimaginavelmente imenso de conexões entre pessoas, processos, dados e coisas, abarcando todo o ecossistema de conectividade em torno de um universo comum[70]. Ocorre que, neste caso, as informações que circulam pela internet não serão colocadas na rede por pessoas, mas por sensores e objetos que trocam dados entre si, possivelmente o tempo todo, gerando incontáveis valores diários ou combinações, para experiências *indoors* ou *outdoors*[71].

Basicamente, os dados pessoais coletados servem como mecanismo de estatísticas, de acesso a conteúdo, de personalização de experiência ou para utilização de um produto ou serviço pelo usuário, sendo fundamentais em termos de navegação eletrônica e comércio eletrônico. Primeiramente, ao navegar na rede, algumas informações que são transmitidas automaticamente entre dispositivos são coletadas como exigências tecnológicas vinculadas à navegação, para fins estatísticos, como nome de domínio de internet, o endereço IP, tipo de navegador e de sistema operacional, data, local e hora, dentre outras, a fim de que o servidor transmita as informações compatíveis com o equipamento do usuário.

Além disso, algumas informações pessoais são obtidas quando do registro em determinas páginas, através de formulário de cadastro, como nome, endereço de e-mail e outras informações pessoais, cuja exatidão podem cada vez mais melhorar a personalização da experiência do usuário. Essas informações coletadas, juntamente com as informações estatísticas, são utilizadas para personalizar um conteúdo e/ou serviços disponibilizados, desde a personalização do acesso à própria página até o oferecimento de conteúdos, produtos e serviços que possuem relação com o perfil que é criado com os dados do usuário.

---

[70] BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything: A $4.6 trillion public-sector opportunity.* San Jose: Cisco. 2013. Disponível em: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf. Acesso em: 21 abr. 2019.

[71] BAJARIN, Tim. *The next big thinh of tech:* the Internet of Everything. [Time, 13/01/2014] Disponível em: http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/. Acesso em: 21 abr. 2019.

Não raras vezes (e, aqui, entra todo uma questão de consentimento e legalidade), as informações pessoais individuais são comercializadas ou fornecidas a terceiros, como parceiros, patrocinadores, anunciantes ou outras empresas externas, a fim de criar nichos mercadológicos e perfis de consumidores para futuras ofertas, propagandas ou outros tipos de comunicações. Nesse mesmo sentido, muitas vezes é concedida a permissão para que determinadas páginas coletem periodicamente informações pessoais do usuário a partir de instituições afiliadas, parceiros de negócios e outras fontes de terceiros independentes, adicionando ao perfil criado do indivíduo, como, muito comum, coleta de dados oriundos de redes sociais.

1.2.7 O fornecimento de dados como condição de acesso à sociedade em rede

As redes sociais ou plataformas de interação social são uma das principais razões pelas quais bilhões de usuários navegam pela rede diariamente, como *Facebook, YouTube, WhatsApp, Messenger, Instagram, Twitter, LinkedIn, Snapchat, Viber, Pinterest, Telegram, Tumblr, Reddit,* dentre inúmeras outras, já que, a partir delas, é possível criar infinitas conexões entre pessoas, empresas e instituições ao redor mundo, sendo, portanto, um dos maiores arcabouços de coleta e armazenamento de dados pessoais. Porém, embora o cadastro, acesso e funcionamento da rede social seja, na maioria das vezes, gratuito, pelo ponto de vista do indivíduo, depende do fornecimento de dados pessoais à plataforma, o que serve como mecanismo de lucro na criação de espaços publicitários nessas aplicações.

Outro mecanismo importante da navegação em rede é a utilização de *cookies,* pequeno pacote de dados que, quando um usuário visita pela primeira vez um site, recebe do navegador para armazenamento de informações, de forma que, sempre que o usuário revisite tal página, o navegador devolve o *cookie* ao servidor para lembrar atividades anteriores

do usuário. A utilização de *cookies* proporciona, numa primeira visão, conteúdos, produtos e serviços diferenciados e personalizados, a partir do momento em que é possível lembrar do usuário a cada acesso, reconhecer hábitos de navegação, calcular dimensão de audiência e de visualização de páginas, facilitar o preenchimento de formulários, dentre outras ações, que parecem facilitar o consumo por parte do usuário.

Essas questões, usualmente, são esclarecidas nas políticas de privacidade, nas políticas de *cookies,* nos termos e condições de uso de produto e serviço e noutros documentos vinculativos, os quais o usuário deve ler e concordar com as condições previstas para permitir o acesso ao conteúdo desejado. Ocorre que, na maior parte das vezes, esses documentos são verdadeiros contratos de adesão, que, conforme a melhor doutrina, são caracterizados pela impossibilidade de discussão ou modificação de cláusulas pelo aderente, devendo este sujeitar-se às imposições deixadas pelo proponente.

Ademais disso, é muito comum que esses termos e condições de uso de determinados aplicativos e plataformas sejam largos e complicados, compostos por inúmeros documentos diferentes e diversas páginas de palavras difíceis e complexas, seja no campo informacional ou jurídico. E, como sabido, a concordância com esses documentos, exteriorizada por meio de um mero clique numa caixa de seleção ou um botão específico, é condicionante à navegação do usuário em determinada aplicação ou plataforma, fazendo com que o indivíduo se vincule a direitos e obrigações que não necessariamente possua a total ciência das implicações daí derivadas.

Isso ocorre especialmente com as permissões que o usuário concede a determinadas aplicações, muitas vezes sem, de fato, saber o que está permitindo, como possibilitando que a plataforma, quando queira, sem necessariamente explicitar que o está fazendo, acesse o calendário, a câmera, a lista de contatos, os sensores, o microfone, as SMS, o armazenamento, a localização, o *bluetooth*, o status da rede, instalar *packages,* utilizar sincronização de dados, gerencie processos de fundo,

habilitar e desabilitar *keyguard* (informações da tela de bloqueio, como senhas, padrões, sensores biométricos e faciais), modificar configurações do dispositivo, transferir infravermelho, utilizar *NFC*, dentre outras ações possíveis[72], que podem implicar em inúmeros novos riscos ao usuário e à proteção dos dados pessoais. A exemplo disso, tem-se o *software* Alphonso, utilizado por diferentes aplicações, que, uma vez permitido pelo usuário, capta dados a partir do microfone do telefone celular sobre hábitos de consumo televisivo ou outros áudios de fundo para fornecimento a anunciantes para que estes ofertem produtos e serviços personalizados ao indivíduo[73].

1.2.8 Os ataques maliciosos e riscos à autonomia informacional

Contudo, não necessariamente, o acesso ao microfone e à câmera, por exemplo, acontece sob o prisma de uma permissão do usuário, pois pode ocorrer por causa de ataques maliciosos dirigidos aos usuários, inclusive por parte de agências governamentais, como revelado pelo portal *Wikileaks* de que a CIA e o FBI, agências de investigação estadunidense, acessavam remotamente essas saídas de áudio e vídeo de *persons of interest*[74] (daí, porque uma fotografia publicada pelo CEO da *Facebook Inc.*, companhia dona da rede social Instagram, viralizou na rede não pelo fato de esta rede social haver alcançado meio bilhão de usuários, mas pelo uso das fitas adesivas para cobrir a câmera e o microfone do seu computador portátil)[75].

---

[72] DAUER, Stella. *Entenda tudo sobre as permissões de aplicativos e proteja seu Android.* Disponível em: https://www.androidpit.com.br/permissoes-aplicativos. Acesso em: 22 abr. 2019.

[73] BLASCO, Lucía. *Cuán cierto es que las empresas usan el micrófono de tu teléfono para escucharte y qué hacer al respecto*. [BBC News, 05/07/2018] Disponível em: https://www.bbc.com/mundo/noticias-44724389. Acesso em: 22 abr. 2019.

[74] PHAM, Sherisse. *WikiLeaks dice que la CIA espía a través celulares y televisores, ¿qué tan preocupado debes estar?* [CNN, 08/03/2017] Disponível em: https://cnnespanol.cnn.com/2017/03/08/wikileaks-dice-que-la-cia-espia-a-traves-de-smartphones-televisores-y-mas-que-tan-preocupado-debes-estar/. Acesso em: 22 abr. 2019.

[75] RODRÍGUEZ-PINA, Gloria. *El método nada tecnológico que usa Mark Zuckerberg para protegerse de los hackers.* [El País, 22/06/2016] Disponível em: https://verne.elpais.com/verne/2016/06/22/articulo/1466617774_991020.html. Acesso em: 22 abr. 2019.

Assim, percebe-se, seja no estado atual das coisas, seja em previsões futurísticas, seja no campo interpessoal, social, econômico, industrial ou político, os dados pessoais são o principal dispositivo dessa nova arquitetura social, sob o argumento de uma necessidade de personalização única e aproveitamento máximo das experiências de vida. O indivíduo deixa de ser somente uma representação corpórea, exteriorizada por sua aparência, falas, ideias e atos, mas passa a ser identificado, monitorizado, qualificado e controlado devido ao conjunto de grandezas informacionais produzidas a todo momento e a todo lugar, não necessariamente de forma consciente, sendo os dados pessoais o *login* dessa sociedade em rede.

Em que pese a proteção necessária que esses dados pressupõem pelas próprias razões de existirem, houve, nos últimos anos, grandes vazamentos de dados que causaram desconfortos internacionais, sejam em virtude de ataques deliberados contra sistemas de informação, sejam bancos de dados esquecidos por empresas de segurança, sejam transferências e/ou compra-e-venda de informações entre corporações e agências estatais. De acordo com um relatório da Avast, os dez piores vazamentos de dados de 2018, envolveram, o menos pior, trinta e sete milhões de usuários, e, o mais grave, um bilhão de pessoas[76].

Em abril de 2018, o The New York Times revelou que, em 2013, os dados de, pelo menos, 30 (trinta) milhões de usuários do Facebook – há notícia de que, em verdade, o número de atingidos supera a 87 (oitenta e sete) milhões – foram indevidamente compartilhados com a empresa de consultoria *Cambridge Analytic*a, que prestou serviços durante a campanha eleitoral dos Estados Unidos ao Presidente Donald Trump, o que pode ter comprometido a lisura do pleito, já que o candidato, à época, teve acesso a diversos dados pessoais, como nomes, gênero, idade, local de residência e os resultados de personalidade projetados pelo *quizz* realizado

[76] HRON, Martin. *Os últimos 10 maiores vazamentos de dados.* [Avast, 14/02/2019] Disponível em: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados. Acesso em: 21 abr. 2019.

pelos usuários, bem como interesses e dados mais elementares da conta, como e-mail ou data de nascimento[77].

A reportagem fez eclodir um escândalo acerca do tratamento e gerenciamento de dados pessoais na rede, especialmente após o CEO da *Facebook Inc.*, Mark Zuckerberg, admitir que a maioria dos quase 2 (dois) bilhões de usuários podem ter tido os dados pessoais acessados de forma indiscriminada. Zuckerberg manifestou que o aplicativo iria tomar mais cuidado, embora o modelo de negócio da ferramenta se baseie na troca de informação com outras empresas para publicidade. Em seguida, o criador da rede social foi chamado para depor e se explicar perante o Congresso dos Estados Unidos, que cobrou responsabilidades e novas políticas de proteção[78].

Ainda assim, novas investigações revelaram que a rede social em comento deu permissão especial a mais de 150 (cento e cinquenta) empresas, dentre elas *Apple, Amazon, Microsoft, Netflix* e *Spotify*, plataformas conhecidas do público, para acessar dados de amigos dos usuários e para ver mensagens privadas das pessoas, embora negado veementemente[79]. Tratam-se de acordos firmados em outra época, quando a rede social tentava expandir rapidamente com a ajuda de uma personalização instantânea para integrar os usuários, que, em muitos casos, seguem valendo, em que pese haver a suposta necessidade de adquirir o consentimento do usuário para tanto, o que novamente traz à tona a questão do consumo da rede[80].

---

[77] CADWALLADR, Carole; CONFESSORE, Nicholas; ROSENBERG, Matthew. *How Trump Consultants Exploited the Facebook Data of Millions*. [The New York Times, 17/03/2018]. Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Acesso em: 21 abr. 2019.

[78] MARS, Amanda. *Zuckerberg pide perdón en el Senado y advierte de la amenaza de Rusia*. [El País, 11/04/2018]. Disponível em: https://elpais.com/internacional/2018/04/10/actualidad/1523380980_341139.html. Acesso em: 21 abr. 2019.

[79] COLOMÉ, Jordi Pérez. *Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas.* [El País, 20/12/2018] Disponível em: https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html. Acesso em: 21 abr. 2019.

[80] COLOMÉ, Jordi Pérez. *Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas.* [El País, 20/12/2018] Disponível em: https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html. Acesso em: 21 abr. 2019.

1.2.9 Perspectivas de futuro: a economia de vigilância

Diante de todas as notícias de existência de programas de vigilância em massa por parte de agências de segurança estatais e de vazamento de dados pessoais dos usuários, percebe-se um cenário de monitorização real dos processos comunicativos em escala mundial, com uma insuficiência, proposital ou não, de medidas de segurança para proteger o usuário desses novos riscos, que, por sua vez, encontra-se em absoluta passividade frente às tecnologias disruptivas. E mais: o indivíduo acaba contribuindo ainda mais com as engrenagens desse sistema, porque se vê obrigado a consumir essas tecnologias de informação e comunicação para participar efetivamente da sociedade em rede.

Depara-se, então, com um determinismo tecnossocial numa releitura da formação do próprio Estado, porém, agora, como um Estado-vigilante. Em outras palavras, parece que o indivíduo, por medo do terror e de outros inimigos, abre mão das próprias liberdades em favor de um ente, abstratamente maior que todos, que garanta uma segurança desejada, chancelando programas de vigilância em massa de combate ao terrorismo. Nessa mesma linha de pensamento, o indivíduo, querendo fazer parte da sociedade, submete-se à cultura do consumo, conscientemente ou não, não se importando de autorizar a monitorização e manipulação dos dados pessoais coletados, já que o custo-benefício de ser excluído da rede, caso não entregue os dados, não compensa nesse novo ambiente digital.

De um lado, agências estatais promovem programas de vigilância em massa de nacionais e estrangeiros, por meio da monitorização e avaliação do tráfego de dados ao redor do globo; de outro lado, indivíduos consomem, a todo momento, produtos e serviços que geram dados de toda ordem, sobre si e sobre outras pessoas; entremeio a isso, grandes corporações cooperam com a atuação das agências de segurança, transmitindo dados ou permitindo o acesso a eles, inventam novos produtos e serviços tecnológicos, oferecendo para consumo de todos, inclusive com obsolescência planejada, bem como colaboram com outras grandes corporações

num mercado mundial para compra-e-venda e transferência de dados de usuários.

Assim, impera uma economia de vigilância, em que os dados dos usuários adquirem valor de mercado e baseiam a criação e o desenvolvimento de produtos e serviços, públicos e privados, em um sem número de interações, competições e cooperações, entre diferentes atores sociais. Numa sociedade em rede, por sua própria arquitetura informacional, o processamento de dados produzidos nos processos comunicativos torna-se o novo ouro do século XXI, de forma que, num Estado geral de vigilância, faz-se necessário analisar essa nova arquitetura social, sob o prisma dos direitos e garantias humanas e fundamentais dos indivíduos, especialmente do direito à privacidade.

2

"1984 *all over again*": o direito à privacidade na era digital

O título do presente capítulo faz referência a que o mundo descrito na obra "1984", de George Orwell, está acontecendo novamente, veio à tona de novo, embora seja um cenário fictício de sociedade distópica imaginado em 1949. Por um lado, depara-se com um regime global de vigilância social, marcado pela interceptação de dados pessoais e pelo monitoramento dos processos comunicativos entre cidadãos, empresas, órgãos públicos e outros países, à diferença de que não há um Partido definido, porque a vigilância e o controle social estão espalhados e aperfeiçoados com o avanço tecnológico da sociedade em rede.

Por outro lado, assim como as teletelas, televisores bidirecionais que funcionavam ao mesmo tempo como emissores de mensagens oficiais e como câmera de monitoramento e estavam em todas as residências do país, as tecnologias de informação e comunicação, especialmente aquelas equipadas com internet, estão espalhadas por todos os cantos do mundo, permitindo com que os cidadãos interajam um com os outros, mas também forneçam dados pessoais para acessar produtos e serviços variados. Assim, a privacidade, como antes conhecida, parece ser cada vez mais uma memória de um passado distante, tais como eram as recordações dos tempos antes do governo do Grande Irmão.

Considerando que o objetivo geral desse livro é analisar os impactos das tecnologias de informação e comunicação e do regime global de vigilância social no direito à privacidade, no contexto da cibersegurança do século XXI, este capítulo, após a análise realizada anteriormente sobre o

regime global de vigilância social, pretende: a) pesquisar a estrutura normativa global e regional do direito à privacidade, mudança e abordagens do conceito ao longo do tempo; e, por fim, b) discutir a ressignificação do direito à privacidade, baseada em novos conceitos, novos espaços, novos limites e novas possibilidades no contexto da cibersegurança.

2.1 A privacidade como a conhecemos: a (r)evolução de um conceito no quadro normativo

Os marcos normativos de direitos humanos e os ordenamentos jurídicos nacionais reconhecem o direito à privacidade, em suas diferentes nuances, como o direito à intimidade ou como o direito à vida privada, elevando-o à categoria de direito humano. Ainda que a motivação legal guarde estrita relação com o desenvolvimento da *mass media*, os avanços tecnológicos produzidos desde a metade do século XX exigem adaptações às recentes necessidades e novas interpretações jurídicas, especialmente no campo de tutela da personalidade.

2.1.1 Breve considerações sobre o conceito de privacidade na história

Para conceituar a privacidade e, especificamente, o direito à privacidade, faz-se necessário retornar à distinção entre privado e público na antiguidade clássica grega – trespassada à cultura romana posteriormente -, onde havia o *oikos*, espaço particular dos indivíduos, e a *pólis*, espaço comum aos cidadãos livres[1]. Nesse sentido, o cidadão precisava de uma esfera privada e ter um "lugar que lhe pertencesse" para poder receber uma segunda vida, *bio politikos,* e participar da esfera pública, onde, neste local, não tratava do que lhe era próprio, *idion,* mas do que lhe era comum, *konion,* de modo que a diferença, num primeiro momento, de privado e público era o âmbito familiar e o âmbito político[2].

[1] ARENDT, Hannah. *A condição humana.* 10 ed. Rio de Janeiro: Forense Universitária, 2005, p. 33.

[2] ARENDT, Hannah. *A condição humana.* 10 ed. Rio de Janeiro: Forense Universitária, 2005, p. 38-39.

Na Idade Média, séculos depois, urgiu, cada vez mais, a necessidade de isolamento em um espaço privado em detrimento daquilo que era comum e girasse em torno do espaço público, tornando-se a casa o local ideal de separação entre essas esferas e o novo centro de poder político, tanto que dinastias começam a ser vinculadas a casas, sobrenomes[3]. Com o declínio da economia feudal e o surgimento da burguesia, o desejo pela individualidade foi aumentado exponencialmente, havendo o burguês ocupado espaços, acumulado riquezas, levantado barreiras, de modo que a busca pela proteção de um local somente seu fortaleceu a noção daquilo que é privado, embora houvesse estrita relação com o direito à propriedade[4].

Essa questão assumiu especial relevância no marco filosófico do liberalismo, em particular na obra de John Locke, considerado o pai do liberalismo, quando este defendeu "la existencia de una esfera de libertad natural a todo sujeto, espacio que debe ser impermeable a la coactividad que despliega la ley civil", de modo que "la 'privacy' es considerada la propiedad más sagrada de la persona humana, pues todo hombre tiene una propriedade em su propia persona"[5]. Em sentido parecido, John Stuart Mill sustentou que as condutas humanas passíveis de análise eram aquelas que produziam deveres e obrigações sociais, quando afetassem a terceiros, de maneira que os aspectos que dizem somente ao indivíduo, isto é, as características privadas, são independentes da esfera pública, sendo o sujeito soberano sobre si[6].

2.1.2 O direito à privacidade desde uma perspectiva jurídica

Como categoria analítica e autônoma de ponderação, o direito à privacidade é uma construção recente estadunidense. Samuel Warren,

[3] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 125.

[4] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 26.

[5] TARODO, Salvador Tarodo. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: *Derecho y Salud*, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006, p. 136.

[6] MILL, John Stuart. *A liberdade.*São Paulo: Martins Fontes, 2000.

motivado por fatos íntimos do casamento de sua filha divulgados por jornais, e Louis Brandeis publicaram, em 1890, um artigo sobre o *right to privacy* (direito à privacidade), inspirado na expressão cunhada por Thomas McIntyre Cooley, *right to be let alone* (direito de ser deixado só), com base nas necessidades da burguesia norte-americana do final do século XIX[7]. A doutrina de Warren e Brandeis, então, distancia o direito à privacidade da necessidade de proteção da propriedade e aproxima da necessidade de proteção da vida privada, em termos relacionados à personalidade humana[8].

Os autores referem que recentes inovações dão azo a um novo nível de proteção da personalidade humana e da segurança do cidadão norte-americano, já que as novas tecnologias de comunicação, as máquinas, as fotografias instantâneas, as empresas de fofocas, dentre outras, acabaram por invadir o privado espaço do lar, porém o indivíduo tem o direito de estar só, ou melhor, o direito de ser deixado só[9]. Trata-se de uma proteção que vai além da tutela do material que contenha uma determinada revelação íntima, mas atinge substancialmente a própria informação, possuindo a pessoa o direito de ser deixada em paz e não tornar aquilo que é privado em público[10].

Essa construção doutrinária vai ganhando força nos ordenamentos jurídicos nacionais com o passar dos anos, de forma que, a partir do desenvolvimento das tecnologias de informação e comunicação e a globalização das relações sociais ao longo do século XX, o direito à privacidade, antes tido como inerente aos direitos da personalidade, passa a ser tratado como um direito de natureza humana e fundamental. Trata-se, em apertada síntese, do direito de cada um de garantir uma paz, uma

---

[7] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. Disponível em: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm. Acesso em; 16 abr. 2019.

[8] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. Disponível em: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm. Acesso em; 16 abr. 2019.

[9] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. Disponível em: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm. Acesso em; 16 abr. 2019.

[10] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. Disponível em: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm. Acesso em; 16 abr. 2019.

tranquilidade, uma reserva de parte de sua vida que não esteja afetada por uma atividade pública; ou de evitar que fatos de sua vida que são entendidos privados sejam expostos, devendo o Estado abster-se de interferir indevidamente em tal âmbito de cada indivíduo e, inclusive, proibir a ingerência também de terceiros.

Na esfera social, as pessoas passam a maior parte do tempo, interagindo umas com as outras, devida à necessidade de ganhar a vida, seguir uma vocação, aliar-se a outros com os mesmos interesses ou negócios; enquanto que na esfera da vida íntima, com base no princípio da exclusividade formulado por Hannah Arendt, por sua vez, inspirado em Kant, as pessoas escolhem aqueles com os quais querem viver, compartilhar momentos, fatos, informações, estando intrinsicamente ligada à pessoa em sua singularidade[11]. O direito à privacidade é, nessa concepção, regido por três atributos, quais sejam, a solidão, o direito de estar só; o segredo, o direito de exigir sigilo; e a autonomia, o direito de decidir sobre si mesmo.

2.1.2 O direito à privacidade e figuras afins

A ideia de categorização do direito à privacidade é complexa e eivada de críticas, uma vez que o termo pode derivar inúmeros outros conceitos, como "vida privada", "intimidade", "sigilo das correspondências", "sigilo das comunicações", "inviolabilidade do domicílio", "sigilo da fonte", "direito à imagem", "direito à honra", "proteção de dados pessoais", dentre outros. Essa significação vai depender do sujeito, do ordenamento jurídico e do contexto abordado, uma vez que, conforme a fluidez dos conteúdos, existe a possibilidade de migração de conceitos, podendo se considerar o direito à privacidade como um gênero abarcando diversos conteúdos.

Porém, importante distinção recai sobre o direito à vida privada e o direito à intimidade, já que tais expressões são utilizadas em alguns ordenamentos jurídicos. Dentro do direito à privacidade, o direito à vida

[11] ARENDT, Hannah. Reflections on Little-Rock. *Dissent Magazine*, v. 6, n. 1, inverno, 1959, p. 52-53.

privada pode ser considerado como a tutela da vida pessoal e familiar do sujeito, bem como do círculo próximo da pessoa, entre a intimidade e a vida social do indivíduo, local em que este pratica os atos jurídicos privados e onde se desenvolve as interações relevantes aos seres humanos[12]. Isto é, a vida privada da pessoa são as relações de proximidade emocional, que podem ser de conhecimento daqueles que estão próximos e foram escolhidos para saber e participar dessa singularidade.

Por outro lado, o direito à intimidade pode ser definido como aquele que intenta assegurar as pessoas frente aos sentidos de outras, na medida em que pretende excluir do conhecimento alheio algo sobre si, sobre seu núcleo essencial como pessoa, sobre seu espaço mais reservado de existência, ou proibir que outros se imiscuam nessa esfera mais particular[13]. A intimidade pode, assim, guardar relação com as informações do âmbito exclusivo de uma pessoa, o qual ela reserva para si mesmo, afastando de qualquer repercussão social e, querendo, do alcance da vida privada, podendo, no entanto, decidir sobre concessões nesse espaço.

Num primeiro momento, a doutrina alemã da teoria das esferas serviu como embasamento para representar os níveis de privacidade. Partindo-se da ideia de círculos concêntricos, o primeiro, mais amplo, é a esfera da vida privada (*Privatsphäre*), onde estão as informações que o sujeito não quer que sejam de domínio público; o segundo, no interior, menor, é a esfera da intimidade (*Vertrauensphäre*), onde estão as informações que o sujeito confidencia somente a certas pessoas, em caráter reservado; e o terceiro, mais ainda no interior, é a esfera do segredo (*Geheimnsphäre*), onde estão as informações que o sujeito não compartilha com ninguém ou somente com algumas pessoas[14].

Essa teoria acabou perdendo credibilidade, por considerar o indivíduo uma "pessoa como uma cebola passiva", sendo superada, em razão da

[12] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

[13] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

[14] HUBMANN, Heinrich. *Das persönlichkeitsrecht*. Münster: Böhlau-Verlag, 1953 *apud* COSTA JR. Paulo José da. *O direito de estar só:* tutela penal da intimidade. 2. ed. São Paulo: RT, 1995, p. 30-36.

insuficiência técnica, da necessidade de subjetivismo quanto ao grau das esferas e das recentes inovações tecnológicas[15]. No lugar dela, advém a teoria do mosaico, sustentando que as informações, *a priori,* podem ser irrelevantes sob determinado prisma ou se consideradas isoladas, porém, se analisadas com outras informações, às vezes também irrelevantes por si só, podem servir para formar uma conjuntura plena de significado, de modo que a proteção da privacidade deve levar em consideração o mosaico possível de formação e revelação com referidos dados[16].

2.1.4 O direito à privacidade nos textos normativos

Embora o direito à privacidade tenha sido uma construção inicialmente doutrinária e depois utilizada em alguns precedentes jurisprudenciais, logo essa tutela passou a ser inserida nas cartas positivas de direitos humanos e nos ordenamentos jurídicos comunitários e nacionais. No entanto, como é notável e como foi discutido anteriormente, o direito à privacidade, nesses marcos normativos, aparece sob diversas formas, por vezes como privacidade em sentido estrito, às vezes como vida privada, outras vezes como intimidade, porém percebe-se a intenção das nações e, em determinadas ocasiões, das organizações supranacionais, em tutelar esse aspecto privado do ser humano.

2.1.4.1 Marco normativo universal, internacional e regional

Nota-se que a Declaração dos Direitos do Homem e do Cidadão de 1789 já continha ideias embrionárias dessa proteção, quando cita, no art. 10, que "ninguém deve ser incomodado por suas opiniões, inclusive religiosas, sempre e quando sua manifestação não perturba a ordem pública

---

[15] BURKERT, 2000, p. 46 *apud* DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. *Âmbito Jurídico*, Rio Grande, XI, n. 51, mar. 2008. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460. Acesso em: 16 abr. 2019.

[16] CONESA, Fulgencio Madrid. *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia, 1984, p. 45.

estabelecida pela Lei" [tradução nossa] e, no art. 11, que "[...] qualquer Cidadão pode falar, escrever e imprimir livremente, sempre e quando responda pelo abuso desta liberdade nos casos determinados pela Lei" [tradução nossa][17].

Expressamente, o direito à vida privada aparece, mundialmente, reconhecido na Declaração Universal dos Direitos do Homem de 1948, no âmbito da Assembleia Geral das Nações Unidas, ao estabelecer, como direito fundamental no art. 12, que "ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação" e "que toda pessoa tem direito à proteção da lei contra tais ingerências" [tradução nossa][18].

Por outro lado, na esfera americana, a Declaração Americana dos Direitos e Deveres do Homem de 1948 foi também um dos primeiros instrumentos normativos a tratar do tema, quando, no art. V, alude que "toda pessoa tem direito à proteção da Lei contra os ataques abusivos a sua honra, a sua reputação e a sua vida privada e familiar" [tradução nossa][19]. Mais tarde, a Convenção Americana de Direitos Humanos de 1969 dita, no art. 11, sobre proteção da honra e dignidade, que "ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ataques ilegais a sua honra ou reputação" [tradução nossa][20].

No âmbito europeu, a Convenção Europeia dos Direitos do Homem de 1950, refere, no art. 8.1, que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua

---

[17] FRANÇA. *Déclaration des Droits de l'Homme et du Citoyen de 1789*. Disponível em: https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789. Acesso em: 17 abr. 2019.

[18] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal de Direitos Humanos de 1948*. Disponível em: https://www.un.org/es/universal-declaration-human-rights/. Acesso em: 17 abr. 2019.

[19] ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Declaração Americana dos Direitos e Deveres do Homem de 1948*. Disponível em: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp. Acesso em: 17 abr. 2019.

[20] ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica) de 1969*. Disponível em: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm. Acesso em: 17 abr. 2019.

correspondência"[21]. Ainda, nesse mesmo sentido, a Carta dos Direitos Fundamentais da União Europeia de 2000, menciona, no art. 7, que "todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações"[22].

Já no âmbito africano, a Organização para a Unidade Africana, quando aprovou a Carta Africana Sobre os Direitos Humanos e dos Povos, depois ratificada pela Unidade Africana, embora não escreva diretamente sobre a privacidade, refere, no art. 4, que "todo ser humano terá o direito ao respeito de sua vida e da integridade de sua pessoa" [tradução nossa][23]. Ainda, a Carta Árabe sobre Direitos Humanos de 2004, documento advindo da Liga Árabe, cita, no art. 21, que "ninguém será submetido a ingerências arbitrarias ou ilegais a respeito da sua privacidade, família, domicílio ou correspondência, nem a ataques ilegais a sua honra ou reputação" [tradução nossa][24].

Especificamente, a Declaração dos Direitos Humanos no Islã de 1990, documento oriundo da Organização da Conferência Islâmica, promulga, no art. 18º, que "todos devem ter o direito à privacidade na condução de assuntos privados, em seu domicílio, em sua família, com respeito aos bens e relações" e que "não será permitido espionar, submeter a vigilância ou danificar sua reputação" [tradução nossa][25].

Ainda, a Carta Asiática de Direitos Humanos de 1998, documento criado pela Comissão Asiática de Direitos Humanos, organização fundada por um grupo de juristas e ativistas de direitos humanos, já que, todavia, não há declaração governamental nesse sentido, traz especialmente o "direito

---

[21] CONSELHO DA EUROPA. *Convênio Europeu de Direitos Humanos de 1950*. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 17 abr. 2019.

[22] UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia de 2000*. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 17 abr. 2019.

[23] UNIDADE AFRICANA. Carta Africana sobre Direitos Humanos e dos Povos de 1981. Disponível em: https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf. Acesso em: 17 abr. 2019.

[24] LIGA ÁRABE. *Carta Árabe sobre Direitos Humanos de 2004*. Disponível em: http://www.lasportal.org/ar/sectors/dep/HumanRightsDep/Documents/%D8%A7%D9%86%D8%AC%D9%84%D9%8A%D8%B2%D9%8A.pdf. Acesso em: 17 abr. 2019.

[25] ORGANIZAÇÃO DA CONFERÊNCIA ISLÂMICA. *Declaração dos Direitos Humanos no Islã de 1990*. Disponível em: https://www.oic-iphrc.org/en/data/docs/legal_instruments/OIC_HRRIT/571230.pdf. Acesso em: 17 abr. 2019.

à paz". Assim, prevê, no art. 4.1, que "todas as pessoas têm direito de viver em paz para que possam desenvolver todas as suas capacidades físicas, intelectuais, morais e espirituais, sem ser objeto de nenhum tipo de violência" [tradução nossa][26].

2.1.4.2 Marco normativo comparado: Brasil e Espanha

Em termos específicos, no caso brasileiro, país de origem do autor, o tema é previsto na Constituição Federal de 1988, a qual, no art. 5º, inc. X, sobre os direitos e deveres individuais e coletivos, garante que "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"[27]. Na legislação ordinária, o Código Civil de 2002, no capítulo sobre os direitos de personalidade, sinala, no art. 21, que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma"[28].

Por outro lado, no caso espanhol, o assunto também é disposto na Constituição Espanhola de 1978, a qual, no art. 18.1, na seção sobre os direitos fundamentais e as liberdades públicas, aduz que "é garantido o direito à honra, à intimidade pessoal e familiar e à própria imagem" [tradução nossa][29]. Ainda, no mesmo artigo, porém no apartado 4, a Constituição Espanhola inova na questão das tecnologias de informação e comunicação e traz que "a lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercícios

[26] COMISSÃO ASIÁTICA DOS DIREITOS HUMANOS. *Carta Asiática dos Direitos Humanos de 1998*. Disponível em: http://www.humanrights.asia/wp-content/uploads/2018/07/Asian-Human-Rights-Charter-2nd-Edition-English.pdf. Acesso em: 17 abr. 2019.

[27] BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 17 abr. 2019.

[28] BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. *Institui o Código Civil*. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 17 abr. 2019.

[29] ESPANHA. *Constitución Española de 1978*. Disponível em: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf. Acesso em: 17 abr. 2019.

dos seus direitos" [tradução nossa][30]. Por fim, no âmbito infraconstitucional, a Lei Orgânica 1/1982, de 5 de maio, de proteção civil do direito à honra, à intimidade pessoal e familiar e à própria imagem, dispõe, no art. 1º, que "o direito fundamental à honra, à intimidade pessoal e familiar e à própria imagem, garantido no artigo dezoito da Constituição, será protegido civilmente frente a todo gênero de intromissões ilegítimas" [tradução nossa][31].

2.1.5 O direito à privacidade e os avanços das tecnologias de informação e comunicação

É possível perceber que a expansão indiscriminada do uso de informações pessoais diante das novidades cibernéticas possibilitou inovadoras formas de violação da privacidade, uma vez que, na rede, toda operação ou conjunto de operações, realizada propriamente pelo usuário ou com o auxílio de meios automatizados, permite a coleta, armazenamento, seleção, avaliação, monitoramento, comparação, modificação, transferência, utilização e tratamento de informações pessoais, neste caso, dados pessoais.

Nesse contexto, a preocupação com o direito à privacidade "decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito", havendo que se falar em um direito à autodeterminação informativa[32]. A expressão "direito à autodeterminação informativa" foi primeiramente utilizada pelo Tribunal Federal Constitucional Alemão, quando do julgamento de um processo relacionado com as informações pessoais coletadas

[30] ESPANHA. *Constitución Española de 1978*. Disponível em: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf. Acesso em: 17 abr. 2019.

[31] ESPANHA. *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196. Acesso em: 17 abr. 2019.

[32] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 24.

de um censo no ano de 1983[33]. De acordo com o tribunal, o direito geral de proteção da pessoa, reconhecido no texto constitucional, abrange, considerando o processamento tecnológico e moderno de dados, a tutela do sujeito contra a coleta, armazenamento, utilização e divulgação ilimitada dos seus dados pessoais, devendo ser considerada um direito fundamental a faculdade do cidadão de dispor livremente dos seus dados[34].

Veja-se que o direito à proteção de dados pessoais supera o conteúdo essencial do tradicional direito à intimidade, porquanto não se baseia somente na tutela do conteúdo de natureza íntima dos dados coletados, mas abraça a faculdade de, primeiramente saber sobre tanto, mas também de decidir sobre a coleta, sobre o tratamento e sobre a possível transferência de tais registros, já que, na sociedade em rede informacional, as possibilidades de geração de dados independente de tempo, espaço e dispositivo. Assim, o direito à proteção de dados é um direito autônomo ao direito à intimidade, constituindo-se como instrumento jurídico para garantia da dignidade humana e desenvolvimento da personalidade, repousando sobre a faculdade do sujeito de dispor das próprias informações pessoais, frente ao uso indiscriminado das tecnologias informáticas.

No caso espanhol, como referido, o próprio texto constitucional separa o direito à intimidade (art. 18.1) do direito à limitação dos usos informáticos para garantir esse direito (art. 18.4). O Tribunal Constitucional, na STC n.º 292/2000, delimita e define a proteção de dados pessoais e refere que o objeto deste direito "não se reduz somente aos dados íntimos da pessoa, senão a qualquer tipo de dado pessoal, seja ou não íntimo, cujo conhecimento ou uso por terceiros possa afetar aos seus direitos, sejam ou

[33] MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, p. 55-63. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877. Acesso em: 17 abr. 2019.

[34] MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, p. 55-63. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877. Acesso em: 17 abr. 2019.

não fundamentais, porque seu objeto não é somente a intimidade individual" [tradução nossa][35].

Sobre o tema, no direito comunitário europeu, justamente por conta da livre circulação de pessoas, bens e dados, esse direito foi previsto autonomamente na Carta de Direitos Fundamentais da União Europeia de 2000, que, no art. 8º, refere que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito", de modo que "esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei", sendo que "todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação"[36]. Por fim, já estabelece que "o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente"[37].

Ainda, algumas diretivas já apontavam o caminho para a tutela desse novo direito, como foi o caso da Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[38]; da Diretiva 97/66/CE, do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações[39]; e da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho,

---

[35] ESPANHA. Tribunal Constitucional da Espanha. *Sentencia nº 292/2000, de 30 de Noviembre en el Recurso de Inconstitucionalidad n.º 1463-2000*. Interposição: Defensor del Pueblo. Ponente: Magistrado Don Julio Diego González. Boletín Oficial del Estado. Madrid. Disponível em: http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292#complete_resolucion. Acesso em: 17 abr. 2019.

[36] UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia de 2000*. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_es.pdf. Acesso em: 17 abr. 2019.

[37] UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia de 2000*. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_es.pdf. Acesso em: 17 abr. 2019.

[38] UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046&from=PT&fromTab=ALL&lang3=choose&lang2=choose&lang1=ES. Acesso em: 18 abr. 2019.

[39] UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações*. Disponível em: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A31997L0066. Acesso em: 18 abr. 2019.

de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas[40].

Trata-se de um duplo matiz, já que tal normatividade "por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio mediante o estabelecimento de regras comuns para proteção de dados na região", sendo de especial relevância considerar "as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações, o que inclui harmonizar as regras relativas a dados pessoais"[41]. Resulta que, nesse contexto, a proteção de dados pessoais garante tanto o direito à privacidade (individual), como promove a livre circulação de dados para o mercado (desde que obedecidas as regras), não na tentativa de frear a circulação de dados, mas, pelo contrário, de promove-la de forma legítima.

2.1.6 Os novos direitos da proteção de dados e a cibersegurança sob o Regulamento Geral de Proteção de Dados

Considerando que as diretivas não possuem obrigatoriedade de aplicação e deixam uma margem de adaptação aos ordenamentos jurídicos nacionais, redige-se, então, o Regulamento Geral de Proteção de Dados (RGPD), com entrada em vigor em 25 de maio de 2018, substituindo a Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, sendo este marco normativo obrigatório e diretamente aplicável, sem necessidade de transposição, embora novas leis nacionais estejam sendo criadas para revogar anteriores e complementar alguns

[40] UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas (Diretiva relativa à privacidade e às comunicações eletrônicas)* Disponível em: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32002L0058. Acesso em: 18 abr. 2019.

[41] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 102. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 out. 2020.

pontos de regramento[42]. O RGPD pressupõe uma mudança em relação à normativa anterior, visto que, para além de uma proteção repressiva, estabelece uma aproximação proativa, exigindo um enfoque baseado no risco (não mais sobre o tipo de dado ou sobre o tipo de tratamento), bem como uma responsabilidade ativa, consciente e diligente pelos órgãos responsáveis pelo tratamento (já que não existe um pacote fechado de medidas de segurança, dependendo da própria política de gestão de riscos)[43].

Ocorre que a ingerência do RGPD acaba por avançar nas fronteiras físicas mundiais, porquanto a proteção é aplicável ao tratamento de dados por uma empresa estabelecida na União Europeia, independentemente do local de tratamento desses dados ou da nacionalidade do titular deles; e, ainda, ao tratamento de dados por uma empresa que, embora não estabelecida na União Europeia, ofereça bens e serviços ou monitoramento para usuários que ali se encontrem, além de servir como fonte de inspiração para normativas sobre proteção de dados pessoas em países de outros continentes[44].

O RGPD baseia-se, então, nos princípios da licitude, lealdade, transparência, limitação da finalidade, minimização dos dados, exatidão, limitação do prazo de conservação, integridade, confidencialidade e responsabilidade proativa[45]. Houve significativas mudanças na forma de

---

[42] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

[43] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

[44] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

[45] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).*

obtenção do consentimento, já que, para tanto, quando o tratamento é baseado no consentimento do usuário (existem outras hipóteses em que independe o consentimento), este deve ser de forma explícita, clara, simples, ativa (não mais sendo permitido o silêncio como permissão para coleta), devendo haver a aprovação do internauta para cada finalidade de monitoramento de dados, mesmo que seja de forma eletrônica e por opção de caixa de seleção[46]. Ademais, o regulamento obriga a informar sobre a base legal do tratamento de dados, o prazo de conservação e transferência dos mesmos, devendo garantir o exercício dos direitos dos titulares dos dados, como à portabilidade dos dados, à eliminação dos dados e à notificação de terceiros sobre a retificação ou apagamento ou limitação de tratamento solicitados pelos titulares[47].

2.1.7 O direito à proteção de dados no contexto brasileiro: o histórico da Lei Geral de Proteção de Dados Pessoais

No caso brasileiro, conforme mencionado anteriormente, a Constituição Federal de 1988 prevê, no art. 5º, inc. X, ser inviolável a intimidade, a vida privada, a honra e a imagem das pessoas; e no art. 5º, inc. XII, estabelece ser inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas[48]. Ainda, como garantia fundamental, a Constituição Federal, no art. 5º, inc. LXXII, refere que o *habeas data* será concedido, gratuitamente, para

Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

[46] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

[47] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

[48] BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 17 abr. 2019.

assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; e para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo, já apontando embrionariamente a proteção de dados pessoais[49].

Em 1990, quando da promulgação do Código de Defesa do Consumidor, a legislação apontou, no art. 43, que "o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes", de forma que "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", dando as raízes de um princípio da qualidade dos dados[50].

Logo, em 2003, houve uma menção, por parte do Governo Brasileiro, sobre o caráter de direito fundamental da proteção de dados, quando da assinatura, em 15 de novembro daquele ano, da Declaração de Santa Cruz de La Sierra, documento final da XIII Cimeira Ibero-Americana de Chefes de Estado e de Governo. Nesta carta, no item 45, os Estados refeririam que "estamos também conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos [...]"[51].

Com as discussões na União Europeia em torno da redação de um Regulamento Geral de Proteção de Dados Pessoais (como mencionado no item anterior), com aplicação obrigatória nos países-membros, bem como

---

[49] BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 17 abr. 2019.

[50] BRASIL. Lei nº 8,078, de 11 de setembro de 1990. *Dispõe sobre a proteção do consumidor e dá outras providências.* Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 17 abr. 2019.

[51] SECRETARIA-GERAL ÍBERO-AMERICANA. XIII Cimeira Ibero-Americana de Chefes de Estado e de Governo. *Declaração de Santa Cruz de La Sierra de 14 e 15 de novembro de 2003*. Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em: 18 abr. 2019.

com as discussões sobre a revisão das Diretivas sobre Proteção da Privacidade e Fluxo de Dados Fronteiriços da Organização para a Cooperação e Desenvolvimento Econômico – OCDE (tradução livre para *OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*), organização intergovernamental que o Brasil quer fazer parte, começa a lenta corrida para a elaboração da própria Lei Geral de Proteção de Dados Pessoais brasileira.

Em 13 de junho de 2012, foi apresentado, pelo Deputado Milton Monti, à Câmara dos Deputados, o Projeto de Lei nº 4.060/2012, baseando o tratamento de dados pessoais inteiramente na lealdade e boa-fé do controlador para fins de atender os legítimos interesses dos titulares, sendo que o projeto de lei tramitou por anos entre comissões técnicas e audiências públicas para ouvir especialistas[52]. Entremeio a isso, a Lei nº 12.965, de 23 de abril de 2014, foi aprovada, criando o Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, dentre eles o princípio da proteção de dados pessoais[53].

Poucos dias depois da aprovação do RGPD, o Poder Executivo brasileiro, em 13 de maio de 2016, enviou, em regime de urgência, o Anteprojeto de Lei nº 5.276/2016, que também dispunha sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, embora tenha sido apensado ao PL 4.060/2012[54]. Dois anos depois, em 29 de maio de 2018, quatro dias depois da implementação do RGPD na União Europeia, a redação final do PL 4.060/2012 foi aprovada pela Câmara dos Deputados, sendo que, em 10 de julho de 2018, o Senado Federal também aprovou o projeto de lei.

---

[52] BRASIL. Câmara dos Deputados. Projeto de Lei nº 4.060, de 13 de junho de 2012. *Dispõe sobre o tratamento de dados pessoais e dá outras providências*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 08 out. 2020.

[53] BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 out. 2020.

[54] BRASIL. Câmara dos Deputados. Projeto de Lei nº 5.276, de 13 de maio de 2016. *Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 08 out. 2020.

Em 14 de agosto de 2018, houve a sanção presidencial da Lei nº 13.709, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), com vetos parciais (inclusive dos artigos que criavam a Autoridade Nacional e Proteção de Dados, sob argumento de vício de iniciativa já que ao Congresso Nacional não caberia criar órgão vinculado à Presidência da República), sendo a entrada em vigor para 18 (dezoito) meses da publicação[55]. Logo, o governo brasileiro editou a Medida Provisória nº 869/2018, posteriormente convertida, pelo Congresso Nacional, na Lei nº 13.853/2019, que altera a ementa da lei para "Lei Geral de Proteção de Dados Pessoais (LGPD)", cria a Autoridade Nacional de Proteção de Dados (ANPD) e define a entrada em vigência, para a ANPD, imediata, e para os demais artigos, em 24 (vinte e quatro) meses da publicação[56].

Contudo, com o advento do estado de calamidade pública decorrente da pandemia de COVID-19, causada pelo coronavírus SARS-CoV-2, reconhecido pelo Decreto Legislativo nº 06, de 20 de março de 2020, que afetou a economia mundial, inclusive a adequação das empresas e do Poder Público à LGPD, fez-se necessário repensar a entrada em vigor da lei[57]. Em 29 de abril de 2020, o governo federal editou a Medida Provisória nº 959, prorrogando a *vacatio legis* das demais disposições da LGPD para 03 de maio de 2021; e, em 10 de junho de 2020, foi sancionada a Lei nº 14.010/2020, que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da

[55] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

[56] BRASIL. Lei nº 13.853, de 08 de julho de 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 08 out. 2020.

[57] BRASIL. Decreto Legislativo nº 6, de 2020. *Reconhece, para os fins do art. 65 da Lei Complementar nº 101, de 4 de maio de 2000, a ocorrência do estado de calamidade pública, nos termos da solicitação do Presidente da República encaminhada por meio da Mensagem nº 93, de 18 de março de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/portaria/DLG6-2020.htm. Acesso em: 08 out. 2020.

pandemia do coronavírus (Covid-19), que, dentre outros temas, posterga a entrada em vigor das sanções da LGPD para 1º de agosto de 2021[58].

A Câmara dos Deputados, em 25 de agosto de 2020, quando da discussão sobre a conversão em Lei da Medida Provisória nº 959, fez um acordo para reduzir a prorrogação da vigência para 31 de dezembro de 2020[59]. No dia seguinte, o Senado Federal, analisando tal discussão, declarou a prejudicialidade do art. 4º da MP 959/2020 sobre a prorrogação do prazo da LGPD, por entender que a matéria, "entrada em vigência da lei", já havia sido discutida pelo Congresso Nacional na época do RJET, de modo que, pela regra de anuidade das proposições legislativas, não poderia ser rediscutida, reconhecendo, então, o texto como não escrito no projeto de lei[60].

Em 26 de agosto de 2020, considerando a votação que ocorreu no Congresso Nacional, o governo brasileiro editou o Decreto nº 10.474/2020, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados (ANPD)[61]. Em 17 de setembro de 2020, houve a sanção presidencial da Lei nº 14.058/2020, referente à conversão em lei da MP 959/2020[62]. Desse modo, a partir de tal data e a par das

---

[58] BRASIL. Lei nº 14.010, de 10 de junho de 2020. *Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19).* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 08 out. 2020.

[59] BRASIL. Congresso Nacional. Medida Provisória nº 959, de 2020 (regras para o auxílio emergencial e adiamento da vigência da LGPD). *Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga* a vacatio legis *da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD.* Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753. Acesso em: 08 out. 2020.

[60] BRASIL. Congresso Nacional. Medida Provisória nº 959, de 2020 (regras para o auxílio emergencial e adiamento da vigência da LGPD). *Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga* a vacatio legis *da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD.* Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753. Acesso em: 08 out. 2020.

[61] BRASIL. Decreto nº 10.474, de 26 de agosto de 2020. *Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm. Acesso em: 08 out. 2020.

[62] BRASIL. Lei nº 14.058, de 17 de setembro de 2020. *Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Lei nº 14.020,*

discussões doutrinárias sobre a vigência durante o interregno entre a votação do Congresso Nacional e a sanção presidencial, a Lei Geral de Proteção de Dados Pessoais está totalmente em vigor, com exceção das sanções administrativas previstas para 1º de agosto de 2021.

Com grande inspiração no RGPD, a LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[63]. De maneira semelhante ao RGPD, a LGPD possui aspectos extraterritoriais, pois aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; ou que a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que os dados pessoais objeto do tratamento tenham sido coletados no território nacional, o que pode, eventualmente, ocasionar um conflito positivo de normas de direito privado internacional, à medida em que, em determinado tratamento de dados, tanto o RGPD quanto a LGPD podem ser aplicáveis.

Ainda, a LGPD estabelece que as atividades de tratamento de dados pessoais devem observar a boa-fé e os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança da prevenção de danos, da não discriminação e da responsabilização e prestação de contas[64]. Ademais, refere que a disciplina da proteção de dados pessoais tem como fundamentos o respeito à

de 6 de julho de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14058.htm. Acesso em: 08 out. 2020.

[63] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

[64] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[65].

Elenca, como bases legais para tratamento de dados, as hipóteses de fornecimento de consentimento pelo titular; cumprimento de obrigação legal ou regulatória; tratamento e uso compartilhado de dados necessários à execução de políticas públicas pela administração pública; realização de estudos por órgão de pesquisa; execução de contrato ou de procedimentos preliminares relacionados a contrato; exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física do titular ou de terceiros; tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; interesses legítimos do controlador ou de terceiro; ou, por fim, proteção do crédito, inclusive quanto ao disposto na legislação pertinente[66].

Pela LGPD, o titular, à semelhança do RGPD, possui, de maneira gratuita e facilitada, os direitos à confirmação da existência de tratamento; ao acesso aos dados; à correção de dados incompletos, inexatos ou desatualizados; à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na legislação; à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; à eliminação dos dados pessoais tratados com o consentimento do titular; à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; à informação sobre a possibilidade

[65] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

[66] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

de não fornecer consentimento e sobre as consequências da negativa; e à revogação do consentimento[67].

A LGPD também cria a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), autoridade de controle responsável por zelar pela proteção de dados no país e por fiscalizar a aplicação da legislação, dentre outras competências. Porém, a ANPD originariamente foi criada como órgão da administração pública federal, integrante da Presidência da República, o que resultou em críticas por parte de especialistas, que consideraram que estar submetida ao governo federal afetaria a independência necessária da instituição. Dessa forma, após grande pressão política, ficou determinado que a natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, isto é, independente, submetida a regime autárquico especial e vinculada à Presidência da República, em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD[68].

2.1.8 Breves comparações entre o RGPD e a LGPD

Vale lembrar que, como referido, a Lei Geral de Proteção de Dados Pessoais (LGDP) possui grande inspiração no Regulamento Geral de Proteção de Dados Pessoais (RGPD) e, considerando não ser uma tradução do modelo europeu, traz algumas nuances e diferenças na gestão do direito à privacidade. Ressalta-se que a LGPD, por sua estrutura, é uma lei, contém cláusulas mais abertas e subjetivas e depende de regulamentação pela ANPD, o que permite uma interpretação sistêmica e teleológica; enquanto que o RGPD, como o próprio nome, é um regulamento, com normas mais objetivas e regras específicas.

O RGPD e a LGPD elencam bases legais para o tratamento de dados pessoais, de modo que cada finalidade deve estar acompanhada de uma

[67] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

[68] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

hipótese de legitimação da legislação. As duas legislações trazem, em comum, embora com palavras diversas, as hipóteses de consentimento explícito, necessidade contratual, execução de políticas públicas, interesse vital, obrigação legal e interesse legítimo. A LGPD, além dessas, traz especificamente outras bases legais, quais sejam, a proteção da saúde em um procedimento realizado por profissionais de saúde, a realização de estudos por um órgão de pesquisa, o exercício de direitos em processos judiciais e a proteção ao crédito.

Em relação aos dados sensíveis, as legislações trazem uma redação divergente: enquanto que a LGPD dispõe que o tratamento de dados pessoais sensíveis somente pode ocorrer nas hipóteses previstas, isto é, em novas bases legais; o RGPD determina que o tratamento de dados pessoais sensíveis é proibido, salvo nas exceções previstas no regulamento. Ainda, a LGPD elenca duas hipóteses sem equivalência na legislação europeia, quais sejam, a execução, pela administração pública, de políticas públicas prevista em lei ou regulamento, e a garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Por sua vez, o RGPD permite o tratamento de dados sensíveis tornados públicos pelo titular e de dados relativos a atuais ou ex-membros de fundações, associações ou organizações sem fins lucrativos, tratados para fins legítimos e com medidas de segurança apropriadas.

Especificamente em relação ao direito de acesso aos dados pessoais, a LGPD determina que o prazo para cumprimento da petição do titular é de 15 (quinze) dias, enquanto que o RGPD determina que o prazo é maior, de 30 (trinta) dias. Questão interessante recai sobre o marketing direto, uma vez que o RGPD define os requisitos e etapas para permitir tal operação, podendo o usuário se opor ao tratamento de dados para criação de perfis de marketing, enquanto que a LGPD fica silente quanto a este aspecto, o que sugere seguir as regras gerais de tratamento.

Sobre a notificação de incidentes de segurança, a LGPD apenas refere que a comunicação deve ser realizada em prazo "razoável", sendo que o

RGPD, por outro lado, prescreve que uma violação de dados pessoais deve ser comunicada à autoridade de controle em até 72 (setenta e duas) horas após o conhecimento do fato. Ademais, o RGPD determina que o responsável pelo tratamento deve comunicar a violação de dados pessoais à autoridade de controle e, quando essa violação for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas, também ao titular dos dados sem demora injustificada; a LGPD somente estabelece que deve haver a comunicação à ANPD e ao titular de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o que deixa uma margem de interpretação se todo incidente deve ser efetivamente comunicado.

Em relação à avaliação e relatório de impacto sobre a proteção de dados pessoais, o RGPD traz uma descrição detalhada sobre o procedimento e conteúdo a ser previsto neste documento, especialmente quando o tratamento resultar em um elevado risco para o direito e a liberdade das pessoas, sendo que, ainda, trouxe a hipótese de haver uma consulta prévia à autoridade de controle. No caso brasileiro, a LGPD dispõe que o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados, dependendo ainda de maiores informações a serem dispostas em regulamento específico.

No que diz respeito aos agentes de tratamento, a LGPD importa uma tradução mitigada da versão em inglês e portuguesa do RGPD, definindo o controlador, no inglês "controller", como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; o operador, no inglês "processor", como a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; e o encarregado como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade de controle. A versão portuguesa do RGPD traz, respectivamente, a pessoa

do responsável, do subcontratante e do encarregado da proteção de dados; enquanto que a versão espanhola do RGPD, que foi o objeto de estudo deste trabalho, apresenta, respectivamente, o "responsable", o "encargado" (embora na tradução ao português entenda-se como "encarregado", aqui funciona como operador/subcontratante) e o "delegado".

Sobre o vínculo entre os agentes de tratamento, a LGPD não dispõe qualquer obrigação de formalização desta relação, porém o RGPD estabelece que o tratamento de dados realizado pelo operador deve estar previsto em contrato ou outro ato jurídico, que possa vincular o controlador ao operador. Ainda, ambas as legislações estabelecem que o controlador e o operador não serão responsabilizados quando a pessoa física ou jurídica não estiver envolvida com o tratamento dos dados; ou quando, apesar do dano, o tratamento for realizado em conformidade com a legislação, porém a LGPD inova referindo também que não serão responsabilizados quando os agentes comprovarem que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros, o que pode gerar discussões sobre reconhecimento de risco fortuito interno, nos termos da Súmula 479, do Superior Tribunal de Justiça.

Em relação às penalidades pelo descumprimento das obrigações legais, ambas legislações trazem um rol de sanções que vai desde uma advertência até a suspensão ou proibição da atividade de tratamento de dados pessoais. Em relação às multas administrativas, o RGPD elenca que, em caso de violação à lei, podem variar de EUR10.000,00 (dez milhões de euros) a EUR20.000,00 (vinte milhões de euros) ou de 2% a 4% do faturamento anual correspondente ao exercício financeiro anterior, o que for maior; a LGPD, por sua vez, estabelece multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$50.000.000,00 (cinquenta milhões de reais) por infração.

Como visto neste tópico e nos dois acima, o RGPD foi publicado em maio de 2016 e está em vigor desde maio de 2018, e a LGPD foi publicada

em agosto de 2018 e está em vigor desde setembro de 2020, porém o histórico e experiência legislativa europeia remonta à década de 80 do século XX, enquanto que, no Brasil, o tema começou a ser tratado com mais força apenas no fim da primeira década do século XXI. Apesar disso, as leis gerais de privacidade estão conectadas e se apoiam em denominadores comuns, sendo urgente e necessária a conscientização dos titulares e a adequação dos agentes de tratamento, inclusive do Poder Público, aos novos matizes do direito à privacidade na sociedade em rede.

2.1.9 Há que se pensar em um novo direito à privacidade?

Em virtude dessa mudança de regras, um sem números de políticas de privacidade, políticas de *cookies*, políticas de uso de aplicações e dispositivos, dentre outros tipos de documentos e termos de adesão firmados pelos usuários, devem ser atualizadas, divulgadas e aceitas, além da adaptação quanto às questões técnicas, científicas, sociais, publicitárias, laborais e setoriais envolvendo tais produtos e serviços. Desta maneira, o direito à proteção de dados pessoais – e em última instância, o direito à privacidade – submete-se a um regime de cibersegurança, isto é, a um conjunto de atividades dirigidas a proteger o ciberespaço contra o uso indevido do mesmo, defendendo-se a infraestrutura tecnológica, os serviços que presta e a informação que maneja[69].

Trata-se do resultado de um longo processo normativo-regulatório, que pode ser classificado, conforme alguns autores, em quatro gerações de leis[70]. A primeira geração de leis sobre proteção de dados pessoais era formada por normas que, preocupadas com o estado da tecnologia e a profusão de bancos de dados elaborados, procuravam a autorização dos usuários para criação dessas estruturas e focavam em regras dirigidas aos

[69] ESPANHA. Ministério de Defesa. *Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas*. Disponível em: http://www.emad.mde.es/Galerias/MOPS/novoperaciones/multimedia/documentos/20130226_CIBERDEFENSA.pdf. Acesso em: 18 abr. 2019.

[70] MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). *Technology and privacy*: The new landscape. Cambridge: MIT Press, 1997, pp. 219-242.

órgãos públicos para processamento das informações[71]. A segunda geração de leis sobre o tema, ciente da diáspora dos bancos de dados, caracterizava-se em regulamentar a privacidade como uma liberdade negativa, de modo que o cidadão pudesse restringir o acesso aos dados pelos órgãos públicos[72].

Considerando, no entanto, que o fornecimento de dados pessoais é indispensável para a vida social, uma terceira geração de leis de proteção de dados surgiu, na década de 80, entendendo se tratar de um processo complexo, cuja proteção precisava ir além da permissão ou não para utilização das informações, mas deveria considerar, incluir e informar o usuário sobre as fases sucessivas do tratamento, numa autodeterminação informativa[73]. Por fim, a quarta geração de leis de proteção de dados, tais quais as atuais, entende que a tutela dos dados não pode ser reduzida a uma escolha individual e considera necessária a implementação de instrumentos coletivos de proteção, reconhecendo o desiquilíbrio na relação entre operadores de tratamento e usuários, fortalecendo a posição do usuário frente às entidades que processam os dados e criando autoridades independentes para supervisão pública do tratamento de dados na sociedade[74].

Em que pese os compromissos políticos e normativos internacionais firmados por parte das nações e das corporações em favor do direito à proteção de dados pessoais e, ademais disso, do direito à privacidade, a vigilância social a que os cidadãos são submetidos e a própria subjetividade

---

[71] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 96. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 out. 2020.

[72] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 97. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 out. 2020.

[73] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 96. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 out. 2020.

[74] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 98. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 out. 2020.

formada pelo medo do terror acabam pondo em xeque tais direitos fundamentais, já que o limite entre conhecimento público, vida privada, intimidade e segredo é fluido. Na sociedade em rede de vigilância social, a privacidade, como conquista popular e direito de primeira geração de liberdade individual, pode necessitar uma reformulação.

2.2 Até um novo direito à privacidade: desafios e caminhos em tempo de cibersegurança

O século XX representou a era de ouro para a normatização dos direitos e garantias fundamentais e, à medida em que os avanços sociais e a própria configuração do Estado foi mudando devido ao aperfeiçoamento das tecnologias de informação e comunicação, novas gerações/dimensões de direitos fundamentais foram surgindo. Dentre eles, o direito à privacidade, na concepção moderna, também passou por transformações, havendo invadido, conquistado e colonizado a esfera pública social, embora nos últimos anos tenha sido marcada pelas quedas vertiginosas do apogeu de sua glória.

2.2.1 A alteração de paradigma e o novo conceito de privacidade

Trata-se, pois, de uma alteração de paradigma e uma necessária ressignificação de conceitos, marcada pelo fluxo informacional em massa, abrangendo-se novas nuances sobre o direito ao segredo, o direito à intimidade, o direito à vida privada e familiar, o direito à autodeterminação informativa e o direito à proteção de dados pessoais. Embora tenha se falado no fim da privacidade no apagar das luzes do século XX, tenta-se conceituar o direito à privacidade como uma superação da concepção sólida e estática dos textos normativos fechados de autoconfinamento para

alcançar uma perspectiva aberta, dinâmica e fluida numa sociedade tecnológica[75].

O direito à privacidade, nos ordenamentos jurídicos modernos, está fundamentado na concepção clássica da privacidade relacionada à ideia isolacionista do "ser", numa lógica excludente de "pessoa-informação-sigilo", possibilitando ao indivíduo proteger-se de intromissões indesejadas naquilo que lhe era mais reservado, ainda que "a partir de la critica denominada pensamiento postmetafísico se hace muy complicado sostener que el sujeto pudiera ser algún género de yo como sustancia autoconsciente de los inicios cartesianos de la filosofia de la consciencia"[76]. Com o desenvolvimento das tecnologias de informação e comunicação, houve uma relativização daquilo que é considerado segredo, de maneira que o sujeito, no panorama das relações sociais conectadas globalmente, adere-se ao virtual – aqui não como digital, mas como potência de ser – e possui a prerrogativa e a necessidade de compartilhar informações para formar uma identidade em rede[77], necessitando que o conceito de privacidade seja reformulado.

Dessa forma, a definição da privacidade somente como o direito de ser deixado só e de restringir o conhecimento público de informações consideradas privadas perdeu há alguns anos o valor de ser o único fundamento dessa tutela, embora essa questão seja um aspecto essencial a ser aplicado a situações determinadas quando se exige essa proteção. Trata-se, então, do fim "de um longo processo evolutivo experimentado pelo conceito de privacidade: de uma definição original como o direito de ser deixado em paz, até o direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser construída"[78].

---

[75] PÉREZ LUÑO, Antonio Enrique. *Los derechos en la sociedad tecnológica*. Madrid: Editorial Universitas, S.A., 2012, p. 93.

[76] MUGUERZA, Javier. De la conciencia al discurso ¿un viaje de ida y vuelta? In: *La filosofía moral y política de Jürgen Habermas*. Madrid: Biblioteca Nueva, 1997, pp. 63-110, p. 98.

[77] CASTELLS, Manuel. *O poder da identidade*. 2. ed. São Paulo: Paz e Terra, 2000.

[78] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 17

Isso não quer dizer que esse aspecto de controle estivesse ausente das definições tradicionais, já que o controle era utilizado justamente como uma ferramenta para realizar a finalidade de ser deixado só e definir o que deveria ficar de fora do conhecimento alheio, sob ângulo individualista e privado que o desenvolvimento atual das tecnologias já não permite. Por outro lado, atualmente, a questão da privacidade como controle chama a atenção para a possibilidade de os sujeitos exercerem os poderes conquistados pelo fornecimento de dados pessoais, dentre eles os de conhecer, controlar, endereçar, opor, interromper e proibir o fluxo de informações que a ele são relacionadas.

Assim, introduz-se uma nova conceituação de privacidade, podendo ser definida mais precisamente, em uma primeira aproximação, como "o direito de manter o controle sobre as próprias informações", identificada com a "tutela das escolhas de vida contra toda forma de controle público e de estigmatização social, em um quadro caracterizado justamente pela 'liberdade das escolhas existenciais"[79]. Verifica-se, então, que a privacidade como a conhecemos, relacionando privado com pessoal e secreto, deu espaço a novos caminhos, podendo ser entendida numa lógica de "pessoa-informação-circulação-controle", não mais restrita à burguesia do século XX, mas destinada à multidão na sociedade em rede[80].

2.2.2 Os paradoxos da privacidade no século XXI

Considerando a difusão das tecnologias de informação e comunicação e a produção em massa de *big data*, percebe-se que o objeto de tutela da privacidade também sofreu alterações, compreendendo um número sempre crescente e exponencialmente maior de informações e situações jurídicas relevantes que necessitam de um controle do indivíduo. Nesse sentido, privacidade não necessariamente guarda relação com algo privado e, por sua vez, privado não precisamente faz referência a algo secreto,

[79] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 92.

[80] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 93.

derivando-se daí, pelo menos, quatro paradoxos e o surgimento de uma nova dimensão da privacidade, a extimidade.

2.2.2.1 O primeiro paradoxo: das muralhas digitais

O primeiro paradoxo da privacidade guarda relação com a própria ideia que originou o regime jurídico moderno desse direito, ou seja, a necessidade de reservar aquilo que é privado. Isso, pois as tecnologias de informação e comunicação, por mais que facilitem o contato interpessoal mundial e criem novas formas de se relacionar, também contribuem para a construção da esfera privada na criação de um casulo pessoal, à medida em que evitam aqueles contatos sociais consolidados e cotidianos, aumentando a sensação de autossuficiência, como, por exemplo, nos casos de ampliação do teletrabalho, de realização de videoconferências, de preferência pelo *e-commerce* e pelas transações bancárias online, de predileção pelo entretenimento dos dispositivos inteligentes e conectados, entre outros[81].

Na aldeia global, essas tecnologias de informação e comunicação possibilitaram o fechamento dos indivíduos em fortalezas eletrônicas digitais e distanciaram os sujeitos das formas de controle social possibilitadas pelo agir em público e da modulação de grupos de interesse a partir da vigilância sólida. Porém, é bem verdade que, como visto no primeiro capítulo, as formas de controle social estão cada vez mais penetrantes e a vigilância cada vez mais líquida, isto é, espalhada como um fluido por todos os dispositivos sociais, justamente fazendo uso da coleta, do tratamento e da transferência de dados advindos dessas tecnologias informacionais, como se fossem *backdoors* nessas muralhas digitais erigidas.

2.2.2.2 O segundo paradoxo: o núcleo duro da privacidade

[81] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 94-95.

Noutro sentindo, o segundo paradoxo da privacidade refere-se à própria ressignificação da proteção das informações íntimas e secretas, isto é, aquelas que o sujeito quer que sejam excluídas em determinada medida da circulação em público. Isso, porque os textos normativos, internacionais, comunitários ou nacionais, seguem, de certa forma, construindo um "núcleo duro" da privacidade relativo às informações sensíveis, que, tradicionalmente, exigiam uma maior camada de proteção e sigilo, cujo tratamento discricionário poderia originar alguma discriminação, como, por exemplo, os dados relacionados a saúde, à origem étnica, à opinião política, à orientação sexual, à filiação sindical, à crença religiosa, dentre outros[82].

Ocorre que muitas dessas informações ditas sensíveis não estão reservadas somente à esfera privada do indivíduo, mas, pelo contrário, em contextos democráticos, estão relacionadas à esfera pública, na medida em que fazem parte da identidade do sujeito, podendo este utilizá-las para manifestar-se como pessoa, para encontrar semelhantes e diferentes, para ocupar o espaço público, para reconhecer-se como ator político[83]. Desse modo, atribui-se um estatuto de mais privado e limita-se fortemente a circulação e o tratamento dos dados sensíveis não porque são secretos, mas para que justamente o indivíduo possa fazê-los públicos.

2.2.2.3 O terceiro paradoxo: o direito como poder da privacidade

Ainda, o terceiro paradoxo da privacidade trata da própria evolução desse direito, conforme visto no capítulo anterior, já que a existência de riscos derivados da coleta e tratamento de dados pessoais fez surgir o direito à autodeterminação informativa, abrangendo a potestade do indivíduo de perguntar, receber informação, limitar a circulação, opor-se, proibir e fazer cessas as informações daí derivadas. Em verdade, o direito fundamental à privacidade, para além de um direito ou um conjunto de

[82] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 95-96.

[83] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 96.

direitos, também é a atribuição de uma série de poderes aos interessados, como se fosse o reconhecimento de direitos implícitos aos direitos de personalidade.

Assim, o direito à privacidade, nessa nova matiz que permite ao sujeito acompanhar a manipulação de seus dados pessoais por outras pessoas ou empresas, põe de relevância o direito ao acesso a tais informações. É dizer, por um lado está o critério formal de posse das informações, baseada na legitimidade da coleta ou no consentimento do indivíduo por parte dos controladores e operadores de tratamento, mas, por outro lado, está a prevalência do direito do indivíduo sobre os próprios dados, de forma que o direito à privacidade acaba por se tornar instrumento capaz de fazer mais transparente e pública a esfera de atuação dos controladores ou operadores de tratamento[84].

2.2.2.4 O quarto paradoxo: o Estado em rede

Por fim, o quarto paradoxo da privacidade, pensado a partir do presente trabalho, está desenvolvido no sentido de que o direito à privacidade, na esteira de outros direitos fundamentais, trata da própria subjetividade do cidadão e exige uma atuação do Estado para garantir a proteção dessas informações pessoais, seja através de uma regulação, ou de mecanismos de controle, ou outros instrumentos normativos. O problema decorre do fato que o Estado, sendo um ator social e um nó da sociedade em rede, para sobreviver à essa nova dinâmica de poder em rede, acaba por violar sistematicamente a privacidade dos indivíduos, nacionais e estrangeiros, sob a justificativa de interesse público, conforme visto no capítulo anterior.

[84] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 96-97.

2.2.3 A extimidade como nova dimensão da privacidade

Conforme mencionado acima, o aperfeiçoamento das tecnologias de informação e comunicação e a democratização do acesso a dispositivos informáticos, com a consequente popularização das redes sociais, fizeram aparecer uma modalidade híbrida de privacidade, quando do surgimento de um indivíduo que quer manter alguns aspectos de sua vida na esfera privada, de forma alheia ao conhecimento geral e espalhado, mas que igualmente quer transformar essa esfera privada, em certa medida, em uma esfera pública, numa espécie de publicidade do privado. Trata-se de um deslocamento do núcleo da privacidade, a partir da espetacularização de si mesmo, da ficcionalização do "eu" e da "socialização da intimidade"[85].

Em outras palavras, na sociedade digitalmente conectada e influenciada globalmente, "não se trata mais da dualidade entre o homem-prisioneiro de seus segredos e o homem que nada tem a esconder; entre a 'casa-fortaleza', que glorifica a privacidade e favorece o egocentrismo, e a 'casa-vitrine', que privilegia as trocas sociais"[86]. É configurada, então, uma nova dimensão da privacidade, caracterizada pela exteriorização da interioridade do indivíduo, ressignificando o critério de público-privado, em razão dos processos comunicativos da sociedade em rede, num exercício de extimidade[87].

A extimidade, sob ponto de vista psicanalítico, está fundamentada na exteriorização da intimidade, isto é, na necessidade de dar visibilidade ao próprio "eu", seja por meio da revelação de segredos, da exposição do singular, da espetacularização da intimidade ou da ficcionalização de si mesmo, abrindo essa esfera privada ao olhar dos outros para que seja validada a própria existência, seja confirmado o próprio ser e existir[88].

---

[85] LIMBERGER, Têmis. *Cibertransparência informação pública em rede:* a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016, p. 60.

[86] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 25.

[87] BOLESINA, Iuri. *O direito à extimidade:* as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017, p. 182.

[88] LACAN, Jacques. *O seminário:* livro 16: de um Outro ao outro. Rio de Janeiro: Jorge Zahar, 2008, p. 241.

Considerando que o custo social da não exposição pode ser alto, os indivíduos acabam por expor a intimidade e o segredo, desejando fama, seguidores, interações, *likes, scores* e visualizações, numa autoafirmação constante, terminando por revelar dados pessoais, padrões sociais e informações de preferências.

Assim, numa suposta autoviolação da privacidade, os indivíduos, objetivando fazerem parte dessa sociedade em rede, qualificada pelo consumismo da informação, fornecem dados relevantes para acesso e manutenção de produtos e serviços, especialmente redes sociais. Não se pode, portanto, "traçar um limite, como se o mundo da defesa da privacidade e o da ação pública fossem hostis ou não comunicantes; não existe uma separação, mas um *continuum*", tornando-se a privacidade, pois, fluida[89].

2.2.4 O consentimento informado livre frente aos termos e condições

Cabe mencionar, contudo, que o fornecimento de dados pessoais em troca dos benefícios sociais que os indivíduos supostamente aproveitam dos produtos e serviços oferecidos não é a única contrapartida dessa relação, uma vez que o tratamento de dados pelas organizações públicas e privadas pode fazer surgir novas concentrações de poder ou fortalecer poderes já existentes, tais como *plus-poder*. Em outras palavras, o oferecimento de produtos e serviços, muitas vezes gratuitos, exige do usuário o fornecimento de dados pessoais, que não necessariamente servem para a própria existência do produto ou serviço que chega ao indivíduo, mas sim para agregar valor à própria organização como nó social na malha do poder em rede.

Dessa forma, considerando que se torna cada vez mais difícil determinar quais tipos de informações os sujeitos estariam dispostos a renunciar uma maior proteção, o controle do tratamento de dados pessoais perpassa justamente por sua legitimidade e legalidade. Nesse sentido,

[89] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 47.

percebe-se uma alteração de paradigma, inclusive pelo advento do Regulamento Geral de Proteção de Dados Pessoais da União Europeia, superando-se o *implied consent*, isto é, o consentimento implícito que supunha que a mera utilização do produto ou serviço implicava na concordância com a manipulação dos dados; pelo *informed consent,* isto é, o consentimento informado que determina o provimento do maior número de explicações ao usuário para que este concorde conscientemente com as circunstâncias e finalidades do tratamento dos dados, embora inicialmente tenha sido pensado no direito à saúde[90].

Nesse contexto, pode-se questionar em que medida o consentimento informado tem potencial de ser um controle social e um exercício de autodeterminação informativa no que tange à permissão de circulação de dados. Em primeiro lugar, importa recordar que o fornecimento do consentimento é *conditio sine qua non* para o acesso de produtos e serviços na sociedade em rede, sem o qual o usuário não pode desfrutar das interações sociais dali permitidas, tornando-se a concordância meramente uma etapa neste processo. Em segundo lugar, a obtenção do consentimento informado se limita a um mero clique do usuário em um botão predeterminado ou em uma caixa de seleção (*blank selection*), dispensando-se o real entendimento dos termos e condições apresentados, já que basta o aceite formal do indivíduo para que supostamente se legitime o tratamento dos dados.

Por outro lado, nem sempre o usuário sabe o que está aceitando, em virtude da extensão dos textos e a utilização de expressões jurídicas, querendo logo acessar o produto ou serviço, independentemente do que esteja aceitando nas entrelinhas das políticas de privacidade. Ainda, na esteira da teoria dos mosaicos que refere não ser o dado, por si só, relevante, mas sim o contexto de informações daí derivadas[91], nem sempre ficam claras as reais finalidades da coleta de informações, já que é possível gerar um

[90] TARODO, Salvador Soria. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: *Derecho y Salud*, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006, p. 143-144.

[91] CONESA, Fulgencio Madrid. *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia, 1984, p. 45.

sem número de variáveis para serem manipuladas, conferindo-se valor a depender do tratamento de dados utilizado e do reconhecimento de padrões informacionais desejados.

Importante citar, como visto no capítulo anterior, que essa questão de consentimento perde em muito a relevância quando posta em confronto com as justificativas do regime de vigilância eletrônica global de pessoas e informações, uma vez que o interesse privado se sujeita ao interesse público de proteção e prevenção de ameaças à segurança pública, sendo que o próprio Regulamento Geral de Proteção de Dados da União Europeia põe essa exclusão de aplicação[92]. Porém, a própria existência dos programas de vigilância em massa para salvaguarda da segurança nacional foram revelados sob polêmicas internacionais, sendo desconhecidas ou insuficientes as condições de supervisão pública ou garantias seguras e reais do cumprimento dos direitos e garantias dos cidadãos por parte dessas agências institucionais[93].

No que tange ao consentimento, cabe a crítica de que este não é necessariamente consciente ou livre, no próprio sentido das palavras, porque submetido a essa lógica informacional e a esse processo de subjetivação criado pelo consumo das tecnologias de informação e comunicação. De tal modo, "raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados", sendo possível que não reflita sobre a periculosidade do uso de tais informações por parte de diferentes controladores, o que faz defasar o poder do indivíduo frente a essas organizações[94].

---

[92] UNIÃO EUROPEIA. Parlamento Europeu. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

[93] PESSOA, João Pedro Seefeldt. OLIVEIRA, Rafael Santos de. "Big Brother Watch and Others v. The United Kingdom": el régimen de vigilancia social y el derecho al respecto a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos. In: *Pensar*: Revista de Ciências Jurídicas, Fortaleza, v. 24, n. 3, pp. 1-12, jul./set. 2019. Disponível em: https://doi.org/10.5020/2317-2150.2019.9528. Acesso em: 10 out. 2019.

[94] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

2.2.5 Das novas características da privacidade do século XXI: o interesse coletivo pela proteção da privacidade

É preciso ter em mente que, em verdade, as normativas quanto à regulação de dados não servem para proibir o tratamento das informações, visto que a livre circulação de dados pessoais é uma realidade da sociedade em rede. Não se pode olvidar que se caminha para um contexto espaço-temporal marcado pelos dados pessoais como bem econômico, especialmente se considerada a perspectiva da *Internet of Things* e *Internet of Everything*, onde a inteligência artificial e o processo de *data learning* e *machine learning* imperam numa economia da informação com o fluxo contínuo de dados pessoais.

Assim, de um lado, parece haver uma chancela social pública que permite a coleta e o tratamento de dados nos casos de interesse geral e de defesa nacional, não havendo poder de disposição de tais informações pelos usuários (até porque nem sabem que são alvos de monitoramento nestes casos); por outro lado, parece haver um determinismo social que obriga os indivíduos a produzirem e a entregarem informações relevantes aos fornecedores de produtos e serviços para enfim participarem da sociedade em rede. Em outras palavras, de um lado, os dados são coletados compulsoriamente por parte das agências institucionais de segurança, mas por outro lado os dados também são coletados compulsoriamente como moeda de troca para acesso a produtos e serviços informacionais.

De qualquer modo, o interessado parece estar compelindo a dispor de seus dados, sendo que, a partir desses novos regulamentos de proteção de dados, essa disposição está legitimamente fundada, já que considerado, por exemplo, no âmbito do RGPD, a licitude do tratamento de dados quando os dados são obtidos a partir do consentimento do usuário, ou para execução de um contrato, ou para cumprimento de uma obrigação a qual o responsável esteja sujeito, ou para defesa dos interesses vitais do interessado, ou para exercício de funções de interesse público ou ao exercício

da autoridade pública de que está investido o responsável pelo tratamento ou, ainda, para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros[95].

Assim, não se trata de limitar a circulação de informações na sociedade em rede, mas sim de defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais. Nessa linha de pensamento, evidencia-se a mudança de paradigma da privacidade, de "pessoa-informação-sigilo" para "pessoa-informação-circulação-controle", chegando-se a um problema ulterior, que, na realidade, desafia o direito à privacidade em tempo de cibersegurança, o controle, que, por sua vez, deve deixar de ser individual e passar a ser coletivo.

Nesse cenário de "pessoa-informação-circulação-controle", há que levar em consideração que, no panorama anterior, as informações pessoais estavam sob domínio do interessado, de forma que ele tinha o controle sobre o que divulgar ou não, porém, atualmente, essas informações estão divididas em uma pluralidade de multidões, espalhadas pela rede. E se, antes, a violação da privacidade era essencialmente a fofoca e a revelação de segredos, agora a violação se dá por métodos desconhecidos, abstratos, pela manipulação de dados informáticos e outras ferramentas obscuras, havendo um aumento do valor agregado das informações pessoais, de maneira que a referência ao valor da pessoa deixa de ser si própria, mas submete-se à lógica do mercado.

O controle do fluxo de informação é tanto interno, isto é, das informações que saem do indivíduo e vão para o exterior, quanto externo, ou seja, das informações que chegam ao indivíduo (direito de não saber, não querer publicidade, não participar). As tecnologias de informação e comunicação, pelo próprio papel de aproximar pessoas e encurtar distâncias,

[95] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Disponível em: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679. Acesso em: 18 abr. 2019.

tornou extremamente sutil a fronteira entre a esfera pública e a privada, sendo que a autodeterminação pessoal e a construção livre da esfera privada passaram a ser condição para o desenvolvimento e efetividade da esfera pública.

Por essas razões, a função sociopolítica do direito à privacidade ultrapassa os limites dos interesses individuais e torna-se um elemento importante na construção da cidadania. Numa sociedade digitalmente conectada, a definição da privacidade somente como o "direito de ser deixado só" é insuficiente, devendo ser expandida para uma tutela global e coletiva, num quadro caracterizado pela liberdade das escolhas pessoais e existenciais. O direito à privacidade deixa de ser apenas um direito de uma pessoa limitar as intromissões de outros indivíduos ou do Estado naquilo que é privado ou um direito de exigir do Estado que impeça tais intromissões, mas passa a ser um direito coletivo, de uma multidão, que o Estado precisa assegurar por padrão, considerando os novos paradoxos e paradigmas da sociedade em rede[96].

2.2.6 Para um novo direito à privacidade: estratégias de tutela

O direito à privacidade, nessa lógica de "pessoa-informação-circulação-controle", pressupõe novas estratégias de tutela, de modo que o direito à autodeterminação informativa e o direito à proteção dos dados pessoais imperam-se como direitos fundamentais e, portanto, sendo condições de cidadania, não podem ser deixados à mercê da auto-regulamentação ou das relações contratuais, exigindo-se do Estado uma tutela positiva e proativa; tais como garantias institucionais, que remetem à "existencia de determinadas instituciones, a las que se considera como componentes esenciales y cuya preservación se juzga indispensable para asegurar los principios constitucionales"[97].

---

[96] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 128-129.

[97] ESPANHA. Tribunal Constitucional de Espanha (Pleno). Sentença nº 32/1981, de 28 de julho. *Boletín Oficial del Estado,* n. 193, 13 de agosto de 1981, p. 31.

Para isso, necessário apontar cinco estratégias para a proteção desse novo direito à privacidade. A primeira estratégia é reforçar e ampliar o direito à oposição contra determinadas formas de coleta e de circulação de dados pessoais, possibilitando tanto iniciativas individuais, quanto proposições coletivas, à medida em que fortalece o equilíbrio de poderes para permitir com que os interessados se oponham ao tratamento de dados e exercem seus direitos[98]. O RGPD, no seu art. 21º, estabelece que "o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito", inclusive no que tange à coleta de dados para efeitos de comercialização direta e a criação de perfis baseada nessa relação[99].

Aliado ao direito de oposição, a segunda estratégia deve levar em conta e aperfeiçoar o direito de não saber, isto é, o direito de resistir ao tratamento e de receber as informações daí provenientes, que possam causam algum trauma ou incômodos à paz e ao bem-estar do suposto interessado[100]. Trata-se, pois, da possibilidade de recusar marketing direto, de não receber publicidade não desejada ou não solicitada ou baseada em tratamento de dados sensíveis, cancelar inscrições em assinaturas para recebimento de correios de diferentes tipos, como publicidade, notícias, *newsletters, spam,* inclusive propagandas políticas.

A terceira estratégia deve pôr de relevância o direito ao esquecimento, isto é, o direito de apagamento dos dados pessoais, sem demora injustificada, especialmente nos casos em que as informações deixarem de ser necessárias para a finalidade que havia motivado o tratamento, ou quando o titular retira o consentimento em que se baseia a manipulação

---

[98] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 133.

[99] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679. Acesso em: 18 abr. 2019.

[100] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 133-134.

das informações, sendo esse direito extensível, inclusive, aos buscadores e indexadores de páginas eletrônicas[101]. Contudo, há que considerar que o direito ao esquecimento é uma das categorias polêmicas do direito à proteção dos dados pessoais, uma vez que, por outro lado, há a argumentação sobre prevalência de motivos de interesse público, liberdade de expressão, liberdade de informação, pessoa ou fato público, cumprimento de determinada obrigação legal, entre outros casos.

A quarta estratégia trata da necessidade de tornar mais claro, mais premente, mais visível e mais compreensível o princípio da finalidade, isto é, a condição que ratifica a coleta e o tratamento dos dados pessoais por parte dos controladores e operadores, devendo este fim ser determinado, explícito e legítimo, conforme, por exemplo, determina o art. 5.1, "b", do RGPD[102]. Isso quer dizer que não deveria bastar a mera aposição da indicação da finalidade, mas, sim, importar em recursos e ferramentas para que o usuário tenha a completa ciência das causas, consequências e impactos do consentimento que está provendo, levando em consideração, inclusive, a crítica acima sobre o consentimento na era do consumo de produtos e serviços em rede.

Por fim, a quinta estratégia é, em realidade, uma virada no pensamento. Isso, pois, se é verdade que o fornecimento de dados pessoais é o *login* da sociedade em rede e o consentimento do titular é virtualmente viciado em razão da necessidade de consumir irracionalmente as redes sociotécnicas em detrimento do correto entendimento das implicações oriundas pela entrega e tratamento das informações pessoais, então a privacidade pode servir como ferramenta para equilíbrio de poderes nessa nova arquitetura social a partir da limitação dos interesses das agências institucionais de segurança e das corporações econômicas, de modo que, nascida como uma particularidade, a privacidade pode ser entendida, cada

---

[101] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 134.

[102] UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679. Acesso em: 18 abr. 2019.

vez mais, como um instrumento coletivo de transcendência social, sendo que os defeitos e os fracassos das leis e regras "[...] son resultado de asociar la privacidade con los intereses de las personas, los que al final suelen verse opacados por necesidades sociales antagónicas"[103].

2.2.7 O Efeito Orwell: o direito à privacidade na sociedade de vigilância

Com a popularização das tecnologias de informação e comunicação, parece emergir uma democratização do público, à medida em que cada vez mais se fala em motivos, interesses e identidades públicas e menos em aquilo que é privado, reservado, íntimo, embora o tema da privacidade esteja no imaginário coletivo. No final do século XX, falava-se no "fim da privacidade", mas adentra-se no novo século com a criação de escudos de privacidade, leis de acesso à informação, leis de regulação da internet, das telecomunicações e dos serviços da sociedade de informação, bem como regulamentos e leis de proteção de dados pessoais por todo o mundo, além de decisões e sentenças defendendo a garantia das dimensões do direito à privacidade.

Há, contudo, quem defenda que a privacidade é um parêntesis da modernidade, ficando entre as pequenas comunidades do mundo pré-moderno que já não existem e a comunidade global da pós-modernidade ainda por vir, ambas, porém, marcadas pelo controle social e vigilância dos cidadãos[104]. Nesse contexto, a tutela da privacidade fica condicionada aos interesses e avanços econômicos ou ainda a uma autorregulação pelo mercado, o que pode comprometer ainda mais a verdadeira proteção desse direito, já que as redes de poder financeiro tendem a eliminar os espaços próprios da privacidade em favor do lucro e da publicidade[105].

---

[103] NISSENBAUM, Helen. *Privacidad amenazada*: tecnología, política y la integridad de la vida social. Tradujo: Enrique Mercado. México: Editorial Océano, 2011, p. 95

[104] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 144.

[105] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 144

Por outro lado, a privacidade entendida como além do direito de ser deixado só pode ser transformada em ferramenta social no jogo de poderes da sociedade em rede, quando consegue limitar e controlar diretamente os sujeitos públicos e privados que coletam e tratam os dados pessoais. Se as informações pessoais são o ouro mais importante do novo século, a exigência de um direito à privacidade positivo, regulado, explícito e sancionador pode contribuir para equilibrar os interesses, de forma que, sendo um contrapeso nessa balança, pode representar um exercício de democracia.

Deve-se, portanto, rechaçar a justificativa de que o cidadão honesto não possui nada a esconder, tampouco a temer, a partir da disseminação das informações e do tratamento oriundo dessa coleta, haja vista que a metáfora do homem de vidro é, na verdade, uma expressão totalitária, que chancela a pretensão do Estado de tudo saber, inclusive os aspectos mais íntimos dos indivíduos. O Efeito Orwell deve ser ao revés, possibilitando que os sujeitos vigiem o Grande Irmão, sob todos os lados e esferas, num Estado de vidro, já que o ente estatal, caracterizado pelo público, deve estar ao controle da multidão.

O direito à privacidade e – especialmente a regulação desse direito, com a criação de limites e princípios –, pode ser usado como moeda de troca para exigir cada vez mais transparência da Administração Pública, não necessariamente uma transparência recebida, mas, se for necessário, uma transparência forçada[106]. É o caso da contravigilância, exercida substancialmente por movimentos e atores de hackativimo, ativismo midiático, *cypherpunks* e *whistleblowers*, que intentam "inverter o vetor dominante de vigilância social, para, com isso, produzir novas narrativas sociais por meio de práticas adjacentes de controle e vigilância do próprio Estado e/ou

[106] CASTELLS, Manuel. *A galáxia internet:* reflexões sobre internet, negócios e sociedade. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007, p. 220.

das grandes corporações empresariais, especialmente por movimentos sociais"[107].

A contravigilância trata do conjunto de atores, processos, atuações e dispositivos, normalmente ligados em redes, para proteger "contra a vigilância perpetrada pelos órgãos institucionais e pelas corporações empresariais e, mais ainda, vigiar quem também vigia o corpo social, na tentativa de fazer cessar violação de direitos e garantias fundamentais e humanas"[108]. A contravigilância em sentido estrito trata da específica tentativa de neutralizar a vigilância perpetrada pelo Estado e pelas grandes corporações, a partir de técnicas de bloqueio de uma vigilância dominante ou desestabilização do vigilante, relevando e divulgando a sua atuação, tornando públicos documentos e informações de interesse público, noticiando violações de direitos e garantias, dentre outras práticas[109].

É dizer, se não há outra alternativa para os indivíduos no século XXI que não seja o controle da circulação das informações, uma vez que a economia de vigilância e ao fornecimento de dados pessoais é a realidade determinista que se aproxima, é possível utilizar-se das tecnologias de informação e comunicação para vigiar o Estado e as grandes corporações causando um incômodo público para que sejam cada vez mais públicas, transparentes, cristalinas[110]. Trata-se de vigiar quem vigia para que estejam desconfortáveis o suficiente para que sigam as regras; trata-se de invadir a publicidade de quem viola a privacidade para que estejam preparados a respeitar as novas dimensões do direito à privacidade na sociedade em rede.

---

[107] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192 f. Dissertação (Mestrado) - Curso de Direito, Departamento do Direito, Universidade Federal de Santa Maria, Santa Maria, 2018, p. 102.

[108] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192 f. Dissertação (Mestrado) - Curso de Direito, Departamento do Direito, Universidade Federal de Santa Maria, Santa Maria, 2018, p. 102.

[109] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192 f. Dissertação (Mestrado) - Curso de Direito, Departamento do Direito, Universidade Federal de Santa Maria, Santa Maria, 2018, 103.

[110] ROSANVALLON, Pierre. *La contrademocracia*: la política en la era de la desconfianza. Buenos Aires: Manantial, 2007.

Conclusão

Com o presente estudo foi possível analisar os impactos das tecnologias de informação e comunicação e do regime global de vigilância social no direito à privacidade, no contexto da cibersegurança do século XXI. Objetivamente refletiu-se sobre: a) as implicações do regime de monitoramento social global e os impactos na sociedade do século XXI; b) a contribuição dos indivíduos nesse regime global de vigilância social a partir do fornecimento de dados para acesso a produtos e serviços; c) a estrutura normativa global e regional do direito à privacidade, mudança e abordagens do conceito ao longo do tempo; e, por fim, d) a ressignificação do direito à privacidade no contexto da cibersegurança.

Na sociedade em rede do século XXI, há o recrudescimento de um regime global de vigilância social, baseado na cooperação entre agências estatais para monitorar o fluxo de dados na sociedade e controlar pessoas e grupos de interesse, por meio da manipulação das informações pessoais. A vigilância social, desde séculos, funciona como um dispositivo para exercício de poder, de forma que tal dominação foi revolucionada com o desenvolvimento das tecnologias de informação e comunicação e com o advento da grandeza informática do *big data*.

Esse regime global de vigilância social está fundamentado em discursos oficiais legitimadores, transpostos a normativas nacionais e internacionais, justificando o monitoramento de cidadãos nacionais e estrangeiros em prol do combate a inimigos abstratos, como o terror, para garantir segurança e defesa nacional, dentre outros argumentos, sem o devido conhecimento público e publicidade necessária, tanto que os programas de monitoramento foram divulgados sob polêmica e embaraços internacionais. Percebeu-se, então, o advento de um Estado de vigilância,

fazendo-se presente na vida das pessoas de forma invisível, não hierárquica, descentralizada e personalizada, numa nova arquitetura social de sociedade em rede.

No marco dessa nova arquitetura social, os usuários contribuem com o funcionamento desse sistema, marcado pela manipulação de algoritmos e criação de padrões comportamentais, a partir do fornecimento de dados pessoais. Nessa sociedade em rede de fluxos comunicacionais mundiais, há uma lógica consumista de tecnologias de informação e comunicação e um processo de subjetivação contínuo e modulado, já que a construção de uma identidade pública depende da entrega das informações pessoais.

Se antes a vigilância dependia de dispositivos institucionais, agora ela está distribuída nos dispositivos pessoais, numa reinvenção do panóptico de poder pelo homem-caramujo, isto é, aquele que carrega em si mesmo uma vigilância, que, por outro lado, também permite a vigilância do outro, numa retroalimentação de dados. No panorama da Internet das Coisas e da Internet de Tudo, trata-se de uma economia de vigilância, a partir do fornecimento de dados pessoais para acesso de produtos e serviços, como se fosse um novo ouro do século XXI, que, ao fim e ao cabo, torna-se condição para participação nesse novo paradigma social tecnológico.

O direito à privacidade, inclusive a partir de figuras afins, como "vida privada e familiar" e "intimidade", é estabelecido nas principais normativas internacionais, comunitárias, regionais e, até mesmo, nacionais espanholas e brasileiras. O desafio é que a privacidade, como a conhecemos, a partir de uma perspectiva histórica, filosófica e jurídica, como substancialmente o direito de ser deixado só e de não sofrer interferências alheias e estatais naquilo que é privado, revolucionou-se nesse novo paradigma social derivado dos avanços das tecnologias da informação e comunicação.

De aí, novos riscos e ameaças surgiram, possibilitando outras formas de violação da privacidade, tendo em vista os diferentes processos de manipulação e tratamento de dados pessoais, de característica automatizada e contínua. Desse modo, o conceito tradicional tornou-se insuficiente para

tratar desse novo quadro tecnológico, fazendo-se referência a novas nuances que foram surgindo, como o direito à autodeterminação informativa e o direito à proteção de dados pessoais, de modo que a privacidade abrangeu também o controle sobre a circulação das próprias informações pessoais.

Há uma preocupação estatal-normativa para tutelar o direito à privacidade (embora muito baseada na lógica de "pessoa-informação-sigilo"), tanto que essa proteção aparece, ainda que como outras figuras, em diferentes normativas internacionais, comunitárias, regionais e nacionais. Porém, recentemente há um esforço da jurisdição em ampliar esse direito frente às novas tecnologias de informação e comunicação, como ocorreu com o estabelecimento do direito à autodeterminação informativa e o direito à proteção de dados pessoais como direitos fundamentais. Há, também, por essa razão, o advento de novas normativas, como é o caso do Regulamento Geral de Proteção de Dados Pessoais da União Europeia e a Lei Geral de Proteção de Dados Pessoais do Brasil, entre outras leis de tutela de informações pessoais.

Diante do recrudescimento do regime global de vigilância social, com dispositivos de vigilância distribuídos pelo globo por meio de tecnologias de informação e comunicações pessoais e personalizadas, bem como diante da necessidade de fornecimento de dados pessoais para acesso e consumo de produtos e serviços da sociedade em rede, numa lógica de subjetivação e exclusão em caso de não participação e não entrega dessas informações pessoais, o conceito de privacidade como o "direito de ser deixado em paz" ou o "direito de ser deixado só" é insuficiente para tutelar essa nova realidade social, ainda que essa nova característica de reservado não deixou de existir em si, senão que há novas dimensões que necessitam uma maior reflexão.

Efetivamente, a privacidade, na concepção tradicional, sofre diferentes tipos de violação de proteção. Ora, o panorama anterior de "pessoa-informação-sigilo", em que o sujeito podia se proteger de intromissões indesejadas naquilo que lhe é reservado, acaba por ser insuficiente

considerando esse regime global de vigilância social e esse fornecimento de dados como *login* da sociedade em rede.

Isso, porque, por um lado, embora o indivíduo queira manter o sigilo sobre determinadas informações e definir aquilo que é sua privacidade, as agências de segurança nacional e agências estatais, em parceria com empresas de tecnologias, interceptam, monitoram, classificam e trocam dados pessoais coletados; por outro lado, o determinismo social que exige o fornecimento de dados pessoais para acesso de produtos e serviços tecnológicos também rompe com a lógica do sigilo, ainda mais quando o sujeito não tem plena consciência e consentimento sobre a entrega das informações pessoais.

Numa realidade em que tudo e todos estão interconectados, ainda que não necessariamente digitalmente, numa sociedade em rede, é preciso reconhecer que o paradigma da arquitetura social está mudando, exigindo-se uma adaptação frente às complexidades de ser. É dizer, se o direito e a normatividade precisam acompanhar a evolução social, buscando ajustarem-se às mudanças e novidades, é imprescindível desapegar de dogmas jurídicos e atualizar as condições de regulação. É o fim do direito à privacidade, mas não no tom aterrorizado do final do século XX, mas como o se conhece e como foi transposto em normativas ao redor do globo.

Em conclusão, é necessário repensar o direito à privacidade, considerando o regime global de vigilância social e a alteração de paradigma permitido com as tecnologias de informação e comunicação. É preciso aceitar que chegou ao fim um largo processo evolutivo de conceituação do direito à privacidade como um direito de ser deixado em paz, passando-se a tratar de um direito de controle sobre as informações pessoais, considerando os diferentes paradoxos que a privacidade abraça no século XXI, especialmente no que tange à fluidez dos espaços público-privado, ao advento de uma nova dimensão de extimidade e à suposta falácia de consentimento informado.

O direito à privacidade mudou para uma lógica "pessoa-informação-circulação-controle", apontando-se, para tutela desse novo direito, cinco estratégias, como a ampliação do direito à oposição contra o tratamento de dados pessoais, o alargamento do direito de não saber e resistir ao recebimento e ao tratamento de informações, o estabelecimento do direito ao esquecimento, especialmente digital, o melhoramento do princípio da finalidade e, por fim, o giro de pensamento sobre o que pode significar a privacidade em tempos de cibersegurança. Assim, analisou-se que a privacidade do século XXI pode ser entendida como um direito coletivo para exigir cada vez mais transparência daqueles que tratam os dados; para que se sintam incômodos a ponto de respeitarem as regras e protegerem a privacidade dos cidadãos, numa revisão da obra orwelliana.

O século XX revolucionou os processos comunicativos e o fluxo de ideias na sociedade hiperconectada, mas o século XXI inicia projetando uma maior troca de informações, numa economia de dados pessoais, sendo cada vez mais iminente a livre circulação de pessoas, produtos, serviços e dados em comunidades digitais do mundo, inclusive numa Internet de Tudo. Trata-se de uma força imparável, em que o direito à privacidade, somente entendido na concepção individual de "pessoa-informação-sigilo" não pode ser um objeto inamovível, sob pena de uma catástrofe normativa e uma falácia reguladora.

No regime global de vigilância social, aqui entendido como o panorama de monitoramento de informações pessoais e de fornecimento de dados pessoais para acesso de produtos e serviços na sociedade em rede, o direito à privacidade pode supor um regime global de contravigilância social. Portanto, pode-se inverter o vetor determinante de vigilância, para vigiar quem vigia, tornando-se os que, até então, eram objetos de vigilância em sujeitos de vigilância, de modo que esse regime, inevitável por si só diante dos avanços das tecnologias de informação e comunicação, siga as regras do jogo democrático.

Em uma visão holística do mundo, sob a lógica "pessoa-informação-circulação-controle", compreende-se o direito à privacidade, além de todas

as dimensões antes discutidas e antes previstas, também como um direito de interesse social coletivo, pertencido a uma coletividade, a uma transindividualidade. Isto é, ademais de ser um direito individual, em que o sujeito pode requerer a tutela para si, o direito à privacidade também pode ser visto como uma garantia institucional, um direito de todos de exigir uma proteção especial e difusa, direcionada ao corpo social, ao corpo multidão.

Parte II

El efecto Orwell en la sociedad en red: ciberseguridad, régimen global de vigilancia social y derecho a la privacidad en el siglo XXI

Introducción

En la sociedad en red, nuevos actores sociales y nuevas relaciones sociales se entremezclan, de modo transversal y multidireccional, proporcionando un mayor flujo de comunicación y una distribución nodal de interacciones, incluso en lo que se refiere a las relaciones de poder. Las redes, formadas por nodos, aristas y *clusters*, compiten o cooperan entre sí, marcadas por el uso de nuevas tecnologías de la información y de la comunicación, en una horizontalización de la comunicación a gran escala, a medida que las nuevas plataformas permiten una interacción expansiva, sin la necesaria intervención de canales de comunicación o liderazgos.

La evolución tecnológica y la globalización han creado nuevos desafíos relacionados con la privacidad y la protección de los datos personales, ya que, en el horizonte del *Internet de las Cosas* y del *Internet de Todo*, la recogida, el tratamiento y el intercambio de datos registraron un aumento significativo, permitiendo que las corporaciones privadas y las instituciones públicas utilicen los datos personales en una escala sin precedentes durante el ejercicio de las actividades de las actividades cotidianas. Por otro lado, las personas suministran cada vez más su información, de manera pública y global, teniendo en cuenta que la disponibilidad de los datos personales es condición para el acceso de productos y servicios en la sociedad en red.

En el siglo XX, con la profusión de las tecnologías de información y comunicación, los mecanismos de control y vigilancia, especialmente estatales, se perfeccionaron y se convirtieron en herramientas útiles para una vigilancia general y diseminada, de forma institucional. En la sociedad en red, la vigilancia es líquida, omnipresente y, a veces, pasa desapercibida por los vigilados, ejerciendo sobre éstos un control sobre las formas de vivir. Y, en sentido inverso, los sujetos acaban renunciando a derechos y

garantías fundamentales, en particular, a la privacidad, al suministrar información personal que les es exigida para acceder a productos y servicios, contribuyendo a una economía de vigilancia y circulación de datos, muchas veces sin verdadera conciencia de las implicaciones y de los impactos de esa subjetivación tecnológica.

La presente investigación tiene por objeto el estudio acerca de la vigilancia social y la privacidad en la sociedad en red. Se pretende analizar la resignificación del derecho a la privacidad afectado por el régimen global de vigilancia social de datos personales en el contexto de la ciberseguridad del siglo XXI, en razón de la alteración de paradigma producida por el avance de las nuevas tecnologías de la información y comunicación. Por lo tanto, ¿se cuestiona en qué medida y por cuáles supuestos el régimen global de vigilancia social de datos personales puede afectar el derecho a la privacidad en el contexto de la ciberseguridad del siglo XXI?

El objetivo general de esta obra es analizar los impactos de las tecnologías de información y la comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de la ciberseguridad del siglo XXI. En lo que se refiere a los objetivos específicos, se pretende: a) investigar las implicaciones del régimen de monitoreo social global y los impactos en la sociedad del siglo XXI; b) identificar la contribución de las personas en dicho régimen global de vigilancia social a partir del suministro de datos para el acceso a productos y servicios; c) establecer la estructura normativa global y regional del derecho a la privacidad, el cambio y los enfoques del concepto a lo largo del tiempo; y, finalmente, d) discutir la resignificación del derecho a la privacidad, basada en nuevos conceptos, nuevos espacios, nuevos límites y nuevas posibilidades en el contexto de la ciberseguridad.

La actualidad del tema está presente, porque el libro aborda discusiones de la posmodernidad y de la sociedad en red, panorama sociopolítico actual, marcado por el flujo continuo de informaciones entre sujetos y multitudes digitalmente conectadas, especialmente considerando los impactos de las nuevas tecnologías de información y la comunicación sobre

los derechos y garantías fundamentales, que se mejoran y perfeccionan cada día. Sin embargo, se percibe que el derecho a la privacidad, uno de los pilares de los derechos fundamentales, está pasando por cambios, incluso de paradigma, en razón de la producción y suministro de datos personales en la red.

Además, la investigación trata detalladamente del derecho a la privacidad y otras dimensiones derivadas, cuyo bien jurídico protegido ha sido recientemente tutelado por el Reglamento General de Protección de Datos de la Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por la que se deroga la Directiva 95/46 / CE, con aplicación obligatoria a partir de mayo de 2018, en atención a nuevos avances de las tecnologías de la información y comunicación. En cuanto a España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se encargó de adaptar la normativa comunitaria en el territorio nacional. En el caso brasileño, la Ley nº 13.709, de 14 de agosto de 2018, ha establecido la Ley General de Protección de Datos Personales (LGPD), que inaugura ese nuevo régimen jurídico en Brasil.

La investigación pone de relieve las implicaciones sociales y doctrinales, teniendo en cuenta que el propio Reglamento pone relevancia en el hecho de que los principios y las reglas en materia de protección de las personas físicas en relación con el tratamiento de sus datos personales, independientemente de la nacionalidad o el lugar de residencia de dichas personas, deben respetar los derechos y libertades fundamentales. Así, cada vez más se hace necesario abordar la problemática del derecho a la privacidad frente a los avances de las tecnologías de información y comunicación, formando profesionales capaces de reflexionar críticamente sobre la materia.

Se registra que la presente obra es derivada de las investigaciones desarrolladas por el autor en los años de 2018 y 2019, así como en el Trabajo Fin de Máster presentado, en el ámbito del Máster Universitario en Derecho de la Ciberseguridad y Entorno Digital de la Universidad de León, en León, España, bajo la tutoría del Prof. Dr. Salvador Tarodo Soria. Dentro del programa español, una competencia a ser desarrollada por los estudiantes es justamente conocer el sistema de fuentes, derechos y libertades fundamentales y los principios básicos del Derecho de la Ciberseguridad y del Entorno Digital, sabiendo integrar conceptos multidisciplinares para poder analizar, interpretar y resolver problemas y conflictos jurídicos, políticos y sociales que surgen en ese campo.

En esa misma perspectiva, el máster se encuadra en el marco de cooperación entre la Fundación Carolina y el Instituto Nacional de Ciberseguridad de España – INCIBE, ya que uno de los objetivos de esa institución, para enfrentar los desafíos planteados por los avances de las tecnologías de información y comunicación, es precisamente intentar satisfacer adecuadamente la demanda social de profesionales altamente calificados en las normativas sobre ciberseguridad y entorno digital, en la medida que las investigaciones realizadas por el autor fueron financiadas por estas dos instituciones.

El recorrido metodológico del presente libro debe pasar, en vista de los objetivos a ser atendidos y del problema de investigación, por cuatro momentos: a) investigación preliminar sobre la temática del régimen global de vigilancia social por parte de las agencias institucionales; b) investigación preliminar sobre la temática de la vigilancia, pero desde el punto de vista de las personas físicas y multitudes: c) revisión de conceptos y normativas relativas al derecho a la privacidad y sus dimensiones, especialmente tratados internacionales, reglamentos comunitarios y leyes específicas; y, d) un debate más profundo sobre el derecho a la privacidad en la sociedad de vigilancia.

En cuanto a la metodología de abordaje, se utiliza el método deductivo, porque se realiza una conexión descendente entre los temas tratados,

partiéndose de un plan general y premisa general para proceder al análisis de panoramas específicos, a fin de obtener una conclusión a partir de ese silogismo lógico. En otras palabras, se investiga, primero, el ascenso de una sociedad basada en una economía de vigilancia de datos, que permite la vigilancia de actores sociales por parte de agencias institucionales y por parte de grandes corporaciones, para, posteriormente, verificar cómo ese nuevo paradigma afecta al derecho a la privacidad.

En cuanto a la metodología de procedimiento, se utiliza el método de revisión bibliográfica, con el objetivo de estudiar la vigilancia social, desde el punto de vista de la razón gubernamental dominante y también del tratamiento de datos personales por las grandes corporaciones, para analizar detalladamente el derecho a la privacidad en el siglo XXI. Para ello, a través del estudio científico de actores sociales, procesos comunicativos y factores organizativos de esta nueva sociedad en red involucrando la vigilancia de datos, se pretende obtener conclusiones sobre el tema e investigar críticamente los efectos en el derecho a la privacidad.

Para ello, se pretende aplicar las técnicas de investigación de documentación indirecta y documentación directa. Así, se utiliza la investigación documental y bibliográfica, considerando que gran parte de la revisión bibliográfica realizada en el presente estudio se centra en la literatura especializada en el tema, especialmente sobre derecho a la privacidad y los efectos de los nuevos paradigmas sociales sobre derechos y garantías fundamentales; otra parte vendrá de normativas internacionales, comunitarias y nacionales, así como de noticias y trabajos científicos realizados sobre la temática, entre otras.

El marco teórico de base adoptado se sirve de las construcciones de, principalmente, Michel Foucault (vigilancia como panóptico de poder), Gilles Deleuze (datos y vigilancia en la sociedad de control), Gleen Greenwald (régimen de vigilancia global), Zigmunt Bauman (vigilancia en la post-modernidad y post-panóptico), Manuel Castells (sociedad en red), Stefano Rodotà (privacidad en la sociedad de vigilancia), entre otros; ya que se intenta analizar el impacto del avance de las tecnologías de información y la

comunicación en la comunidad global, evidenciando las relaciones de vigilancia características de la sociedad en red basadas en el tratamiento de datos personales, así como analizando el impacto de ese nuevo paradigma en el derecho a la privacidad

En términos estructurales, la investigación está desarrollada en dos grandes capítulos, demostrando la relación existente entre la premisa general y específica. El primer capítulo, por su vez, es subdividido en dos grandes bloques: el primer apartado trata sobre el panóptico del siglo XXI y la vigilancia realizada por las agencias de seguridad nacionales; el segundo aborda la contribución de los usuarios para el suministro de datos para acceso a productos y servicios. Por otro lado, el segundo capítulo también está subdividido en dos grandes bloques: el primero analiza la evolución del derecho a la privacidad hasta el derecho a la protección de datos personales; el segundo reflexiona sobre el cambio del paradigma del derecho a la privacidad hacia un régimen colectivo de protección.

3

“El Gran Hermano te vigila”: la vigilancia social y el procesamiento de datos en la sociedad en red del siglo XXI

El título del presente capítulo hace referencia a una de las frases más conocidas de la obra “1984”, de George Orwell: “El Gran Hermano te vigila”, significando la vigilancia marcada de Oceanía, escenario de fondo para las reflexiones del personaje principal, Winston Smith. En la ciudad en que pasa la historia, hay carteles enormes, en diferentes lugares, con una imagen del Gran Hermano, líder del Partido, para recordar en todo momento que los ciudadanos están siendo vigilados y deben comportarse según lo determinado por las fuentes de poder.

La frase - y la propia historia referenciada - es oportuna para el presente capítulo, ya que el avance de las tecnologías de la información y comunicación, especialmente de la microelectrónica y de la nanoelectrónica, han posibilitado la creación de mecanismos de vigilancia de los ciudadanos, a partir de la interceptación de los datos personales que, a su vez, pueden ser entendidos como el oro de esta nueva arquitectura social surgida después del final de la Segunda Guerra Mundial, ya que el suministro de la información personal es condición para el acceso y la participación en la sociedad en red.

Considerando que el objetivo general de este libro es analizar los impactos de las tecnologías de información y comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de la ciberseguridad del siglo XXI, este capítulo, como forma de introducir premisas generales sobre el tema, pretende: a) investigar las implicaciones

del régimen de monitoreo social global y los impactos en la sociedad del siglo XXI; y b) identificar la contribución de las personas en dicho régimen global de vigilancia social a partir del suministro de datos para el acceso a productos y servicios.

3.1 La búsqueda del oro del siglo XXI: el régimen global de vigilancia social

El poder puede ser entendido como una práctica social construida a lo largo del tiempo, de forma heterogénea y dinámica, como resultado de una relación de fuerzas en una determinada sociedad, en un determinado momento, estando disuelto por todo el tejido social, siendo ejercido por medio de los dispositivos, es decir, caminos, formas y medios de ejercicio del poder, como el castigo, la disciplina, la sexualidad, la locura, el examen[1]. A partir del siglo XVIII, la vigilancia se transformó en uno de los principales dispositivos para el ejercicio del poder, siendo, a lo largo del tiempo, amplificada y perfeccionada, con el objetivo de imprimir procesos de coerción sobre los sujetos vigilados[2].

3.1.1 Del panoptismo a la vigilancia como dispositivo de poder

En la sociedad disciplinar - el "tiempo de las disciplinas" -[3], los dispositivos de poder, entre ellos, utilizados en las instituciones totales - familia, escuela, cuartel, fábrica, hospital y prisión -, lograban vigilar y castigar a los individuos, en el intento de domesticar y someter los sujetos a moldes predefinidos y utilitaristas, en una especie de disciplina y control sobre el cuerpo[4]. El panoptismo, inspirado en el modelo de Jeremy Bentham, fue, entonces, el arquetipo arquitectónico ideal del "tiempo de las

[1] FOUCAULT, Michel. *Microfísica do poder*. 23 ed. São Paulo: Graal, 2004.

[2] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 196.

[3] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 196.

[4] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 197-198.

disciplinas", ya que, a través de técnicas ópticas y solares, especialmente en composiciones circulares, como prisiones, fábricas y manicomios, era posible crear una vigilancia literalmente institucional[5]. En ese modelo, el individuo sujeto a la disciplina entendía y propiamente visualizaba que estaba siendo permanentemente vigilado, aunque no siempre lo estaba de verdad, pero saber que podría estar siendo vigilado por alguien ya era suficiente para mantener la disciplina y el control, en un "funcionamiento automático del poder"[6].

En la segunda mitad del siglo XVIII, tras la profusión de las medidas disciplinarias, el ejercicio del poder, que antes estaba limitado al cuerpo-individuo en un espacio-tiempo definido, pasó a ser dirigido a una multiplicidad de cuerpos, por medio de procedimientos colectivos, en una biopolítica dirigida al cuerpo-población como masa modular[7]. Es decir, la idea no era sólo moldear al individuo en sí, sino modular una colectividad, para un mayor control, de modo que, para ese fin, los dispositivos de poder deberían adaptarse, la vigilancia debería acompañar los nuevos desafíos, incluso como una táctica de guerra[8].

3.1.2 La revolución de las TICs y el régimen global de vigilancia social

Con el final de la Segunda Guerra Mundial, un sin número de transformaciones ayudaron al cambio de paradigma social, ya que cayeron los muros y las fronteras, permitiendo un flujo de interacciones entre actores sociales en un campo abierto[9]. La vigilancia sufrió intensos cambios y se perfeccionó proporcionalmente a la evolución de las tecnologías de información y comunicación, tornándose horizontalizada (no más

[5] BENTHAM, Jeremy. O panóptico ou a casa de inspeção. In: TADEU, Tomaz (Org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008, pp. 17-30.

[6] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 224-225.

[7] FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005, pp. 285-289.

[8] FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005, p. 293-294.

[9] DELEUZE, Gilles. *Conversações:* 1972-1990. São Paulo: 34, 1992, p. 220.

verticalizada) y difundiéndose por innumerables campos de captación y actuación (no sólo instituciones cerradas), para afectar al mayor número de cuerpos de interés[10].

Durante el conflicto internacional mencionado, agencias estatales y organizaciones de diferentes países, especialmente Reino Unido y Estados Unidos, interceptaron, leyeron y analizaron diversas informaciones intercambiadas por las tropas alemanas y japonesas, creando desde el final de la guerra una red planetaria de inteligencia para escucha y captación de señales, desarrollada a través del Tratado de Seguridad UK-USA (también grafado UKUSA, remitiéndose a las iniciales de los países involucrados). Este acuerdo y la conjetura desarrollada contó con la ayuda de los "Cinco Ojos": Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos; siendo sólo revelado al final del siglo XX y confirmado a principios del siglo XXI[11].

Por lo tanto, el marco de cooperación de inteligencia secreta UKUSA, liderado sustancialmente por la Agencia de Seguridad Nacional de los Estados Unidos (*National Security Agency,* en inglés), entidad también mantenida en secreto por décadas, hizo crear un sistema de vigilancia global, denominado *Echelon*, con capacidad para captar y analizar virtualmente informaciones provenientes de llamadas telefónicas y mensajes de fax, télex, correo electrónico y otros dispositivos, enviados desde cualquier lugar del mundo[12]. Se trata, pues, de una red de espionaje, que,

---

[10] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192p. Tutor: Rafael Santos de Oliveira. [Trabajo Final de Máster]. Máster en Derecho. Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, 2018, p. 41.

[11] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014; NORTON-TAYLOR, Richard. *Not so secret: deal at the heart of UK-US intelligence*. [The Guardian, 25/06/2010]. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.

[12] UNIÓN EUROPEA. *Parlamento Europeo. Informe de 11 de julio de 2001 sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON).* [en línea] [Fecha de consulta: 16/04/2019] Disponible en:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//ES.

por interceptación, capta el tráfico de datos ocurrido por satélite, fibra óptica, frecuencia de radio, microondas, cables submarinos, internet y otras formas de procesamiento de información y comunicación, aunque hay un avance en las técnicas de encriptación.

Conforme a una investigación realizada por el Parlamento Europeo, divulgada en el Informe de 11 de julio de 2011, en el marco del sistema Echelon, datos brutos de comunicación captados por las agencias de inteligencia, tanto de voz, télex, fax e internet, pudieron ser interceptados, registrados, analizados, intercambiados, vendidos y clasificados por medio de filtros, permitiendo la elaboración fácil de perfiles y otros informes por las partes interesadas[13].

Los informes elaborados dan cuenta de que los programas de vigilancia global en masa se perfeccionaron durante el siglo XX, imprimiendo importantes avances tecnológicos para el sistema de inteligencia de señales[14]. En síntesis, se puede decir que, en la década de los 40, cuando el acuerdo de cooperación fue establecido, el objetivo principal de la vigilancia fue el espionaje militar y diplomático; en la década de los 60, el objetivo fue el espionaje comercial e industrial, pasando por sectores económicos y científicos; en la década de los 90, fue el combate contra el crimen organizado, el lavado de dinero, el tráfico de drogas, armas y personas y, más recientemente, y en los próximos años, el combate contra el terrorismo[15].

En 2006, Julian Assange, periodista y ciberactivista, constituyó la WikiLeaks, una organización transnacional en favor de la transparencia, a fin de publicar informaciones y datos confidenciales, especialmente sensibles,

---

[13] UNIÓN EUROPEA. *Parlamento Europeo. Informe de 11 de julio de 2001 sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON).* [en línea] [Fecha de consulta: 16/04/2019] Disponible en:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//ES.

[14] UNIÓN EUROPEA. *Parlamento Europeo. Informe de 11 de julio de 2001 sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON).* [en línea] [Fecha de consulta: 16/04/2019] Disponible en:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//ES.

[15] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

filtrados o hackeados de gobiernos u otras instituciones para que fueran objeto de conocimiento, acceso y crítica públicos[16]. Assange defiende la figura de los *cypherpunks,* los que "defienden la utilización de la criptografía y de métodos similares como medio para provocar cambios sociales y políticos", de forma que "creado a principios de los años 1990, el movimiento alcanzó su auge durante las 'criptoguerras' y después de la censura de internet en 2011, en la Primavera Árabe" [traducción libre][17].

En 2010, Chelsea Manning, en la época, Bradley Manning, suministró a WikiLeaks más de 700.000 archivos secretos, vídeos de enfrentamientos y comunicaciones diplomáticas del Departamento de Estado de los Estados Unidos, siendo detenida en 2013 en una penitenciaría militar y sometida a técnicas de privación de sueño, desnudez forzada y tortura psicológica, detención considerada inhumana e ilegal por Amnistía Internacional[18]. La activista fue llevada a juicio y condenada a 35 años de prisión, pero el ex presidente de Estados Unidos, Barack Obama, conmutó su sentencia antes de dejar el cargo en 2017[19].

En 2013, Edward Snowden, analista de sistemas hasta entonces funcionario del gobierno estadounidense, hizo público una gran cantidad de informaciones confidenciales sobre la existencia y actuación de la Agencia Nacional de Seguridad de Estados Unidos, así como sobre los programas que componen un sistema de vigilancia global americano, entre ellos el PRISM[20]. En detalle, Snowden viajó a Hong Kong en mayo de 2013, donde entregó documentos probatorios a los periodistas Glenn Greenwald y Laura Poitras, los cuales fueron revelados por los portales *The Guardian,*

---

[16] WIKILEAKS. *What is WikiLeaks*. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: https://wikileaks.org/What-is-Wikileaks.html.

[17] ASSANGE, Julian. *Cypherpunks*: liberdade e futuro da internet. São Paulo: Boitempo, 2013, p. 5.

[18] AYUSO, Silvia; PEREDA, Cristina. *Obama conmuta la pena de la soldado Chelsea Manning.* [El País, 18 jan. 2017] [en línea] [Fecha de consulta: 10/04/2019] Disponible en: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html.

[19] AYUSO, Silvia; PEREDA, Cristina. *Obama conmuta la pena de la soldado Chelsea Manning.* [El País, 18 jan. 2017] [en línea] [Fecha de consulta: 10/04/2019] Disponible en: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html.

[20] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

The Washington Post y *The Intercept*, generando una crisis institucional y una incomodidad global, tanto que el activista vive actualmente bajo asilo político[21].

A partir de 2013, con la filtración de documentos ultrasecretos, se descubrió la existencia de otros programas de vigilancia global, tanto en el marco del sistema Echelon, es decir, vinculados a él o sometidos a él, o no. Por ejemplo, *PRISM*, de Estados Unidos, Australia, Reino Unido y Países Bajos; *XKeyscore*, de Estados Unidos, Alemania, Australia y Nueva Zelanda; *Project 6,* de Alemania y Estados Unidos; *Stateroom,* de Cinco Ojos; *Lustre,* de Estados Unidos y Francia; *Optic Nerve*, de Estados Unidos y Reino Unido; *Turbine*, de Estados Unidos, Reino Unido y Japón; *Operation Socialist*, de Reino Unido; *Tempora, Muscular, Follow The Money, Marina, Dishfire, Mystic*, estos todos de Estados Unidos, pudendo haber o no coordinación con otras agencias asociadas[22].

Los Estados Unidos, en el seno de la *National Security Agency*, admitieron tener dos programas: *PRISM* y *UPSTREAM*. PRISM es un programa de inteligencia que permite la obtención de material de inteligencia solicitado junto a los proveedores de servicios (desde que previa intervención judicial que debe autorizar la intervención), de manera detallada y direccionada, aunque sin gran capacidad de *data mining*, estando regulado por el *Foreign Intelligence Service Act* (FISA)[23]. Por su parte, UPSTREAM es un programa de inteligencia que recoge datos oriundos de comunicación por cables de fibra óptica e infraestructura de los proveedores de servicio, el

[21] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

[22] PIRES, Hindenburgo Francisco. Geografia das indústrias globais de vigilância em massa: limites à liberdade de expressão e organização na internet. *Ar@cne Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales*, Universidad de Barcelona, n.º 183, abr. 2014. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: http://www.ub.edu/geocrit/aracne/aracne-183.htm#_edn16.

[23] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15).* Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

cual permite acceso a los datos globales, incluso de ciudadanos no estadounidenses[24].

El Reino Unido, a través de la agencia *Government Communications Headquarters*, con la sigla GCHQ, confirmó operar con el programa denominado *Tempora*, que hace posible el acceso y almacenamiento de informaciones de datos de portadores[25]. El programa permite comparar el tráfico de datos con un rol de selecciones y búsquedas predeterminadas de un objeto específico para realizar una clasificación de la comunicación realizada[26]. La agencia argumenta que el sistema es refrendado por el *Regulation of Investigatory Powers Act 2000 (RIPA),* legislación interna que permite que el Secretario de Estado expida órdenes de interceptación de comunicaciones[27].

Importante tratar sobre otros tres de estos programas para comprender la magnitud del monitoreo de datos. Así, *XKeyscore*, uno de los primeros sistemas informáticos operados por la *NSA* y compartido con Alemania, Australia y Nueva Zelanda, en la forma de un motor de búsqueda, permite, según Snowden que ya tuvo autorización para acceder a él, la recuperación de datos de todos los registros recolectados diariamente en todo el mundo, disponiendo de herramientas capaces de captar todo lo que los usuarios hacen en la red[28].

---

[24] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[25] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[26] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[27] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[28] GREENWALD, Glenn. *XKeyscore*: NSA tool collects 'nearly everything a user does on the internet'. [The Guardian, 31/07/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Por otra parte, el programa *Lustre*, dirigido especialmente por la *Direction Générale de la Sécurité Extérieure - DGSE*, agencia de seguridad de Francia, con cooperación de los Cinco-Ojos, especialmente de la *NSA*, se basa en la posición geoestratégica en el tráfico de datos electrónicos, puesto que la mayoría de los cables submarinos de comunicaciones que conecta África adentra al continente europeo por el territorio francés, de modo que el *DGSE* puede interceptar los datos transmitidos y compartirlos con sus socios[29]. Por último, el programa *Stateroom*, creado por las agencias de seguridad de Estados Unidos, Canadá, Australia y el Reino Unido, es un proyecto de interceptación global masiva basada en operaciones en más de ochenta embajadas y consulados estadounidenses repartidos por el globo, que, a través de un *exploit*, generado a partir de la infección de más de 50.000 redes de comunicaciones en todo el mundo por un *malware* de vigilancia masiva, puede interceptar mensajes en cualquier momento, independientemente del conocimiento del usuario[30].

Además de agencias de seguridad e inteligencia de los países referidos, se verificó que importantes universidades también estuvieron involucradas en el proyecto para proveer bases científicas para tales programas de vigilancia, como, por ejemplo, *University of California, Stanford University, Massachusetts Institute of Technology (MIT), University of California Berkeley, California Institute of Technology (Caltech)* y *Johns Hopkins University*. Más aún, documentos secretos mostraron la cooperación y suministro de informaciones por parte de empresas y organizaciones de sectores económicos, como *Google, Facebook, Microsoft, Apple, Verizon, Vodafone, EDS, AT&T, Qwest, Motorola, Intel, IBM, Qualcomm, Cisco, H-P, Oracle*, entre otras[31].

---

[29] FOLLOUROU, Jacques. *Surveillance*: la DGSE a transmis des données à la NSA américaine. [Le Monde, 30/10/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html.

[30] DERIX, Steven. MODDERKOLK, Huib. *50.000 pakketjes kwaardaardige software*. [NRC, 23/11/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.nrc.nl/nieuws/2013/11/23/50000-pakketjes-kwaardaardige-software-1316266-a1157982.

[31] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014, p. 83.

3.1.3 El régimen global de vigilancia social en los discursos de legitimación

A través de las sistemáticas revelaciones, se observan extensas y complejas redes de cooperación y de competencia entre agencias de seguridad e inteligencia estatales, especialmente localizadas en países desarrollados, con el objetivo de interceptar, analizar, almacenar y monitorear informaciones y comunicaciones entre individuos, grupos, instituciones, corporaciones, empresas y gobiernos alrededor del globo. La principal justificación para la creación de zonas de excepción para permitir el monitoreo de informaciones y comunicaciones de la población de forma inconmensurable es la lucha contra el terrorismo, ya que, con la vigilancia electrónica realizada, es posible identificar redes de cooperación, anticipar actos terroristas y prevenir los crímenes resultantes.

Al respecto, la "guerra contra el terror", hace que las naciones de todo el mundo actúen buscando enemigos, especialmente a partir de 2001, luego de los atentados terroristas del 11 de septiembre en Estados Unidos. Oportunamente, el gobierno norteamericano dispuso y, con el tiempo, recrudeció, una política estratégica de antiterrorismo, con la formación de alianzas o con el mando de iniciativas de otros países en el marco del Consejo de Seguridad de las Naciones Unidas, de la Organización del Tratado del Atlántico Norte y de la Organización de los Estados Americanos, en contra de aquel enemigo común, el terror, aunque este enemigo, tácticamente, cambie para redes terroristas, para países financiadores del terrorismo o para gobiernos paralelos terroristas[32].

Documentos expuestos por los movimientos contravigilantes revelaron que el discurso del terrorismo parece ser mucho más una justificación para acciones tomadas con fines oscuros y una táctica gubernamental para infligir miedo social. Es decir, “un porcentaje importante de los programas

[32] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014, p. 74.

no tenía nada que ver con la seguridad nacional", ya que "los documentos no dejaban dudas de que la NSA practicaba también espionaje económico y diplomático, además de la vigilancia de poblaciones enteras sin base para sospechas" [traducción libre][33]. En virtud de ese miedo al terrorismo, la población, preocupada por la seguridad interna, acepta el ideal vigilante y, que pese a que tales programas de vigilancia hayan sido pensados en escala global, las innovaciones tecnológicas y el flujo de personas, permitieron monitoreo doméstico de ciudadanos, ya que la amenaza también puede ser interna.

De este modo, una guerra justa se encuentra justificada por sí misma, aunque banaliza, por un lado, quién es el enemigo, puesto que cualquiera puede ser objeto de vigilancia, pero también, por otro lado, absolutiza al enemigo, ya que la amenaza al orden es permanente y debe ser constantemente combatida y aniquilada[34]. La guerra al terror se convierte, así, en un completo estado de excepción en tonos de guerra global permanente como fondo, exigiendo a las naciones que estén preparadas y combativas, anticipando, vigilando, actuando ante cualquier movimiento sospechoso en el juego del poder[35].

Además, los periodistas revelaron que las agencias de seguridad no sólo trabajan para romper los códigos de las conversaciones privadas de los individuos, sino también para boicotear la propia seguridad de la información para facilitar la vigilancia de la información, como, por ejemplo, el caso de la NSA que intenta obligar a que grandes compañías crearan *backdoors* en los códigos de criptografía de las redes sociales para permitir el acceso y manipulación de las informaciones dejadas por los usuarios, hecho este que la agencia alega tratarse de medida de seguridad contra ataques terroristas[36]. Se visualiza, entonces, una dicotomía de personajes

---

[33] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014, p. 75.

[34] HARDT, Michael; NEGRI, Antonio. *Império*. São Paulo: Record, 2012, p. 31.

[35] HARDT, Michael; NEGRI, Antonio. *Império*. São Paulo: Record, 2012, p. 34.

[36] McCARTHY, Tom. *NSA director defends plan to maintain 'backdoors' into technology companies.* [The Guardian, 23/02/2015] [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies.

públicos, a medida que, por un lado, "Assanges", "Mannings" y "Snowdens", que revelan la existencia de programas de vigilancia, son considerados villanos, mientras que "Gates", "Jobs" y "Zuckerbergs", que contribuyen, con sus plataformas, a esos sistemas, son considerados héroes de la tecnología.

3.1.4 La relevancia del *big data* y la toma de decisiones basadas en datos

En este contexto, se opera la obtención a gran escala de una cantidad exorbitante de datos, la cual tiene especial importancia, ya que, a partir de la recolección, del almacenamiento, de la manipulación y de la transferencia de dichos datos, es posible crear patrones y vigilar a individuos y masas. En este sentido, *big data* es una grandeza informacional, producida y suministrada por los usuarios de las redes sociotécnicas, cuya manipulación permite, por parte de corporaciones y gobiernos, "analizar, procesar y gestionar un conjunto de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación a la conducta humana y a las interacciones de los usuarios"[37].

Aunque el concepto de *big data* sea relativamente nuevo y no tan difundido socialmente, ya es posible identificar al menos cinco aspectos que involucran esa grandeza, conocidos como "cinco Vs": *volumen, velocidad, variedad, veracidad* y *valor*. El *volumen* hace referencia a la cantidad de datos producidos, estimándose en la casa de *exabytes* y *zettabytes* diariamente; la *velocidad* se refiere a que la manipulación de tales datos se da en tiempo muy hábil y simultáneo; la *variedad* quiere decir sobre la diversidad de datos que se recogen; la *veracidad* asimila que el procesamiento de estos datos debe garantizar la confiabilidad e integridad de ellos; y, por

[37] REAL ACADEMIA ESPAÑOLA. Diccionario del español jurídico. *Big data*. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://dej.rae.es/lema/big-data.

último, el *valor* se refiere a los beneficios significativos provenientes del procesamiento de los datos recopilados[38].

De acuerdo con el estudio *The Economic Value of Data: discussion paper*, del Ministerio de Finanzas del Reino Unido, la explotación de datos, según lo previsto por la Unión Europea y la Organización para la Cooperación y el Desarrollo Económico, va, cada vez más, a generar valor público y privado[39]. La toma de decisiones basada en el procesamiento de datos (*data-driven decisión)* es capaz de mejorar el rendimiento, la productividad y la rentabilidad de las empresas, así como capaz de incrementar la eficiencia de los productos y servicios públicos, los datos poseen el potencial de agilizar y personalizar métodos y técnicas de negocios[40].

En ese ínterin, diversos mecanismos contribuyen a la recogida y almacenamiento de datos informativos de usuarios en la red, destacándose, entre otros, las *cookies, web beacons, spywares, tagging y tracking*. Por medio de tecnologías de todo tipo, incluso de técnicas de *doxxing* y *hacking*, es posible crear perfiles de usuarios, identificar cuáles y cuántos usuarios están involucrados en red y mapear cómo ocurre el comportamiento de esas personas. Actualmente, estos mecanismos están dispersos en diversos ambientes y espacios, a través de los dispositivos móviles personales inteligentes, utilizados alrededor del globo por miles de millones de personas, como, por ejemplo, teléfonos móviles, *tablets*, ordenadores portátiles, relojes, televisores, entre otros.

Ante todo esto, es posible deducir que la sociedad actual vive bajo un superpanóptico, que tiene en el panoptismo analizado por Jeremy

---

[38] FERNÁNDEZ, Déborah. *Las cinco V's del Big Data.* [DataHack, 27/08/2018] [Fecha de consulta: 20/04/2019] Disponible en: https://www.datahack.es/cinco-v-big-data/; TAURION, Cezar. *Volume, variedade, velocidade, veracidade e valor:* os cinco Vs do Big Data. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://computerworld.com.br/volume-variedade-velocidade-veracidade-e-valor-os-cinco-vs-do-big-data.

[39] REINO UNIDO. *The economic value of data:* discussion paper. Londres: HM Treasury, 2018. p. 04-07. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf.

[40] REINO UNIDO. *The economic value of data:* discussion paper. Londres: HM Treasury, 2018. p. 04-07. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf.

Bentham y Michel Foucault un modelo de inspiración, un punto de partida - ya que esas ideas de domesticación y disciplina del cuerpo todavía subsisten - pero esta técnica de biopoder sobrepasa progresivamente todos los límites ya pensados, a la medida del perfeccionamiento de las tecnologías de información y comunicación, ya que "lo que cuenta es que estamos al principio de algo" [traducción libre][41].

3.1.5 El Estado de vigilancia: la vigilancia social pública frente a los derechos humanos y garantías

En la doctrina del derecho administrativo, se impone la supremacía del interés público sobre los intereses privados y particulares, como propia razón de existir de la Administración Pública, que debe actuar orientada al bien de la colectividad. Bajo el temor generado por la guerra al terror, los gobiernos justifican esa vigilancia en masa en expresiones tales como: "seguridad nacional", "defensa nacional", "situaciones de emergencia", "mantenimiento de la paz", "garantía de la ley y del orden", "prevención de la práctica de infracciones", "garantía de la integridad territorial", "defensa de la soberanía" y otros sinónimos; de manera que, aunque inicialmente entendidos como limitación a la potestad del Estado para garantizar derechos y libertades humanas y fundamentales; hoy, en día, son resignificados.

En el ámbito comunitario europeo, el derecho a la privacidad, previsto como un derecho humano desde el final de la Segunda Guerra Mundial, tiene limitaciones ya definidas en el propio ordenamiento, lo que, por sí solo, constituye el fundamento de los programas de vigilancia social, bajo las expresiones antes mencionadas[42]. Sobre el derecho al respeto a la vida privada y familiar, la Convención menciona que puede haber injerencia de autoridad pública en los casos de "seguridad nacional, para la

[41] DELEUZE, Gilles. *Conversações:* 1972-1990. São Paulo: 34, 1992, p. 225.

[42] CONSEJO DE EUROPA. *Convenio Europeo de Derechos Humanos de 1950*, p. 11. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf.

seguridad pública, para el bienestar económico del país, la defensa del orden y la prevención infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y libertades de terceros"[43].

Sin embargo, en septiembre de 2018, en importante posicionamiento judicial aún pasible de revisión vía recurso, la Corte Europea de Derechos Humanos juzgó el caso intitulado *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*, propuesto por diversas entidades, entre ellas *Big Brother Watch*, en contra del Reino Unido, sede de la GCHQ[44]. En ese caso, el Tribunal ponderó que, aunque los programas de vigilancia están dentro del margen de aplicación de los Estados y se justifican en las excepciones existentes, la forma en que fueron y vienen siendo desarrollados por las agencias de seguridad puede violar los derechos fundamentales de los administrados, debido a la falta de supervisión pública del proceso de interceptación, a la falta de garantías adicionales a sectores específicos que pueden ser objeto de investigación y a la falta de publicidad relacionada con los programas, aunque la propia existencia de estos programas únicamente fue revelada bajo polémicas internacionales[45].

Este *Estado de vigilancia,* característico de las sociedades contemporáneas, tiende a incorporar la vigilancia en los más diversos dispositivos, ambientes y sectores, haciéndose omnipresente en la vida de las personas de forma invisible, desapercibida, no jerárquica, descentralizada, individualizada, personalizada[46]. Esta vigilancia permanente y desmedida es,

---

[43] CONSEJO DE EUROPA. *Convenio Europeo de Derechos Humanos de 1950*, p. 11. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf.

[44] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15).* Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[45] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15).* Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[46] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192p. Tutor: Rafael Santos de Oliveira. [Trabajo Final de Máster]. Máster en Derecho. Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, 2018, pp. 47-60.

sino la principal, una de las características de esta nueva arquitectura social iniciada a partir de la Segunda Guerra Mundial y que se perfecciona a lo largo de los años, cuyo poder intenta, por excelencia, modular los individuos y las masas para, al fin y al cabo, controlar todas las formas de vida en esa sociedad en red.

3.2 El hombre-caracol: los datos como login en la sociedad en red

Como antes mencionado, las relaciones de poder dependen de las características de la arquitectura social en que los actores sociales interactúan entre sí en un determinado contexto histórico El siglo XX está marcado por diferentes transformaciones sociales, culturales y económicas, a partir de los cambios originados por el incremento de la velocidad de las relaciones sociales y de las complejidades del ser, especialmente con la proliferación y desarrollo de la microelectrónica durante la Segunda Guerra Mundial y posteriormente de la nanoelectrónica.

3.2.1 La sociedad en red: nuevos caminos en la mundialización

Con el desarrollo de las tecnologías de información y comunicación, el concepto de red ha adquirido un nuevo significado, teniendo una importante relevancia en las relaciones intersubjetivas, lo que inauguró, inicialmente en los Estados Unidos, pero poco después extendiéndose en todo el globo, la denominada *Era de la Información*, según Manuel Castells[47]. Sin embargo, la visualización de los procesos por medio de redes no es única y exclusiva de las sociedades del siglo XXI, porque "la red es una estructura común a cualquier vida; donde quiera que veamos vida, vemos redes" [traducción libre][48].

[47] CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura, vol. 3. 3. ed. São Paulo: Paz e Terra. 2002.

[48] CAPRA, Fritjof. *As conexões ocultas*. São Paulo: Cultrix, 2002.

En realidad, la idea de red viene siendo utilizada en diversas áreas del conocimiento, adquiriendo resignificación propia, con intento de explicar, visualizar y contestar estructuras y procesos, sean biológicos, físicos, espaciales, temporales y sociales. Esto, pues, no hay como perder de vista que "el nuevo paradigma puede ser llamado de una visión de mundo holística que concibe el mundo como un todo integrado y no como una colección de partes disociadas" [traducción libre][49]. La evolución de las tecnologías de información y comunicación posibilitó la introducción y remoción de nuevos actores sociales y nuevos procesos en las redes, otorgando autonomía y multidireccionalidad necesarias para proporcionar un mayor flujo de comunicación y autoconciencia.

Esta nueva arquitectura social, se ha caracterizado por una refundación de las fronteras entre el mundo real-vivo y el mundo virtual-artificial, permitiendo la visualización de las relaciones sociales a partir de nodos y aristas, debido a la horizontalización del proceso comunicativo. Para Castells, la sociedad en red "es aquella cuya estructura social está compuesta de redes activadas por tecnologías digitales de comunicación e información basadas en microelectrónica", de modo que "las redes digitales son globales por su capacidad para autoconfigurarse de acuerdo con las instrucciones de los programadores, trascendiendo los límites territoriales e institucionales a través de redes de ordenadores conectados entre sí" [traducción libre][50].

En ese contexto, las innovaciones traídas por los avances de las tecnologías de información y comunicación, han provocado la aparición de nuevos actores sociales, espacios sociales y procesos en red, que han otorgado autonomía y multidireccionalidad a las relaciones. En la sociedad en red, las actividades básicas que configuran y controlan la vida humana en cada rincón del planeta se organizan en redes globales, afectando a todo el mundo, aunque no necesariamente todas las personas participen en las redes, ya que el proceso de inclusión y exclusión de redes también forma

[49] CAPRA, Fritjof. *A Teia da Vida:* uma nova compreensão científica dos sistemas vivos. São Paulo: Cultrix, 1996.

[50] CASTELLS, Manuel. *O poder da comunicação*. São Paulo: Paz e Terra, 2013, p. 59.

parte de esa nueva arquitectura social, lo que, a su vez, influye en la propia formación de la identidad humana[51].

3.2.2 La construcción de una identidad por *big data*

Si en las configuraciones sociales anteriores, el sujeto era identificado, principalmente, por medio de una firma y un número de matrícula o registro general; en las nuevas sociedades, importa la cifra, que es una contraseña, un lenguaje numérico de información y control, que logra transformar a los individuos en dividendos divisibles y las masas en muestras, mercados, porcentajes[52]. Así, por medio de la cifra, está permitido o prohibido el acceso a determinada información y está permitida o prohibida determinada comunicación entre actores sociales, ya que, por ejemplo, pagos con tarjetas de crédito, envío de mensajes, acceso a perfiles en redes sociales, entre otras acciones, dependen necesariamente de una contraseña, de un código, de una identificación peculiar[53].

Es importante señalar que, para que el individuo acceda a la información deseada sobre la base de una cifra específica utilizada, una máquina de procesamiento de datos, basada en algoritmos, necesita determinar, permitiendo o rechazando, el proceso de comunicación[54]. Entonces, además de la barrera de acceso a la información creada por la necesidad de utilizar de una cifra específica para acceso a determinados procesos comunicacionales, se percibe que, en ese sentido, las tecnologías de la información y comunicación identifican a cada individuo, en una modulación universal y matemáticamente conocida, de forma autónoma y automática, haciendo que sea la cifra relevante y no la persona que la utiliza[55].

---

[51] CASTELLS, Manuel. *O poder da comunicação*. São Paulo: Paz e Terra, 2013, p. 59.

[52] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 222.

[53] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 222.

[54] BAUMAN, Zygmunt. *Vida para consumo***.** A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 11.

[55] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 223.

3.2.3 ¿Quién soy yo?: la creación de perfiles a través de algoritmos

Se hace posible, por medio de las cifras elegidas y con base en criterios cartográficos, catalogar datos, manipular informaciones, rastrear patrones de comportamiento, prever acciones, reduciéndose las masas en menores grupos para análisis y control[56]. De esta forma, se pueden visualizar, por ejemplo, grupos de personas con determinada condición financiera, específico nicho mercadológico, índice de propensión a alguna enfermedad, gusto por actividad deportiva, orientación sexual, diagnóstico de crédito de algún grupo poblacional, monitoreo de transferencias de los valores, acompañamiento de llamadas y conexiones entre personas y grupos y otros varios ejemplos de lo cotidiano, características de esta nueva sociedad, caracterizada por la grandeza del *big data*.

Se puede decir que la sociedad en red crea sus propios dispositivos de poder, como, por ejemplo, la sustitución de la firma, que, por muchos siglos fue el principal signo de identidad personal por el código informativo, con el objetivo de una mayor seguridad y singularidad[57]. De esta forma, el individuo pasa a ser identificado por los códigos que los sistemas producen, como en los casos del número de la tarjeta de identidad en el registro general (DNI), del número de seguridad social, del número del pasaporte, del número de la tarjeta de cliente bancario, del Bizum, o de la combinación de números, letras y signos en un *username* en determinada red social, entre otros ejemplos; pero también pasa a ser monitoreado y catalogado por los datos que, consciente o inconscientemente, produce.

Por otro lado, las técnicas publicitarias, como dispositivos de control, fueron ampliadas y perfeccionadas en virtud de la profusión de las tecnologías de información y comunicación, ya que han podido avanzar en el campo digital y ser dirigidas a una pluralidad de individuos, que en todo

[56] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 222.

[57] DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992, p. 222.

momento buscan consumir en diferentes nichos mercadológicos. La publicidad acaba por involucrar a los sujetos en una nueva lógica consumista, basada en un mercado de informaciones y comportamientos, ya que los datos personales recogidos y monitoreados por las empresas con fines comerciales posibilita una mercadotécnica especial, direccional y colaborativa[58].

Además, a través de ese rastreo de informaciones y cruzamiento de datos, es factible modular grupos de control y forjar identidades, determinándose lo que necesita, cuánto necesita y cómo necesita ser consumido, en un verdadero proceso de subjetivación continua[59]. Este consumismo, marcado por la insatisfacción perpetua del consumidor, ya que siempre hay algo mejor y más nuevo para consumir, y por la lógica de la exclusión social, ya que si no hay el consumo de determinados bienes y servicios no se participa de la vida social; acaba afectando la dignidad del individuo y lo esclaviza, porque "apuesta por la irracionalidad de los consumidores, y no sus estimaciones sobrias y bien informadas; estimula emociones consumistas y no cultiva la razón" [traducción libre][60].

3.2.4 El panóptico está vivo: el post-panóptico, el banóptico y el sinóptico

Se da así un control sobre la población, como un todo objeto, no sólo caracterizado por personas físicas, sino por datos informativos multiplicados y multiplicables, de tal modo que es posible sujetar ese cuerpo social a un proceso de subjetivación y modulación continua de la identidad en la sociedad en red. Se ve que el poder es diseminado por todas las formas de vida en un *sin tiempo* y en un *sin espacio*, en razón de la ausencia de las

[58] BAUMAN, Zygmunt. *Vida para consumo***.** A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 20.

[59] BAUMAN, Zygmunt. *Vida para consumo***.** A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 20.

[60] BAUMAN, Zygmunt. *Vida para consumo***.** A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 65.

barreras y límites físicos, posibilitando la actuación de dispositivos específicos, entre ellos la vigilancia de los datos personales, que hace necesario repensar la propia noción del panóptico en la nueva arquitectura social.

Se vive, pues, en un post-panóptico, con el prefijo sugerido por Bauman, que nace del mejoramiento y recrudecimiento de las tecnologías de vigilancia, de forma que el panoptismo "está vivo y bien de salud, en realidad, armado de músculos (electrónicamente reforzados, ciborguizados) tan poderosos que Bentham, o incluso Foucault, no serían capaces ni siquiera de imaginarlo"[61] [traducción libre]. El post-panóptico, con nuevas formas de vigilancia y de panoptismo posibilitadas por las innovaciones tecnológicas, se remite a una vigilancia liquida, fundamentada en la fluidez de las relaciones entre sujetos e instituciones, permitiendo la volatilidad de la mirada vigilante, microcapilarizada en diferentes dispositivos informáticos[62]

Aliado a ello, el banóptico, sugerido por Didier Bigo, sobre la base de la idea de seguridad nacional, señala que las tecnologías de la información y la comunicación ayudan en la elaboración de perfiles de individuos, definiendo quién debe ser puesto bajo vigilancia por los agentes de seguridad y estableciendo quién está del lado de dentro y quien está del lado de afuera[63]. Estos dispositivos se asignan en las entradas de los espacios comunitarios, no sólo en términos internacionales, como fronteras viales o aeropuertos, sino también domésticos, en centros comerciales, supermercados y otros departamentos constantemente vigilados, confinando a quienes están del lado de dentro y excluyendo quienes están del lado fuera[64].

---

[61] BAUMAN, Zygmunt. *Vigilância líquida***:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 22.

[62] BAUMAN, Zygmunt. *Vigilância líquida***:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 22-23.

[63] BIGO, Didier; TSOUKALA, Anastassia. *Terror, insecurity and liberty:* illiberal practices of liberal regimes after 9/11. New York: Routledge, 2008.

[64] BIGO, Didier; TSOUKALA, Anastassia. *Terror, insecurity and liberty:* illiberal practices of liberal regimes after 9/11. New York: Routledge, 2008.

3.2.5 El hombre-caracol: la vigilancia personal

Por último, el sinóptico invierte el vector de vigilancia, haciendo que muchos observen a pocos, a partir del hecho que se espera que los propios sujetos y objetos de vigilancia se autodisciplinen y paguen por los costos materiales y psíquicos de esa disciplina, para ejercerla sobre sí mismo y sobre los demás un control continuo[65]. Sucede, así, una distribución de minipanópticos, representados por el tipo *do it yourself*, donde, por medio de dispositivos móviles y portátiles, suministrados comercialmente, los usuarios, a través de innumerables acciones, vigilan a todos en todo momento, en una servidumbre contemporánea de ese régimen de vigilancia[66].

En este contexto, Bauman trae la idea del hombre caracol, que lleva en su concha un panoptismo personal, posibilitando una autovigilancia y la vigilancia del otro, en una metodología más económica y popular que el panoptismo clásico[67]. Cada sujeto, emprendedor de sí mismo, transporta, consigo, dispositivos de control, sujetándose al mismo tiempo en que sujeta a los demás, en una retroalimentación de datos, de tal manera que la vigilancia no es impuesta verticalmente por poderes hegemónicos, sino surge del proprio individuo, que no necesariamente consciente, se ve obligado a consumir una autovigilancia y una vigilancia de los demás para poder pertenecer a la sociedad en red y produce, de nuevo no necesariamente consciente, un infinito número de datos personales.

3.2.6 Los datos: del Internet de las Cosas al Internet de Todo

En el siglo XXI, esta cuestión reviste especial importancia si se considera el avance de las tecnologías de información y comunicación, como el uso de la identificación por radiofrecuencia (RFID), el *Quick Response*

[65] BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 26.

[66] BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 26.

[67] BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 22-23.

Code (QRCode) y la red de sensores inalámbricos (RSSF) revolucionando la comunicación máquina a máquina (*machine to machine*, en inglés, o por el acrónimo M2M). En la etapa actual, en *Internet de las Cosas* (*Internet of Things*, en inglés, o por el acrónimo IoT), es posible la interconexión digital de los objetos a través de Internet, formando una red inteligente de cosas a disposición de los usuarios, de donde derivan conceptos como *smart things*, *smart phones, smart TV, smart watchs, smart home, smart cities,* entre otros.

En este escenario, muchas cosas que rodean al usuario se configuran y se conectan a Internet, capturando, monitoreando y procesando datos para un buen funcionamiento. De esta forma, el individuo puede, a través de la red mundial de computadoras y dispositivos inteligentes, controlar remotamente tales objetos o permitir que los proveedores de servicios utilicen tales objetos para una determinada función, lo que genera un abanico de oportunidades y desafíos en el campo tecno-social[68]. Se observa que la IoT, aunque puede ser mejor extendida con el advenimiento de mejores protocolos de Internet, ya es una realidad social, inscrita, inclusive, como técnica de publicidad para consumo de dispositivos[69].

Al avanzar en ese panorama, según algunos expertos en el área, se llegará a *Internet de Todo* (*Internet of Everything*, en inglés, o por el acrónimo IoE), donde habrá un flujo continuo e inimaginablemente inmenso de conexiones entre personas, procesos, datos y cosas, abarcando todo el ecosistema de conectividad alrededor de un universo común[70]. Ocurre que, en este caso, la información que circula por Internet no será colocada en la red por personas, sino por sensores y objetos que intercambian datos

[68] BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything: A $4.6 trillion public-sector opportunity.* San Jose: Cisco. 2013. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf.

[69] BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything: A $4.6 trillion public-sector opportunity.* San Jose: Cisco. 2013. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf.

[70] BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything: A $4.6 trillion public-sector opportunity.* San Jose: Cisco. 2013. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf.

entre sí, posiblemente todo el tiempo, generando incontables valores diarios o combinaciones, para experiencias *indoors* u *outdoors*[71].

Básicamente, los datos personales recogidos sirven como mecanismo de estadísticas, acceso a contenido, personalización de experiencia o para uso de un producto o servicio por el usuario, siendo fundamentales en términos de navegación electrónica y comercio electrónico. En primer lugar, al navegar por la red, algunas informaciones que se transmiten automáticamente entre dispositivos se recogen como requisitos tecnológicos vinculados a la navegación, con fines estadísticos, como el nombre de dominio de Internet, la dirección IP, tipo de navegador y del sistema operativo, fecha, ubicación y hora, entre otras, para que el servidor transmita la información compatible con el equipo del usuario.

Además, algunas informaciones personales se obtienen en el registro en determinadas páginas, a través de un formulario de registro, como nombre, dirección de correo electrónico y otra información personal, cuya exactitud puede mejorar cada vez más la personalización de la experiencia del usuario. Esta información recopilada, junto con la información estadística, se utiliza para personalizar un contenido y/o servicios disponibles, desde la personalización del acceso a la propia página hasta el ofrecimiento de contenidos, productos y servicios que tienen relación con el perfil que se crea con los datos del usuario.

No raras veces (y, aquí, adentra toda una cuestión de consentimiento y legalidad), la información personal individual se comercializa o se suministra a terceros, como socios, patrocinadores, anunciantes u otras empresas externas, con el fin de crear nichos de mercado y perfiles de consumidores para futuras ofertas, propagandas u otros tipos de comunicaciones. En este mismo sentido, a menudo se concede el permiso para que ciertas páginas recopilen periódicamente información personal del usuario a partir de instituciones afiliadas, socios de negocios y otras

[71] BAJARIN, Tim. *The next big thinh of tech:* the Internet of Everything. [Time, 13/01/2014] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

fuentes de terceros independientes, añadiendo al perfil creado del individuo, datos provenientes de las redes sociales.

3.2.7 El suministro de datos como condición de acceso a la sociedad en red

Las redes sociales o plataformas de interacción social son una de las principales razones por las que miles de millones de usuarios navegan por la red diariamente, como *Facebook, YouTube, WhatsApp, Messenger, Instagram, Twitter, LinkedIn, Snapchat, Viber, Pinterest, Telegram, Tumblr, Reddit,* de entre muchas otras, ya que, a partir de ellas, es posible crear infinitas conexiones entre personas, empresas e instituciones alrededor del mundo, siendo, por lo tanto, una de las mayores fuentes de recogida y almacenamiento de datos personales. Sin embargo, aunque el registro, acceso y funcionamiento de la red social es, en la mayoría de las veces, gratuito, desde el punto de vista del individuo, depende del suministro de datos personales a la plataforma, lo que sirve como mecanismo de ganancia en la creación de espacios publicitarios en esas aplicaciones.

Otro mecanismo importante de la navegación en red es el uso de *cookies*, pequeño paquete de datos que, cuando un usuario visita por primera vez un sitio, recibe del navegador para el almacenamiento de información, de forma que, siempre que el usuario revisite dicha página, el navegador devuelve la *cookie* al servidor para recordar actividades anteriores del usuario. El uso de *cookies* proporciona, a primera vista, contenidos, productos y servicios diferenciados y personalizados, desde el momento en que es posible recordar el usuario a cada acceso, reconocer hábitos de navegación, calcular la dimensión de la audiencia y la visualización de páginas, el relleno de formularios, entre otras acciones, que parecen facilitar el consumo por parte del usuario.

Estas cuestiones, usualmente, se aclaran en las políticas de privacidad, en las políticas de *cookies*, en los términos y condiciones de uso de producto y servicio y en otros documentos vinculantes, los cuales el usuario debe leer, y autorizar las condiciones previstas para permitir el acceso

al contenido deseado. En la mayoría de los casos, estos documentos son verdaderos contratos de adhesión, que, según la mejor doctrina, se caracterizan por la imposibilidad de discusión o modificación de cláusulas por el adherente, debiendo sujetarse a las cláusulas impuestas por el proponente.

Además, es muy común que estos términos y condiciones de uso de determinadas aplicaciones y plataformas sean amplios y complicados, compuestos por innumerables documentos diferentes y diversas páginas de palabras difíciles y complejas, ya sea en el campo informativo o jurídico. Y, como sabido, la concordancia con esos documentos, exteriorizada por medio de un simple *clic* en una caja de selección o un botón específico, es condicionante de la navegación del usuario en determinada aplicación o plataforma, haciendo que el individuo se vincule a derechos y obligaciones, sin que necesariamente posea total conocimiento de las implicaciones que de ello derivan.

Esto ocurre, especialmente, con los permisos que el usuario concede a determinadas aplicaciones, sin saber realmente lo que está permitiendo, como posibilitando que la plataforma, cuando quiera, sin necesariamente explicitar que lo está haciendo, acceda al calendario, a la cámara, a la lista de contactos, a los sensores, al micrófono, a los SMS, al almacenamiento, a la ubicación, al *bluetooth*, al estado de la red; instale paquetes, utilice sincronización de datos, gestione procesos de fondo, habilite y deshabilite *keyguard* (información de la pantalla de bloqueo, como contraseñas, patrones, sensores biométricos y faciales); modifique la configuración del dispositivo, transfiera infrarrojos, utilice NFC, entre otras posibles acciones[72]. Estas acciones pueden implicar innumerables nuevos riesgos para el usuario y para la protección de los datos personales. Como ejemplo de esto, basta citar el *software Alphonso*, utilizado por diferentes aplicaciones, que, una vez permitido por el usuario, capta datos del micrófono del teléfono celular sobre hábitos de consumo televisivo u otros audios de fondo

[72] DAUER, Stella. *Entenda tudo sobre as permissões de aplicativos e proteja seu Android.* [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://www.androidpit.com.br/permissoes-aplicativos.

para suministro a anunciantes para que éstos ofrecen productos y servicios personalizados al individuo[73]

3.2.8 Los ataques maliciosos y riesgos a la autonomía informacional

Sin embargo, no necesariamente, el acceso al micrófono y a la cámara, por ejemplo, ocurre bajo el prisma de un permiso del usuario, pues puede ocurrir a causa de ataques maliciosos dirigidos a los usuarios, incluso por parte de agencias gubernamentales, como ha sido revelado por el portal *Wikileaks,* que mostró que la CIA y el FBI, agencias de investigación estadounidenses, accedían remotamente a estas salidas de audio y video de *persons of interest*[74] (de ahí, el porqué de una fotografía publicada por el CEO de Facebook Inc., compañía dueña de la red social Instagram, se tornó viral en la red no por el hecho de que esta red social hubiera alcanzado medio billón de usuarios, sino por el uso de las cintas adhesivas para cubrir la cámara y el micrófono de su equipo portátil)[75].

Así, se percibe, sea en el estado actual de las cosas, sea en previsiones futurísticas, sea en el campo interpersonal, social, económico, industrial o político, que los datos personales son el principal dispositivo de esta nueva arquitectura social, bajo el argumento de una necesidad de personalización única y aprovechamiento máximo de las experiencias de vida. El individuo deja de ser solo una representación corpórea, exteriorizada por su apariencia, palabras, ideas y actos, para pasar a ser identificado, monitoreado, calificado y controlado debido al conjunto de magnitudes informacionales

---

[73] BLASCO, Lucía. *Cuán cierto es que las empresas usan el micrófono de tu teléfono para escucharte y qué hacer al respecto*. [BBC News, 05/07/2018] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://www.bbc.com/mundo/noticias-44724389.

[74] PHAM, Sherisse. *WikiLeaks dice que la CIA espía a través celulares y televisores, ¿qué tan preocupado debes estar?* [CNN, 08/03/2017] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://cnnespanol.cnn.com/2017/03/08/wikileaks-dice-que-la-cia-espia-a-traves-de-smartphones-televisores-y-mas-que-tan-preocupado-debes-estar/.

[75] RODRÍGUEZ-PINA, Gloria. *El método nada tecnológico que usa Mark Zuckerberg para protegerse de los hackers.* [El País, 22/06/2016] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://verne.elpais.com/verne/2016/06/22/articulo/1466617774_991020.html.

producidas en todo momento y a todo lugar, no necesariamente de forma consciente, siendo los datos personales el *login* de esa sociedad en red.

A pesar de la protección necesaria que estos datos presuponen por las propias razones de existieren, hubo en los últimos años grandes filtraciones de datos que causaron incomodidad internacional, ya sea por ataques deliberados contra sistemas de información, sean bancos de datos olvidados por empresas de seguridad, sean transferencias y/o compra-y-venta de información entre corporaciones y agencias estatales. De acuerdo con un informe de *Avast*, las diez peores fugas de datos de 2018 involucraron, como poco, treinta y siete millones de usuarios, y el más grave, mil millones de personas[76].

En abril de 2018, el *The New York Times* reveló que en 2013 los datos de al menos treinta millones de usuarios de *Facebook* - hay noticia de que, en verdad, el número de afectados pudo haber superado los ochenta y siete millones – fueron indebidamente compartidos con la consultora *Cambridge Analytica*, que prestó servicios durante la campaña electoral de Estados Unidos al Presidente Donald Trump, en lo cual pudo haber comprometido la limpieza de las elecciones, ya que, en la época, el candidato tuvo acceso a diversos datos personales, como nombres, género, edad, lugar de residencia y los resultados de personalidad proyectados por un *quizz* realizado por los usuarios, así como a los intereses y datos más elementales de la cuenta, como e-mail o fecha de nacimiento[77].

El reportaje hizo estallar un escándalo sobre el tratamiento y la gestión de datos personales en la red, especialmente después de que el CEO de Facebook Inc., Mark Zuckerberg, admitiera que la mayoría de los casi dos billones de usuarios pudieron haber tenido los datos personales abiertos de forma indiscriminada. Zuckerberg manifestó que la aplicación iba a implantar un sistema de seguridad con más precauciones, aunque aclaró

[76] HRON, Martin. *Os últimos 10 maiores vazamentos de dados*. [Avast, 14/02/2019] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados.

[77] CADWALLADR, Carole; CONFESSORE, Nicholas; ROSENBERG, Matthew. *How Trump Consultants Exploited the Facebook Data of Millions*. [The New York Times, 17/03/2018]. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

que el modelo de negocio de la herramienta se basa en el intercambio de información con otras empresas para la publicidad. El creador de la red social fue llamado a declarar y explicarse ante el Congreso de Estados Unidos, asumiendo responsabilidades y un compromiso de implementación de nuevas políticas de protección[78].

A pesar de todo, las investigaciones revelaron que la red social en cuestión dio permiso especial a más de 150 empresas, entre ellas *Apple, Amazon, Microsoft, Netflix* y *Spotify*, plataformas conocidas del público, para acceder a datos de amigos de los usuarios y para ver mensajes privados de las personas, aunque negado vehementemente[79]. Se tratan de acuerdos firmados en otra época, cuando la red social intentaba expandirse rápidamente con la ayuda de una personalización instantánea para integrar a los usuarios, que, en muchos casos, siguen valiendo, pese ya estar vigente la supuesta necesidad de adquirir el consentimiento del usuario para la cesión de datos, lo que nuevamente trae a la superficie la cuestión del consumismo en la red[80].

3.2.9 Perspectivas de futuro: la economía de vigilancia

Frente a todas las noticias de existencia de programas de vigilancia masiva por parte de agencias de seguridad estatales y de fuga de datos personales de los usuarios, se percibe un escenario de monitoreo real de los procesos comunicativos a escala mundial, con una insuficiencia, con propósito o no, de medidas de seguridad para proteger al usuario de esos nuevos riesgos, que, a su vez, se encuentra en absoluta debilidad frente a las tecnologías disruptivas. El individuo acaba, incluso, contribuyendo aún

---

[78] MARS, Amanda. *Zuckerberg pide perdón en el Senado y advierte de la amenaza de Rusia*. [El País, 11/04/2018]. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://elpais.com/internacional/2018/04/10/actualidad/1523380980_341139.html.

[79] COLOMÉ, Jordi Pérez. *Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas.* [El País, 20/12/2018] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html.

[80] COLOMÉ, Jordi Pérez. *Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas.* [El País, 20/12/2018] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html.

más con los engranajes de ese sistema, porque se ve obligado a consumir esas tecnologías de información y comunicación para participar efectivamente de la sociedad en red.

Nos encontramos, entonces, con un determinismo tecno-social en una relectura de la formación del propio Estado, pero ahora, como un Estado vigilante. En otras palabras, parece que el individuo, por miedo al terror y otros enemigos, renuncia a las propias libertades a favor de un ente, que garantice una seguridad deseada, aceptando programas de vigilancia masiva de combate al terrorismo. En esta misma línea de pensamiento, el individuo, queriendo formar parte de la sociedad, se somete a la cultura del consumo, conscientemente o no, dejando de preocuparse por la autorización del monitoreo y manipulación de los datos personales recogidos, ya que el coste-beneficio de ser excluido de la red, si no entrega los datos, no compensa en este nuevo entorno digital.

Por un lado, las agencias estatales promueven programas de vigilancia masiva de nacionales y extranjeros, a través de la supervisión y evaluación del tráfico de datos alrededor del globo; por otro lado, los individuos consumen, en todo momento, productos y servicios que generan datos de todo orden, sobre sí y sobre otras personas; en el medio de eso, grandes corporaciones cooperan con la actuación de las agencias de seguridad, transmitiendo datos o permitiendo el acceso a ellos, inventan nuevos productos y servicios tecnológicos, ofreciendo para consumo de todos, incluso con obsolescencia programada, así como colaboran con otras grandes corporaciones en un el mercado mundial para la compra-venta y la transferencia de datos de los usuarios.

Así, impera una economía de la vigilancia, en la que los datos de los usuarios adquieren valor de mercado y basan la creación y el desarrollo de productos y servicios, públicos y privados, en un sin número de interacciones, competiciones y cooperaciones, entre diferentes actores sociales. En una sociedad en red, por su propia arquitectura informacional, el procesamiento de datos producidos en los procesos comunicativos se convierte en el nuevo oro del siglo XXI, de forma que, en un Estado general

de vigilancia, se hace necesario analizar esta nueva arquitectura social, bajo el prisma de los derechos y garantías humanas y fundamentales de los individuos, especialmente del derecho a la privacidad.

4

"1984 *all over again*": el derecho a la privacidad en la era digital

El título del presente capítulo hace referencia a que el mundo descrito en la obra "1984", de George Orwell, está sucediendo nuevamente o salió a la luz de nuevo, aunque es un escenario ficticio de sociedad distópica imaginada en 1949. Por un lado, se observa un régimen global de vigilancia social, marcado por la interceptación de datos personales y por el monitoreo de los procesos comunicativos entre ciudadanos, empresas, organismos públicos y otros países, con la diferencia de que no hay un Partido definido, porque la vigilancia y el control social están dispersos y perfeccionados con el avance tecnológico de la sociedad en red.

Por otro lado, al igual que las telepantallas, televisores bidireccionales que funcionaban al mismo tiempo como emisores de mensajes oficiales y como cámara de monitoreo y estaban en todas las residencias del país, las tecnologías de información y comunicación, especialmente aquellas equipadas con internet, están diseminados por todos los rincones del mundo, permitiendo a los ciudadanos interactuar uno con los demás, pero también proporcionar datos personales para acceder a productos y servicios variados. Así, la privacidad, como era antes conocida, parece ser cada vez más una memoria de un pasado distante, tales como los recuerdos de los tiempos antes del gobierno del Gran Hermano.

Considerando que el objetivo general de este libro es analizar los impactos de las tecnologías de información y comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de

la ciberseguridad del siglo XXI, este capítulo, tras el análisis realizado anteriormente sobre el régimen global de la vigilancia social, pretende: a) establecer la estructura normativa global y regional del derecho a la privacidad, el cambio y los enfoques del concepto a lo largo del tiempo; y, finalmente, b) discutir la resignificación del derecho a la privacidad, basada en nuevos conceptos, nuevos espacios, nuevos límites y nuevas posibilidades en el contexto de la ciberseguridad.

4.1 La privacidad como la conocemos: la (r)evolución de un concepto en el cuadro normativo

Los marcos normativos de derechos humanos y los ordenamientos jurídicos nacionales reconocen el derecho a la privacidad, en sus diferentes matices, como derecho a la intimidad o como derecho a la vida privada, elevándolo a la categoría de derecho humano. Aunque la motivación legal guarde estricta relación con el desarrollo de los *mass media*, los avances tecnológicos producidos desde la mitad del siglo XX han exigidos adaptaciones a las recientes necesidades y nuevas interpretaciones jurídicas, especialmente en el campo de la tutela de la personalidad.

4.1.1 Breves consideraciones sobre el concepto de la privacidad en la historia

Para conceptuar la privacidad y, específicamente, el derecho a la privacidad, es necesario volver a la distinción entre privado y público en la antigüedad clásica griega - traspasada a la cultura romana posteriormente -, donde se distinguía el *oikos*, espacio particular de los individuos, y la *pólis*, espacio común a los ciudadanos libres[1]. En ese sentido, el ciudadano necesitaba una esfera privada y tenía un "lugar que le pertenecía", para poder recibir una segunda vida, *bio politikos*, y participar de la esfera pública, donde, en este lugar, no trataba de lo que le era propio, *idion*, sino

[1] ARENDT, Hannah. *A condição humana.* 10 ed. Rio de Janeiro: Forense Universitária, 2005, p. 33.

de lo que le era común, *konion*, de modo que la diferencia, en un primer momento, de privado y público era el ámbito familiar y el ámbito político[2].

En la Edad Media, siglos después, urgió, cada vez más, la necesidad de aislamiento en un espacio privado en detrimento de lo que era común y giraba en torno al espacio público, convirtiéndose la casa en el lugar ideal de separación entre esas esferas y el nuevo centro de poder político, tanto que las dinastías empiezan a vincularse a casas, apellidos[3]. Con el declive de la economía feudal y el surgimiento de la burguesía, el deseo por la individualidad fue aumentado exponencialmente, habiendo el burgués ocupado espacios, acumulado riquezas, levantado barreras, de modo que la búsqueda por la protección de un lugar solamente suyo fortaleció la noción de aquello que es privado, en una estrecha relación con el derecho a la propiedad[4].

Esta cuestión asumió especial relevancia en el marco filosófico del liberalismo, en particular en las obras de John Locke, considerado el padre del liberalismo, cuando éste defendía "la existencia de una esfera de libertad natural a todo sujeto, espacio que debe ser impermeable a la coactividad despliega la ley civil", de modo que "la 'privacy' es considerada la propiedad más sagrada de la persona humana, pues todo hombre tiene una propiedad en su propia persona" [traducción libre][5]. En sentido parecido, John Stuart Mill sostuvo que las conductas humanas pasibles de análisis eran aquellas que producían deberes y obligaciones sociales, cuando afectan a terceros, de manera que los aspectos que sólo se refieren al individuo, es decir, las características privadas, son independientes de la esfera pública, siendo el sujeto soberano sobre sí[6].

---

[2] ARENDT, Hannah. *A condição humana.* 10 ed. Rio de Janeiro: Forense Universitária, 2005, pp. 38-39.

[3] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 125.

[4] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 26.

[5] TARODO, Salvador Soria. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: *Derecho y Salud*, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006, p. 136.

[6] MILL, John Stuart. *A liberdade*. São Paulo: Martins Fontes, 2000.

4.1.2 El derecho a la privacidad desde una perspectiva jurídica

Como categoría analítica y autónoma de ponderación, el derecho a la privacidad es una construcción reciente estadounidense. Samuel Warren, motivado por hechos íntimos del matrimonio de su hija divulgados por periódicos, y Louis Brandeis publicaron en 1890 un artículo sobre el *right to privacy* (derecho a la privacidad), inspirado en la expresión acuñada por Thomas McIntyre Cooley, *right to be alone* (derecho de ser dejado en paz), con base en las necesidades de la burguesía norteamericana de finales del siglo XIX[7]. La doctrina de Warren y Brandeis aleja el derecho a la privacidad de la necesidad de protección de la propiedad y aproxima la necesidad de protección de la vida privada con factores relacionados con la personalidad humana[8].

Los autores refieren que recientes innovaciones dan lugar a un nuevo nivel de protección de la personalidad humana y de la seguridad del ciudadano norteamericano, ya que las nuevas tecnologías de comunicación, las máquinas, las fotografías, las empresas de chismes, entre otras, acabaron por invadir el espacio privado del hogar, pero el individuo tiene el derecho de estar solo, o mejor, el derecho de ser dejado en paz[9]. Se trata de una protección que va más allá de la tutela del material que contenga una determinada revelación íntima, pues alcanza sustancialmente a la propia información, confiriendo a la persona el derecho de ser dejada en paz y no hacer público aquello que considera privado[10]

---

[7] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. [en línea] [Fecha de consulta: 16/04/2019] Disponible en:

http://faculty.uml.edu/sgallagher/brandeisprivacy.htm.

[8] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. [en línea] [Fecha de consulta: 16/04/2019] Disponible en:

http://faculty.uml.edu/sgallagher/brandeisprivacy.htm.

[9] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. [en línea] [Fecha de consulta: 16/04/2019] Disponible en:

http://faculty.uml.edu/sgallagher/brandeisprivacy.htm.

[10] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. [en línea] [Fecha de consulta: 16/04/2019] Disponible en:

http://faculty.uml.edu/sgallagher/brandeisprivacy.htm.

Esta construcción doctrinal va ganando fuerza en los ordenamientos jurídicos nacionales con el paso de los años, de forma que, a partir del desarrollo de las tecnologías de la información y comunicación y la globalización de las relaciones sociales a lo largo del siglo XX, el derecho a la privacidad, antes considerado como inherente a los derechos de la personalidad, pasa a ser tratado como un derecho de naturaleza humana y fundamental. Se presenta el derecho de cada uno de garantizar una paz, una tranquilidad, una reserva de parte de su vida que no esté afectada por una actividad pública; o de evitar que los hechos de su vida que son entendidos privados sean expuestos y el Estado debe abstenerse de interferir indebidamente en tal ámbito de cada individuo e incluso prohibir la injerencia también de terceros.

En la esfera social, las personas pasan la mayor parte del tiempo interactuando unas con otras, debido a la necesidad de ganarse la vida, seguir una vocación, aliarse a otros con los mismos intereses o negocios; mientras que en la esfera de la vida íntima, con base en el principio de la exclusividad formulado por Hannah Arendt, a su vez, inspirado en Kant, las personas escogen aquellos con los cuales quieren vivir, compartir momentos, hechos, informaciones, estando intrínsecamente conectada a la persona en su singularidad[11]. El derecho a la privacidad está, en esa concepción, caracterizado por tres atributos, que son: la *soledad*, el derecho de estar solo; el *secreto*, el derecho de exigir secreto; y la *autonomía*, el derecho de decidir sobre sí mismo.

4.1.3 El derecho a la privacidad y figuras afines

La idea de categorización del derecho a la privacidad es compleja y susceptibles de críticas, ya que el término puede derivar en innumerables figuras afines, como “vida privada”, “intimidad”, “sigilo de las correspondencias”, “sigilo de las comunicaciones”, “inviolabilidad del domicilio”,

[11] ARENDT, Hannah. Reflections on Little-Rock. En: *Dissent Magazine*, v. 6, n. 1, invierno, 1959, pp. 52-53.

"sigilo de la fuente", "derecho a la imagen", "derecho al honor", "protección de datos personales", entre otros. Esta significación dependerá del sujeto, del ordenamiento jurídico y del contexto abordado, ya que, según la fluidez de los contenidos, existe la posibilidad de migración de conceptos, pudiendo considerarse el derecho a la privacidad como un género con diversos contenidos.

Sin embargo, una importante distinción recae sobre el derecho a la vida privada y el derecho a la intimidad, ya que tales expresiones se utilizan en algunos ordenamientos jurídicos. En el derecho a la privacidad, el derecho a la vida privada puede ser considerado como la tutela de la vida personal y familiar del sujeto, así como del círculo cercano de la persona, entre la intimidad y la vida social del individuo, lugar en que éste practica los actos jurídicos privados y donde se desarrollan las interacciones relevantes a los seres humanos[12]. Es decir, la vida privada de la persona son las relaciones de proximidad emocional, que pueden ser de conocimiento de aquellos que están cerca y fueron elegidos para saber y participar de esa singularidad.

Por otro lado, el derecho a la intimidad puede ser definido como aquel que intenta proteger a las personas frente a la indiscreción ajena, en la medida en que pretende excluir del conocimiento ajeno algo sobre sí, sobre su núcleo esencial como persona, sobre su espacio más reservado de la existencia, o prohibir que otros se inmiscuyan en esa esfera más particular[13]. La intimidad puede, pues, guardar relación con las informaciones del ámbito exclusivo de una persona, que ella reserva para sí mismo, alejándose de cualquier repercusión social y, pudiendo determinar ella misma el alcance de su vida privada, tomando decisiones sobre los límites de ese espacio.

En un primer momento, la doctrina alemana de la teoría de las esferas sirvió como base para representar los niveles de privacidad. A partir de las ideas de círculos concéntricos, el primero, más amplio, es la esfera

[12] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

[13] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

de la vida privada (*Privatsphäre*), donde están las informaciones que el sujeto no quiere que sean de dominio público; el segundo, en el interior, menor, es la esfera de la intimidad (*Vertrauensphäre*), donde están las informaciones que el sujeto confía solamente a ciertas personas, en carácter reservado; y el tercero, más aún en el interior, es la esfera del secreto (*Geheimnsphäre*), donde están las informaciones que el sujeto no comparte con nadie o sólo con algunas personas[14].

Esta teoría acabó perdiendo credibilidad por considerar al individuo como una persona como una "cebolla pasiva", siendo superada, en razón de la insuficiencia técnica, de la necesidad de subjetivismo en cuanto al grado de las esferas y de las recientes innovaciones tecnológicas[15]. En su lugar, adviene la teoría del mosaico, sosteniendo que las informaciones, *a priori*, pueden ser irrelevantes bajo determinado prisma o si se las considera aisladas; pero si se analizan en relación con otras informaciones, a veces también irrelevantes por sí solas, pueden servir para formar una coyuntura plena de significado, de modo que la protección de la privacidad debe tener en cuenta el mosaico resultante y la revelación posible con estos datos[16].

4.1.4 El derecho a la privacidad en los textos normativos

Aunque el derecho a la privacidad ha sido una construcción inicialmente doctrinal y después utilizada en algunos precedentes jurisprudenciales, luego esta tutela pasó a ser insertada en las cartas positivas de derechos humanos y en los ordenamientos jurídicos comunitarios y nacionales. Sin embargo, como es notable y como se

---

[14] HUBMANN, Heinrich. *Das persönlichkeitsrecht*. Münster: Böhlau-Verlag, 1953 apud COSTA JR. Paulo José da. *O direito de estar só:* tutela penal da intimidade. 2. ed. São Paulo: RT, 1995, pp. 30-36.

[15] BURKERT, 2000, p. 46 apud DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. *Âmbito Jurídico*, Rio Grande, XI, n. 51, mar. 2008. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460.

[16] CONESA, Fulgencio Madrid. *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia, 1984, p. 45.

discutió anteriormente, el derecho a la privacidad, en estos marcos normativos, aparece bajo diversas formas, a veces como privacidad en sentido estricto, a veces como vida privada, otras veces como intimidad, pero en todos los casos se percibe intención de tutelar ese aspecto privado del ser humano.

4.1.4.1 Marco normativo universal, internacional y regional

La Declaración de los Derechos del Hombre y del Ciudadano de 1789 ya contenía ideas embrionarias de la protección de la privacidad, al establecer en su art. 10, que "nadie debe ser incomodado por sus opiniones, inclusive religiosas, siempre y cuando su manifestación no perturbe el orden público establecido por la Ley" [traducción libre] y, en su art. 11, que "[...] cualquier Ciudadano puede hablar, escribir e imprimir libremente, siempre y cuando responda del abuso de esta libertad en los casos determinados por la Ley" [traducción libre][17].

Expresamente, el derecho a la vida privada aparece, mundialmente, reconocido en la Declaración Universal de los Derechos Humanos de 1948, en el marco de la Asamblea General de las Naciones Unidas, que lo reconoce como un derecho humano, en su art. 12, al disponer que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor o a su reputación" y "que toda persona tiene derecho a la protección de la ley contra tales injerencias"[18].

Por otro lado, en la esfera americana, la Declaración Americana de los Derechos y Deberes del Hombre de 1948 fue también uno de los primeros instrumentos normativos a recoger el tema, cuando, en su art. V, dispone que "toda persona tiene derecho a la protección de la Ley contra

[17] FRANCIA. *Déclaration des Droits de l'Homme et du Citoyen de 1789*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789.

[18] ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Declaración Universal de Derechos Humanos de 1948*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.un.org/es/universal-declaration-human-rights/.

los ataques abusivos a su honor, a su reputación y a su vida privada y familiar"[19]. Más tarde, la Convención Americana de Derechos Humanos de 1969 dicta, en su art. 11, sobre la protección del honor y la dignidad, que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honor o reputación"[20].

En el ámbito europeo, el Convenio Europeo de Derechos Humanos de 1950, refiere, en su art. 8.1, que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"[21]. En este mismo sentido, la Carta de los Derechos Fundamentales de la Unión Europea de 2000 menciona, en su art. 7, que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"[22].

En el ámbito africano, la Organización para la Unidad Africana, cuando aprobó la Carta Africana sobre los Derechos Humanos y de los Pueblos, luego ratificada por la Unidad Africana, aunque no se refería directamente sobre la privacidad, establece, en su art. 4, que "todo ser humano tendrá derecho al respeto de su vida y de la integridad de su persona" [traducción libre][23]. La Carta Árabe sobre Derechos Humanos de 2004, documento proveniente de la Liga Árabe, cita, en su art. 21, que "nadie será sometido a injerencias arbitrarias o ilegales con respecto a su

[19] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Declaración Americana de los Derechos y Deberes del Hombre de 1948*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp.

[20] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) de 1969*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm.

[21] CONSEJO DE EUROPA. *Convenio Europeo de Derechos Humanos de 1950*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf.

[22] UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea de 2000*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

[23] UNIDAD AFRICANA. *Carta Africana sobre los Derechos Humanos y de los Pueblos de 1981*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf.

privacidad, familia, domicilio o correspondencia, ni a ataques ilegales a su honor o su reputación" [traducción libre][24].

Por otro lado, la Declaración de los Derechos Humanos en el Islam de 1990, documento oriundo de la Organización de la Conferencia Islámica, promulga, en su art. 18, que "todos deben tener el derecho a la privacidad en la conducción de asuntos privados, en su casa, en su familia, con respecto a sus bienes y relaciones" y que "no será permitido espiar, someterlo a vigilancia o dañar su reputación" [traducción libre][25].

Finalmente, la Carta Asiática de Derechos Humanos de 1998, documento creado por la Comisión Asiática de Derechos Humanos, organización fundada por un grupo de juristas y activistas de derechos humanos, ya que, todavía, no hay declaración intergubernamental en ese sentido, trae especialmente el "derecho a vivir en paz". Así, prevé, en su art. 4.1, que "todas las personas tienen el derecho a vivir en paz para que puedan desarrollar todas sus capacidades físicas, intelectuales, morales y espirituales, sin ser objeto de ningún tipo de violencia" [traducción libre][26].

4.1.4.2 Marco normativo comparado: Brasil y España

En términos específicos, en el caso brasileño, país de origen del autor, el tema está previsto en la Constitución Federal de 1988, la cual, en su art. 5º, inc. X, sobre los derechos y deberes individuales y colectivos, garantiza que "son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurado el derecho a indemnización por el daño material

[24] LIGA ÁRABE. *Carta árabe sobre los derechos humanos 2004*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.lasportal.org/ar/sectors/dep/HumanRightsDep/Documents/%D8%A7%D9%86%D8%AC%D9%84%D9%8A%D8%B2%D9%8A.pdf.

[25] ORGANIZACIÓN DE LA CONFERENCIA ISLÁMICA. *Declaración de los Derechos Humanos en el Islam de 1990*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.oic-iphrc.org/en/data/docs/legal_instruments/OIC_HRRIT/571230.pdf.

[26] COMISIÓN ASIÁTICA DE DERECHOS HUMANOS. *Carta Asiática de los Derechos Humanos de 1998*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.humanrights.asia/wp-content/uploads/2018/07/Asian-Human-Rights-Charter-2nd-Edition-English.pdf.

o moral resultante de su violación" [traducción libre][27]. En la legislación ordinaria, el Código Civil de 2002, en el capítulo sobre los derechos de personalidad, señala, en su art. 21, que "la vida privada de la persona natural es inviolable, y el juez, a petición del interesado, adoptará las providencias necesarias para impedir o hacer cesar acto contrario a esta norma" [traducción libre][28].

Por otro lado, en el caso español, el tema también aparece reconocido en la Constitución Española de 1978, la cual, en su art. 18.1, en la sección sobre los derechos fundamentales y las libertades públicas, deduce que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"[29]. En el mismo artículo, pero en el apartado 4, la Constitución Española innova en la cuestión de las tecnologías de información y comunicación e incluye la denominada libertad informática, al establecer que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[30]. Por último, en el ámbito ordinario, la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, dispone, en su art. 1 que "el derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas"[31].

---

[27] BRASIL. *Constituição da República Federativa do Brasil de 1988*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

[28] BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. *Institui o Código Civil*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm

[29] ESPAÑA. Constitución Española de 1978. *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311, pp. 29313 a 29424.

[30] ESPAÑA. Constitución Española de 1978. *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311, pp. 29313 a 29424.

[31] ESPAÑA. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. *Boletín Oficial del Estado*, 14 de mayo de 1982, núm. 115, pp. 12546 a 12548.

4.1.5 El derecho a la privacidad y los avances de las tecnologías de la información y comunicación

Es posible percibir que la expansión indiscriminada del uso de informaciones personales, provocado por el avanzo de las novedades cibernéticas, ha posibilitado innovadoras formas de violación de la privacidad, ya que, en la red, toda operación o conjunto de operaciones, realizada propiamente por el usuario o con la ayuda de medios automatizados, permite la recolección, almacenamiento, selección, evaluación, monitoreo, comparación, modificación, transferencia, utilización y tratamiento de información personal, en este caso, de datos personales.

En ese contexto, la preocupación con el derecho a la privacidad "decae en pro de definiciones cuyo centro de gravedad está representado por la posibilidad de cada uno de controlar el uso de las informaciones que le conciernen" [traducción libre], siendo más propio hablar de un derecho a la autodeterminación informativa[32]. La expresión "derecho a la autodeterminación informativa" fue utilizada en primer lugar por el Tribunal Federal Constitucional Alemán, en una resolución de un proceso relacionado con las informaciones personales recogidas de un censo en el año 1983[33]. De acuerdo con el Tribunal, el derecho general de protección de la persona, reconocido en el texto constitucional, abarca, considerando el procesamiento tecnológico y moderno de datos, la tutela del sujeto contra la recolección, almacenamiento, utilización y divulgación ilimitada de sus datos personales, debiendo se considerar un derecho fundamental la facultad del ciudadano de disponer libremente de sus datos[34].

---

[32] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 24.

[33] MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, p. 55-63. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877.

[34] MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, p. 55-63. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877.

Se ve que el derecho a la protección de datos personales supera el contenido esencial del tradicional derecho a la intimidad, ya que no se basa solamente en la tutela del contenido de naturaleza íntima de los datos recogidos; sino que abarca la facultad, primero de conocer, pero también de decidir sobre la recogida, sobre el tratamiento y sobre la posible transferencia de tales registros, ya que, en la sociedad en red informacional, las posibilidades de generación de datos, en ocasiones, no depende de tiempo, espacio y dispositivo determinado. Así, el derecho a la autodeterminación informativa es un derecho autónomo al derecho a la intimidad, constituyéndose como instrumento jurídico para garantizar la dignidad humana y el desarrollo de la personalidad, reposando sobre la facultad del sujeto de disponer de las propias informaciones personales, frente al uso indiscriminado de las tecnologías informáticas.

En el caso español, como se ha dicho, el propio texto constitucional separa el derecho a la intimidad (artículo 18.1) del derecho a la limitación de los usos informáticos para garantizar ese derecho (artículo 18.4). El Tribunal Constitucional, en la decisión STC nº 292/2000, delimita y define la protección de datos personales y señala que el objeto de este derecho "no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual"[35].

Sobre el tema, en el derecho comunitario europeo, precisamente por la libre circulación de personas, bienes y datos, ese derecho está previsto autónomamente en la Carta de Derechos Fundamentales de la Unión Europea de 2000, que, en su art. 8, señala que "todas las personas tienen derecho a la protección de los datos de carácter personal que les conciernen", de modo que "esos datos deben ser objeto de un trato leal, con fines específicos y con el consentimiento de la persona interesada o con otro fundamento legítimo previsto por la ley", y que "todas las personas tienen

[35] ESPAÑA. Tribunal Constitucional de España (Pleno). Sentencia nº 292/2000, de 30 de noviembre. *Boletín Oficial del Estado*, n. 4, 4 de enero de 2001, pp. 104-118.

derecho a acceder a los datos recopilados que les conciernen y obtener su rectificación"[36]. Por último, establece que "el cumplimiento de estas normas está sujeto a la supervisión por parte de una autoridad independiente"[37].

Además, algunas directivas ya apuntaban el camino para la tutela de este nuevo derecho, como fue el caso de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que se refiere tratamiento de datos personales y la libre circulación de estos datos[38]; de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[39]; y de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[40].

Se trata de un doble matiz, ya que dicha normatividad "por un lado, busca proteger a las personas en relación al tratamiento de sus datos personales, por otro lado, se destaca su misión de inducir al comercio a través del establecimiento de reglas comunes para la protección de datos en la región" [traducción libre], con especial relevancia por considerar "las exigencias de un mercado unificado como el europeo para reducir ampliamente los costos de transacciones, lo que incluye la armonización

---

[36] UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea de 2000*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

[37] UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea de 2000*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

[38] UNIÓN EUROPEA. Parlamento Europeo. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de la Unión Europea,* L 281, 23 de noviembre de 1995, pp. 31-50.

[39] UNIÓN EUROPEA. Parlamento Europeo. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de la Unión Europea,* L 281, 23 de noviembre de 1995, pp. 31-50.

[40] UNIÓN EUROPEA. Parlamento Europeo. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de la Unión Europea* L 201, 31 de julio de 2002, pp. 37-47.

de las reglas en materia de datos personales" [traducción libre][41]. De ello se desprende que, en este contexto, la protección de datos personales garantiza tanto el derecho a la privacidad (individual) como promueve la libre circulación de datos al mercado (siempre que se cumplan las normas), no en un intento de frenar la circulación de datos, sino al contrario, promoverlo legítimamente.

4.1.6 Los nuevos derechos de la protección de datos y la ciberseguridad bajo el Reglamento General de Protección de Datos

Considerando que las directivas no son de aplicación directa, sino que necesitan ser transpuestas a los ordenamientos jurídicos nacionales, se redacta, entonces, el Reglamento General de Protección de Datos (RGPD), con entrada en vigor el 25 de mayo de 2018, substituyendo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, siendo ese marco normativo de obligatorio cumplimiento y directamente aplicable, sin necesidad de transposición, aunque nuevas leyes nacionales están siendo creadas para adaptar la normativa interna anterior al nuevo reglamento[42]. El RGPD presupone un cambio en relación a la normativa anterior, ya que, además de una protección represiva, establece una aproximación proactiva, exigiendo un enfoque basado en el riesgo (no sobre el tipo de dato o sobre el tipo de tratamiento), así como una responsabilidad activa, consciente y diligente por los órganos responsables del tratamiento (ya que no existe un paquete cerrado de medidas de seguridad, dependiendo de la propia política de gestión de riesgos)[43].

---

[41] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 102. [en línea] [Fecha de consulta: 01/10/2020] Disponible en: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315.

[42] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88

[43] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88

Ocurre que la injerencia del RGPD acaba por avanzar en las fronteras físicas mundiales, ya que la protección no solo es aplicable al tratamiento de datos por una empresa establecida en la Unión Europea, independientemente del lugar de tratamiento de esos datos o de la nacionalidad del titular de los mismos; sino también, tratamiento de datos por una empresa no establecida en la Unión Europea que ofrezca bienes y servicios o monitoreo a los usuarios que allí se encuentren; además de servir como fuente de inspiración para normativas sobre protección de datos personas en países de otros continentes[44].

El RGPD se basa en los principios de la licitud, lealtad, transparencia, limitación de la finalidad, minimización de los datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva[45]. Se han producido cambios significativos en la forma de obtener el consentimiento, pues cuando el tratamiento se basa en el consentimiento del usuario (existen otras hipótesis que no dependen del consentimiento), éste debe ser explícito, claro, simple, activo (no se permite solamente el silencio como permiso para la recolección), debiendo contar con la aprobación del internauta para cada finalidad de monitoreo de datos, aunque sea de forma electrónica y por opción de caja de selección[46]. Además, el Reglamento obliga a informar sobre la base legal del tratamiento de datos, el plazo de conservación y transferencia de los mismos, garantizando el ejercicio de los derechos de los titulares de los datos, como la portabilidad, la eliminación de los datos y la notificación de

[44] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88

[45] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88

[46] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88

terceros sobre la rectificación o supresión o limitación de tratamiento solicitados por los titulares[47].

4.1.7 El derecho a la protección de datos en el contexto brasileño: el histórico de la Ley General de Protección de Datos Personales

En el caso brasileño, como se ha mencionado anteriormente, la Constitución Federal de 1988 dispone, en el art. 5º, inc. X, ser inviolable la intimidad, la vida privada, el honor y la imagen de las personas; y en el art. 5º, inc. XII, establece ser inviolable el sigilo de la correspondencia y de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas[48]. Además, como garantía fundamental, la Constitución Federal, en el art. 5º, inc. LXXII, establece que se concederá *habeas data*, en forma gratuita, para asegurar el conocimiento de información relacionada con la persona del peticionario, contenida en registros o bases de datos de entidades gubernamentales o de carácter público; y para la rectificación de datos, cuando no se prefiera hacerlo a través de un proceso confidencial, judicial o administrativo, abarcando ya la protección de datos personales, aunque de manera embrionaria.[49].

En 1990, cuando se ha promulgado el Código de Defensa del Consumidor, la legislación indicó, en el art. 43, que "el consumidor tendrá acceso a la información existente en los ficheros, registros y datos personales y del consumo archivados sobre él, así como de sus respectivas fuentes", por lo que "los registros y datos de los consumidores deben ser objetivos, claro, verdadero y en un lenguaje fácil de entender, y no puede

[47] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88

[48] BRASIL. *Constituição da República Federativa do Brasil de 1988*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

[49] BRASIL. *Constituição da República Federativa do Brasil de 1988*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

contener información negativa durante más de cinco años" [traducción libre], lo que da origen a un principio de calidad de los datos[50].

Luego, en 2003, hubo una mención por parte del Gobierno brasileño sobre el derecho fundamental a la protección de datos, cuando se ha firmado, el 15 de noviembre de ese año, la Declaración de Santa Cruz de La Sierra, el documento final de la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. En esta carta, en el ítem 45, los Estados manifestaron que "también somos conscientes de que la protección de los datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas normativas iberoamericanas para proteger la privacidad de los ciudadanos [...]"[51].

Con las discusiones en la Unión Europea en torno a la redacción de un Reglamento General de Protección de Datos Personales (como se menciona en el ítem anterior), con aplicación obligatoria en los países miembros, así como con las discusiones sobre la revisión de las Directivas de Protección de la Privacidad y Flujo de Datos Fronterizos de la Organización para la Cooperación y el Desarrollo Económicos - OCDE (traducción libre para *OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*), organización intergubernamental de la que Brasil quiere formar parte, comienza la lenta carrera por la redacción de la Ley General de Protección de Datos Personales brasileña.

El 13 de junio de 2012, el Proyecto de Ley nº 4.060/2012 fue presentado a la Cámara de Diputados, por el Diputado Milton Monti, basando íntegramente el tratamiento de los datos personales en la lealtad y buena fe del responsable del tratamiento con el fin de satisfacer el legítimo interese de los titulares, siendo que el proyecto de ley pasó durante años entre comisiones técnicas y audiencias públicas para

[50] BRASIL. Lei nº 8,078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União,* 12 de septiembre de 1990. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

[51] SECRETARIA-GERAL ÍBERO-AMERICANA. XIII Cimeira Ibero-Americana de Chefes de Estado e de Governo. *Declaração de Santa Cruz de La Sierra de 14 e 15 de novembro de 2003*. [en línea] [Fecha de consulta: 18/04/2019] Disponible en: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf.

escuchar a los expertos[52]. Entre tanto, la Ley nº 12.965, del 23 de abril de 2014, que crea el Marco Civil de la Internet, fue aprobada, estableciendo principios, garantías, derechos y deberes para el uso de Internet en Brasil, entre ellos el principio de la protección de datos[53].

Pocos días después de la aprobación del RGPD, el Poder Ejecutivo brasileño, el 13 de mayo de 2016, envió, de manera urgente, el Proyecto de Ley nº 5.276/2016, que también preveía el tratamiento de datos personales para garantizar el libre desarrollo de la personalidad y dignidad de la persona natural, aunque adjunto al Proyecto de Ley 4.060/2012[54]. Dos años después, el 29 de mayo de 2018, cuatro días después de la implementación del RGPD en la Unión Europea, la redacción final del PL 4.060/2012 ha sido aprobada por la Cámara de Diputados, y el 10 de julio de 2018, el Senado Federal también ha aprobado el proyecto de ley.

El 14 de agosto de 2018 se ha sancionado la Ley nº 13.709, que prevé la protección de datos personales y modifica la Ley nº 12.965, de 23 de abril de 2014 (Marco Civil de la Internet), con vetos parciales (incluidos de los artículos que creaban la Autoridad Nacional de Protección de Datos, bajo el argumento de defecto de iniciativa, ya que el Congreso Nacional no podría crear un organismo vinculado a la Presidencia de la República), con la entrada en vigencia a los 18 (dieciocho) meses de publicación[55]. Luego, el gobierno brasileño emitió la Medida Provisional nº 869/2018, posteriormente convertida, por el Congreso Nacional, en Ley nº 13.853/2019, que cambia el nombre de la ley para "Ley General de

[52] BRASIL. Câmara dos Deputados. Projeto de Lei nº 4.060, de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais e dá outras providências. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066.

[53] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União,* 24 de abril de 2014. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[54] BRASIL. Câmara dos Deputados. Projeto de Lei nº 5.276, de 13 de maio de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm.

[55] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União,* 15 de agosto de 2018. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

Protección de Datos Personales (LGPD)", crea la Autoridad Nacional de Protección de Datos (ANPD) y define la entrada en vigor, para la ANPD, de forma inmediata, y para los demás artículos, dentro de los 24 (veinticuatro) meses de su publicación[56].

Sin embargo, con el advenimiento del estado de calamidad pública resultante de la pandemia COVID-19, provocada por el coronavirus SARS-CoV-2, reconocido por el Decreto Legislativo nº 06, de 20 de marzo de 2020, que ha afectado a la economía mundial, incluyendo la adecuación de empresas y poderes públicos a la LGPD, fue necesario repensar la entrada en vigor de la ley[57]. El 29 de abril de 2020, el gobierno federal emitió la Medida Provisional nº 959, extendiendo la *vacatio legis* de las demás disposiciones de la LGPD hasta el 3 de mayo de 2021; y, el 10 de junio de 2020, se ha aprobado la Ley nº 14.010/2020, que establece el Régimen Jurídico de Emergencia y Transitorio para las Relaciones Jurídicas de Derecho Privado (RJET) durante la pandemia de coronavirus (COVID-19), que, entre otras cuestiones, pospone la entrada en vigor de las sanciones de la LGPD hasta el 1 de agosto de 2021[58].

La Cámara de Diputados, el 25 de agosto de 2020, al discutir la conversión en Ley de la Medida Provisional nº 959, acordó reducir la extensión del plazo de prórroga al 31 de diciembre de 2020[59]. Al día siguiente, el Senado Federal, analizando esta discusión, declaró el perjuicio

---

[56] BRASIL. Lei nº 13.853, de 08 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. *Diário Oficial da União,* 09 de julio de 2019. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm.

[57] BRASIL. Decreto Legislativo nº 6, de 2020. Reconhece, para os fins do art. 65 da Lei Complementar nº 101, de 4 de maio de 2000, a ocorrência do estado de calamidade pública, nos termos da solicitação do Presidente da República encaminhada por meio da Mensagem nº 93, de 18 de março de 2020. *Diário Oficial da União,* 20 de março de 2019. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/portaria/DLG6-2020.htm.

[58] BRASIL. Lei nº 14.010, de 10 de junho de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). *Diário Oficial da União,* 11 de julio de 2020. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm.

[59] BRASIL. Congresso Nacional. Medida Provisória nº 959, de 2020 (regras para o auxílio emergencial e adiamento da vigência da LGPD). Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a *vacatio legis* da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de

del art. 4 de la MP 959/2020 sobre la prórroga del plazo de la LGPD, pues entendió que el asunto, "entrada en vigencia de la ley", ya había sido discutido por el Congreso Nacional en el momento del RJET, por lo que, por la regla de anualidad de las proposiciones legislativas, no se podría volver a discutir, reconociendo, entonces, el texto como no escrito en el proyecto de ley[60].

El 26 de agosto de 2020, considerando la votación que tuvo lugar en el Congreso Nacional, el gobierno brasileño ha emitido el Decreto nº 10.474/2020, que aprueba la Estructura Regimental y el Cuadro Demostrativo de los Cargos en Comisión y las Funciones de Confianza de la Autoridad Nacional de Protección de Datos (ANPD)[61]. El 17 de septiembre de 2020, hubo la sanción presidencial de la Ley nº 14.058/2020, referente a la conversión en ley de la MP 959/2020[62]. Así, a partir de esa fecha y paralelamente a las discusiones doctrinales sobre la vigencia entre el voto del Congreso Nacional y la sanción presidencial, está plenamente vigente la Ley General de Protección de Datos Personales, salvo las sanciones administrativas previstas para el 1 de agosto de 2021.

Con gran inspiración en el RGPD, la LGPD prevé el tratamiento de datos personales, incluso en medios digitales, por persona natural o por persona jurídica de derecho público o privado, con el objetivo de proteger los derechos fundamentales de libertad y privacidad y el libre desarrollo

---

Dados Pessoais - LGPD. *Diário do Senado Federal,* 27 de agosto de 2020, pp. 9-24. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753.

[60] BRASIL. Congresso Nacional. Medida Provisória nº 959, de 2020 (regras para o auxílio emergencial e adiamento da vigência da LGPD). Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a *vacatio legis* da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. *Diário do Senado Federal,* 27 de agosto de 2020, pp. 9-24. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753.

[61] BRASIL. Decreto nº 10.474, de 26 de agosto de 2020. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. *Diário Oficial da União,* 27 de agosto de 2020. en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm.

[62] BRASIL. Lei nº 14.058, de 17 de setembro de 2020. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Lei nº 14.020, de 6 de julho de 2020. *Diário Oficial da União,* 18 de septiembre de 2020. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14058.htm.

de la personalidad de la persona natural[63]. Al igual que el RGPD, la LGPD tiene aspectos extraterritoriales, ya que se aplica a cualquier operación de tratamiento realizada por una persona natural o por una persona jurídica de derecho público o privado, independientemente del medio, del país de su sede o del país donde se encuentren ubicados los datos, siempre que la operación de tratamiento se realice en el territorio nacional; o que la actividad de tratamiento tenga como objetivo ofrecer o proveer bienes o servicios o tratamiento de datos de personas naturales ubicadas en el territorio nacional; o que los datos personales objeto del tratamiento hayan sido recogidos en el territorio nacional, lo que eventualmente puede provocar un conflicto positivo de normas de derecho internacional privado, ya que, en un determinado tratamiento de datos, tanto el RGPD como la LGPD pueden ser aplicables.

Además, la LGPD establece que las actividades de tratamiento de datos personales deben respetar la buena fe y los principios de finalidad, adecuación, necesidad, libre acceso, calidad de los datos, transparencia, seguridad, prevención de daños, no discriminación y rendición de cuentas[64]. Señala que la disciplina de protección de datos personales se basa en el respeto a la privacidad; autodeterminación informativa; libertad de expresión, información, comunicación y opinión; la inviolabilidad de la intimidad, del honor y de la imagen; desarrollo e innovación económica y tecnológica; libertad de prensa, libre competencia y protección del consumidor; y derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por las personas naturales[65].

Enumera, como bases legales para el tratamiento de datos, las posibilidades de suministro del consentimiento por parte del titular;

---

[63] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União,* 15 de agosto de 2018. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[64] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União,* 15 de agosto de 2018. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[65] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União,* 15 de agosto de 2018. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

cumplimiento de obligación legal o regulatoria; tratamiento y uso compartido de datos necesarios para la implementación de políticas públicas por parte de la administración pública; realización de estudios por un organismo de investigación; ejecución de procedimientos contractuales o preliminares relacionados con el contrato; ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales; protección de la vida o seguridad física del titular o de terceros; tutela de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria; intereses legítimos del responsable del tratamiento o de un tercero; o, finalmente, protección crediticia, incluidas las disposiciones de la legislación pertinente[66].

Por la LGPD, el titular, al igual que el RGPD, tiene, de manera facilitada y gratuita, los derechos a la confirmación de la existencia del tratamiento; al acceso a los datos; a la corrección de datos incompletos, inexactos o desactualizados; a la anonimización, bloqueo o eliminación de datos innecesarios, excesivos o tratados en desacuerdo con lo dispuesto en la legislación; a la portabilidad de los datos a otro proveedor de servicios o productos, previa solicitud expresa, de acuerdo con la normativa de la autoridad nacional, sujeta a secretos comerciales e industriales; a la eliminación de los datos personales tratados con el consentimiento del titular; a la información de entidades públicas y privadas con las que el responsable del tratamiento ha compartido el uso de datos; a la información sobre la posibilidad de no suministrar consentimiento y sobre las consecuencias de la negación; y la revocación del consentimiento[67].

La LGPD también crea la Autoridad Nacional de Protección de Datos Personales (ANPD), una autoridad de control responsable por garantizar la protección de los datos en el país y de supervisar la aplicación de la legislación, entre otras competencias. Sin embargo, la ANPD fue creada

[66] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União,* 15 de agosto de 2018. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[67] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União,* 15 de agosto de 2018. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

originalmente como un órgano de la administración pública federal, miembro de la Presidencia de la República, lo que generó críticas por parte de expertos, quienes consideraron que ser sometido al gobierno federal afectaría la necesaria independencia de la institución. Así, luego de una gran presión política, se ha determinado que la naturaleza jurídica de la ANPD es transitoria y podrá ser transformada por el Poder Ejecutivo en una entidad de la administración pública federal indirecta, es decir, independiente, sometida a un régimen especial y vinculada a la Presidencia de la República dentro de los 2 (dos) años a partir de la fecha de entrada en vigor de la estructura regulatoria de la ANPD[68].

4.1.8 Breves comparaciones entre el RGPD y la LGPD

Cabe recordar que, como se ha mencionado, la Ley General de Protección de Datos Personales (LGPD) tiene una gran inspiración en el Reglamento General de Protección de Datos Personales (RGPD) y, considerando que no es una traducción del modelo europeo, trae algunos matices y diferencias en la gestión del derecho a la privacidad. Se señala que la LGPD, por su estructura, es una ley, contiene cláusulas más abiertas y subjetivas y depende de regulación por la ANPD, lo que permite una interpretación sistémica y teleológica; mientras que el RGPD, como su nombre, es un reglamento, con reglas más objetivas y reglas específicas.

El RGPD y la LGPD enumeran bases legales para el tratamiento de datos personales, por lo que cada finalidad debe ir acompañada de una hipótesis de legitimación normativa. Las dos leyes traen, en común, aunque en diferentes palabras, las hipótesis de consentimiento explícito, necesidad contractual, ejecución de políticas públicas, interés vital, obligación legal e interés legítimo. La LGPD, además de estos, aporta específicamente otras bases legales, a saber, la protección de la salud en

[68] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União,* 15 de agosto de 2018. [en línea] [Fecha de consulta: 08/10/2020] Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

un procedimiento realizado por profesionales de la salud, la realización de estudios por un organismo de investigación, el ejercicio de derechos en juicios y la protección de las relaciones crediticias.

En relación a los datos sensibles, la legislación prevé una redacción divergente: mientras que la LGPD establece que el tratamiento de datos personales sensibles solo puede ocurrir en los casos previstos, es decir, sobre las bases legales; el RGPD determina que el tratamiento de datos personales sensibles está prohibido, excepto en las excepciones previstas en el reglamento. Además, la LGPD enumera dos hipótesis sin equivalencia en la legislación europea, a saber, la ejecución, por parte de la administración pública, de políticas públicas previstas por ley o reglamento, y la garantía de prevención del fraude y seguridad del titular en los procesos de identificación y autenticación de registro en sistemas electrónicos. A su vez, el RGPD permite el tratamiento de datos sensibles hechos públicos por el titular y datos relativos a miembros actuales o anteriores de fundaciones, asociaciones u organizaciones sin ánimo de lucro, tratados con fines legítimos y con las medidas de seguridad adecuadas.

Específicamente en relación al derecho de acceso a los datos personales, la LGPD determina que el plazo para dar cumplimiento a la petición del titular es de 15 (quince) días, mientras que el RGPD determina que el plazo es mayor, 30 (treinta) días. Una cuestión interesante recae sobre el *marketing* directo, ya que el RGPD define los requisitos y pasos para permitir tal operación, y el usuario puede oponerse al tratamiento de los datos para crear perfiles de *marketing*, mientras que la LGPD guarda silencio sobre este aspecto, lo que sugiere seguir las reglas generales de tratamiento.

En cuanto a la notificación de incidentes de seguridad, la LGPD solo establece que la comunicación debe realizarse en un plazo "razonable", y el RGPD, por su parte, prescribe que una violación de datos personales debe ser reportada a la autoridad de control dentro de las 72 (setenta y dos) horas después del conocimiento del hecho. Además, el RGPD determina que el responsable debe informar la violación de datos personales a

la autoridad supervisora y, cuando esta violación pueda implicar un alto riesgo para los derechos y libertades de las personas, también al interesado sin demoras indebidas; la LGPD solo establece que debe existir una comunicación a la ANPD y al titular del incidente de seguridad que pueda ocasionar un riesgo o daño significativo a los titulares, lo que deja un margen de interpretación si cada incidente debe ser reportado efectivamente.

En cuanto al informe de evaluación e impacto sobre la protección de datos personales, el RGPD proporciona una descripción detallada del procedimiento y contenido a prever en este documento, especialmente cuando el tratamiento resulta en un alto riesgo para los derechos y libertades de la persona, siendo que, aún, trae la posibilidad de haber una consulta previa con la autoridad de control. En el caso brasileño, la LGPD establece que el informe debe contener, como mínimo, una descripción de los tipos de datos recopilados, la metodología utilizada para la recopilación y garantía de la seguridad de la información y el análisis del responsable del tratamiento en relación con las medidas, salvaguardias y adopción de mecanismos de mitigación de riesgos, dependiendo de información adicional que se proporcione en la normativa específica de la ANPD.

Sobre los agentes de tratamiento, la LGPD importa una traducción mitigada de la versión inglesa y portuguesa del RGPD, definiendo el "controlador" del tratamiento, en inglés "controller", como la persona natural o jurídica, de derecho público o privado, ante quien compite las decisiones sobre el tratamiento de datos personales; el "operador", en inglés "processor", como persona natural o jurídica, de derecho público o privado, que realiza el tratamiento de datos personales en nombre del "controlador"; y el "encargado" como la persona designada por el responsable del tratamiento y el operador para actuar como canal de comunicación entre el responsable del tratamiento, los titulares de los datos y la autoridad de control. La versión portuguesa del RGPD incluye, respectivamente, el "responsable", el "subcontratante" y el "encargado de protección de datos"; mientras que la versión española del RGPD, objeto de estudio de este trabajo, presenta, respectivamente, el "responsable", el "encargado" (aunque

en la traducción portuguesa se entiende como “encargado” el que es, en España, el “delegado”) y el “delegado”.

En lo que se refiere al vínculo entre los agentes de tratamiento, la LGPD no dispone de cualquier obligación de formalizar esta relación, sin embargo el RGPD establece que el tratamiento de datos realizado por el encargado debe estar previsto en un contrato u otro acto jurídico, que pueda vincular al responsable del tratamiento con el encargado. Además, ambas leyes establecen que el responsable y el encargado no serán responsables cuando la persona natural o jurídica no esté involucrada en el tratamiento de los datos; o cuando, a pesar del daño, el tratamiento se lleva a cabo de conformidad con la ley; pero la LGPD innova al señalar también que no se responsabilizaran cuando los agentes demuestren que el daño es por culpa exclusiva del titular de los datos o de terceros, lo que puede generar discusiones sobre el reconocimiento del riesgo fortuito interno, conforme Enunciado 473, del Superior Tribunal de Justicia de Brasil.

Sobre la responsabilización por el incumplimiento de las obligaciones legales, ambas leyes traen un listado de sanciones, que van desde una advertencia hasta la suspensión o prohibición del tratamiento de datos personales. En cuanto a las multas administrativas, el RGPD establece que, en caso de infracción de la ley, pueden variar de EUR 10,000,00.00 (diez millones de euros) a EUR 20,000,00.00 (veinte millones de euros) o del 2% (dos por ciento) al 4% (cuatro por ciento) de los ingresos anuales correspondientes al ejercicio anterior, el que sea mayor; la LGPD, a su vez, establece una multa simple de hasta el 2% (dos por ciento) de la facturación de una empresa privada, grupo o conglomerado en Brasil en su último año, sin impuestos, limitada en total a R$50,000,000.00 (cincuenta millones de reales) por infracción.

Como se ve en este apartado y en los dos anteriores, el RGPD ha sido publicado en mayo de 2016 y ha estado en vigor desde mayo de 2018, y la LGPD ha sido publicada en agosto de 2018 y está en vigor desde septiembre de 2020, pero la historia y la experiencia legislativas europea se remontan a la década de 1980, mientras que en Brasil el tema comenzó a

ser tratado con más fuerza recién a fines de la primera década del siglo XXI. A pesar de ello, las leyes generales de privacidad están conectadas y respaldadas por denominadores comunes, y es urgente y necesario concienciar a los titulares y adecuar los agentes de tratamiento, incluido el Poder Público, a los nuevos matices del derecho a la privacidad en la sociedad red.

4.1.9 ¿Hay que pensar en un nuevo derecho a la privacidad?

De ahí que, en virtud de este cambio de reglas, un sin número de políticas de privacidad, políticas de cookies, políticas de uso de aplicaciones y dispositivos, entre otros tipos de documentos y términos de adhesión firmados por los usuarios, deben ser actualizados, divulgados y aceptados, además de la adaptación en cuanto a las cuestiones técnicas, científicas, sociales, publicitarias, laborales y sectoriales involucrando tales productos y servicios. De esta manera, el derecho a la protección de datos personales - y en última instancia, el derecho a la privacidad - se somete a un régimen de ciberseguridad, es decir, a un conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo la infraestructura tecnológica, los servicios que presta y la información que maneja[69].

Se trata del resultado de un largo proceso normativo-regulatorio, que se puede clasificar, según algunos autores, en cuatro generaciones de leyes[70]. La primera generación de leyes de protección de datos personales fue formada por normas que, preocupadas por el estado de la tecnología y la profusión de bases de datos elaboradas, buscaban la autorización de los usuarios para crear estas estructuras y se enfocaban en reglas dirigidas a

[69] ESPAÑA. Ministerio de Defensa. Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. *Boletín Oficial de Ministerio de Defensa*, 26 de febrero de 2013, n. 40, pp. 4154-4156.

[70] MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). *Technology and privacy*: The new landscape. Cambridge: MIT Press, 1997, pp. 219-242.

los organismos públicos para el procesamiento de las informaciones[71]. La segunda generación de leyes sobre la materia, consciente de la diáspora de las bases de datos, se caracterizó por regular la privacidad como una libertad negativa, para que el ciudadano pudiera restringir el acceso a los datos por parte de los organismos públicos[72].

Sin embargo, considerando que el suministro de datos personales es indispensable para la vida social, en la década de 1980, surgió una tercera generación de leyes de protección de datos, entendiendo que se trata de un proceso complejo, cuya protección debe ir más allá del permiso o no para el uso de información, sino que debe considerar, incluir e informar al usuario sobre las sucesivas etapas del tratamiento, en una autodeterminación informativa[73]. Finalmente, la cuarta generación de leyes de protección de datos, como las actuales, entiende que la protección de datos no se puede reducir a una elección individual y considera necesario implementar instrumentos de protección colectiva, reconociendo el desequilibrio de la relación entre operadores de tratamiento y usuarios, fortaleciendo la posición del usuario frente a las entidades que procesan los datos y creando autoridades independientes para la supervisión pública del procesamiento de datos en la sociedad[74].

A pesar de los compromisos políticos y normativos internacionales firmados por parte de las naciones y de las corporaciones en favor del derecho a la protección de datos personales, y del desarrollo del derecho a la privacidad; la vigilancia social a la que los ciudadanos son sometidos y la propia subjetividad formada por el miedo al terror acaban poniendo en

---

[71] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 96. [en línea] [Fecha de consulta: 01/10/2020] Disponible en: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315.

[72] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 97. [en línea] [Fecha de consulta: 01/10/2020] Disponible en: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315.

[73] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 97. [en línea] [Fecha de consulta: 01/10/2020] Disponible en: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315.

[74] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico,* Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 98. [en línea] [Fecha de consulta: 01/10/2020] Disponible en: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315.

jaque estos derechos fundamentales, ya que el límite entre conocimiento público, vida privada, intimidad y secreto es fluido. En la sociedad en red de vigilancia social, la privacidad, como conquista popular y derecho de primera generación de libertad individual, puede necesitar una reformulación.

4.2 Hacia un nuevo derecho a la privacidad: desafíos y caminos en tiempos de ciberseguridad

El siglo XX representó la era de oro para la normatividad de los derechos y garantías fundamentales y, a medida en que los avances sociales y la propia configuración del Estado fue cambiando debido al perfeccionamiento de las tecnologías de la información y comunicación, nuevas generaciones/dimensiones de derechos fundamentales fueron surgiendo. Entre ellos, el derecho a la privacidad, en la concepción moderna, también pasó por transformaciones, habiendo invadido, conquistado y colonizado la esfera pública social, aunque en los últimos años ha sido marcada por las caídas vertiginosas del apogeo de su gloria.

4.2.1 El cambio de paradigma y el nuevo concepto de privacidad

Se trata, pues, de una alteración de paradigma y una necesaria resignificación de conceptos, marcada por el flujo informacional masivo, abarcando nuevos matices sobre el derecho al secreto, el derecho a la intimidad, el derecho a la vida privada y familiar, el derecho a la autodeterminación informativa y el derecho a la protección de datos personales. Aunque al final sobre el pasado siglo se ha hablado del final de la privacidad, parece más oportuno intentar conceptualizar el derecho a la privacidad como una superación de la concepción sólida y estática de los

textos normativos cerrados de auto confinamiento para alcanzar una perspectiva abierta, dinámica y fluida en una sociedad tecnológica[75].

El derecho a la privacidad, en los ordenamientos jurídicos modernos, está fundado en la concepción clásica de la privacidad relacionada con la idea aislacionista del ser, en una lógica excluyente de "persona-información-sigilo", posibilitando al individuo protegerse de intromisiones indeseadas en lo que le era más reservado, aunque que "a partir de la crítica del denominado pensamiento postmetafísico se hace muy complicado sostener que el sujeto pudiera ser algún género de yo como sustancia autoconsciente de los inicios cartesianos de la filosofía de la conciencia"[76]. Con el desarrollo de las tecnologías de la información y comunicación, se ha producido una relativización de lo que es considerado secreto, de manera que el sujeto, en el panorama de las relaciones sociales conectadas globalmente, se adhiere al virtual – aquí no como digital, sino como potencia de ser – y posee la prerrogativa y la necesidad de compartir información para formar una identidad en red[77], necesitando que el concepto de privacidad sea reformulado.

De esta forma, la definición de la privacidad sólo como el derecho de ser dejado sólo (*right to be let alone)* y de restringir el conocimiento público de informaciones consideradas privadas perdió hace algunos años el valor de ser el único fundamento de esta tutela, aunque esta cuestión es un aspecto esencial a ser aplicado a situaciones determinadas cuando se exige esa protección. Se trata, entonces, del fin de un largo proceso evolutivo experimentado por el concepto de privacidad: de una definición original como el derecho de ser dejado en paz, hasta el derecho de control que permite al sujeto ser dueño de su propia información y determinar cómo quiere construir su propia esfera privada[78].

---

[75] PÉREZ LUÑO, Antonio Enrique. *Los derechos en la sociedad tecnológica***.** Madrid: Editorial Universitas, S.A., 2012, p. 93.

[76] MUGUERZA, Javier. De la conciencia al discurso ¿un viaje de ida y vuelta? In: *La filosofía moral y política de Jürgen Habermas*. Madrid: Biblioteca Nueva, 1997, pp. 63-110, p. 98.

[77] CASTELLS, Manuel. *O poder da identidade.* 2. ed. São Paulo: Paz e Terra, 2000.

[78] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 17.

Esto no quiere decir que ese aspecto de control del sujeto sobre la propia esfera de privacidad estuviera ausente de las definiciones tradicionales, ya que el control era utilizado justamente como una herramienta para realizar la finalidad de ser dejado sólo y definir lo que debería quedar fuera del conocimiento ajeno, pero bajo ángulo exclusivamente individualista y privado, que el desarrollo actual de las tecnologías ya no permite. Por otro lado, actualmente, la cuestión de la privacidad como control llama la atención sobre la posibilidad de que los sujetos ejerzan los poderes conquistados por el suministro de datos personales, entre ellos los de conocer, controlar, enderezar, oponer, interrumpir y prohibir el flujo de informaciones que se relacionan con él.

Así, se introduce una nueva concepción de privacidad, pudiendo ser definida más precisamente, en una primera aproximación, como el derecho de mantener el control sobre las propias informaciones, identificada con la tutela de las elecciones de vida contra toda forma de control público y de estigmatización social, en un cuadro caracterizado precisamente por la libertad de las elecciones existenciales[79]. Se verifica, entonces, que la privacidad como la conocemos, relacionando privado con ámbito personal y secreto, dio espacio a nuevos caminos, pudiendo ser entendida en una lógica de "persona-información-circulación-control", no más restringida a la burguesía del siglo XX sino destinada a la multitud en la sociedad en red[80].

4.2.2 Las paradojas de la privacidad en el siglo XXI

Considerando la difusión de las tecnologías de información y comunicación y la producción en masa de *big data*, se percibe que el objeto de tutela de la privacidad también ha sufrido cambios, comprendiendo un número creciente y exponencialmente mayor de informaciones y situaciones jurídicas relevantes que necesitan de un control del individuo. En este

[79] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 92.

[80] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 93.

sentido, la privacidad no necesariamente guarda relación con algo privado y, a su vez, lo privado ya no hace referencia a algo secreto, derivándose de allí, al menos, cuatro paradojas y el surgimiento de una nueva dimensión de la privacidad, la extimidad.

4.2.2.1 La primera paradoja: de las murallas digitales

La primera paradoja de la privacidad guarda relación con la propia idea que originó el régimen jurídico moderno de ese derecho, o sea, la necesidad de reservar aquello que es privado. Las tecnologías de la información y comunicación, por más que faciliten el contacto interpersonal mundial y creen nuevas formas de relacionarse, también contribuyen a la construcción de la esfera privada en la creación de un torre de marfil personal, a medida que evitan aquellos contactos sociales consolidados y cotidianos, aumentando la sensación de autosuficiencia, como, por ejemplo, en los casos de la ampliación del teletrabajo, de la realización de videoconferencias, de la preferencia por el comercio electrónico y por las transacciones bancarias en línea, de predilección por el entretenimiento de los dispositivos inteligentes y conectados, entre otros[81].

En la aldea global, esas tecnologías de la información y comunicación han provocado el enclaustramiento de los individuos en fortalezas electrónicas digitales y han distanciado a los sujetos de las formas de control social posibilitadas por el actuar en público y por la modulación de grupos de interés a partir de la vigilancia sólida. Sin embargo, es verdad que, como se ve en el primer capítulo, las formas de control social son cada vez más invasivas y la vigilancia cada vez más líquida, es decir, dispersa como un fluido por todos los dispositivos sociales, justamente haciendo uso de la recogida, del tratamiento y la transferencia de datos provenientes de esas tecnologías informacionales, como si fueran *backdoors* en esas murallas digitales erigidas.

[81] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, pp. 94-95.

4.2.2.2 La segunda paradoja: el núcleo duro de la privacidad

En otro sentido, la segunda paradoja de la privacidad se refiere a la propia resignificación de la protección de las informaciones íntimas y secretas, es decir, aquellas que el sujeto quiere que sean excluidas en determinada medida de la circulación en público. Esto, porque los textos normativos, internacionales, comunitarios o nacionales, siguen, en cierta forma, construyendo un "núcleo duro" de la privacidad relativo a la información sensible, que tradicionalmente exigían una mayor capa de protección y secreto, cuyo tratamiento discrecional podría originar una cierta discriminación, como, por ejemplo, los datos relacionados con la salud, el origen étnico, la opinión política, la orientación sexual, la filiación sindical, la creencia religiosa, entre otros[82].

Ocurre que muchas de esas informaciones calificadas como sensibles no están reservadas solamente a la esfera privada del individuo, sino que, por el contrario, en contextos democráticos, están relacionadas con la esfera pública, en la medida en que forman parte de la identidad del sujeto, pudiendo éste utilizarlas para manifestarse como persona, para encontrar semejantes y diferentes o para ocupar el espacio público, para reconocerse como actor político[83]. De ese modo, se atribuye un estatuto de más privado y se limita fuertemente la circulación y el tratamiento de los datos sensibles no porque sean secretos, sino justamente para que el individuo pueda hacerlos públicos.

4.2.2.3 La tercera paradoja: el derecho como poder de la privacidad

La tercera paradoja de la privacidad trata de la propia evolución de ese derecho, conforme analizado en el capítulo anterior, ya que la existencia de riesgos derivados de la recogida y tratamiento de datos personales hizo surgir el derecho a la autodeterminación informativa,

[82] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, pp. 95-96.

[83] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 96.

abarcando la potestad del individuo de preguntar, recibir información, limitar la circulación, oponerse, prohibir y eliminar la información que de ahí se deriva. En verdad, el derecho fundamental a la privacidad, además de un derecho o un conjunto de derechos, también es la atribución de una serie de poderes a los interesados, como si fuera el reconocimiento de derechos implícitos a los derechos de personalidad.

Así, el derecho a la privacidad, en ese nuevo matiz que permite al sujeto acompañar la manipulación de sus datos personales por otras personas o empresas, pone de relevancia el derecho al acceso a dicha información. Es decir, por un lado está el criterio formal de posesión de las informaciones, basada en la legitimidad de la recogida o en el consentimiento del individuo por parte de los responsables y encargados del tratamiento, pero, por otro lado, está la prevalencia del derecho del individuo sobre los propios datos, de forma que el derecho a la privacidad acaba por convertirse en instrumento capaz de hacer más transparente y pública la esfera de actuación de los responsables o encargados del tratamiento[84].

4.2.2.4 La cuarta paradoja: el Estado en red

Por último, la cuarta paradoja de la privacidad, pensada a partir del presente trabajo, está desarrollada en el sentido de que el derecho a la privacidad, en comparación con otros derechos fundamentales, trata de la propia subjetividad del ciudadano y exige una actuación del Estado para garantizar la protección de esas informaciones personales, ya sea a través de una regulación, o de mecanismos de control, u otros instrumentos normativos. El problema deriva del hecho de que el Estado, siendo un actor social y un nudo de la sociedad en red, para sobrevivir a esa nueva dinámica de poder en red, acaba por violar sistemáticamente la privacidad de

[84] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, pp. 96-97.

los individuos, nacionales y extranjeros, bajo la justificación del interés público, tal como se ha puesto de relieve en el capítulo anterior.

4.2.3 La extimidad como nueva dimensión de la privacidad

Como se mencionó anteriormente, el perfeccionamiento de las tecnologías de información y comunicación y la democratización del acceso a dispositivos informáticos, con la consiguiente popularización de las redes sociales, han hecho aparecer una nueva modalidad híbrida de privacidad, cuando el individuo quiere mantener algunos aspectos de su vida en la esfera privada, de forma ajena al conocimiento general, pero, al mismo tiempo, también quiere transformar esa esfera privada, en cierta medida, en una esfera pública, en una especie de publicidad de lo privado. Se trata de un desplazamiento del núcleo de la privacidad, a partir de la espectacularización de sí mismo, de la ficcionalización del yo y de la socialización de la intimidad[85].

En otras palabras, en la sociedad digitalmente conectada e influenciada globalmente, no puede hablarse ya más de "la dualidad entre el hombre prisionero de sus secretos y el hombre que nada tiene que esconder; entre la 'casa-fortaleza', que glorifica la privacidad y favorece el egocentrismo, y la 'casa-vitrina', que privilegia los intercambios sociales" [traducción libre][86]. Se configura, entonces, una nueva dimensión de la privacidad, caracterizada por la exteriorización de la interioridad del individuo, resignificando el criterio de público-privado, en razón de los procesos comunicativos de la sociedad en red, en un ejercicio de extimidad[87].

La extimidad, desde el punto de vista psicoanalítico, está fundamentada en la exteriorización de la intimidad, es decir, en la necesidad de dar

---

[85] LIMBERGER, Têmis. *Cibertransparência informação pública em rede:* a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016, p. 60.

[86] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 25.

[87] BOLESINA, Iuri. *O direito à extimidade:* as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017, p. 182.

visibilidad al propio "yo", sea por medio de la revelación de secretos, de la exposición del singular, de la espectacularización de la intimidad o de la ficcionalización de sí mismo, abriendo esa esfera privada al mirar de los demás para que sea validada la propia existencia, para que sea confirmado el propio ser y existir[88]. Considerando que el coste social de la no exposición puede ser grande, los individuos acaban por exponer la intimidad y el secreto, deseando fama, seguidores, interacciones, *likes, scores* y visualizaciones, en una autoafirmación constante, terminando por revelar datos personales, patrones sociales e informaciones de preferencias.

Así, en una supuesta autoviolación de la privacidad, los individuos, con el objetivo de formar parte de esa sociedad en red, caracterizada por el consumismo de la información, proporcionan datos relevantes para el acceso y el mantenimiento de productos y servicios, especialmente redes sociales. No se puede, por lo tanto, "trazar un límite, como si el mundo de la defensa de la privacidad y el de la acción pública fueran hostiles o no comunicantes; no existe una separación, sino un *continuum*" [traducción libre], convirtiéndose la privacidad, pues, en un fluido[89].

4.2.4 El consentimiento informado libre frente a los términos y condiciones

Cabe señalar, sin embargo, que el suministro de datos personales a cambio de los beneficios sociales que las personas supuestamente aprovechan de los productos y servicios ofrecidos no es la única contrapartida de esa relación, ya que el tratamiento de datos por las organizaciones públicas y privadas puede hacer surgir nuevas concentraciones de poder o el fortalecimiento de poderes ya existentes, como si fuera *plus-poder*. En otras palabras, el ofrecimiento de productos y servicios, a menudo gratuitos, exige del usuario el suministro de datos personales, que no necesariamente sirven para la propia existencia del producto o servicio que llega al

[88] LACAN, Jacques. *O seminário:* livro 16: de um Outro ao outro. Rio de Janeiro: Jorge Zahar, 2008, p. 241.

[89] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 47.

individuo, sino para agregar valor a la propia organización como nudo social en la malla del poder en red.

De esta forma, considerando que se vuelve cada vez más difícil determinar sobre qué tipos de información los sujetos están dispuestos a renunciar a una mayor protección, el control del tratamiento de datos personales depende de la legitimidad y legalidad de esa decisión. En este sentido, se percibe una alteración de paradigma, incluso por el advenimiento del Reglamento General de Protección de Datos Personales de la Unión Europea, superando el *implied consent*, es decir, el consentimiento implícito que suponía que la mera utilización del producto o servicio implicaba en concordancia con la manipulación de los datos; por el *informed consent,* que determina la provisión del mayor número de explicaciones al usuario para que éste concuerde conscientemente con las circunstancias y finalidades del tratamiento de los datos, inicialmente pensado en el ámbito de la salud[90].

En este contexto, se puede cuestionar en qué medida el consentimiento informado tiene potencial de ser un control social y un ejercicio de autodeterminación informativa en lo que se refiere al permiso de circulación de datos. En primer lugar, es importante recordar que el suministro del consentimiento es *conditio sine qua non* para el acceso de productos y servicios en la sociedad en red, sin el cual el usuario no puede disfrutar de las interacciones sociales allí permitidas, convirtiéndose la autorización en una mera etapa en este proceso. En segundo lugar, la obtención del consentimiento informado se limita a un simple *clic* del usuario en un botón predeterminado o en una caja de selección (*blank selection*), eximiendo del real entendimiento de los términos y condiciones presentados, ya que basta la aceptación formal del individuo para que supuestamente se legitime el tratamiento de los datos.

Por otro lado, no siempre el usuario sabe lo que está aceptando, dada la extensión de los textos y la utilización de expresiones jurídico-técnicas,

[90] TARODO, Salvador Soria. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: *Derecho y Salud*, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006, p. 143-144.

queriendo, además, acceder al producto o servicio, independientemente de lo que esté aceptando en las entrelíneas de las políticas de privacidad. En el marco de la teoría de los mosaicos que refiere que no es el dato, por sí solo, relevante, sino el contexto de informaciones de ahí derivadas[91], no siempre quedan claras las reales finalidades de la recogida de informaciones, ya que es posible generar un sin número de variables para ser manipuladas, confiriéndose valor a depender del tratamiento de datos utilizado y del reconocimiento de patrones informacionales deseados.

Es importante citar, como se ha observado en el capítulo anterior, que esa cuestión de consentimiento pierde relevancia cuando se enfrenta a las justificaciones del régimen de vigilancia electrónica global de personas e informaciones, una vez que el interés privado se pliega al interés público de protección y prevención de amenazas contra la seguridad pública. El propio Reglamento General de Protección de Datos de la Unión Europea contempla esta excepción al régimen jurídico de aplicación general[92]. Sin embargo, la propia existencia de los programas de vigilancia masiva para salvaguardar la seguridad nacional fue descubiertos bajo polémicas internacionales, demostrando ser desconocidas o insuficientes las condiciones de supervisión pública o garantías seguras y reales del cumplimiento de los derechos y garantías de los ciudadanos por parte de esas agencias institucionales[93].

En lo que se refiere al consentimiento, cabe la crítica de que éste no es necesariamente consciente o libre, en el propio sentido de las palabras, porque sometido a esa lógica informacional y a ese proceso de subjetivación creado por el consumo de las tecnologías de la información y

[91] CONESA, Fulgencio Madrid. *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia, 1984, p. 45.

[92] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.

[93] PESSOA, João Pedro Seefeldt. OLIVEIRA, Rafael Santos de. "Big Brother Watch and Others v. The United Kingdom": el régimen de vigilancia social y el derecho al respecto a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos. En: *Pensar*: Revista de Ciências Jurídicas, Fortaleza, v. 24, n. 3, pp. 1-12, jul./sept. 2019. [en línea] [Fecha de consulta: 10/10/2019] Disponible en: https://doi.org/10.5020/2317-2150.2019.9528.

comunicación, "raramente el ciudadano es capaz de percibir el sentido que la recogida de determinada información puede asumir en organizaciones complejas y dotadas de medios sofisticados para el tratamiento de datos" [traducción libre], siendo posible que no conozca o hay reflexionado sobre la peligrosidad del uso de tales informaciones por parte de diferentes responsables, lo que convierte en inerme al individuo frente a esas organizaciones[94].

4.2.5 De las nuevas características de la privacidad del siglo XXI: el interés colectivo por la protección a la privacidad

Es necesario tener en cuenta que, en realidad, las normativas en cuanto a la regulación de datos no sirven para prohibir el tratamiento de la información, ya que la libre circulación de datos personales es una realidad de la sociedad en red. No se puede olvidar que se camina hacia un contexto espacio-temporal marcado por los datos personales como bien económico, especialmente si se considera la perspectiva de *Internet of Things* e *Internet of Everything*, donde la inteligencia artificial y el proceso de *data learning* y *machine learning* imperan en una economía de la información con el flujo continuo de datos personales.

Así, por un lado, parece haber un justificación social pública que permite la recogida y el tratamiento de datos en los casos de interés general y de defensa nacional, no habiendo poder de disposición de tales informaciones por los usuarios (hasta porque ni siquiera saben que son blancos de monitoreo en estos casos); por otro lado, parece haber un determinismo social que obliga a los individuos a producir y entregar informaciones relevantes a los proveedores de productos y servicios para que participen en la sociedad en red. En otras palabras, por un lado, los datos son recolectados compulsivamente por parte de las agencias institucionales de

[94] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

seguridad, pero por otro lado los datos también se recolectan obligatoriamente como moneda de cambio para acceso a productos y servicios informacionales.

En cualquier caso, el interesado parece estar obligando a disponer de sus datos, siendo que, a partir de esos nuevos reglamentos de protección de datos, esta disposición está legítimamente fundada, ya que, por ejemplo, en el ámbito del RGPD, la licitud del tratamiento de datos se observa cuando los datos se obtienen a partir del consentimiento del usuario, o para la ejecución de un contrato, o para el cumplimiento de una obligación a la que el responsable esté sujeto, o para la defensa de los intereses vitales del interesado, o para el ejercicio de funciones de interés público o al ejercicio de la autoridad pública de la que está investido el responsable del tratamiento o, aún, a efectos de los intereses legítimos perseguidos por el responsable del tratamiento o por terceros[95].

Así pues, no se trata de limitar la circulación de información en la sociedad en red, sino de defender los derechos y las libertades fundamentales de las personas físicas, en particular, su derecho a la protección de los datos personales. En esta línea de pensamiento, se evidencia el cambio de paradigma de la privacidad, de "persona-información-sigilo" a "persona-información-circulación-control", llegando a un problema ulterior, que, en realidad, desafía el derecho a la privacidad en tiempo de ciberseguridad: el control, que, a su vez, debe dejar de ser individual y pasar a ser colectivo.

En este escenario de "persona-información-circulación-control", hay que tener en cuenta que, en el panorama anterior, la información personal estaba bajo dominio del interesado, de forma que era él quien tenía el control sobre lo que divulgar o no, pero, actualmente, estas informaciones son compartidas y quedan esparcidas en la red. Y si, antes, la violación de la privacidad era esencialmente el chisme y la revelación de secretos, ahora,

[95] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.

la violación se da por métodos desconocidos, abstractos, por la manipulación de datos informáticos, el empleo de algoritmos y otras herramientas oscuras, produciéndose un aumento del valor agregado de las informaciones personales, de modo que el valor de la persona deja de estar en ella misma y pasa a sus datos, sometiéndose a la lógica del mercado.

El control del flujo de información es tanto interno, es decir, de las informaciones que salen del individuo y van hacia el exterior, como externo, o sea, de las informaciones que llegan al individuo (derecho de no saber, no querer publicidad, no participar). Las tecnologías de la información y la comunicación, por el propio papel de aproximar a las personas y acortar distancias, ha hecho extremadamente sutil la frontera entre la esfera pública y la privada, siendo que la autodeterminación personal y la construcción libre de la esfera privada pasaron a ser condición para el desarrollo y la efectividad de la esfera pública.

Por estas razones, la función sociopolítica del derecho a la privacidad sobrepasa los límites de los intereses individuales y se convierte en un elemento importante en la construcción de la ciudadanía. En una sociedad digitalmente conectada, la definición de la privacidad sólo como el "derecho a ser dejado sólo" es insuficiente, debiendo ser extendida a una tutela global y colectiva, en un cuadro caracterizado por la libertad de las elecciones personales y existenciales. El derecho a la privacidad deja de ser sólo un derecho de una persona a limitar las intromisiones de otros individuos o del Estado en lo que es privado o un derecho de exigir del Estado que impida tales intromisiones, pasando a ser un derecho colectivo, de una multitud. Un derecho que el Estado necesita asegurar por defecto, considerando las nuevas paradojas y paradigmas de la sociedad en red[96].

[96] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, pp. 128-129.

4.2.6. Para un nuevo derecho a la privacidad: estrategias de tutela

El derecho a la privacidad, en esta lógica de "persona-información-circulación-control", presupone nuevas estrategias de tutela, de modo que el derecho a la autodeterminación informativa y el derecho a la protección de los datos personales, que se configuran como condiciones de ciudadanía, no pueden dejarse a merced de la autorregulación o de las relaciones contractuales, exigiendo del Estado una tutela positiva y proactiva; tales como garantías institucionales, que remite a "la existencia de determinadas instituciones, a las que se considera como componentes esenciales y cuya preservación se juzga indispensable para asegurar los principios constitucionales"[97].

Para ello, es necesario apuntar cinco estrategias para la protección de este nuevo derecho a la privacidad. La primera estrategia es reforzar y ampliar el derecho a la oposición contra determinadas formas de recogida, tratamiento y circulación de datos personales, posibilitando tanto iniciativas individuales, como proposiciones colectivas, en la medida que fortalece el equilibrio de poderes para permitir que los interesados se opongan al tratamiento de datos y ejerzan sus derechos[98]. El RGPD, en su art. 21, establece que "el titular de los datos tiene el derecho de oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de los datos personales que le conciernen", incluso en lo que se refiere a la recogida de datos a efectos de comercialización directa y la creación de perfiles basada en esa relación[99].

Junto al derecho de oposición, la segunda estrategia debe tener en cuenta y perfeccionar el derecho a no saber, es decir, el derecho de resistir al tratamiento y de recibir la información procedente, que pueda causar

---

[97] ESPAÑA. Tribunal Constitucional de España (Pleno). Sentencia nº 32/1981, de 28 de julio. *Boletín Oficial del Estado,* n. 193, 13 de agosto de 1981, p. 31.

[98] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 133.

[99] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.

algún trauma o incomodidad a la paz y al bien del presunto interesado[100]. Se trata, pues, de la posibilidad de rechazar marketing directo o indirecto, de no recibir publicidad no deseada o no solicitada o basada en tratamiento de datos sensibles, cancelar inscripciones en listas para recibir correos de diferentes tipos, como publicidad, noticias, *newsletters*, *spam*, incluso los anuncios políticos.

La tercera estrategia debe poner de relevancia el derecho al olvido, es decir, el derecho de supresión de los datos personales, sin demora injustificada, especialmente en los casos en que las informaciones dejen de ser necesarias para la finalidad que había motivado el tratamiento, o cuando el titular retira el consentimiento en que se basa la manipulación de las informaciones, siendo ese derecho extensible, incluso, a los buscadores e indexadores de páginas electrónicas[101]. Sin embargo, hay que considerar que el derecho al olvido es una de las categorías más polémicas del derecho a la protección de los datos personales, ya que, por otro lado, existe la argumentación sobre la prevalencia de motivos de interés público, libertad de expresión, libertad de información, persona o hecho público, cumplimiento de determinada obligación legal, entre otros casos.

La cuarta estrategia se refiere a la necesidad de hacer más claro, más urgente, más visible y más comprensible el principio de la finalidad, es decir, la condición que ratifica la recogida y el tratamiento de los datos personales por parte de los responsables y encargados, debiendo este fin ser determinado, explícito y legítimo, según, por ejemplo, establece el art. 5.1, "b", del RGPD[102]. Esto quiere decir que no debería bastar el mero enunciado de la indicación de la finalidad, sino la importación de recursos y herramientas para que el usuario tenga el completa conocimiento de las

[100] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, pp. 133-134.

[101] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 134.

[102] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.

causas, consecuencias e impactos del consentimiento que está proporcionando, teniendo en cuenta, inclusive, la crítica anteriormente mencionada sobre el consentimiento en la era del consumo de productos y servicios en red.

Por último, la quinta estrategia es, en realidad, un giro en el pensamiento. Si es verdad que el suministro de datos personales es el *login,* condición de entrada a la sociedad en red, y el consentimiento del titular está virtualmente viciado en razón de la necesidad de consumir irracionalmente las redes sociotécnicas, en detrimento del correcto entendimiento de las implicaciones derivadas de la entrega y el tratamiento de la información personal; entonces la privacidad puede y debe servir como herramienta para el equilibrio de poderes en esta nueva arquitectura social a partir de la limitación de los intereses de las agencias institucionales de seguridad y de las corporaciones económicas, de modo que, nacida como una particularidad, la privacidad puede ser entendida, cada vez más, como un instrumento colectivo de trascendencia social, siendo que los defectos y los fracasos de las leyes y reglas "[...] son resultado de asociar la privacidad con los intereses de las personas, los que al final suelen verse opacados por necesidades sociales antagónicas"[103].

4.2.7. El Efecto Orwell: el derecho a la privacidad en la sociedad de vigilancia

Con la popularización de las tecnologías de información y comunicación, parece emerger una democratización del "público", a medida que cada vez se habla más de motivos, intereses e identidades públicas; y menos de lo que es privado, reservado, íntimo, aunque el tema de la privacidad esté en el imaginario colectivo. A finales del siglo XX, se hablaba del "fin de la privacidad", pero la discusión se adentra en el nuevo siglo con la creación de escudos de privacidad, leyes de acceso a la información,

[103] NISSENBAUM, Helen. *Privacidad amenazada*: tecnología, política y la integridad de la vida social. Tradujo: Enrique Mercado. México: Editorial Océano, 2011, p. 95

leyes de regulación de Internet, de telecomunicaciones y de servicios de la sociedad de información, así como regulaciones y leyes de protección de datos personales por todo el mundo, además de decisiones y sentencias defendiendo la garantía de las diversas dimensiones del derecho a la privacidad.

Hay, sin embargo, quien defiende que la privacidad es un paréntesis de la modernidad, quedando entre las pequeñas comunidades del mundo pre-moderno que ya no existen y la comunidad global de la postmodernidad aún por venir, ambas marcadas por el control social y vigilancia de los ciudadanos[104]. En este contexto, la tutela de la privacidad queda condicionada a los intereses y avances económicos o a una autorregulación por el mercado, lo que puede comprometer aún más la verdadera protección de ese derecho, ya que las redes de poder financiero tienden a eliminar los espacios propios de la privacidad haciendo prevalecer el beneficio lucrativo y la publicidad[105].

Por otro lado, la privacidad, entendida como algo más que el "derecho de ser dejado sólo", puede ser transformada en herramienta social en el juego de poderes de la sociedad en red, cuando logra limitar y controlar directamente a los sujetos públicos y privados que recogen y tratan los datos personales. Si la información personal es el oro más importante del nuevo siglo, la exigencia de un derecho a la privacidad positivo, regulado, explícito y sancionador puede contribuir a equilibrar los intereses, de modo que, siendo un contrapeso en esa balanza, puede representar un ejercicio de democracia.

Se debe, por lo tanto, rechazar la justificación de que el ciudadano honesto no tiene nada que esconder, tampoco qué temer, a partir de la difusión de las informaciones y del tratamiento derivado de esa recogida, una vez que la metáfora del hombre de cristal es una expresión totalitaria, que subraya la pretensión del Estado de saber todo, incluso los aspectos

[104] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 144.

[105] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 144.

más íntimos de los individuos. El Efecto Orwell debe ser al revés, posibilitando a los sujetos vigilar al Gran Hermano, bajo todos los lados y esferas, en un Estado de cristal, ya que el ente estatal, caracterizado por la defensa del interés público, debe estar sometido al control de la multitud.

El derecho a la privacidad y, especialmente la regulación de ese derecho, puede ser utilizado como moneda de cambio para exigir cada vez más transparencia a la Administración Pública, no necesariamente una transparencia recibida, pues es necesario una transparencia exigida/impuesta[106]. Es el caso de la contravigilancia, ejercida sustancialmente por movimientos y actores de hackativismo, activismo mediático, *cypherpunks* y *whistleblowers*, que intentan "invertir el vector dominante de vigilancia social, para, con ello, producir nuevas narrativas sociales por medio de prácticas adyacentes de control y vigilancia del propio Estado y/o de las grandes corporaciones empresariales, especialmente por movimientos sociales" [traducción libre][107].

La contravigilancia trata de los conjuntos de actores, procesos, actuaciones y dispositivos, normalmente conectados en redes, para proteger "contra la vigilancia perpetrada por los órganos institucionales y por las corporaciones empresariales y, más aún, vigilar a quién también vigila al cuerpo social, en el intento de hacer cesar la violación de derechos y garantías fundamentales y humanas" [traducción libre][108]. La contravigilancia en sentido estricto trata de la específica tentativa de neutralizar la vigilancia realizada por el Estado y por las grandes corporaciones, a partir de técnicas de bloqueo de una vigilancia dominante

[106] CASTELLS, Manuel. *A galáxia internet:* reflexões sobre internet, negócios e sociedade. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007, p. 220.

[107] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192p. Tutor: Rafael Santos de Oliveira. [Trabajo Final de Máster]. Máster en Derecho. Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, 2018, p. 102.

[108] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192p. Tutor: Rafael Santos de Oliveira. [Trabajo Final de Máster]. Máster en Derecho. Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, 2018, p. 102.

o desestabilización del vigilante, revelando y divulgando su actuación, haciendo públicos documentos e informaciones de interés público, informando sobre violaciones de derechos y garantías, entre otras prácticas[109].

Es decir, si no hay otra alternativa para los individuos en el siglo XXI que no sea el control de la circulación de las informaciones, una vez que la economía de vigilancia y el suministro de datos personales es la realidad determinista que se aproxima, es posible utilizar las propias tecnologías de información y comunicación para vigilar al Estado y a las grandes corporaciones, promoviendo un control público para que cada vez sean más públicas, transparentes y cristalinas[110]. Se trata de vigilar a quien vigila, para que estén incómodos lo suficiente, para seguir las reglas; se trata de aumentar la transparencia pública de quien viola la privacidad para que estén preparados para respetar las nuevas dimensiones del derecho a la privacidad en la sociedad en red.

[109] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192p. Tutor: Rafael Santos de Oliveira. [Trabajo Final de Máster]. Máster en Derecho. Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, 2018, p. 103.

[110] ROSANVALLON, Pierre. *La contrademocracia*: la política en la era de la desconfianza. Buenos Aires: Manantial, 2007.

Conclusión

Con el presente estudio, se ha podido reflexionar sobre los impactos de las tecnologías de la información y comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de la ciberseguridad del siglo XXI. Objetivamente, se han analizado a) las implicaciones del régimen de monitoreo social global y los impactos en la sociedad del siglo XXI; b) la contribución de las personas en dicho régimen a partir del suministro de datos para el acceso a productos y servicios; c) la estructura normativa global y regional del derecho a la privacidad, el cambio y los enfoques del concepto a lo largo del tiempo; y d) la resignificación del derecho a la privacidad en el contexto de la ciberseguridad.

En la sociedad en red del siglo XXI, hay el recrudecimiento de un régimen global de vigilancia social, basado en la cooperación entre agencias estatales para monitoreo del flujo de datos en la sociedad y control de personas y grupos de interés, por medio de la manipulación de las informaciones personales. La vigilancia social, desde hace siglos, funciona como un dispositivo para el ejercicio de poder, de forma que tal dominación se ha visto acrecentada con el desarrollo de las tecnologías de información y comunicación y con el advenimiento de la grandeza informática del *big data*.

Ese régimen global de vigilancia social está fundamentado en discursos oficiales legitimadores, transpuestos a normativas nacionales e internacionales, justificando el monitoreo de ciudadanos nacionales y extranjeros en favor del combate a enemigos abstractos, como el terror, para garantizar la seguridad y defensa nacional, entre otros argumentos, sin el debido conocimiento público y publicidad necesaria, tanto que los programas de monitoreo fueron divulgados bajo polémica y vergüenza

internacionales. Entonces, perceptible el advenimiento de un Estado de vigilancia, haciéndose presente en la vida de las personas de forma invisible, no jerárquica, descentralizada y personalizada en una nueva arquitectura social de sociedad en red.

En el marco de esta nueva arquitectura social, los usuarios contribuyen con el funcionamiento de ese sistema, marcado por la manipulación de algoritmos y la creación de patrones de comportamiento, a partir del suministro de datos personales. En esta sociedad en red de flujos comunicacionales mundiales, hay una lógica consumista de tecnologías de información y comunicación y un proceso de subjetivación continuo y modulado, ya que la construcción de una identidad pública depende de la entrega de las informaciones personales.

Si antes la vigilancia dependía de dispositivos institucionales, ahora está distribuida en los dispositivos personales, en una reinvención del panóptico de poder por el hombre caracol, es decir, el que lleva en sí mismo una vigilancia, que, por otro lado, también permite la vigilancia del otro, en una retroalimentación de datos. En el panorama del *Internet de las Cosas* y del *Internet de Todo*, se trata de una economía de vigilancia, a partir del suministro de datos personales para acceso a productos y servicios, como si fuese un nuevo oro del siglo XXI, que, al fin y al cabo, se ha convertido en condición para participar en este nuevo paradigma social tecnológico.

El derecho a la privacidad, incluso a partir de figuras afines, como "vida privada y familiar" e "intimidad", se establece en las principales normativas internacionales, comunitarias, regionales y nacionales, incluso españolas y brasileñas. El reto es que la privacidad como la conocemos, a partir de una perspectiva histórica, filosófica y jurídica, como substancialmente el "derecho de ser dejado solo" y de no sufrir interferencias ajenas y estatales en lo que es privado, se ha revolucionado en ese nuevo paradigma social derivado de los avances de las tecnologías de la información y comunicación.

De ahí, surgieron nuevos riesgos y amenazas, que hacen posibles otras formas de violación de la privacidad, teniendo en cuenta los diferentes procesos de manipulación y tratamiento de datos personales, de característica automatizada y continua. De ese modo, el concepto tradicional se ha vuelto insuficiente para tratar este nuevo marco tecnológico, en especial con referencia a nuevos matices que han surgido, como el derecho a la autodeterminación informativa y el derecho a la protección de datos personales, de manera que la privacidad se extiende también al control sobre la circulación de la propia información personal.

Existe una preocupación estatal-normativa para tutelar el derecho a la privacidad (aunque muy basada en la lógica de "persona-información-sigilo"), tanto que esa protección aparece, aunque como otras figuras, en diferentes normativas internacionales, comunitarias, regionales y nacionales. Sin embargo, debe haber un esfuerzo por ampliar ese derecho frente a las nuevas tecnologías de información y comunicación, como ocurrió con el establecimiento del derecho a la autodeterminación informativa y el derecho a la protección de datos personales como derechos fundamentales, lo que se puede percibir con el advenimiento de nuevas normativas, como es el caso del Reglamento General de Protección de Datos Personales de la Unión Europea y la Ley General de Protección de Datos Personales de Brasil, entre otras leyes de tutela de informaciones personales.

Ante el recrudecimiento del régimen global de vigilancia social, con dispositivos de vigilancia distribuidos por el globo, personales y personalizados, así como ante la necesidad de proporcionar datos personales para acceso y consumo de productos y servicios de la sociedad en red, en una lógica de subjetivación, el concepto de privacidad como el "derecho a ser dejado en paz" o el "derecho a ser dejado solo" es insuficiente para tutelar esa nueva realidad social, aunque esa propia característica de reservado no ha dejado de existir en si, sino que hay nuevas dimensiones que necesitan una mayor reflexión.

En efecto, la privacidad, en la concepción tradicional, ha sufrido diferentes tipos de violaciones de protección. Ahora bien, el panorama anterior

de "persona-información-sigilo", en el que el sujeto podía protegerse de intromisiones no deseadas en lo que le es reservado, acaba por ser insuficiente, considerando ese régimen global de vigilancia social y ese suministro de datos como ingreso de la sociedad en red.

Esto, porque, por un lado, aunque el individuo quiera mantener el secreto sobre ciertas informaciones y definir lo que es su privacidad, las agencias de seguridad nacional y las agencias estatales, en asociación con empresas de tecnologías, interceptan, monitorean, clasifican e intercambian datos personales recogidos. Por otro lado, el determinismo social que exige el suministro de datos personales para acceso de productos y servicios tecnológicos también rompe con la lógica del sigilo, aún más cuando el sujeto no tiene plena conciencia y consentimiento sobre la entrega de la información personal.

En una realidad en que todo y todos están interconectados, aunque no necesariamente digitalmente, en una sociedad en red, hay que reconocer que el paradigma de la arquitectura social está cambiando, exigiéndose una adaptación frente a las complejidades de ser. Es decir, si el derecho y la normatividad necesitan acompañar la evolución social, buscando ajustarse a los cambios y novedades, es imprescindible desapegar de dogmas jurídicos y actualizar las condiciones de regulación. Es el fin del derecho a la privacidad, pero no en el tono aterrorizado de finales del siglo XX, sino como se lo conoce y cómo fue transpuesto en normativas alrededor del globo.

En conclusión, es necesario repensar el derecho a la privacidad, considerando el régimen global de vigilancia social y la alteración del paradigma permitido con las tecnologías de la información y comunicación. Es decir, es preciso aceptar que ha llegado al fin un largo proceso evolutivo de conceptualización del derecho a la privacidad como un derecho de ser dejado en paz, pasando a tratarse de un derecho de control sobre las informaciones personales. Dicho nuevo derecho debe llevar en consideración las diferentes paradojas que la privacidad abraza en el siglo XXI; especialmente, en lo que se refiere a la fluidez de los espacios público-

privado, al advenimiento de una nueva dimensión de extimidad y a la supuesta falacia del consentimiento informado.

El derecho a la privacidad ha cambiado a una lógica "persona-información-circulación-control", apuntándose, para tutela de ese nuevo derecho, cinco estrategias, como la ampliación del derecho a la oposición contra el tratamiento de datos personales, la ampliación del derecho de no saber y resistir al recibimiento y al tratamiento de la información, el establecimiento del derecho al olvido, especialmente digital, la mejora del principio de la finalidad y, finalmente, el giro de pensamiento sobre lo que puede significar la privacidad en tiempos de ciberseguridad. Así, se puede concluir que la privacidad del siglo XXI puede ser entendida como un derecho colectivo para exigir cada vez más transparencia de aquellos que tratan los datos; para que se sienten incómodos hasta el punto de respetar las reglas y proteger la privacidad de los ciudadanos en una revisión de la obra orwelliana.

El siglo XX ha revolucionado los procesos comunicativos y el flujo de ideas en la sociedad hiperconectada, pero el siglo XXI comienza proyectando un mayor intercambio de informaciones, en una economía de datos personales, siendo cada vez más inminente la libre circulación de personas, productos, servicios y datos en comunidades digitales del mundo, incluso en un *Internet de Todo*. Se trata de una fuerza imparable, en la que el derecho a la privacidad, sólo entendido en la concepción individual de "persona-información-sigilo" no puede ser un objeto inamovible, bajo peligro de una catástrofe normativa y una falacia reguladora.

En el régimen global de vigilancia social, aquí entendido como el panorama de monitoreo de información personal y de suministro de datos personales para acceso de productos y servicios en la sociedad en red, el derecho a la privacidad puede suponer un régimen global de contravigilancia social. Por lo tanto, se puede invertir el vector determinante de vigilancia, para vigilar a quien vigila, tornándose los que, hasta entonces, eran objetos de vigilancia en sujetos de vigilancia, de modo

que ese régimen, inevitable por sí solo ante los avances de las tecnologías de la información y comunicación, siga las reglas del juego democrático.

En una visión holística del mundo, bajo la lógica "persona-información-circulación-control", se debe comprender el derecho a la privacidad, además de todas las dimensiones antes discutidas y antes previstas, también como un derecho de interés social colectivo, perteneciente a una colectividad, a una transindividualidad. Esto es, además de ser un derecho individual, en que el sujeto puede requerir la tutela para sí, el derecho a la privacidad también puede ser visto como una garantía institucional, un derecho de todos de exigir una protección especial y difusa, dirigida al cuerpo social, al cuerpo multitud.

Referências [1]

ARENDT, Hannah. *A condição humana.* 10 ed. Rio de Janeiro: Forense Universitária, 2005.

ARENDT, Hannah. *La condición humana*. Barcelona: Paidos Iberica, 2016.

ARENDT, Hannah. Reflections on Little-Rock. In: *Dissent Magazine*, v. 6, n. 1, inv., 1959.

ASSANGE, Julian. *Cypherpunks*: liberdade e futuro da internet. São Paulo: Boitempo, 2013.

Julian. *Cypherpunks*: la libertad y el futuro de internet. Barcelona: Deusto S.A., 2013.

AYUSO, Silvia; PEREDA, Cristina. *Obama conmuta la pena de la soldado Chelsea Manning*. [El País, 18 jan. 2017] Disponível em: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html. Acesso em: 10 abr. 2019.

BAJARIN, Tim. *The next big thinh of tech:* the Internet of Everything. [Time, 13/01/2014] Disponível em: http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/. Acesso em: 21 abr. 2019.

BAUMAN, Zygmunt. *Vida para consumo.* A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008.

BAUMAN, Zygmunt. *Vida de consumo.* Madrid: S.L. Fondo de Cultura Económica de España, 2007.

BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013.

BAUMAN, Zygmunt. *Vigilancia líquida*. Barcelona: Planeta, 2015.

[1] A presente seção está escrita levando em consideração a norma NBR 6023, da Associação Brasileira de Normas Técnicas – ABNT, sendo adicionadas, para conferência do leitor, quando houver, uma versão espanhola das obras consultadas.

BENTHAM, Jeremy. O panóptico ou a casa de inspeção. In: TADEU, Tomaz (Org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008, pp. 17-30.

BIGO, Didier; TSOUKALA, Anastassia. *Terror, insecurity and liberty:* illiberal practices of liberal regimes after 9/11. New York: Routledge, 2008.

BLASCO, Lucía. *Cuán cierto es que las empresas usan el micrófono de tu teléfono para escucharte y qué hacer al respecto*. [BBC News, 05/07/2018] Disponível em: https://www.bbc.com/mundo/noticias-44724389. Acesso em: 22 abr. 2019.

BOLESINA, Iuri. *O direito à extimidade*: as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017.

BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal et al. *Internet of Everything:* A $4.6 trillion public-sector opportunity. San Jose: Cisco. 2013. Disponível em: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf. Acesso em: 21 abr. 2019.

BRANDEIS, Louis. WARREN, Samuel. The right to privacy. In: *Harvard Law Review*, v. IV, n. 5, dez. 1890. Disponível em: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm. Acesso em; 16 abr. 2019.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 4.060, de 13 de junho de 2012. *Dispõe sobre o tratamento de dados pessoais e dá outras providências*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 08 out. 2020.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 5.276, de 13 de maio de 2016. *Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 08 out. 2020.

BRASIL. Congresso Nacional. Medida Provisória nº 959, de 2020 (regras para o auxílio emergencial e adiamento da vigência da LGPD). *Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD*. Disponível em:

https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753. Acesso em: 08 out. 2020.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 17 abr. 2019.

BRASIL. Decreto Legislativo nº 6, de 2020. *Reconhece, para os fins do art. 65 da Lei Complementar nº 101, de 4 de maio de 2000, a ocorrência do estado de calamidade pública, nos termos da solicitação do Presidente da República encaminhada por meio da Mensagem nº 93, de 18 de março de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/portaria/DLG6-2020.htm. Acesso em: 08 out. 2020.

BRASIL. Decreto nº 10.474, de 26 de agosto de 2020. *Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm. Acesso em: 08 out. 2020.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. *Dispõe sobre a proteção do consumidor e dá outras providências*. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 17 abr. 2019.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. *Institui o Código Civil*. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 17 abr. 2019.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 out. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 out. 2020.

BRASIL. Lei nº 13.853, de 08 de julho de 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*. Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 08 out. 2020.

BRASIL. Lei nº 14.010, de 10 de junho de 2020. *Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 08 out. 2020.

BRASIL. Lei nº 14.058, de 17 de setembro de 2020. *Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Lei nº 14.020, de 6 de julho de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14058.htm. Acesso em: 08 out. 2020.

CADWALLADR, Carole; CONFESSORE, Nicholas; ROSENBERG, Matthew. *How Trump Consultants Exploited the Facebook Data of Millions*. [The New York Times, 17/03/2018]. Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Acesso em: 21 abr. 2019.

CAPRA, Fritjof. *A Teia da Vida:* uma nova compreensão científica dos sistemas vivos. São Paulo: Cultrix, 1996.

CAPRA, Fritjof. *La trama de la vida:* una nueva perspectiva de los sistemas vivos. 3. ed. Barcelona: Anagrama, 2009.

CAPRA, Fritjof. *As conexões ocultas*. São Paulo: Cultrix, 2002.

CAPRA, Fritjof. *Las conexiones ocultas*: implicaciones sociales, medioambientales, económicas y biológicas de una nueva visión del mundo. Barcelona: Anagrama, 2006.

CASTELLS, Manuel. *A Era da Informação:* economia, sociedade e cultura, vol. 3. 3. ed. São Paulo: Paz e Terra. 2002.

CASTELLS, Manuel. *La Era de la Información:* economía, sociedad y cultura. La sociedad en red, vol. 3. Madrid: Alianza Editorial, 2002.

CASTELLS, Manuel. *A galáxia internet:* reflexões sobre internet, negócios e sociedade. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007.

CASTELLS, Manuel. *La galaxia internet:* reflexiones sobre internet, empresa y sociedad. Madrid: Debolsillo, 2003.

CASTELLS, Manuel. *O poder da comunicação.* São Paulo: Paz e Terra, 2013.

CASTELLS, Manuel. *Comunicación y Poder*. Madrid: Alianza Editorial, 2009.

CASTELLS, Manuel. *O poder da identidade*. 2. ed. São Paulo: Paz e Terra, 2000.

CASTELLS, Manuel. *La Era de la Información:* economía, sociedad y cultura. El poder de la identidad, vol. 2. Madrid: Alianza Editorial, 2003.

COLOMÉ, Jordi Pérez. *Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas*. [El País, 20/12/2018] Disponível em: https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html. Acesso em: 21 abr. 2019.

COMISSÃO ASIÁTICA DOS DIREITOS HUMANOS. *Carta Asiática dos Direitos Humanos de 1998*. Disponível em: http://www.humanrights.asia/wp-content/uploads/2018/07/Asian-Human-Rights-Charter-2nd-Edition-English.pdf. Acesso em: 17 abr. 2019.

CONESA, Fulgencio Madrid. *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia, 1984.

CONSELHO DA EUROPA. *Convênio Europeu de Direitos Humanos de 1950*, p. 11. Disponível em: https://www.echr.coe.int/Documents/Convention_SPA.pdf. Acesso em: 17 abr. 2019.

COSTA JR. Paulo José da. *O direito de estar só:* tutela penal da intimidade. 2. ed. São Paulo: RT, 1995.

DAUER, Stella. *Entenda tudo sobre as permissões de aplicativos e proteja seu Android*. Disponível em: https://www.androidpit.com.br/permissoes-aplicativos. Acesso em: 22 abr. 2019.

DELEUZE, Gilles. *Conversações*: 1972-1990. São Paulo: 34, 1992.

DELEUZE, Gilles. *Conversaciones*. Valencia: Pre-textos, 1995.

DERIX, Steven. MODDERKOLK, Huib. *50.000 pakketjes kwaardaardige software*. [NRC, 23/11/2013] Disponível em: https://www.nrc.nl/nieuws/2013/11/23/50000-pakketjes-kwaardaardige-software-1316266-a1157982. Acesso em: 24 abr. 2019.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: *Espaço Jurídico*, Joaçaba, v. 12, n. 2, pp. 91-10, jul./dez. 2011, p. 102. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 out. 2020.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. In: *Âmbito Jurídico*, Rio Grande, XI, n. 51, mar. 2008. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460. Acesso em: 16 abr. 2019.

ESPANHA. *Constitución Española de 1978*. Disponível em: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf. Acesso em: 17 abr. 2019.

ESPANHA. *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196. Acesso em: 17 abr. 2019.

ESPANHA. Ministério de Defesa. *Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas*. Disponível em: http://www.emad.mde.es/Galerias/MOPS/novoperaciones/multimedia/documentos/20130226_CIBERDEFENSA.pdf. Acesso em: 18 abr. 2019.

ESPANHA. Tribunal Constitucional da Espanha. *Sentencia nº 292/2000, de 30 de Noviembre en el Recurso de Inconstitucionalidad n.º 1463-2000*. Interposição: Defensor del Pueblo. Ponente: Magistrado Don Julio Diego González. Boletín Oficial del Estado. Madrid. Disponível em: http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292#complete_resolucion. Acesso em: 17 abr. 2019.

ESPANHA. Tribunal Constitucional de Espanha (Pleno). Sentença nº 32/1981, de 28 de julho. *Boletín Oficial del Estado*, n. 193, 13 de agosto de 1981.

FERNÁNDEZ, Déborah. *Las cinco V's del Big Data.* [DataHack, 27/08/2018] Disponível em: https://www.datahack.es/cinco-v-big-data/. Acesso em: 20 abr. 2019.

FOLLOUROU, Jacques. *Surveillance*: la DGSE a transmis des données à la NSA américaine. [Le Monde, 30/10/2013] Disponível em: https://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html. Acesso em: 20 abr. 2019.

FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005.

FOUCAULT, Michel. *Hay que defender la sociedad:* curso del Collège de France (1976). Madrid: Akal, 2003.

FOUCAULT, Michel. *Microfísica do poder*. 23 ed. São Paulo: Graal, 2004.

FOUCAULT, Michel. *Microfísica del poder:* genealogía del poder. Madrid: La Piqueta, 1978

FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013.

FOUCAULT, Michel. *Vigilar y castigar:* nacimiento de la prisión. Ciudad del México: Siglo XXI, 2012.

FRANÇA. *Déclaration des Droits de l'Homme et du Citoyen de 1789*. Disponível em: https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789. Acesso em: 17 abr. 2019.

GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

GREENWALD, Gleen. *Sin un lugar donde esconderse*: Edward Snowden, la NSA y el Estado de Vigilancia en los Estados Unidos. Barcelona: Ediciones B, 2014.

GREENWALD, Glenn. XKeyscore: *NSA tool collects 'nearly everything a user does on the internet'*. [The Guardian, 31/07/2013] Disponível em: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Acesso em: 20 de abr. 2019

HARDT, Michael; NEGRI, Antonio. *Império*. São Paulo: Record, 2012.

HARDT, Michael; NEGRI, Antonio. *Imperio*. Barcelona: Paidos Iberica, 2005.

HRON, Martin. *Os últimos 10 maiores vazamentos de dados.* [Avast, 14/02/2019] Disponível em: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados. Acesso em: 21 abr. 2019.

LACAN, Jacques. *O seminário:* livro 16: de um Outro ao outro. Rio de Janeiro: Jorge Zahar, 2008.

LACAN, Jacques. *El seminario:* libro 16: de un Outro al otro. Barcelona: Paidos Iberica, 2008.

LIGA ÁRABE. *Carta Árabe sobre Direitos Humanos de 2004*. Disponível em: http://www.lasportal.org/ar/sectors/dep/HumanRightsDep/Documents/%D8%A7%D9%86%D8%AC%D9%84%D9%8A%D8%B2%D9%8A.pdf. Acesso em: 17 abr. 2019.

LIMBERGER, Têmis. *Cibertransparência informação pública em rede*: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016.

MARS, Amanda. *Zuckerberg pide perdón en el Senado y advierte de la amenaza de Rusia*. [El País, 11/04/2018]. Disponível em: https://elpais.com/internacional/2018/04/10/actualidad/1523380980_341139.html. Acesso em: 21 abr. 2019.

MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão*: decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, p. 55-63. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877. Acesso em: 17 abr. 2019.

MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). *Technology and privacy*: The new landscape. Cambridge: MIT Press, 1997, pp. 219-242.

McCARTHY, Tom. *NSA director defends plan to maintain 'backdoors' into technology companies*. [The Guardian, 23/02/2015] Disponível em: https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies. Acesso em: 06 jan. 2018.

MILL, John Stuart. *A liberdade*. São Paulo: Martins Fontes, 2000.

MILL, John Stuart. *Sobre la libertad*. Madrid: Verbum, 2016.

MUGUERZA, Javier. De la conciencia al discurso ¿un viaje de ida y vuelta? In: *La filosofía moral y política de Jürgen Habermas*. Madrid: Biblioteca Nueva, 1997, pp. 63-110.

NISSENBAUM, Helen. *Privacidad amenazada*: tecnología, política y la integridad de la vida social. México: Editorial Océano, 2011.

NORTON-TAYLOR, Richard. *Not so secret: deal at the heart of UK-US intelligence*. [The Guardian, 25/06/2010]. Disponível em: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released. Acesso em: 16 abr. 2019.

ORGANIZAÇÃO DA CONFERÊNCIA ISLÂMICA. *Declaração dos Direitos Humanos no Islã de 1990*. Disponível em: https://www.oic-iphrc.org/en/data/docs/legal_instruments/OIC_HRRIT/571230.pdf. Acesso em: 17 abr. 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal de Direitos Humanos de 1948*. Disponível em: https://www.un.org/es/universal-declaration-human-rights/. Acesso em: 17 abr. 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica) de 1969*. Disponível em: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm. Acesso em: 17 abr. 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Declaração Americana dos Direitos e Deveres do Homem de 1948*. Disponível em: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp. Acesso em: 17 abr. 2019.

PÉREZ LUÑO, Antonio Enrique. *Los derechos en la sociedad tecnológica*. Madrid: Editorial Universitas, S.A., 2012.

PESSOA, João Pedro Seefeldt. "*Verás que um filho teu não foge à luta*": a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. 2018. 192 f. Dissertação (Mestrado) - Curso de Direito, Departamento do Direito, Universidade Federal de Santa Maria, Santa Maria, 2018.

PESSOA, João Pedro Seefeldt. OLIVEIRA, Rafael Santos de. "Big Brother Watch and Others v. The United Kingdom": el régimen de vigilancia social y el derecho al respecto a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos. In: *Pensar*: Revista de Ciências Jurídicas, Fortaleza, v. 24, n. 3, pp. 1-12, jul./set. 2019. Disponível em: https://doi.org/10.5020/2317-2150.2019.9528. Acesso em: 10 out. 2019.

PHAM, Sherisse. *WikiLeaks dice que la CIA espía a través celulares y televisores, ¿qué tan preocupado debes estar?* [CNN, 08/03/2017] Disponível em: https://cnnespanol.cnn.com/2017/03/08/wikileaks-dice-que-la-cia-espia-a-traves-de-smartphones-televisores-y-mas-que-tan-preocupado-debes-estar/. Acesso em: 22 abr. 2019.

PIRES, Hindenburgo Francisco. Geografia das indústrias globais de vigilância em massa: limites à liberdade de expressão e organização na internet. In: *Ar@cne Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales,* Universidad de Barcelona, n.º 183, abr. 2014. Disponível em: http://www.ub.edu/geocrit/aracne/aracne-183.htm#_edn16. Acesso em: 20 abr. 2019.

REAL ACADEMIA ESPAÑOLA. *Diccionario del español jurídico*. Big data. Disponível em: https://dej.rae.es/lema/big-data. Acesso em: 20 abr. 2019.

REINO UNIDO. *The economic value of data*: discussion paper. Londres: HM Treasury, 2018. p. 04-07. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf. Acesso em: 20 abr. 2019.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRÍGUEZ-PINA, Gloria. *El método nada tecnológico que usa Mark Zuckerberg para protegerse de los hackers*. [El País, 22/06/2016] Disponível em: https://verne.elpais.com/verne/2016/06/22/articulo/1466617774_991020.html. Acesso em: 22 abr. 2019.

ROSANVALLON, Pierre. *La contrademocracia*: la política en la era de la desconfianza. Buenos Aires: Manantial, 2007.

SECRETARIA-GERAL ÍBERO-AMERICANA. XIII Cimeira Ibero-Americana de Chefes de Estado e de Governo. *Declaração de Santa Cruz de La Sierra de 14 e 15 de novembro de 2003*. Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em: 18 abr. 2019.

TARODO, Salvador Soria. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. In: *Derecho y Salud*, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006.

TAURION, Cezar. *Volume, variedade, velocidade, veracidade e valor:* os cinco Vs do Big Data. Disponível em: http://computerworld.com.br/volume-variedade-velocidade-veracidade-e-valor-os-cinco-vs-do-big-data. Acesso em: 16 abr. 2019.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia de 2000*. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 17 abr. 2019.

UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)*. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas (Diretiva relativa à privacidade e às comunicações eletrônicas)*. Disponível em: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32002L0058. Acesso em: 18 abr. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046&from=PT&fromTab=ALL&lang3=choose&lang2=choose&lang1=ES. Acesso em: 18 abr. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. *Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações*. Disponível em: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A31997L0066. Acesso em: 18 abr. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 18 abr. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. *Relatório de 11 de julho de 2001 sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON")*. Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//PT. Acesso em: 16 abr. 2019.

UNIDADE AFRICANA. *Carta Africana sobre Direitos Humanos e dos Povos de 1981*. Disponível em: https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf. Acesso em: 17 abr. 2019.

WIKILEAKS. *What is WikiLeaks*. Disponível em: https://wikileaks.org/What-is-Wikileaks.html. Acesso em: 16 abr. 2019.

Sobre o autor

João Pedro Seefeldt Pessoa
Mestre em Direito (Derecho de la Ciberseguridad y Entorno Digital) pela Universidad de León, Espanha (ULE), pelo qual bolsista da Fundación Carolina.
Mestre em Direito (Direitos Emergentes na Sociedade Global) pela Universidade Federal de Santa Maria (UFSM), pelo qual bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES.
Bacharel em Direito pela Faculdade de Direito de Santa Maria (FADISMA).
Pesquisador do Centro de Estudos e Pesquisas em Direito e Internet (CEPEDI), grupo de pesquisa certificado pelo CNPq, com atuação na linha de pesquisa "Riscos e (des)controles do ciberespaço". Integrante do projeto de pesquisa "Ativismo digital e cibercidadania: desafios, oportunidades e riscos do ciberespaço", da Universidade Federal de Santa Maria (UFSM). Integrante do projeto de desenvolvimento institucional "Observatório de Proteção de Dados Pessoais na Internet", da Universidade Federal de Santa Maria (UFSM).
E-mail: jpseefeldt@gmail.com.
Currículo: http://lattes.cnpq.br/3238221565472756.
Orcid: https://orcid.org/0000-0003-1974-0247.

A Editora Fi é especializada na editoração, publicação e divulgação de pesquisa acadêmica/científica das humanidades, sob acesso aberto, produzida em parceria das mais diversas instituições de ensino superior no Brasil. Conheça nosso catálogo e siga as páginas oficiais nas principais redes sociais para acompanhar novos lançamentos e eventos.

www.editorafi.org
contato@editorafi.org