UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO DE SÃO PAULO

GUSTAVO MASCARENHAS LACERDA PEDRINA

# A VIOLAÇÃO DA PRIVACIDADE E DA INTIMIDADE POR ATORES PRIVADOS NA INTERNET

Dissertação de Mestrado

Orientador: Professor Associado Víctor Gabriel de Oliveira Rodríguez

São Paulo - SP
**2017**

GUSTAVO MASCARENHAS LACERDA PEDRINA

# A VIOLAÇÃO DA PRIVACIDADE E DA INTIMIDADE POR ATORES PRIVADOS NA INTERNET

Dissertação de Mestrado apresentada à Banca examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, na área de concentração de Direito Penal, sob orientação do Prof. Associado Víctor Gabriel de Oliveira Rodríguez

São Paulo - SP

**2017**

L131v
Lacerda Pedrina, Gustavo Mascarenhas A VIOLAÇÃO DA PRIVACIDADE E DA INTIMIDADE POR ATORES PRIVADOS NA INTERNET / Gustavo Mascarenhas Lacerda Pedrina; orientador Víctor Gabríel de Oliveira Rodríguez.
São Paulo, 2017.
148 p.
Dissertação (Mestrado - Programa de Pós-Graduação em Direito) -Faculdade de Direito de, Universidade de São Paulo, 2017.
1. DIREITO PENAL. 2. DIREITO DIGITAL. 3.PRIVACIDADE. 4. INTIMIMDADE. 5. INTERNET.

**FOLHA DE APROVAÇÃO**

Nome: Gustavo Mascarenhas Lacerda Pedrina

Título: A Violação da Privacidade e da Intimidade por Atores Privados na Internet

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo para obtenção do título de Mestre em Direito Penal.

**Banca Examinadora**

| | |
|---|---|
| Prof(a). Dr(a).: | Instituição: |
| Julgamento: | Assinatura: |
| Prof(a). Dr(a).: | Instituição: |
| Julgamento: | Assinatura: |
| Prof(a). Dr(a).: | Instituição: |
| Julgamento: | Assinatura: |
| Prof(a). Dr(a).: | Instituição: |
| Julgamento: | Assinatura: |

Para Bruna, pelo amor e companheirismo,
Para minha avó, Maria do Carmo, meu exemplo,
Para Monica e Sidnei, Gui e Clarinha: todas as vitórias são nossas.

## AGRADECIMENTOS

Ninguém realiza nada sem o apoio dos ombros e abraços dos que lhe querem bem. Eu tenho muitos a agradecer, seria impossível nomeá-los lodos. Em primeiro lugar, sou grato ao meu orientador e amigo, Professor Víctor Gabriel Rodríguez. Se este espaço me permite, aprendi muito mais que Direito Penal com o Professor Víctor, tanto nos bancos da Faculdade quanto nos bancos dos cafés, durante as nossas conversas, e nas leituras das suas colunas. Aprendi, acima de tudo, a ouvir e respeitar. Fui sempre incentivado por ele a escrever e opinar, sempre de maneira espontânea, mas diante do estudo. Aprendi com ele que os verdadeiros sábios nunca utilizam de pretensa erudição: as lições são simples e estão em cada conversa.

Agradeço também ao Professor e amigo Eduardo Saad-Diniz pelos ensinamentos ricos, recomendações valiosas e constante incentivo, desde a graduação. Agradeço ainda aos Professores Renato de Mello Jorge Silveira e Helena Regina Lobo da Costa pelas imprescindíveis e precisas contribuições por ocasião da banca de qualificação deste trabalho.

Agradeço a Bruna Ceotto Gomes pelo amor, pelo cuidado, pelo incentivo e companheirismo de todas as horas: eu não conseguiria nada sem você.

Agradeço a minha avó, Maria do Carmo Mascarenhas, por ser a definição de amor e apoio incondicionais. Aos meus pais, Sidnei e Mônica, se tive a oportunidade rara de me graduar bacharel e agora, possivelmente, mestre na Universidade de São Paulo, sei que foi em virtude do seu apoio, trabalho árduo e verdadeiro exemplo abnegação. Ao Gui e a Clarinha, que são os melhores irmãos e amigos que alguém poderia desejar: obrigado por cada momento.

Ao Gustavo de Carvalho Marin, amigo e companheiro desde o primeiro dia de Faculdade e para todos os próximos. Ao Caio Chaves Morau, pelos debates incansáveis que teremos até o fim da vida. Ao André Gardinal, Alexandre Hideto, Jesus Pacheco Simões, Isabela Bolloti, Thais Fiorucci, Caio Henrique Lima, Francisco Agosti, Luciana Padilla Guardia, João Pimenta Camargo e Davi Villar, por todo o apoio e incentivo durante esses quase três anos. Ao Fernando Amorim e à Mariana Piccinini pelas leituras e necessárias correções.

Agradeço, por fim, ao IBCCrim, nas pessoas de Luciana Zaffalon, Carolina Diniz e Cristiano Maronna, por me deixarem desenvolver ideias e por me apoiarem em cada uma delas, proporcionando espaço e abertura sem igual em instituições com a grandeza deste Instituto. O IBCCrim é uma entidade plural e aberta, da qual tenho orgulho genuíno em participar.

Devo muito a todos vocês. Muito Obrigado, de verdade!

*Dos Conselhos que deu D. Quixote de La Mancha a Sancho Pança*

> "Nunca interpretes arbitrariamente a lei, como costumam fazer os ignorantes que têm presunção de agudos. Achem em ti mais compaixão as lágrimas do pobre, mas não mais justiça do que as queixas dos ricos. Quando se puder atender à equidade, não carregues com todo o rigor da lei no delinquente, que não é melhor a fama do juiz rigoroso que do compassivo. Se dobrares a vara da justiça, que não seja menos com o peso das dádivas, mas sim com o da misericórdia. Quando te suceder julgar algum pleito de inimigo teu, esquece-te da injúria e lembra-te da verdade do caso."

CERVANTES, Miguel, *Dom Quixote de La Mancha*

> "Pois quando assisto a sustentações orais de advogados e os vejo tentando fazer correr lágrimas após um discurso sobre sinistro de seguro e cláusula de adesão, ou, ainda, quando um voto de um juiz tenta proferir lição de moral em vez de solver um problema do jurisdicionado, de modo direto e objetivo, logo imagino o Gorpo voando por detrás do discursante, sorridente por ter arranjado um substituto, alguém que veio pagar o mico em seu lugar"

RODRÍGUEZ, Víctor Gabriel. *O emocionante discurso do Gorpo*

**RESUMO**

Apresenta-se este estudo como uma exame pormenorizado concernente aos novos limites da intimidade e a privacidade no ambiente da *internet*. Frente aos novos desafios, oriundos da alteração ocorrida na rede no decorrer última década, a fim de inserir condutas inéditas no âmbito, é mister a observação de possíveis violações ao direito fundamental à intimidade. Vale ressaltar a intimidade como sendo essencial à formação da personalidade do indivíduo, merecedora, assim, de tutela penal sempre que ver-se ameaçada.

Na última década, sofisticaram-se os desafios à intimidade dos indivíduos. Com o surgimento das *fake news*, das *blockchains*, das novas formas de inteligência artificial, da *internet* das coisas, do armazenamento em nuvem, das redes sociais, enfim, de maneira geral, da coleção e do processamento de dados pessoais inseridos e disponibilizados em dispositivos informáticos.

Em face do exposto, a breve análise das legislações dos Estados Unidos e da União Europeia, bem como dos marcos legais existentes no Brasil, propõe o panorama atual de possíveis proteções e, simultaneamente, de inegáveis omissões. Apesar de constitucionalmente protegida, a intimidade ainda carece de amparo infraconstitucional específico. O estabelecimento de tipos penais para a proteção desta, que é um dos bens jurídicos mais significativos ao homem moderno, o que recomenda-se neste estudo. Em um último instante, também, sugere-se a instituição de um possível modelo: a regulamentação que está sendo implantada na União Europeia, ao nosso país.

Examina-se, portanto, o futuro da gestão de dados no Brasil, e as formas de fragilização da privacidade e da intimidade dos indivíduos titulares desses dados. Recomenda-se, por fim, uma lei geral de dados para o Brasil, inclusive com aspectos penalizantes, bem como a instituição de uma autoridade nacional de proteção de dados, e a atualização de diplomas penais específicos.

**ABSTRACT**

The following study is presented as a detailed examination concerning the new limits of intimacy and privacy in the internet environment. Faced with the new challenges, arising from the change in the network over the last decade, in order to insert new behaviors in the scope, it is required to observe possible violations of the fundamental right to intimacy. Worth mentioning intimacy as being essential to the formation of the personality of the individual, deserving criminal protection whenever it is threatened.

In the last decade, the challenges to the privacy of individuals have become more sophisticated. With the emergence of fake news, blockchains, new forms of artificial intelligence, the internet of things, cloud storage, social networks, overall, the gathering and processing of personal data inserted and made available in computer devices.

On this point of view, we ofer a brief analysis of the laws of the United States and European Union regarding to privacy, as well as the legal frameworks in Brazil, proposes the current outlook of possible protections and, at the same time, undeniable omissions. Although constitutionally protected, the privacy still lacks specific infraconstitutional protection. The establishment of criminal types for the protection of this fundamental right, which is one of the most significant legal goods to the modern man, is recommended over this study. The regulation that is being implemented in the European Union can be a model to our country.

Therefore, the future of data management in Brazil is examined, as well as the ways in which privacy and intimacy of the individuals bearing these data are fragilized. Finally, a general law of data is recommended for Brazil, including with criminal aspects, as well as the establishment of a national data protection authority and the updating of specific criminal laws.

# SUMÁRIO

## INTRODUÇÃO

A internet desempenha papel fundamental em nossas vidas. MANUEL CASTELLS argumenta que vivemos na sociedade da informação, na qual o conjunto de informações disponíveis é aplicável ao tempo em que se vive e ao passado, já que, em nossos tempos, a informação "desempenha um papel importante na organização, operação e desenvolvimento de diferentes sociedades, para construir-se como uma realidade"[1].

O filósofo espanhol enfatiza a importância de se estudar as mudanças tecnológicas em relação aos contextos culturais, condições históricas e intervenções políticas. Segundo ele, as estruturas sociais são construídas de acordo com o *espaço-tempo* em que vivemos, mas com os avanços que presenciamos, o próprio conceito de Estado-nação é afetado pelas novas fronteiras descobertas com o uso da tecnologia.[2] Parece-nos pertinente, portanto, o estudo sobre a afetação da intimidade dos indivíduos pelas novas tecnologias de interação social, parte fundamental do fenômeno descrito por aquele autor.

A visão do pensador corrobora a percepção embarcada nessa pesquisa: há uma transformação social em curso, e a história da comunicação da humanidade jamais se deparou com um ponto de mudança tão paradigmático quanto a popularização da internet de banda larga e o desenvolvimento das redes sociais. VAN DIJK[3] e DEL GIUDICE[4] levam a crer que na verdade estamos deixando a sociedade da informação, cruzando a ponte da evolução para uma sociedade completamente interligada pela internet – a "sociedade em rede". Para DEL GIUDICE:

---

[1] CASTELLS, Manuel. *Communication Power*. Nova York: Oxford University Press, 2013. p. 10. Conferir também: CASTELLS, Manuel. *Internet Galaxy*: reflections on the internet, business and society. Nova York: Oxford University Press, 2001. p. 12.

[2] "In sum: if power relationships exist in specific social structures that are constituted on the basis of spatiotemporal formations, and these spatiotemporal formations are no longer primarily located at the national level, but are global and local at the same, the boundary of society changes, and so does the frame of reference of power relationships that transcend the national (Fraser, 2007). This is not to say that the nation-state disappears. But it is to say that the national boundaries of power relationships are just one of the dimensions in which power and counterpower operate. Ultimately, this affects the nation-state itself. Even if it does not fade away as a specific form of social organization, it changes its role, its structure, and its functions, gradually evolving toward a new form of state: the network state." (CASTELLS, Manuel. *Communication*... cit., p. 10. Ver também: CASTELLS, Manuel. *Internet*... cit., p.18). E ainda em: CHAN, Melanie. *Virtual reality:* representations in Contemporary Media. London: Bloombury Academic, 2014. p. 17-25.

[3] VAN DIJK, J. *The network society*. Londres: SAGE, 2006.

[4] DEL GIUDICE, M. From informational Society to Network Society: the challenge. In: DEL GIUDICE, M.; PERUTA, M.R.D.; CARAYANNIS, E.G. *Social Media and Emerging Economies*: technological, cultural and economic emplications. Springer: Nova York, 2014.

> o processo de convergência de mídias tem sido permitido por redes digitais, e vários processos econômicos e sociais foram ativados por essa convergência. As limitações enfrentadas pelas indústrias anteriormente separadas durante a execução de seus negócios foram alteradas pelo uso da mesma tecnologia digital. Assim, a convergência não é uma mera mudança tecnológica, mas tem um impacto sobre as mudanças que influência relações em uma sociedade.[5]

**Esta é, então, a raiz do problema ora apresentado e pergunta reitora da pesquisa: quanto a transformação histórica pela qual passamos tem afetado e transformado a intimidade, a vida privada e a privacidade do cidadão em que medida deve o direito penal tutelar tal transformação?**

Diante de todo o conjunto de informações que os usuários da rede geram, é provável que, enquanto estas linhas estão sendo redigidas, os dados eletrônicos causados pela mera subsunção das ideias ao papel sejam suficientes para a geração, em tempo real, de criação de cenários de influência por meio de algoritmos do sistema informático e, consequentemente, de receita para os agentes detentores desse tipo de poder.

É possível, por conseguinte, que a tomada de decisões em nossa sociedade seja antevista por máquinas e *bots* – robôs gestores de dados informáticos. Esse cenário de antecipação de desejos e exposição a opções previamente definidas é bastante grave porque está alicerçado em limites obscuros no tocante ao respeito à vida privada do usuário das redes informáticas.

Diversos atores privados na internet aferem a geolocalização de seus usuários ininterruptamente. Boa parte das aplicações disponíveis na rede hoje *sabem* exatamente onde seus usuários dormem[6]. É possível que nesse ponto da história a reunião de dados entre acessos à internet, ligações e uso de cartões de crédito já esteja superada pelo domínio do algoritmo de um só aplicativo. Fossem as coletas de dados por parte dos atores privados procedimentos isolados o estudo presente não seguiria, dada a constatação óbvia de que passamos por uma

---

[5] "The process of media convergence has been allowed by digital networks, and various economic and social processes have been activated by such a convergence. The limitations faced by previously separated industries while running their businesses were changed by the use of the same digital technology. Thus, convergence is not a mere technological shift, but has an impact on the changes that influence relations in a society." (trad. livre) (DEL GIUDICE, M. *From informational*… cit.,. p. 72.)

[6] Segundo López Ortega ""capacidad de determinar cómo, cuándo y en qué medida se comunica información a otros" LÓPEZ ORTEGA, J. J. *Intimidad informática y Derecho Penal (La protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación)*. In: Derecho a la intimidad y nuevas tecnologías. Centro de Documentación Judicial del Consejo General del Poder Judicial. Cuadernos de Derecho Judicial IX. Madrid, 2004, pp. 110-111.

revolução e de que a segurança dos dados é fundamental e, dizem as redes, parte da política de uso.

Mas o problema proposto vai além: está na mudança fundamental nas interações que a reunião desses dados pode gerar sobre a intimidade e a vida privada dos cidadãos, e em que medida as regulações existentes dão conta de mediar a utilização de tão profundas e interessantes coleções. Ao que nos parece, os detentores dos algoritmos que controlam as aplicações que estão a coletar continuamente os dados dos usuários da internet detêm um poder inédito na história da humanidade: o controle das emoções de seus usuários.

Isso pode obrigar, num futuro próximo, as empresas que colecionam dados a desenvolverem novas tecnologias para personalizar seus ambientes de rede, de modo a garantir que o usuário, e apenas ele, detenha o controle do conteúdo a que é submetido.

Na era dos dispositivos móveis geridos por aplicativos, ao contrário do que parece, não há produto gratuito. Quando um serviço é oferecido sem um custo para o usuário é importante que se demonstre que essa gratuidade é apenas aparente: o indivíduo está pagando a conta com a disponibilização de seus dados para o agente detentor da aplicação – e isso significa a possível cessão de parte de sua intimidade. RODOTÀ é preciso neste aspecto, segundo ele "a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações"[7].

**Regular o acesso aos dados é fundamental para as democracias modernas. Por isso, depois de bem expostas as nuances do tema, está o objetivo específico deste trabalho: apontar, diante das possibilidades de violações à autodeterminação informativa e da intimidade dos indivíduos por parte dos agentes privados detentores das coleções, a possibilidade de reconhecimento da intimidade enquanto bem jurídico suficiente a amparar a proposição de normas penais para os responsáveis pelo eventual dano por má gestão ou invasão das grandes coleções de dados.**

Em 2014, o Facebook se retratou por autorizar e apoiar o estudo de ADAM KRAMER, JAMIE GUILLORY e JEFFREY HANCOCK com relação ao comportamento de seus usuários. Os três pesquisadores manipularam, durante uma semana, o *feed* de notícias de 689.003 usuários em

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

língua inglesa para testar suas reações a uma avalanche de notícias positivas ou negativas de seus amigos. Concluíram que "as emoções expressas por outras pessoas no Facebook influenciam nossas próprias emoções, constituindo o estudo evidencia experimental de que existe contagio por redes sociais"[8].

É possível que a intimidade dos usuários do Facebook tenha sido afetada em seu âmbito informacional. Ainda que eticamente duvidoso – os participantes do estudo, apesar de terem suas identidades preservadas, não foram avisados de que faziam parte da amostragem. O artigo confirma experimentalmente a importância desta pesquisa: as redes sociais podem ser capazes de influenciar nossa tomada de decisão e podem fazer isso a partir da disponibilidade de acesso a nossa vida privada[9] e da nossa intimidade, que ganham diante da mera troca pelo acesso livre a uma plataforma.

Não se busca juízo de reprovação pela manipulação, mas que sejam estudados os novos limites de tolerância do acesso à intimidade do usuário e em que medida a utilização mal intencionada deste acesso merece gerar repercussões penais.

Mesmo que tenha se desculpado, o Facebook demonstrou ser capaz de manipular usuários que confiaram seus dados à rede social que, dessa maneira, detinha acesso privilegiado a esferas de liberdade pessoal desses sujeitos. Fez isso sem infringir a Lei norte-americana de proteção a pessoas alvo de estudos[10], por exemplo, porque seus usuários assentem com uma espécie de contrato de adesão ao entrarem para a rede, abrindo mão da titularidade de seus dados quando se trata de pesquisas controladas.[11] No entanto, os limites éticos dessa mitigação dos direitos individuais dos usuários constitui-se ainda em tema carente de uma discussão mais verticalizada, especialmente pelas ciências criminais.

---

[8] KRAMER, A.; GUILLORY, J.; HANCOCK, J. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS Review*, vol. 111, n. 24., jun. 2014. Disponível em: <http://www.pnas.org/content/111/24/8788.full.pdf>. Acesso em: 06/09/2017.

[9] Não se desconhece a discussão apresentada por Rodríguez; a expressão é aqui utilizada em sentido amplo, conforme sua lição. (Cf. RODRÍGUEZ, Víctor Gabriel de Oliveira. *Tutela da Penal da Intimidade*: perspectivas da atuação penal na sociedade da informação. São Paulo: Atlas, 2008. p. 33.)

[10] A US Department of Health and Human Services Policy for the Protection of Human Research Subjects. Disponível em: <http://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html>. Acesso em 22.05.2016.

[11] É verdade que o Marco Civil da internet proíbe a imposição de contratos de adesão e torna nulo qualquer ato desse tipo, mas basta a tentativa de criar uma conta em qualquer rede social para ser posto em frente a um instrumento desse tipo.

Diante desta nova e conflitiva realidade, é preciso ir além: é necessário que o Estado garanta a autodeterminação informativa e das decisões dos indivíduos no mundo digital com base na garantia constitucional da intimidade. A política criminal do Estado Brasileiro precisa levar em consideração as novas formas de violação da intimidade, em atenção aos princípios da lesividade e da fragmentariedade do direito penal. É preciso regular o uso das coleções de dados, de modo que as tomadas de decisão do indivíduo não se apoiem no conjunto de informações que recebeu, por imposição de um algoritmo[12], desse ou daquele ator privado da rede.

Conquanto o direito penal não possa olvidar-se do seu papel, de acordo com Roxin, o fundamento da sociedade não poderia ser qualquer política criminal, mas somente aquela ligada intrinsecamente com a ideia de Estado Democrático de Direito, baseado na subsidiariedade do Direito Penal, que deve tutelar somente os bens jurídicos mais sensíveis da sociedade, sempre através da prevenção geral e especial e com observância aos direitos e garantias constitucionalmente salvaguardados [13] . Nós entendemos, conforme será bem delineado nessa pesquisa, que a intimidade, especialmente quando relacionada aos dados pessoais inseridos na internet, é um desses bens jurídicos sensíveis que merecem tutela específica.

A União Europeia, por exemplo, vem dedicando-se a estabelecer princípios para a coleta, armazenamento e uso de dados pessoais por indivíduos, organizações e pessoas desde o início da década de 1980. Faz isso, como se verá a seguir, justamente com base na tutela da privacidade.

Resultado desse movimento de regulação foi a promulgação de um novo *Charter of Fundamental Rights*[14] para revisar a regulação dos direitos fundamentais, incluindo neste documento a proteção dos dados pessoais, equiparando-a à liberdade de expressão e à garantia a um julgamento isento. Pode-se entender o caráter protetivo da lei como uma evolução do direito à intimidade: a proteção dos dados pessoais passou a ser um novo campo de proteção,

---

[12] Quanto a esse ponto, o explicativo e profundo estudo de Zoran Majkic: MAJKIC, Zoran, *Big data integration theory* – theory and methods of database mappings, programming languages, and semantics. Tallahasee, FL, EUA, 2014.

[13] ROXIN, Claus. *Derecho Penal: parte general*. Madrid: Civitas, 1997. (Tomo I). P. 181 e ss.

[14] EUROPEAN COMISSION *Charter of Fundamental Rights*. Bruxelas: Secretaria do Comissariado, 2009. Disponível em: <http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm>. Acesso em 20.04.2016

um direito autônomo, derivado da intimidade. Acertada doutrina a tratar do tema descreve a privacidade e proteção de dados como "direitos diferentes, complementares e fundamentais"[15].

A distinção seria necessária, conforme afirmaram os mesmos autores mais recentemente[16], porque as leis de proteção à privacidade destinam-se a proteção da não interferência nos atos privados da vida, criando um campo de autonomia e liberdade para os indivíduos, enquanto as leis de proteção aos dados devem destinar-se à transparência no tratamento dos dados de indivíduos e organizações por parte de outros indivíduos e organizações, possibilitando aos cidadãos o controle de seus dados e a consciência de como sua intimidade é manejada por esses atores privados.

O que se discute, então, é justamente a interação entre esses dois direitos, de não intervenção na intimidade e de consciência na utilização de uma coleção de dados. Ao colecionar dados, uma rede social passa a oferecer, por exemplo, mais publicações ligadas a este ou àquele partido político, podendo exercer considerável influência nas decisões de seus utilizadores.

Um estudo publicado pela revista científica *Nature* mostra que nas eleições legislativas norte-americanas de 2010, 340.000 pessoas compareceram para votar movidas pelo *status* "I voted", um botão específico do Facebook para aquele dia, clicado por quem já tinha votado.[17] Trata-se de um indício de que a rede social pode ir além da capacidade de influência no estado emocional de seus usuários, podendo aproveitar do acesso privilegiado ao íntimo para induzir comportamentos. A informação está ligada diretamente ao poder. RODRÍGUEZ leciona ser "possível afirmar que a intimidade corre graves riscos diante do arsenal tecnológico controlado por indivíduos e grandes corporações que têm interesse imediato na detenção de informações complexas e recombinadas sobre toda a sociedade"[18].

---

[15] DE HERT, Paul; GUTWIRTH, Serge. *Privacy and criminal law* – privacy, data protection and law enforcement: opacity of the individual and transparency of power. Oxford: Intersentia, 2006. p.61.
[16] DE HERT, Paul [et al.]. *Reinventing data protection?* Springer: Bruxelas, 2014. p.X (prefácio).

[17] BOND, R. [et al.]. *A 61-million-person experiment in social influence and political mobilization. Nature Magazine*, Nova York, *n.* 489, p. 295–298, 2012. Disponível em: <http://www.nature.com/articles/nature11421.epdf>. Acesso em: 22.05.2016
[18] RODRÍGUEZ, Víctor Gabriel de Oliveira. *Tutela*... cit., p.02.

Ainda que não se desconheça que o direito penal deve alicerçar-se na intervenção mínima[19], entendemos que ele é um ramo, como se verá, que tem papel decisivo na mediação dessas novas interações, possibilitadas pelas redes. A proposição do debate aqui busca exatamente evitar o surgimento de gestores atípicos da moral a criminalizar sobremaneira um campo ainda pouco regulado[20]

Na mesma medida, ROUVROY e POULLET anotam que a privacidade não é uma liberdade com o mesmo *status* de outras: para os autores, a privacidade é essencial para a formação da dignidade humana e para a autonomia individual e traduz esses princípios morais para a esfera legal.[21]

Intimidade é precondição necessária para o usufruto de muitas outras liberdades e direitos fundamentais[22], sendo que para exercitá-la é indispensável a autonomia do ser, retratada por FAIDEN e BEAUCHAMPS como resultado fundamental e infungível da "privacidade, voluntariedade, autodomínio, livre escolha, livre posicionamento moral e aceitação de responsabilidade pelas próprias escolhas"[23].

---

[19] ROXIN, Claus. Las formas de intervención en el delito: estado de la cuestión. In: ROXIN, Claus [et al]. *Sobre el estado de la teoría del delito:* Seminario en la Universitat Pompeu Fabra. Madrid: Civitas, 2000. p. 155-178.

[20]Quanto a isso, Renato de Mello Jorge Silveira "Indelével é a presença atual, de influência, de todo deletéria no meio penal, dos chamados gestores atípicos da moral. Cunhados no novo momento por que passa a humanidade, a partir de avanços tecnológicos e da valorização das diversas camadas sociais, onde ganham relevo os chamados direitos de terceira geração, consistem eles das diversas associações de cunho organizacional, as quais passaram a ter papel de destaque nas decisões políticas. Bradando por seus direitos, entidades representativas ecológicas, feministas, de consumidores, raciais, etc., empenham todos os esforços para a defesa de seus interesses, mesmo em seara penal. Desvirtuando o sistema, tentam criar, sem fundamento dogmático, proteções as quais, no mais das vezes, mostram-se unicamente simbólicas". SILVEIRA, Renato de Mello Jorge. "A imprensa e a lei da mordaça". In: Boletim do IBCCrim, Setembro, 2000. Sobre os gestores da moral coletiva ver também SILVA SANCHEZ, Jesús María. La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales. 2. ed. Madrid: Civitas, 2001, p. 67. A relação com os meios de comunicação em Silva Sanchez pode ser vista desde o enfoque da manipulação da "sensação de insegurança" da sociedade, pp. 37 e ss e , POLAINO-NAVARRETE, Miguel. La controvertida legitimación del derecho penal en las sociedades modernas: más derecho penal? In: JAKOBS, Günther; POLAINO-NAVARRETE, Miguel. El derecho penal ante las sociedades modernas: dos estudios de dogmática penal y política criminal, 2006, pp. 77 e ss.

[21] "Privacy is not a freedom on the same rank than the others: essential to human dignity and individual autonomy and translating these moral principles in the legal sphere, privacy is a necessary precondition to the enjoyment of most other fundamental rights and freedoms." (trad. livre). (POULLET, Yves; ROUVROY, Antoinette. The right to informational self-determination and the value of self-development: Resseassing the importance of privacy to democracy. In: DE HERT, Paul [et al.]. *Reinventing data protection?* Bruxelas: Springer, 2014. p. 61.)

[22] Idem.

[23] "Autonomy may also be defined as privacy, voluntariness, self-mastery, choosing freely, choosing one's own moral position and accepting responsibility for one's choices" (trad. livre) (FAIDEN, Ruth; BEUCHAMPS, Thomas Beauchamps. *A History and Theory of Informed Consent*. Oxford: Oxford University Press, 1986. p. 41.)

Ao receber um volume muito maior de dados, notícias, propagandas e afins relacionados a uma determinada ideologia ou ideário, o indivíduo pode acreditar que está a escolher esta ou aquela alternativa intimamente[24] – quando na verdade pode estar sob influência de um movimento artificial.

É preciso estabelecer, por fim, o liame de responsabilidade que deverá atingir os tomadores de decisão que detêm domínio do uso dessas coleções de dados e algoritmos. Conforme esclarece LOPES DA SILVA:

> "a informação encerra, nos dias atuais, importância vital para a sociedade, podendo ser-lhe atribuído um interesse social valioso, digno de tutela penal, uma vez que é objeto de armazenamento, tratamento e transmissão, por meio de sistemas informáticos, impondo a necessidade de tutela penal (...)Por outro lado, pode ser reconhecida como mercadoria, uma coleta de dados registrados sob a forma de impulsos magnéticos, como uma nova matéria-prima, pertencente ao gênero especial dos bens imateriais"[25]

Ao que se pode complementar com RODRÍGUEZ, para quem "o exercício do comando pela força física, salvo raras exceções, perdeu lugar para o conhecimento e, principalmente, para o controle que se pode levar a efeito sobre cada indivíduo por meio da capacidade de obtenção de dados"[26-27]. Eis o cenário atual de fragilidade da intimidade: os dados informáticos são capazes de encerrar em si importantes violações a intimidade. Se os

---

[24] Sobre a ilusão de liberdade, ver a parábola da pedra de Spinoza, explicada por Rodríguez em RODRÍGUEZ, Víctor Gabriel de Oliveira. *Livre arbítrio e direito penal e direito penal*: revisão frente aos aportes da neurociência e à evolução dogmática. 321p. Tese (Livre-docência em Direito Penal) – Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2015. p. 90.

[25] SILVA, Rita de Cássia Lopes da. *Direito Penal e sistema informático*. São Paulo: Revista dos Tribunais, 2003. p. 19.

[26] RODRÍGUEZ, Víctor Gabriel de Oliveira. *Tutela*... cit., p.21.

[27] Quanto a este ponto, ver as importantes observações: "[s]everal Latin American countries have adopted a general data protection law: in addition to Argentina, which pioneered the issue, Mexico, Uruguay, Colombia, Peru and others have statutes governing the area. In Brazil, the lack of a broad regulation in this field has increasingly been considered as a problem both by citizens and by companies: on the one hand, citizens are more and more aware of the risks of an uncontrolled data flow, as issues such as identity theft and commercial abuse of personal data have gained visibility; on the other hand, compliance with international standards concerning the international transfer of personal data and a strong set of rules governing data protection in general are considered a necessity for the development of new businesses in the country, such as cloud computing. In this context, a comprehensive data protection act is seen at the same time as a way of ensuring more protection to the citizens, concerning the processing of their personal data, and increasing legal certainty to the companies, regarding how to process and use personal data within the legal framework. Furthermore, analyzing the current data protection framework in Brazil, we see that there are some challenges to be faced, which would need a sectorial approach."(DONEDA, Danilo; MENDES, Laura S. Data protection in Brazil: new developments and current challenges. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014. p. 16-17.)

dados são capazes de prever como os indivíduos podem se comportar a partir do privilégio de acesso a vida privada, a tutela de sua utilização, por mais banal que possa parecer, equivale à proteção da própria democracia.[28]

Restam incertas quais seriam as propostas jurídicas mais adequadas para gerenciar o conflito, havendo, no entanto, experiências legislativas estrangeiras que podem oferecer bons indicativos. O primeiro a ser adotado por atores relevantes foi o *APEC Privacy Framework* – da Organização para Cooperação Econômica Ásia-Pacífico. Ele prevê, desde 1980, o "Princípio da Limitação à coleta de dados" afirmando ser "[a] coleta de informações pessoais relevantes para efeitos de coleção [de dados] que deve ser obtida por meios legais e justos, e quando apropriado, com aviso prévio, ou consentimento, do indivíduo em questão"[29]. Meses depois da entrada em vigor do acordo da APEC, o Conselho da Europa colocou em prática a *Convenção 108*, para proteção do indivíduo em relação ao processamento automático de dados pessoais, com princípios na mesma linha dos adotados pela OCDE.[30]

Todavia, o marco normativo mais importante atualmente nesse campo é provavelmente o novo Regulamento Geral de Proteção de Dados da União Europeia – o GDPR, na sigla em inglês, que terá tópico próprio nesse texto.

Do ponto de vista penal, pode-se mencionar ainda as resoluções que a Associaçãao Internacional de Direito Penal – AIDP – adotou em seu 19º Congresso Internacional, em 2014[31].

---

[28] Busca-se na pesquisa uma expansão para a conclusão de RODRÍGUEZ de que "Bartolomé de las Casas merece nova revisão de sua obra, sob a ótica do Direito Penal: sua defesa da não-influência do Estado na liberdade de querer e, mais, a necessidade de um agir positivo do Estado para a informação mínima que permite o exercício da liberdade tem lugar no debate da sociedade atual" (RODRÍGUEZ, Víctor Gabriel de Oliveira. Tutela... cit., p. 302.) para testar a necessidade de não-influência também por parte de determinados agentes privados, os detentores de coleções de dados.

[29] "The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned" (ASIA-PACIFIC ECONOMIC COOPERATION. *APEC Privacy Framework*. Singapore: APEC Secretariat, 2005. p. 15.)

[30] "This text promotes basic principles for data protection. Unsurprisingly these principles are in the line of those proclaimed by OECD" (TERWANGNE, Cécile de. Is a Global Data Protection Regulatory Model Possible? In: DE HERT, Paul [et al.]. *Reinventing data protection?* Bruxelas: Springer, 2014. p. 182.)

[31] Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

A regulação do uso dos dados por parte dos novos atores privados na rede aos quais, quase sem notar, submetemo-nos, é um problema de primeiro plano na Sociedade da Informação[32], mas apesar de sua importância, ainda é discutida em círculos bastante restritos.

A sociedade de vigilância imaginada por ORWELL[33] em 1949, na publicação de seu "1984", toma corpo a cada dia. No lugar de um Estado supremo, onisciente e onipresente, é possível que atores privados detenham o domínio da intimidade dos indivíduos.

Para que se proteja a intimidade diante das novas formas de poder, é necessário o constante estudo dos novos agentes e das novas habilidades que surgem todos os dias na sociedade da informação e a conveniência da aplicação de normas penais.

O cenário evoluiu em termos impensáveis há uma década. Oferecemos, então, um novo estudo do tema, de modo a prevenir que uma regulação de emergência tome o lugar do necessário debate. As violações da privacidade e da intimidade na internet são um campo amplo, seria pretensioso tentar esgotá-lo. Mas é possível encontrar, nestas páginas, um panorama daquilo que consideramos serão os próximos desafios relacionados à privacidade, intimidade e ao direito penal no ciberespaço brasileiro.

---

[32] Nas palavras de Cécile de Terwangne "Data protection can also be perceived as just a problem of trust. Data protection is then reduced to a question of security. The World Summit on the Information Society Declaration in 2003 follows this point of view and treats data protection as part of cyber-security. Data protection coincides with confidentiality and confidentiality breaches are the problem to tackle" referindo-se à declaração de princípios do World Summit of the Information Society: "Declaration of Principles – Building the Information Society: a global challenge in the new Millennium, Document WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003: 'Building confidence and security in the use of ICTs. Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade." (TERWANGNE, Cécile de. *Is a Global*… cit., p. 181.)

[33] ORWELL, George. *1984.* 29ª ed. São Paulo: Cia Editora Nacional, 2005.

# 1. INTIMIDADE, COLEÇÃO DE DADOS E VIOLAÇÕES ATUAIS

## 1.1 Conceitos preliminares

A informática é o ramo do conhecimento que estuda as tecnologias de informação e comunicação por dispositivos de tratamento de dados (computadores, celulares, *tablets*, robôs etc.). Em seu bojo têm se desenvolvido, notadamente na última década, as redes de comunicação e relacionamentos que ficaram conhecidas como redes sociais, fenômeno da sociedade pós-industrial que tem levado a novos desafios nas várias áreas do conhecimento. Mas não só. Diversas aplicações recolhem dados por emissão de *cookies* e controle de permanência, plataformas distribuem notícias falsas, uma nova cadeia de informações, provavelmente a mais importante desde a criação da web (a *Blockchain*) se forma, novas formas de pagamento e manutenção do patrimônio (as criptomoedas) se desenvolvem, e a inteligência artificial e as neurociências aliadas à computação preditiva avançam. Isto tudo impõe novas e importantes questões também à privacidade, à intimidade e ao direito penal.

Em 1890, WARREN e BRANDEIS publicaram nos EUA seu artigo com a teoria do direito à privacidade (*The right to privacy*[34]), popularizada quando BRANDEIS, então *Justice* na Suprema Corte norte-americana, aplicou-a no julgamento de *Olmstead v. United States*[35]. Segundo ele o direito de privacidade (*the right of privacy*) é o direito de ser deixado em paz (*the right to be let alone*), sendo esse o direito mais valorizado pelos homens civilizados.[36] As discussões em seu entorno desde então – quanto a vida privada, a intimidade, a reserva, ou a mais de uma esfera de íntima – têm sido intensas.[37]

Nos limites desta dissertação, adotam-se os mesmos conceitos enunciados por RODRÍGUEZ[38], para quem a vida privada contém a intimidade, sem se ignorar, como aduz ele, que o termo *privacy* "abarca um e outro e se encontra traduzido, pela doutrina como intimidade"[39]. Também se preferirá o termo mais estrito "intimidade", mas, por vezes, quando

---

[34] WARREN, Samuel D., BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, vol. IV, n.5, 1890.
[35] *Olmstead v. United States*, 277 U. S. 438 (1928). Disponível em: https://supreme.justia.com/cases/federal/us/277/438/case.html Acessado em 27.06.2016.
[36] "(…) the most comprehensive of the rights and the right most valued by civilezed men". Ibid.
[37] MATA BARRANCO, Norberto J. de la; BARINAS UBIÑAS, Desirée. La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redeginir el objeto de tutela? *Revista de Derecho Penal y Criminología*, Madrid, 3ª Época, n. 11, p.13-92, jan./jun. 2014. p. 35.
[38] RODRÍGUEZ, Víctor Gabriel. *Tutela....* cit., p. 33. Ver também FERREIRA, Ivette Senise. A intimidade e o direito penal. *Revista Brasileira de Ciências Criminais*, São Paulo, vol. 2, n. 5, p.96-106, jan./mar. 1994.
[39] Ibid. Idem.

se entender por um cenário mais amplo, será usado o termo "vida privada" ou, ligeiramente mais reservado, mas menos pessoal, o vocábulo "privacidade".

A privacidade se expandiu, tornando-se uma nova expressão da liberdade e abarcando novos ramos do direito. Uma dessas evoluções está associada diretamente à tecnologia: a proteção ao sigilo de dados. O mais notável esforço nesse campo vem da União Europeia que se dedica a estabelecer princípios para a coleta, armazenamento e uso de dados pessoais por indivíduos, organizações e pessoas desde o início da década de 1980, pela instituição da *Convenção 108* do Conselho da Europa. Ali já se estabelecia que os dados deveriam ser "obtidos e processados de maneira justa e legal", devendo ser arquivados "para fins específicos e legítimos e nunca usados de maneira incompatível com estes fins"[40]. Em 1995, com a diretiva 95/46/EC – complementada em 2002 pela diretiva 2002/58/EC, a UE passou a regular o uso deste tipo de informação de seus residentes. Com o advento do novo Regulamento Geral de Proteção de Dados em 2016 – que entrará em vigor em 25 de maio de 2018 –, o bloco deu um importante passo na proteção de dados diante do oceano azul de novas aplicações para as coleções atuais.

Pelo nível de privacidade que a reunião de dados digitais de um indivíduo pode fornecer para quem tem a o domínio de coleções, em 2006 a EU adotou a "Directive on retention of communication traffic data[41]", promovendo a uniformização das regras para provisão de dados por parte dos provedores de aplicações às autoridades do bloco e para regular os limites de armazenagem desses dados.

Em 2009, o bloco europeu adotou um reformado *Charter of Fundamental Rights* para revisar a regulação dos direitos fundamentais. Dentre as inovações, a proteção aos dados pessoais ganhou caráter de direito fundamental, equiparando-se à liberdade de expressão e à garantia a um julgamento isento. Pode-se entender o novo caráter protetivo da lei como uma evolução do direito à intimidade: a proteção a autodeterminação dos dados é um novo campo de direitos, originado da proteção à intimidade mas e indissociável dela.

HERT e GUTWIRTH postulam que privacidade e proteção de dados são "direitos diferentes, complementares e fundamentais"[42]. A distinção seria necessária, conforme

---

[40] CONSELHO DA EUROPA. *Treaty 108*. Strasburgo, 1981. Disponível em <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acessado em 29.06.2016.
[41] UNIÃO EUROPEIA. Directive on Retention of Communication Traffic Data. Bruxelas, 2006. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006L0024>. Acesso em 29.06.2016.
[42] DE HERT, Paul; GUTWIRTH *Privacy*… cit. p. 61.

descrevem mais recentemente, porque as leis de proteção à privacidade destinam-se a proteção da não-interferência nos atos privados da vida, criando um campo de autonomia e liberdade para os indivíduos, enquanto as leis de proteção aos dados devem destinar-se à transparência no tratamento dos dados de indivíduos e organizações por parte de outros atores privados e governos, possibilitando a cada um o controle de seus dados e a consciência de como serão utilizados por terceiros[43] .

A privacidade, afirmam ROUVROY e POULLET, "não é uma liberdade com o mesmo status de outras". Segundo os autores, "é essencial para a formação da dignidade humana e para a autonomia individual e traduz esses princípios morais para a esfera legal" sendo, deste modo, "precondição necessária para o usufruto de muitas outras liberdades e direitos fundamentais"[44].

Para exercitar a privacidade é indispensável a autonomia do ser, retratada por FAIDEN e BEAUCHAMPS como "resultado fundamental e infungível da privacidade, voluntariedade, autodomínio, livre escolha, livre posicionamento moral e aceitação de responsabilidade pelas próprias escolhas"[45]. É só com a garantia da intimidade que o indivíduo pode ser livre para tomar decisões e formar sua opinião.

Nos últimos anos, contudo, a informação e a detenção dos dados sobre ela foram ressignificados, transformadas em ativos importantes, vendidos principalmente a anunciantes, que sustentam a riqueza dos novos proprietários de algoritmos que "conectam" os usuários da rede. Essa conectividade, porém, está baseada num acesso privilegiado a vida intima do usuário.

Nesse cenário a vida privada e a intimidade são cada dia mais ameaçadas, mesmo diante das diversas garantias presentes no ordenamento jurídico brasileiro. Segundo KLIP "se os Estdos não conseguirem encontrar uma maneira de desenhar sua responsabilidade na internet e de trazê-la para o estado de direito, o ciberespaço será similar a um estado de coisas anarquista. E isso resultaria em um mundo em que as regras relativas ao crime organizado e em matédria de direitos humanos não teriam sentido"[46]

O artigo 5º da Constituição Federal, dispõe, por exemplo, sobre os direitos e garantias fundamentais, assegurando, em seu inciso X, de forma expressa, a proteção da

---

[43] DE HERT, Paul [et al.]. *Reinventing*...cit., p. x (prefácio).
[44] POULLET, Yves; ROUVROY, Antoinette. *The right*… cit., p. 61.
[45] FAIDEN, Ruth; BEUCHAMPS, Thomas Beauchamps. *A History and Theory of Informed Consent*. Oxford: Oxford University Press, 1986. p. 41.
[46] KLIP, Andre. *Relación General al Coloquio Preparatorio de Helsinki*. Revenue International de Droit Penal. 2014 (1-2). P. 430 e ss.

intimidade e da vida privada. Neste sentido, afirma serem "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".

Também em convenções internacionais erigidas para a contemplação de direitos humanos essenciais, o tema relativo à proteção do sigilo é objeto de específico tratamento. Para exemplificar, tem-se o artigo 11 da Convenção Americana de Direitos Humanos (Pacto de San José da Costa Rica), a qual passou a integrar o ordenamento jurídico nacional com a promulgação do Decreto nº 678/1992, que assim estabelece:

> Art. 11 – Proteção da honra e da dignidade:
> [...]
> Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em outras correspondências, nem de ofensas ilegais à sua honra ou reputação.

Corolário do Estado Democrático de Direito, a proteção do direito à intimidade, considerado por RODRÍGUEZ MARÍN "un superderecho garantia de otras libertades individuales"[47], confere aos indivíduos a possibilidade de oposição a ingerências indevidas no âmbito de sua individualidade. BELOQUE pontifica a salvaguarda:

> intimidade é indispensável ao desenvolvimento da identidade pessoal e da personalidade humana, pois possibilita a experimentação de situações privativas particulares, de forma independente, sem interferências exteriores de repressão ou julgamentos sociais.[48]

É possível que o direito penal desempenhe papel importante nessas relações, como se verá a seguir. Antes de adentrar a questão, é preciso, contudo, apresentar os nossos desafios na área.

## 1.2 Novos desafios

Compreendida a importância do direito à intimidade e a sua estreita vinculação com as bases fundantes dos Estados Democráticos de Direito, tem-se justificada a atenção dispensada no Brasil pelo constituinte originário à intimidade, à vida privada e aos sigilos de

---

[47] MARÍN, Fernando Rodríguez. Los delitos de escuchas ilegales y el derecho a la intimidad. *Anuaria de Derecho Penal y Ciências Penales*, Madrid, t. XLIII, jan-abr., 1990, p. 207.
[48] BELOQUE, Juliana Garcia. *Sigilo Bancário* – Análise Crítica da LC 105/2001. São Paulo: Revista dos Tribunais, 2003. P. 21.

dados – que somente poderão ser mitigados em situações excepcionais, com observância às "hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Nada além disso.

Ainda na leitura do artigo 5º da Carta da República, o inciso XII revela, com clareza, que, no cerne da ordem jurídica brasileira, apenas "por ordem judicial" é admitida a mitigação da inviolabilidade dos sigilos. Referida questão não é passível de ser questionada, pois evidente que a relativização de direitos fundamentais, em qualquer Estado que se pretenda Democrático, há passar pelo crivo judicial. Trata-se de matéria "inteiramente submetida ao princípio constitucional da reserva de jurisdição (CF, art. 5º, XII)", sendo vedada a mitigação do sigilo de dados e das comunicações telefônicas e telemáticas dos indivíduos sem a existência de fundamentada decisão judicial, conforme se extrai de importante precedente do Egrégio Supremo Tribunal Federal:

> O postulado da reserva constitucional de jurisdição importa em submeter, à esfera única de decisão dos magistrados, a prática de determinados atos cuja realização, por efeito de explícita determinação constante do próprio texto da Carta Política, somente pode emanar do juiz, e não de terceiros (...). A cláusula constitucional da reserva de jurisdição – que incide sobre determinadas matérias (...) traduz a noção de que, nesses temas específicos, assiste ao Poder Judiciário não apenas o direito de proferir a última palavra, mas, sobretudo, a prerrogativa de dizer, desde logo, a primeira palavra (...).[49]

Tudo isto posto, é importante notar que os novos atores que detêm grandes quantidades de dados na internet possuem considerável poder sobre as vidas de seus usuários, comparável apenas ao que o próprio Estado detém. A diferença é que o Estado, conforme dissecado acima, depende, para acessar legitimamente um banco de informações, de uma série de ritos e procedimentos. Um detentor de uma rede, na prática, nem tanto.

Não se quer com essa colocação causar alarde: a reflexão proposta está muito mais centrada no debate acerca da regulamentação da tutela dessas coleções, com parâmetros claros e proteções bem delimitadas.

Não nos parece razoável, por exemplo, que um mesmo detentor possua todos os dados de geolocalização, os dados de cadastro, os dados de conversas e os *cookies* de pesquisa de um mesmo indivíduo sem que, ao menos, veja-se obrigado a estabelecer regras de integridade na gestão dessa coleção. Esse conjunto de dados dá ao detentor poder semelhante

---

[49] Supremo Tribunal Federal, Mandado de Segurança nº 23452, Min. Rel. Celso de Mello, j. 16.09.1999.

ou superior ao do Estado na sociedade em rede – com pouca ou nenhuma regulação.

Há quem diga que a criptografia de ponta a ponta é capaz de solucionar parte desse problema. É, em boa parte, verdade já que retira – teoricamente – o controle do banco de dados dos proprietários das coleções. Mesmo assim, é impossível ter inequívoca certeza de que os demais componentes de uma coleção não sejam capazes de, mesmo que excluídas conversas, por exemplo, indicar os comportamentos dos usuários de uma aplicação. E isso se, de fato, os detentores das aplicações estabelecerem uma criptografia sem domínio de chaves privadas dos usuários – algo jamais comprovado empiricamente até esse ponto da história.

O desafio é imenso: a intimidade e a vida privada sofrem modificações constantes diante dessas coleções de dados. Talvez o maior campo de impacto esteja, como se verá a seguir, na democracia.

As eleições estadunidenses de 2016 deram um vívido exemplo disso: desde uma investigação para apurar se a Rússia interferiu de alguma maneira para favorecer um dos candidatos majoritários, até o cruzamento de dados que levavam a crer que eleitores de um estado decisivo ("swing state") iriam às urnas enquanto os de outro não. Trump venceu a eleição justamente por ganhar nos colégios de delegados nestes estados, mesmo ficando atrás em números absolutos. *Cookies* já são bem mais importantes do que as pesquisas eleitorais jamais foram – eles *aprendem* as atitudes dos eleitores a partir dos dados inseridos inconscientemente pelos próprios cidadãos.

Não bastasse isso, percebemos de forma significativa um fenômeno que já contabiliza pelo menos meia década: a programação massiva de robôs algorítmicos, os *bots*, para a disseminação de notícias falsas, que certamente influenciaram parte do eleitorado, como se verá adiante.

No Brasil, há relatos do uso desse tipo de robô pelo menos desde as eleições de 2012 e é possível que a tática tenha sido decisiva para a vitória de Marcelo Crivella sobre Marcelo Freixo nas eleições para a prefeitura do Rio de Janeiro em 2016.[50]

Antes disso, nas eleições presidenciais de 2014, Dilma Rousseff (PT) apresentou

[50] ALBUQUERQUE, Ana Luiza. Eleição no Rio tem tática 'antiboato' e suspeita de uso de robôs. Folha de São Paulo, online, 18.10.2016. Disponível em: <http://www1.folha.uol.com.br/poder/eleicoes-2016/2016/10/1823713-eleicao-no-rio-tem-tatica-antiboato-e-suspeita-de-uso-de-robos.shtml>. Acessado em: 02.07.2017.

uma representação no Ministério Público Eleitoral contra a campanha de Aécio Neves (PSDB) pelo suposto uso de robôs nas redes sociais.[51] Aécio Neves, por sua vez, foi ao judiciário para que o Twitter liberasse os dados cadastrais de 66 perfis que, de acordo com sua campanha, formavam uma rede de disseminação de mentiras contra o tucano.[52]

Por uma via ou por outra, os dados informáticos – e o acesso a eles – podem decidir eleições nos EUA ou no Brasil. Esse o poder de fogo dessas coleções, daí, também, todo o interesse de grandes corporações em colecioná-los.

Os ativistas da privacidade de dados contra-atacam com novas técnicas e tecnologias de proteção da intimidade dos usuários: a criptografia e a *Blockchain* são a ponta do futuro. Trataremos delas diante. As criptomoedas, por exemplo, utilizam-se de ambas para entregar ao detentor um meio privado, e – em boa parte – seguro, de manter ativos fora do alcance de autoridades fiscais. Além de eleitor, o cidadão é um consumidor e usuário de produtos inserido numa economia capitalista.

Em meio a tudo isso, é importante notar que o Brasil estabeleceu em 2014 uma legislação moderna de proteção da rede – mas não dos dados –, que deu boa proteção aos seus cidadãos, o Marco Civil da internet e seu respectivo decreto regulamentador. Ao mesmo tempo, porém o país está bastante atrasado na legislação específica de dados: ao contrário de vários outros países, ainda não contamos com uma Lei Geral de Proteção de Dados. No aspecto penal, então, é seguro dizer que não há qualquer norma suficiente. Por isso, importante pontuar o debate com observações advindas da pesquisa.

### 1.2.1 Fake News

O fenômeno das notícias falsas não é novo: segundo ROBERT DARNTON, elas existem pelo menos desde o século VI, quando o historiador bizantino Procópio arruinou a reputação do Imperador Justiniano com um texto intitulado "Anedokta".[53] O primeiro registro

---

[51] UMPIERRE, Flávia. Dilma vai à Justiça contra os robôs de Aécio. *Agência PT de Notícias*, online, 10.10.2014. Disponível em: <http://www.pt.org.br/dilma-vai-a-justica-contra-os-robos-de-aecio>. Acessado em 02.07.2017.
[52] MENEZES, Enzo. Aécio Neves aciona Twitter na Justiça para ter acesso a dados de 66 usuários *R7*, online, 08.09.2014. Disponível em: <http://noticias.r7.com/eleicoes-2014/aecio-neves-aciona-twitter-na-justica-para-ter-acesso-a-dados-de-66-usuarios-08092014>. Acessado em 05.07.2017.
[53] "E as notícias falsas sempre existiram. Procópio foi um historiador bizantino do século 6 famoso por escrever a história do império de Justiniano. Mas ele também escreveu um texto secreto, chamado 'Anekdota', e ali ele

detalhado que o ocidente testemunhou uma primeira difusão escrita de um boato como notícia verdadeira data de 1755, quando um grande terremoto atingiu Lisboa. Mais especificamente, foram divulgados na ocasião os panfletos de *relações de sucessos* que, segundo ARAÚJO, eram "histórias tipicamente distorcidas que continham omissões, elementos de fantasia, negligência e incerteza"[54] difundiram a "notícia'' de que uma aparição da Virgem Maria teria salvo as vidas de alguns dos sobreviventes.

Os jornais com informações apuradas, como conhecemos hoje, apenas se popularizaram no século XIX. De fato, foi só a partir do lançamento do *New York Times*, em 1896, que o modelo de negócios de jornais diários de notícias como fonte fiável de informação se popularizou no ocidente. Mesmo naquela época, ainda eram comuns as publicações que mixavam notícias verdadeiras e exageradas – bom exemplo disso era o *Morning Journal* de William Randolph Hearst (inspiração mais tarde para personagem principal de Cidadão Kane de Orson Welles) que incentivou, em boa medida com notícias falsas ou, no mínimo, bastante infladas, a guerra hispano-americana.[55]

Na contemporaneidade, a internet trouxe novos desafios também na aferição de veracidade das notícias que são divulgadas, agora em meios sociais expandidos e potencializados pela conexão em rede. Os últimos anos certamente consistiram no ápice da circulação de notícias falsas em toda a história da humanidade. Se antes a limitação de um boato dificilmente transpassava os limites de uma cidade ou, quando muito, de um país, hoje um boato torna-se global sem grandes dificuldades, com consequências imprevisíveis.

---

espalhou "fake news", arruinando completamente a reputação do imperador Justiniano e de outros. Era bem similar ao que aconteceu na campanha eleitoral americana." (VICTOR, Fabio. Notícias falsas existem desde o século 6, afirma historiador Robert Darnton. *Folha de São Paulo*, online, 19.02.2017. Disponível em: <http://www1.folha.uol.com.br/ilustrissima/2017/02/1859726-noticias-falsas-existem-desde-o-seculo-6-afirma-historiador-robert-darnton.shtml>. Acessado em 30.07.2017.)

[54] "These typically distorted accounts contained omissions, elements of fantasy, sloppiness and uncertainty. They were short-lived and hastily written. Distributed by blind sellers, they were the main sources of information for the illiterate". (ARAÚJO, Ana Cristina. The Lisbon Earthquake of 1755 – Public Distress and Political Propaganda. *E-JPH*, Brown University, vol. 4, n.01, verão 2006. Disponível em https://www.brown.edu/Departments/Portuguese_Brazilian_Studies/ejph/html/issue7/html/aaraujo_main.html. Acessado em 20.07.2017.)

[55] "In the 1890s, plutocrats like William Randolph Hearst and his *Morning Journal* used exaggeration to help spark the Spanish-American War. When Hearst's correspondent in Havana wired that there would be no war, Hearst—the inspiration for Orson Welles' *Citizen Kane*—famously responded: "You furnish the pictures, I'll furnish the war." Hearst published fake drawings of Cuban officials strip-searching American women—and he got his war." (SOLL, Jacob. The Long and Brutal History of Fake News. *Politico*, online, 18.12.2016. Disponível em: <http://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535> Acessado em 21.07.2017.)

Com o avanço da tecnologia, testemunhamos a difusão de casos nada críveis vendidos como notícias verdadeiras [56].

O principal meio de difusão deste tipo de "informação" tem sido as redes sociais[57]. Em 2016 o Pew Research Center apurou que 62% dos americanos adultos usuários de redes sociais buscavam nessas redes fonte do que consideram notícia (66% dos usuários do Facebook, 59% dos usuários do Twitter, 70% dos usuários do Reddit, entre outros). Dos usuários pesquisados que buscam notícias nas redes sociais, 64% declararam que têm uma única fonte de informação na rede – para a maior parte deles essa fonte é o Facebook.[58]

Nesse cenário, a difusão de notícias falsas tem poder social que não pode ser ignorado. O próprio Facebook foi alvo de uma notícia falsa no começo de 2016 que dava conta de que ex-funcionários da empresa teriam declarado que a rede social "suprimiu rotineiramente publicações e notícias tidas como de caráter conservador"[59]. Reportagens de jornais respeitados

---

[56] O nível baixo e o caráter perigoso de algumas *fake news* ocorreu em Washington, nos Estados Unidos, quando um atirador chegou ao ponto de invadir uma pizzaria, diante da notícia falsa de que o local integraria uma rede de pedofilia comandada por Hillary Clinton, uma das lideranças políticas do Partido Democrata naquele país. Cf. KANG, Cecilia; GOLDMAN, Adam. In Washington Pizzeria Attack, Fake News Brought Real Guns. The *New York Times*, online, 05.12.2016. Disponível em: < https://www.nytimes.com/2016/12/05/business/media/comet-ping-pong-pizza-shooting-fake-news-consequences.html>. Acesso em 22 jul.2017.

[57] Redes sociais podem ser definidas como serviços *web-based* que permitem aos indivíduos: (a) criar um perfil em determinado sistema comum aos demais usuários daquele serviço; (b) articular listas de outros usuários com quem são realizadas interações sociais em níveis definidos pelo *site*; e (c) visualizar e transitar entre suas listas de conexão e aquelas construídas pelos outros usuários. O traço característico das *social networks* seria que estas não apenas permitem que os sujeitos conheçam estranhos, mas o fato de que também viabilizam uma articulação e exposição pelos usuários de suas conexões sociais, potencializando a criação de laços interpessoais que não seriam possíveis em formas pretéritas de interação social. Cf. BOYD, D. M.; Ellison, N. B. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, n. 13, p. 210–230, 2007. Complexificando o tema, Daniel Trottier and Christian Fuchs afirmam que, a rigor, todos os sistemas computacionais e aplicativos virtuais poderiam ser considerados como "mídias sociais", na medida em que armazenam e transmitem conhecimento humano gestado no avanço das relações sociais. No entanto, redes sociais como atualmente conhecidas se caracterizam por um componente adicional, o qual permite novas formas de relação intersubjetiva. Segundo estes autores, a delimitação do *como* e do *quão* social uma rede é dependeria de como ela se estrutura, considerando três paradigmas de sociabilidade: (a) *cognição* (processos informacionais como websites de jornais e outros periódicos); (b) *comunicação*, característica de ferramentas que permite uma interação mais direta entre atores sociais (é o caso de meios não mais tão recentes, como o *e-mail*); e (c) *cooperação*, presente em sistemas pensados a partir de um conceito de comunidade e trabalho colaborativo entre os usuários (é o caso, por exemplo, do Facebook e da Wikipedia). TROTTIER, Daniel; FUCHS, Christian. Theorising social media, politics and the State: na introduction. In: TROTTIER, Daniel; FUCHS, Christian (ed.). *Social media, politics and the State:* protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and Youtube. Nova York: Routledge, 2015, p. 4-6.

[58] GOTTFRIED, Jeffrey; SHEARER, Elisa. News Use Across Social Media Platforms. *Journalism.org*, online, 26.05.2016. Disponível em: <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016>. Acesso em 22.07.2017.

[59] NUNEZ, Michael. Former Facebook workers" we routinely suppressed conservative News. *Gizmodo*, online, 05.09.2016. Disponível em <http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006>. Acesso em 22.07.2017.

se seguiram ao suposto vazamento e revelaram que a plataforma teria inclusive impulsionando fatos ligados a candidatos do partido democrata e deliberadamente sabotado Republicanos nas eleições de 2012[60]. Tudo falso – ou um "engano", como preferiram os periódicos.

A notícia nunca encontrou uma evidencia crível que a comprovasse, mas foi capaz de causar impacto severo à imagem pública da rede social. Em agosto de 2016 o Facebook demitiu toda a equipe de moderadores e os substituiu na função por uma equipe de engenheiros que desenvolveram um algoritmo que selecionaria as notícias que eram mais lidas[61].

O alcance e o grau de sucesso desta iniciativa, no entanto, mostra-se passível de dúvidas: ainda em 2016, às vésperas de um 11 de setembro, uma das notícias que lideravam a lista de mais lidas da rede social – ganhando ainda mais audiência como *trending topic* – dava como verdadeira a já antiga teoria conspiratória de que o World Trade Center na verdade fora implodido[62].

Diante disso, o Washington Post elaborou um teste empírico para provar o novo algoritmo de organização de "mais lidos" da rede social. Os repórteres do periódico rapidamente concluíram que o novo algoritmo "continua repetidamente repercutindo notícias falsas"[63] desde que o Facebook demitiu a equipe de editores. É impossível saber ao certo se

---

[60] Diversas reportagens da imprensa especializada deram conta de tais denúncias, entre elas, Gizmodo (cf. nota de rodapé anterior), The Guardian (BOWLES, Nellie; THIELMAN, Sam. Facebook accused of censoring conservatives, report says. *The Guardian*, online, 09.05.2016. Disponível em <https://www.theguardian.com/technology/2016/may/09/facebook-newsfeed-censor-conservative-news>.) e The Telegraph (TITCOMB, James. Facebook denies it censors right-wing news after political bias claims. *The Telegraph*, online, 10.05.2016. Disponível em: http://www.telegraph.co.uk/technology/2016/05/10/facebook-denies-it-censors-right-wing-news-after-political-bias/ ). Acesso em 22.05.2016.

[61] Cf. WONG, Joon Ian; GERSHGORN, Dave; MURPHY, Mike. Facebook is trying to get rid of bias in Trending news by getting rid of humans. *Quartz*, online, 26.08.2016. Disponível em: <https://qz.com/768122/facebook-fires-human-editors-moves-to-algorithm-for-trending-topics>. Acessado em 05.08.2016.

[62] "Facebook users looking for more context on why the Sept. 11 terrorist attack anniversary was trending on the platform on Friday were, for a time, directed to a tabloid article claiming that "experts" had footage that "proves bombs were planted in Twin Towers." The Daily Star piece promoted by Facebook repeats a lot of common claims from 9/11 "trutherism," a conspiracy theory based on an idea (unsupported by any actual evidence) that the World Trade Center must have collapsed in 2001 because of a "controlled demolition" and not from the damage caused by the airliner crashes. "Facebook's trending topics promoted an article "trutering" the Sept. 11 attacks" (OHLHEISER, Abby. Facebook's trending topics promoted an article 'truthering' the Sept. 11 attacks. *The Washington Post*, online, 09.09.2016. Disponível em: <https://www.washingtonpost.com/news/the-intersect/wp/2016/09/09/an-article-truthering-the-sept-11-attacks-just-trended-on-facebook/?utm_term=.54671f5a14b9> Acessado em 05.08.2017.)

[63] Cf. DEWEY, Caitlin. Facebook has repeatedly trended fake news since firing its human editors. *The Washington Post*, online, 12.10.2016. Disponível em: <https://www.washingtonpost.com/news/the-intersect/wp/2016/10/12/facebook-has-repeatedly-trended-fake-news-since-firing-its-human-editors/?utm_term=.b8f7c824f579>. Acessado em 05.08.2017.

robôs causaram o fenômeno ou se as pessoas acessam notícias falsas com tamanha intensidade a ponto de torná-las relevantes.

O que leva alguém a investir na disseminação de notícias falsas? Há várias respostas para esse questionamento. A mais óbvia delas é a financeira: propagar notícias falsas em redes sociais pode ser uma boa fonte de renda em algumas partes de um mundo globalizado caracterizado por economias integradas[64]; a outra tem cunho mais ideológico, no sentido de difundir *fake news* para atingir determinada ideia, agenda, organização, movimento ou agente político[65]. Ambas as possibilidades ensejam sérias preocupações no que concerne à intimidade dos internautas. A disseminação de notícias falsas pode levar à definição de aspectos ideológicos dos indivíduos – ou, pelo menos, à sua reafirmação –, prejudicando a formação de convencimentos em espaços sociais que deveriam viabilizar níveis mais adequados de simetria informacional. Os algoritmos de redes sociais favorecem a criação de vínculos "em bolha", facilitando as interações entre os usuários que compartilham de similares interesses, opiniões, localizações etc. – fenômeno conhecido pela literatura especializada como *filter bubble*.[66]

O problema nisso é que, enquanto no século passado havia maior conhecimento acerca de quem eram os *gatekeepers* da informação – os editores dos veículos de comunicação –, podendo-se, até certo ponto, escolher os meios de informação e comparar opiniões em meridianos opostos do espectro político, na internet os algoritmos assumiram este papel de *gatekeepers* informacionais. O cidadão comum perdeu, em boa parte, a capacidade de tomar contato com notícias e opiniões diversas das suas próprias e do seu círculo imediato de contatos. ALLCOTT e GENTZKOW destacam que, graças a esse novo paradigma, na era da sociedade em

---

[64] SUBRAMANIAN, Samanth. Inside the Macedonian fake-news complex. *Wired*, online, 15.02.2017. Disponível em: <https://www.wired.com/2017/02/veles-macedonia-fake-news>. Acessado em 05.08.2017.

[65] ALCOTT, H.; GENTZKOW, M. Social Media and Fake News in the 2016. *Journal of Economic Perspectives*, vol. 31, n. 2, primavera 2017. Disponível em https://web.stanford.edu/~gentzkow/research/fakenews.pdf. Acesso em: 05/08/2017. "There appear to be two main motivations for providing fake news. The first is pecuniary: news articles that go viral on social media can draw significant advertising revenue when users click to the original site. This appears to have been the main motivation for most of the producers whose identities have been revealed. The teenagers in Veles, for example, produced stories favoring both Trump and Clinton that earned them tens of thousands of dollars (Subramanian 2017). Paul Horner produced pro-Trump stories for profit, despite claiming to be personally opposed to Trump (Dewey 2016). The second motivation is ideological. Some fake news providers seek to advance candidates they favor. The Romanian man who ran endingthefed. com, for example, claims that he started the site mainly to help Donald Trump's campaign (Townsend 2016). Other providers of right-wing fake news actually say they identify as left-wing and wanted to embarrass those on the right by showing that they would credulously circulate false stories (Dewey 2016; Sydell 2016)." (ALCOTT, H.; GENTZKOW, M. *Social*… cit., p. 221.)

[66] PARISER, Eli. Tenha cuidado com os "filtros-bolha". *TED Talks*, online. Disponível em: <https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=pt-br>. Acesso em 09.09.2017.

rede "um indivíduo sem qualquer histórico ou reputação pode, em alguns casos, alcançar tantos leitores quanto a Fox News, CNN ou The New York Times"[67], bastando que a sua postagem seja compartilhada de forma massiva por apoiadores de um determinado ponto de vista.

A discussão sobre *fake news* tem garantido especial força no contexto político estadunidense. Em 2016, o jornal New York Times elaborou um estudo sobre uma notícia falsa circulada em meio ao processo eleitoral local, consistindo no rumor de que uma manifestação espontânea anti-Trump na cidade de Austin seria iniciativa de um comboio de apoiadores de Hillary Clinton, então candidata à presidência pelo Partido Democrata – o que veio a se demonstrar uma inverdade[68]. A notícia falsa foi construída especialmente a partir da postagem, por um apoiador do candidato de oposição pelo Partido Democrata, Donald Trump, de uma imagem de um comboio de ônibus estacionado em Austin. Foi o que bastou para que a "notícia" se espalhasse, chegando até mesmo a ser tuitada pelo agora Presidente dos EUA.[69] Trump, aliás, mostra-se como interessante caso ilustrativo do fenômeno das notícias falsas, na medida em que sua figura é frequentemente associada à divulgação daquilo que ele próprio e sua equipe denominam como "verdades alternativas" (*alternative facts*)[70]. Desde sua posse como presidente dos Estados Unidos, em 2017, Trump tem se referido a veículos jornalísticos tradicionais que não apoiaram a sua candidatura como propagadores de *Fake News*, em um uso distorcido do termo que parece visar a construção de narrativas sobrepostas, de forma politicamente orientada.

No campo ideológico, as notícias falsas certamente têm papel supranacional. Há uma guerra de desinformação na internet, com *players* importantes no cenário geopolítico mundial, destacando-se os EUA, a Rússia e a China.

---

[67] ALCOTT, H.; GENTZKOW, M. Social Media and Fake News in the 2016. *Journal of Economic Perspectives*, vol. 31, n.2, 2017. Disponível em: <https://web.stanford.edu/~gentzkow/research/fakenews.pdf>. Acesso em: 09.09.2017.

[68] MAHESHWARI, Sapna. How fake news Goes Viral: A case study. *The New York Times*, online. Disponível em: <https://www.nytimes.com/2016/11/20/business/media/how-fake-news-spreads.html>. Acesso: 09.09.2017.

[69] Disponível em: https://twitter.com/realDonaldTrump/status/796900183955095552?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwww.nytimes.com%2F2016%2F11%2F20%2Fbusiness%2Fmedia%2Fhow-fake-news-spreads.html. Acesso em: 09.09.2017.

[70] SWAINE, Jon. Donald Trump's team defends alternative facts after widespread protests. *The Guardian*, online, 23.01.2017. Disponível em: <https://www.theguardian.com/us-news/2017/jan/22/donald-trump-kellyanne-conway-inauguration-alternative-facts>. Acessado em 06.08.2017.

As campanhas de desinformação são uma criação soviética. O próprio termo "desinformação" deriva da palavra "dezinformatsiya" – o nome que designava o departamento de contrapropaganda da KGB[71]. Nos últimos anos, a Rússia vem intensificando o uso da desinformação como tática de influência geopolítica.

A Guerra da Criméia e o ataque de um míssil russo ao voo MH17 da Malasya Airlines, que matou 283 pessoas são exemplos disso.[72] No primeiro caso, a Rússia atacou deliberadamente uma região da Ucrânia, anexada posteriormente ao território russo, e negou continuamente a presença de tropas suas na região, notadamente por notícias falsas disseminadas pela internet, enquanto na verdade o seu exército tomava de assalto a península da Criméia – importante ponto geoestratégico.

No segundo, o exército russo, ainda no contexto da guerra na Criméia, derrubou um avião de passageiros da Malaysia Airlines, ao que tudo indica, por engano, com o uso de um dos mais poderosos mísseis do tipo terra-ar disponíveis no seu armamento, o BUK. A Rússia negou – e continua negando – o ataque e promoveu uma campanha de falsas notícias dando conta de que fora o exército ucraniano o responsável pela tragédia. Uma investigação independente, liderada pela Holanda, país de onde o avião decolou e de nacionalidade da maior parte dos passageiros, provou que fora a Rússia a responsável.

Durante as investigações, a comissão de investigadores foi constantemente atacada, inclusive com a disseminação de notícias falsas e com reiteradas tentativas de furto de dados por hackers provavelmente apoiados pelo governo russo.[73]

Todavia, o caso mais representativo na campanha russa de promoção de notícias falsas é certamente a tentativa deliberada do Kremlin em intervir no cenário eleitoral americano em 2016. WEISBURG, WATTS e BERGER alertam que o objetivo dos russos está longe do apoio ao nome de Trump para a presidência. Segundo bem observam os autores, a campanha atual de

---

[71] JOWETT, G., O'DONELL, V. *Propaganda and Persuasion*, Londres: Sage Publications, 2005 p. 21–23.
[72] POLLOCK, John. Russian Desinformation Technology. MIT Technology Review, online, 13.04.2017. Disponível em: <https://www.technologyreview.com/s/604084/russian-disinformation-technology>. Acessado em 05.08.2017.
[73] Idem.

desinformação quer "manchar e diminuir" a democracia estadunidense, "produzindo um eleitorado dividido e um presidente sem um mandato claro para governar"[74].

O Twitter tem se mostrado uma das principais vias para a realização destas sofisticadas iniciativas. Análises indicam que robôs controlados possivelmente controlados pelo governo russo estariam disseminando notícias de forma estratégica, explorando fragilidades políticas e características pessoais de agentes políticos dos Estados Unidos. Exemplo disso se deu no caso Nicole Mincey, usuária da rede Twitter sob o endereço "@ProTrump45", e que teria feito elogios ao presidente norte-americano e a sua forma de governar. Em um curto espaço de tempo, Trump repostou os elogios que teria recebido de Mincey. O problema nisso é que se apurou que tal usuária, em verdade, sequer existia, tendo a conta correspondente sido posteriormente suspensa pelo Twitter. A partir disso, levantou-se a suspeita de que o perfil teria sido criado por um robô russo para atrair a atenção e influenciar as escolhas do presidente dos EUA.[75] Em dado momento, Nicole tinha mais de 150 mil seguidores, os quais não puderam ser identificados como pessoas reais ou outros robôs, seguidos por ela também para passarem a falsa impressão de que consistiam em usuários populares na rede social.[76]

Em resposta a problemas como esse, pesquisadores e professores de universidades norte-americanas criaram uma aplicação que passou a monitorar os movimentos de prováveis robôs algoritmos que controlam contas de Twitter a partir da Rússia – o denominado projeto *Hamilton 68*.

---

[74] "But most observers are missing the point. Russia is helping Trump's campaign, yes, but it is not doing so solely or even necessarily with the goal of placing him in the Oval Office. Rather, these efforts seek to produce a divided electorate and a president with no clear mandate to govern. The ultimate objective is to diminish and tarnish American democracy. Unfortunately, that effort is going very well indeed. Russia's desire to sow distrust in the American system of government is not new. It's a goal Moscow has pursued since the beginning of the Cold War. Its strategy is not new, either. Soviet-era "active measures" called for using the "force of politics" rather than the "politics of force" to erode American democracy from within. What is new is the methods Russia uses to achieve these objectives." (WEISBURD, A., WATTS, C., BERGER, JM., *Trolling for Trump:* how Russia is trying to destroy our democracy. *War on Rocks*, online. 11.2016. Disponível em: <https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy>. Acessado em 07.08.2017.)

[75] PHILLIP, Abby. The curious case of Nicole Mincey, the Trump fan who may be a bot. *The Washington Post*, online, 07.08.2017. Disponível em https://www.washingtonpost.com/politics/the-curious-case-of-nicole-mincey-the-trump-fan-who-may-actually-be-a-russian-bot/2017/08/07/7aa67410-7b96-11e7-9026-4a0a64977c92_story.html?utm_term=.d41bf6befc45 Acessado em 07.08.2017.

[76] PHILLIP, Abby. Para especialistas, fã de Trump em rede social pode ser robô russo. *Folha de São Paulo*, online, 09.08.2017. Disponível em: http://www1.folha.uol.com.br/mundo/2017/08/1908419-fa-de-donald-trump-em-rede-social-talvez-seja-um-robo-russo.shtml. Acessado em 09.08.2017.

De acordo com os dados do mecanismo, os robôs russos foram responsáveis por disseminar a hashtag #FireMcMaster (*#DemitaMcMaster*) em julho de 2017. Herbert Raymond McMaster é um general de cinco estrelas, assessor de Donald Trump para assuntos de segurança nacional. Os robôs "pediam" a demissão do general depois de McMaster demitir dois outros integrantes do Conselho de Segurança Nacional.[77] O movimento foi tão forte que obrigou Trump a fazer uma declaração pública defendendo o assessor.[78]

Os robôs de algoritmos podem ir além. BESSI e FERRARA estimaram em estudo que havia 400.000 contas do Twitter comandadas por robôs nas eleições de 2016 nos EUA. Essas contas foram responsáveis por 3.8 milhões de postagens no mês que antecedeu as eleições, algo em torno de 20% de todas as postagens sobre o tema no período pesquisado. A intervenção, segundo esses pesquisadores foi capaz de distorcer os debates online sobre o tema.[79] O FBI abriu uma investigação para apurar até que ponto os russos interferiram no resultado da eleição.

Há outros exemplos claros da afetação de eleições majoritárias por *bots.* A França também teve suas eleições afetadas por robôs em maio de 2017. Na semana das eleições presidenciais francesas, um pacote de dados contendo fotos e dados bancários do presidenciável Emanuel Macron foi vazado no influente fórum de hackers ''/pol/'', que fica hospedado no site de anonimato 4chan.org.[80] O escândalo que se seguiu ao vazamento ficou conhecido como *McaronLeakes.* A Equipe de Macron reconheceu que dados haviam sido furtados, mas alegou que o então candidato não era o dono de todos os documentos bancários apresentados, muitos dentre os quais davam conta da existência de contas bancarias supostamente não declaradas por Macron.

Nos dias que se seguiram que o ataque na verdade fora orquestrado pelo 28 APT, também conhecido como Fancy Bear, um grupo de hackers que é provavelmente parte do Diretório Central de Inteligência Russo, a principal agencia de inteligência daquele país.[81]

---

[77] Hamilton 68. Disponível em http://dashboard.securingdemocracy.org/ Acessado em 10.08.2017.
[78] BORGER, Julian. A good man, very pro-Israel: Trump defends McMaster from far-right snipers. *The Guardian*, online, 05.08.2017. Disponível em: <https://www.theguardian.com/us-news/2017/aug/05/donald-trump-hr-mcmaster-israel-breitbart>. Acessado em 10.08.2017.
[79] BESSI, A.; FERRARA, E. Social bots distort the 2.016 U.S. Presidential election discussion. *First Monday*, vol. 21, n.11. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653a#p4>. Acessado em 08.08.2017.
[80] MOHAN. Megha. Macron Leaks: the anatomy of a hack. *BBC*, online, 09.05.2017. Disponivel em: <http://www.bbc.com/news/blogs-trending-39845105>. Acessado em 12.08.2017.
[81] THIELMAN, Sam; ACKERMAN, Spencer. Cozy Bear and Fancy Bear: did Russians hack democratic party and if so, why? *The Guardian*, online, 29.07.2016. Disponível em:

Desde o momento em que os dados vazaram, robôs algoritmos que estavam desativados desde o término das eleições estadunidenses passaram a imediatamente distribuir o conteúdo.

FERRARA, em mais um estudo, concluí que nem todos esses *bots* eram controlados por um governo – o russo como principal candidato: parte deles estava provavelmente sob controle de ultradireitistas norte-americanos, ao que indicam os dados de análise. O movimento pode indicar que além do domínio geopolítico-estratégico de governos, pode existir um mercado negro de robôs algoritmos que controlam contas de redes sociais para espalhar notícias.[82]

A questão é bastante mais profunda do que parece. FERRARA, VAROL, DAVIS e MENCZER, em outro artigo, argumentam que a dificuldade real está em estabelecer a veracidade da informação oferecida, o que, conforme bem acentuam, sempre foi um problema. Segundo os pesquisadores "o novo desafio trazido pelos robôs está no fato de que eles podem passar a falsa impressão de que algumas partes da informação, apesar de imprecisas, são altamente aceitas, exercendo influencia num campo em que nós ainda não desenvolvemos anticorpos"[83].

Esses robôs contaram com avanços significativos nos últimos anos e conseguem agora predizer e emular comportamentos humanos com relativa facilidade. Podem até buscar na rede informações que preencham seus perfis e imitar padrões de publicações de humanos[84] e são capazes de se envolver em discussões populares para, com publicações baseadas em palavras-chave, adquirir a confiança de usuários reais que passam a segui-los.

---

<https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc>. Acessado em 12.08.2017.

[82] FERRARA, E. *Desinformation and social bot operations in the run up to the 2017 french presidential election.* University of Southern California. Disponivel em: <https://arxiv.org/ftp/arxiv/papers/1707/1707.00086.pdf>. Acesso em 09.09.2017.

[83] "The problem is not just establishing the veracity of the information being promoted—this was an issue before the rise of social bots, and remains beyond the reach of algorithmic approaches. The novel challenge brought by bots is the fact they can give the false impression that some piece of information, regardless of its accuracy, is highly popular and endorsed by many, exerting an influence against which we haven't yet developed antibodies. Our vulnerability makes it possible for a bot to acquire significant influence, even unintentionally.2 Sophisticated bots can generate personas that appear as credible followers, and thus are more difficult for both people and filtering algorithms to detect. They make for valuable entities on the fake follower market, and allegations of acquisition of fake followers have touched several prominent political figures in the U.S. and worldwide." (FERRARA, E. [et. al]. The rise of social bots. *Communications of the ACM*, vol. 59, n. 7, 2016. Disponível em https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext. Acessado em 14.08.2017.)

[84] CAO, Q [et al.]. Uncovering large groups of active malicious accounts in online social networks. *Proceedings of the 2014 ACM SIGSAC* – Conference on Computer and Communications Security. Disponivel em <https://users.cs.duke.edu/~xwy/publications/SynchroTrap-ccs14.pdf>. Acessado em 14.08.2017.

Alguns deles aprendem a mimetizar tão bem um usuário real que podem se tornar um verdadeiro "clone" de um perfil verdadeiro.[85]

Há um paradoxo nas redes: não é mais possível saber se um usuário é real ou se ele é um robô utilizando-se do conjunto de informações de um usuário real para mimetizá-lo. Esse tipo de comportamento pelos detentores desse tipo de tecnologia, meio principal de disseminação de notícias falsas, representa um sério desafio para a intimidade dos usuários da rede, que veem seus dados subtraídos para a construção de perfis falsos.

A par disso tudo, é certo que o aumento de postagens e compartilhamentos – por usuários reais ou robôs – beneficia os detentores das redes socais na medida em que torna possível o oferecimento aos anunciantes de um público maior e mais ativo, que busca incessantemente novidades em sua rede.

É importante notar que os padrões de dados que alimentam as escolhas algorítmicas não emergiriam "naturalmente", mas são, eles próprios, derivados dos dados de navegação que alimentamos continuamente. Portanto, a geração de todo o conteúdo de procedência duvidosa, sejam os robôs, sejam as notícias falsas por eles distribuídas, origina-se do uso dos nossos dados de navegação. De acordo com MAGALHÃES:

> Dados de sociedades estruturalmente desiguais, como a nossa, inevitavelmente representarão essas desigualdades, mesmo que de maneira indireta e não intencional (...) sistemas algorítmicos também parecem afetar nossa liberdade de expressão e informação. Se a visibilidade é escassa, ela precisa ser conquistada. Mas a luta pela visibilidade algorítmica em redes sociais pode implicar na mimetização de comportamentos, assuntos e linguagem que o usuário imagina serem "populares", mas que não necessariamente correspondem ao que gostaria de dizer, numa espécie de homogeneização da expressão.[86]

---

[85] "To acquire visibility, they can infiltrate popular discussions, generating topically appropriate—and even potentially interesting— content, by identifying relevant keywords and searching online for information fitting that conversation. After the appropriate content is identified, the bots can automatically produce responses through natural language algorithms, possibly including references to media or links pointing to external resources. Other bots aim at tampering with the identities of legitimate people: some are identity thieves, adopting slight variants of real usernames, and stealing personal information such as pictures and links. Even more advanced mechanisms can be employed; some social bots are able to "clone" the behavior of legitimate users, by interacting with their friends and posting topically coherent content with similar temporal patterns." (FERRARA, E. [et. al]. The rise of social bots. *Communications of the ACM*, vol. 59, n. 7, 2016. Disponível em https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext. Acessado em 14.08.2017.)

[86] MAGALHÃES, João Carlos. Democracia e internet: precisamos falar sobre algoritmos. *Nexo*, online, 25.09.2016. Disponível em: <https://www.nexojornal.com.br/ensaio/2016/09/25/Democracia-e-internet-precisamos-falar-sobre-algoritmos>. Acesso em 09.08.2017.

Há, conforme a maior parte da população passa a se informar por plataformas digitais, e mesmo empresas jornalísticas tradicionais passam a depender dessas plataformas para distribuir seus produtos, a concessão jamais experimentada de poderes para atores privados sem uma regulação específica. De maneira diversa das revistas tradicionais e dos jornais, por exemplo, as redes sociais não são compreendidas ou cobradas enquanto verdadeiros veículos de mídia – que acabaram, voluntária ou involuntariamente, por se tornar. Nessa nova realidade, é impossível auferir os padrões editoriais que orientam os algoritmos.

Uma possível via de resolução do problema é o estabelecimento de *standards* de colaboração entre esses novos agentes privados difusores de notícias – as redes sociais – e o Estado – contanto que não representem ameaça à intimidade.

Afinal, além da democracia, a disseminação de robôs de algoritmos e das notícias falsas espalhadas por eles pode inclusive ameaçar as próprias redes sociais. Os responsáveis pela segurança da informação no Facebook, maior e mais notável rede, dizem, em *paper* recente, que vêm aumentando seus esforços de colaboração com as autoridades, e que planejam implementar técnicas de *machine learning* para coibir os abusos das *fake news*.[87] Contudo, depender de iniciativas advindas tão somente dessas redes não parece ser, contudo, uma opção desejável a longo prazo.

Diante das ameaças de alguns países em regulá-las[88-89], as redes têm começado a engendrar esforços para checar as notícias que os usuários veiculam[90-91]. sustentável e tem inclusive fomentado agências específicas com tal finalidade.[92] Todavia, é preciso ir além e

---

[87] WEEDON, Jen; NULAND, William; STAMOS, Alex. *Information Operations and Facebook* (versão 1.0). 27.04.2017. Disponível em: <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>. Acesso em 09.09.2017.

[88] COPLEY, Caroline. German minister says Facebook should be treated as a media company. *Reuters*, online, 17.11.2016. Acesso em: <http://www.reuters.com/article/us-germany-facebook-hatespeech-idUSKBN13C29A>. Acesso em 09.09.2017.

[89] CHASE, Jefferson. Facebook slams proposed German 'anti-hate speech' social media law. *DW*, online, 20.05.2017. Acesso em: <http://www.dw.com/en/facebook-slams-proposed-german-anti-hate-speech-social-media-law/a-39021094>. Acesso em 09.09.2017.

[90] HUNT, Elle. Disputed by multiple fact-checkers': Facebook rolls out new alert to combat fake news. *The Guardian*, online, 22.03.2017. Acesso em: <https://www.theguardian.com/technology/2017/mar/22/facebook-fact-checking-tool-fake-news>. Acesso em 09.09.2017.

[91] Fake news: Facebook and Google team up with French media. *BBC*, online, 06.02.2017. Acesso em: <http://www.bbc.com/news/world-europe-38882236>. Acesso em 09.09.2017.

[92] "To the extent that fake news imposes social costs, what can and should be done? In theory, a social planner should want to address the market failures that lead to distortions, which would take the form of increasing information about the state of the world and increasing incentives for news consumers to infer the true state of the world. In practice, social media platforms and advertising networks have faced some pressure from consumers and

estabelecer marcos de regulação que inibam a captura massiva de informações para distribuição dessas notícias, como se discutira mais adiante.

O combate à disseminação de notícias falsas deve ter na mesma mira a criação do efeito bolha. Não basta combater uma sem discutir eficazmente a outra. O caminho, nesse sentido, parece ser a cooperação do Estado com os detentores e administradores das redes sociais, para que se estabeleça uma via de difusão da informação que não viole a privacidade dos usuários, direta ou indiretamente, permitindo-se ainda o pensamento e a formação de convencimentos sem que haja interferências algorítmicas pouco perceptíveis aos usuários do serviço.

### 1.2.2 Blockchain

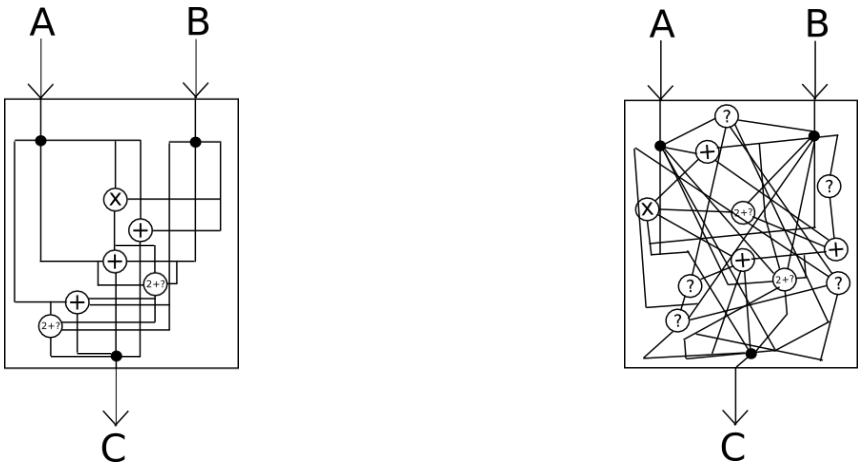
Conquanto as preocupações estatais com a segurança no meio digital sejam justificáveis, é necessário certo esforço intelectual dos agentes do Estado para compreender avanços legítimos e razoáveis da tecnologia. A criptografia, por exemplo, é das maiores benesses que se tem notícia na proteção dos dados. É preciso que os agentes públicos entendam que o uso dessa tecnologia por parte das aplicações disponíveis na rede não pretende encobrir malfeitos, mas proteger o sigilo informacional estratégico e o direito constitucional à intimidade.

Para se ter clareza no funcionamento da criptografia, valem os desenhos abaixo: na segunda figura é praticamente impossível de se alcançar o ponto C, o trabalho para alcançá-lo inviabiliza a tarefa – a capacidade computacional aplicada não é viável. Enquanto isso, na primeira figura há um caminho criptografado que, apesar de complexo, com as chaves criptográficas adequadas é facilmente encontrado[93]:

---

civil society to reduce the prevalence of fake news on their systems. For example, both Facebook and Google are removing fake news sites from their advertising platforms on the grounds that they violate policies against misleading content (Wingfield, Isaac, and Benner 2016). Furthermore, Facebook has taken steps to identify fake news articles, flag false articles as "disputed by 3rd party fact-checkers," show fewer potentially false articles in users' news feeds, and help users avoid accidentally sharing false articles by notifying them that a story is "disputed by 3rd parties" before they share it (Mosseri 2016). In our theoretical framework, these actions may increase social welfare, but identifying fake news sites and articles also raises important questions about who becomes the arbiter of truth." (ALCOTT, H.; GENTZKOW, M. *Social Media…* cit., p.233.)

[93] A imagem é de autoria desconhecida e circula há vários anos como exemplificação da criptografia como técnica de opacidade.




Uma das ferramentas que se desenvolveram de maneira mais notável nos últimos anos utilizando a criptografia foi a Bitcoin, a pioneira entre as criptomoedas. A Bitcoin tem por premissa a existência de uma rede de computadores que, interligados, possam confirmar a validade de uma cadeia de blocos de informação, a Blockchain.

A Blockchain é permanente, imutável, descentralizada e bem distribuída. Essa tecnologia registra as operações em sistema *P-2-P* (pessoa-para-pessoa) e está baseada em 4 fundamentos: o registro compartilhado das transações (*ledger*), o consenso para verificação das transações, um contrato que determina as regras de funcionamento das transações e finalmente, a criptografia, que é o fundamento de tudo. Processos complexos e lentos, suscetíveis a confirmações de vários níveis e expostos a furto de dados em toda a cadeia podem, com o uso dessa tecnologia, tornarem-se rastreáveis e permanentes.

Na Blockchain, os registros são encadeados, de forma que cada novo registro dependa do anterior. Esses registros são blocos de transações, daí o nome Blockchain (cadeia de blocos). Ao mesclar o conceito de um livro-razão, que contém as entradas contábeis de uma empresa e seu caráter distribuído, a Blockchain também passou a ser chamada de *distributed ledger* (livro-razão distribuído).

Eleito o processo que utilizará a tecnologia, inclui-se o Blockchain como uma camada intermediária de transações entre a camada de *systems of insight* e a camada de estrutura legada. Programam-se na Blockchain o contrato (regras de negócio aplicadas aos

sistemas) que são chamados de *chaincodes*[94] – os códigos de formação da cadeia. Nesta programação também são incluídos os níveis de acesso dos membros da rede às informações contidas no *ledger*. A partir daí, todas as novas transações serão registradas e operadas de acordo com o que foi programado.

Trata-se de uma maneira revolucionária de estocar e registrar informações online. Ela funciona como um grande registro público de dados em que cada bloco na cadeia de informações contém dados com contratos, registros de operações, provas de autenticidade, entre outras possibilidades. Cada bloco nessa cadeia está conectado de forma segura ao próximo por uma assinatura digital criptografada, o código *hash*. O *hash* de um bloco é único e representa ao final todas as informações contidas no bloco que ele "fechou" da cadeia. Assim, o próximo bloco não precisará conter toda a informação do bloco anterior – começará apenas com o *hash* do anterior.[95]

Com o crescimento da cadeia de blocos, a informação torna-se cada vez mais segura e estável, vez que cada novo bloco inserido legitima todos os anteriores, porque depende deles para existir. Com mais blocos e mais usuários, a tecnologia também ganha em segurança: a

---

[94] ANDERSON, D. L.; SHAPIRO, L. *Introduction to chain codes.* The mind Project – Consortium on cognitive Science Instruction. Disponível em <http://www.mind.ilstu.edu/curriculum/chain_codes_intro/chain_codes_intro.php>. Acessado em 20.08.2016.

[95] Aqui vale uma explanação maior, para os estudiosos: Uma função *hash* (ou função de dispersão) pode ser definida como uma função que recebe como entrada uma cadeia de tamanho arbitrário e dá como saída uma cadeia de tamanho fixo denominada valor de *hash*. O cálculo da saída da função deve ser computável eficientemente, em tempo linear sobre o tamanho da cadeia de entrada. Uma função hash criptográfica é uma função hash que é resistente a colisão, resistente a pré-imagem e resistente a segunda pré-imagem. Essas três propriedades estão relacionadas e seguem suas definições:
1. Resistência a colisão: Uma função *hash H* é considerada resistente a colisão se é impraticável encontrar duas cadeias, $x$ e $y$ , tal que $x \neq y$ , e $H(x) = H(y)$.
Intuitivamente, ela será resistente a colisão se é difícil encontrar duas mensagens com o mesmo valor de *hash*.
2. Resistência a pré-imagem (ou propriedade de mão-única): Uma função de *hash H* é considerada resistente a pré-imagem se, dado um valor de hash $y$, é impraticável computar qualquer cadeia de entrada $x$ tal que $H(x) = y$.
3. Resistência a segunda pré-imagem: Uma função *hash H* é considerada resistente a segunda pré-imagem se, dado uma cadeia $x$, é impraticável encontrar uma cadeia $y$, tal que $x \neq y$, e $H(x) = H(y)$.
Em relação às definições acima, o termo "impraticável" significa que a computação de um cálculo pode demandar tantos passos que é considerado impossível realizá-lo num tempo aceitável. Dada uma função hash cujas saídas tem comprimento $n$, é esperado encontrar uma colisão em $O(2n2)$ interações, por conta do paradoxo do aniversário. A quantidade de iterações necessárias para encontrar uma pré-imagem ou uma segunda pré-imagem é $O(2n)$, através de ataque de força bruta. Computações que requerem tempo exponencial são consideradas impraticáveis. Para se ter uma noção mais apurada, a quebra da chave criptográfica de uma mensagem de 16 bits (o equivalente ao texto "oi" enviado por mensagem de aplicativos como WhatsApp ou Telegam) por 1.000 computadores 1.000 vezes mais potentes que o mais potente computador atualmente (o chinês Sunway ThaihuLight) demoraria $2^{58}$ segundos – ou metade do tempo transcorrido desde o Big Bang. Sobre o tema, ler mais em SMART, Nigel Paul. *Cryptography*: an introduction. 3.ed. New York: McGraw-Hill, 2003 e em NARAYANAN, Arvind [et al.]. Bitcoin and Cryptocurrency Technologies. Draft, 2015.

Blockchain é baseada na checagem contínua de dados públicos, ou seja, se um usuário mal-intencionado inserir uma informação inverídica em blocos anteriores, o bloco ilegítimo não poderá ser encaixado na cadeia, tornando-se imprestável.

A ideia da Blockchain é bastante similar, por exemplo, a que norteia o funcionamento do Sistema Financeiro e as suas transações, com uma diferença fundamental: baseada num registro público difuso de informações, ela elimina a figura do intermediário, o "homem do meio" – no exemplo das criptomoedas, o banco. A Blockchain torna possível que uma pessoa transfira uma quantia em moeda digital para outro indivíduo sem precisar de nenhuma conta bancária, apenas registrando isso no bloco de informações que está sendo criado naquele momento.

Mas a funcionalidade da Blockchain vai muito além das transações bancárias: como qualquer tipo de dado pode ser gravado numa cadeia de informações desse tipo, a indústria de pedras preciosas, por exemplo, está usando a Blockchain para catalogar diamantes.[96] A tecnologia poderia também simplificar sobremaneira os registros cartoriais, evitar a falsificação de medicamentos e melhorar o rastreio de animais ou mercadorias desde a sua origem. Basta registrar todos esses dados em blocos.

Essa cadeia de dados permite ainda a criação dos *smart contracts,* contratos inteligentes que podem ser executados automaticamente desde uma ordem pré-agendada na cadeia de informações. Os *smart contracts* são contratos escritos em código de computador que se diferenciam de suas contrapartes jurídicas por serem autoexecutáveis, isto é, uma vez aceitos, cumprem automaticamente o acordo estabelecido nas linhas de código, ou garantem que este seja cumprido. Um *smart contract* de compra e venda de um imóvel poderia tornar a transação tão simples quanto uma compra num mercado local: uma parte concorda em transferir a quantia, a outra concorda em transferir a chave e imediatamente os valores e a propriedade são transferidos de forma autêntica, sem a necessidade de se fazerem alterações de registro em cartório para autenticar aquela transação. Cria-se, assim, o que se chama de *trustless trust*, um sistema que não depende de confiança entre as partes, já que é confiável em si mesmo.

A Blockchain garante que A transferiu o valor X para B e que em troca B passou sua propriedade sobre o imóvel Z para A. Todos os nódulos da rede olham para essa transação

---

[96] Cf. VOLPICELLI, Gian. How the blockchain is helping stop the spread of conflict Diamonds. *Wired*, online, 15.02.2017. Disponível em:http://www.wired.co.uk/article/blockchain-conflict-diamonds-everledger. Acessado em 14.08.2017.

para garantir que ela tenha ocorrido de acordo com as regras do código e posteriormente garantem sua autenticidade caso um terceiro C tentasse, por exemplo, afirmar que o imóvel Z na verdade é seu. Tudo criptografado e, se bem gerido, à prova de fraudes.

Para trazer o exemplo mais próximo às relações do direito, imagine que a distribuição do dinheiro da venda de um livro pode ser previamente programada num bloco de informações, se o comprador escolher como meio de pagamento a Blockchain. Ao vender um livro, o dinheiro será automaticamente distribuído em suas exatas porcentagens para a editora, para o autor e para o fisco. Enquanto o caminho tradicional envolveria o depósito ao vendedor, que então distribuiria a editora e essa, por sua vez, pagaria os direitos ao autor, há, com a Blockchain um automatismo das relações. O mesmo caminho poderia ser aplicado ao recolhimento de impostos, por exemplo.

Sob o aspecto da intimidade e da privacidade de dados, essa nova tecnologia traz evoluções consideráveis. Em primeiro lugar porque tem efeito dissuasório para invasões por *hackers* para o furto de informações bancárias: é inútil invadir apenas um computador para efetivar transações, toda a cadeia pública de informação do restante daquela Blockchain negará a utilização do dado ao usuário mal intencionado. Hackear a cadeia só seria efetivo se a maior parte dos computadores-usuários, que mantêm e autenticam as informações fosse hackeada ao mesmo tempo (ataque dos 51%) o que, numa cadeia difusa e bem distribuída de informações que tem confirmação em rede por todos os usuários, é praticamente inviável.

Além disso, a Blockchain é capaz de dificultar ao máximo a extração de dados dos usuários. Os dados contidos nos blocos são criptografados tornando praticamente impossível o uso deles nos moldes comerciais que fazem hoje, por exemplo, *players* como Google e Facebook. O rastreio da informação para aplicações de marketing é impraticável, para ficarmos ainda nesse exemplo.

Solução que viabilizou a existência da criptomoeda *bitcoin*[97], a Blockchain chama a atenção dos bancos e do mercado financeiro por seu grande potencial disruptivo, é a aposta dessas instituições para a evolução do sistema financeiro. Nos EUA, Bank of America,

[97] A questão das *bitcoins* e suas imbricações com o direito penal será mais detidamente analisada no item seguinte. O tema é trazido também nesta parte do trabalho, contudo, para se delinear as correlações que tal modelo de criptomoeda mantém com a problemática da *blockchain*.

Citibank, Credit Suisse, DTCC e J. P. Morgan Chase têm conduzido testes com Blockchain.[98] No Brasil, Itaú, Bradesco e B3 testam a tecnologia.[99]

Com a tecnologia do livro-razão distribuído podemos estar diante de um daqueles momentos na história em que testemunhamos a explosão do potencial criativo da humanidade, como ocorreu com a web há alguns anos, levando ao crescimento exponencial de usos e aplicações de uma tecnologia. A diferença entre o Blockchain e a web está na criação de uma nova capacidade de entrega de confiança na segurança da informação.

A Blockchain não vai provocar rupturas imediatas[100], mas manter o pensamento no futuro é fundamental. Se quisermos efetivamente criar novas fontes de valor, temos de entender para onde todas estas mudanças estão nos conduzindo. A Blockchain é uma dessas mudanças disruptivas importantes, notadamente para a intimidade e a proteção dos dados pessoais.

Infelizmente, há muito pouco da experiência coletiva e *standards* sobre o assunto que possam nos ajudar a trilhar o caminho. Mas sabemos que mudanças exponenciais acontecem muito mais rapidamente do que pensamos. É nossa tarefa o aprofundamento na pesquisa para contribuir no estabelecimento de balizas, como se verá adiante.

### 1.2.3 Criptomoedas

O Bitcoin foi a primeira criptomoeda em larga escala que conhecemos, em 2008. A característica essencial do bitcoin vem do fato de ser um programa de computador, de código aberto, numa rede de livre ingresso, transparente e auditável para notarização de transferências, por meio da internet, sem necessidade de servidor central. É tão simples quanto duas pessoas trocarem pessoalmente dinheiro sem que ninguém possa testemunhar a troca – a diferença está na escala. O que possibilita a existência dessa aplicação é a *Blockchain*: está nela o registro

---

[98] DALY, Rich. Blockchain: Wall Street's Most Game-Changing Technology Advance Since The Internet. *Forbes*, online, 11.07.2016. Disponível em: <https://www.forbes.com/sites/richdaly/2016/07/11/blockchain-wall-streets-most-game-changing-technology-advance-since-the-internet/#5e8036e54d87>. Acessado em 20.08.2017.

[99] BRIGATTO, Gustavo. Itaú, Bradesco e B3 testam a tecnologia Blockchain. *Valor Econômico*, online, 27.04.2017. Disponível em: <http://www.valor.com.br/empresas/4951308/itau-bradesco-e-b3-testam-tecnologia-blockchain>. Acessado em 20.08.2017.

[100] TAPSCOOT, D.; TAPSCOOT, A. *Blockchain Revolution:* How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Nova York: Penguin, 2017. p.11

dessas transferências, de ponto a ponto, sem identificar as pessoas pelas suas identidades civis, mas sim pelas suas chaves públicas na cadeia de dados.

O artigo que lançou o bitcoin para o mundo, "Bitcoin: a peer-to-peer Eletronic Cash System"[101], foi publicado menos de dois meses depois da quebra do banco Lehman Brothers (o banco estadunidense quebrou em setembro de 2008, Satoshi Nakamoto divulgou o artigo seminal em novembro do mesmo ano). A data pode ser mera coincidência, mas o principal argumento das criptomoedas é justamente a desnecessidade do *homem-do-meio*, o setor bancário – e isso em tempos de crise econômica, que viria a culminar em novos e mais intensos padrões jurídicos de regulação do mercado financeiro. Ao analisarem aspectos penais da lei brasileira de regularização de ativos mantidos no exterior, RENATO DE MELLO JORGE SILVEIRA e EDUARDO SAAD-DINIZ afirmam, inclusive, que o ímpeto estatal de regular de forma absoluta os mercados financeiros nacionais, em postura próxima a um *overenforcement*, poderia ter dado margem à criação e fomento de mercados desregulados, tendo na figura da *bitcoin* um de seus mais ilustrativos exemplos[102].

Há alguns modelos da tecnologia de livro-razão distribuído, mas nos casos de criptomoedas as cadeias são comumente não permissionárias públicas[103], em que qualquer um pode "minerar" novas moedas. Essa mineração, contudo, depende de uma prova de validação, em geral a prova de trabalho (*proof of work*). Uma vez minerada a moeda, ela será inserida numa carteira de moeda virtual e poderá ser negociada.

Há centenas de criptomoedas na rede hoje. O que destaca quase todas elas, além da facilidade da transmissão, é a privacidade dos dados de detenção. Pode até ser possível rastrear o dono de uma carteira de criptomoedas na maior parte dos casos (basta checar onde o dinheiro digital está sendo convertido em mercadorias reais e verificar a identidade do comprador da mercadoria real), mas as transações ocorridas dentro das Blockchains de quase todas essas moedas é envolta por criptografia. Ou seja, nestes meios virtuais específicos, é praticamente impossível descobrir a quem pertence cada moeda.

---

[101] NAKAMOTO, Satoshi. *Bitcoin:* a peer-to-peer Eletronic Cash System. Disponível em: https://bitcoin.org/bitcoin.pdf Acessado em 15.08.2017.

[102] SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. *Repatriação e crime:* aspectos do binômio crise econômica e direito penal. Belo Horizonte: Editora D'Plácido, 2017. p. 218.

[103] UK Government Office of Sciences. *Distributed Ledger Technology:* beyond block chain. p. 17. Disponível em <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>. Acessado em 01.09.2017.

O Estado Brasileiro, entretanto, na ânsia de tributar, incluiu o bitcoin nas instruções para declaração anual de Imposto de Renda[104]. Sobre isso, esclareceu o Fisco que "muito embora não sejam consideradas como moeda nos termos do marco regulatório atual, as moedas virtuais como o bitcoin devem ser declaradas na Ficha Bens e Direitos como "outros bens", uma vez que podem ser equiparadas a um ativo financeiro".

A autodeclaração nesse caso é quase que uma prova de desapego do declarante: mantida onde está e se gasta apenas em transações fora do alcance do fisco nacional, a detenção do ativo tem o anonimato garantido pela criptografia.

Importa tratar aqui das violações da privacidade e da intimidade na internet. Nesse passo, as criptomoedas representam avanço significativo. Além da criptografia, todas elas utilizam algum protocolo de segurança na formação do código *hash* na cadeia. A emissão e a circulação são feitas de modo distribuído e na ausência de uma autoridade central. A detenção é de fácil acesso ao possuidor e de impossível visualização por terceiros. Essa dinâmica, contudo, levanta dúvidas de autoridades e tem sido capaz de causar polêmica.

Nos EUA, o Estado de Nova York impôs regras para a negociação de criptomoedas em seu território – a BitLicense[105], que tinha apenas três concessões até 2017, desde o seu lançamento em 2015 – e a Receita Federal norte-americana (o *Internal Revenue Service – IRS*), iniciou uma batalha judicial contra o maior *marketplace* de moedas digitais do mundo, o também norte-americano Coinbase, para ter acesso aos dados de todos os clientes do site. A alegação do fisco é que apesar da explosão no acesso às criptomoedas quase nenhum contribuinte declara os ganhos advindos desse negócio. Em 2013 apenas 807 indivíduos declararam ganhos por criptomoedas nos EUA, em 2014 foram 893 e em 2015 somente 802 contribuintes[106][107].

O número, de fato, é baixíssimo, o mercado de criptomoedas tem hoje em circulação ao menos US$ 150 bi (US$ 76 bi apenas em bitcoin)[108], mas a mera possibilidade de violação dos dados dos usuários de um *marketplace* de moedas é gravíssima. Para ficarmos

---

[104] Perguntão. Receita Federal do Brasil. Disponível em: <https://idg.receita.fazenda.gov.br/interface/cidadao/irpf/2017/perguntao>. Acesso em: 09.05.2017.
[105] New York State. BitLicense. Disponível em: <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>. Acessado em 01.09.2017
[106] Disponível em http://fortune.com/2017/03/19/irs-bitcoin-lawsuit/ Acessado em 02.09.2017
[107] Sobre o assunto, vale ainda a leitura de BARBOSA, T. C. B. M. (coord.), *A revolução das moedas digitais:* aspectos jurídicos, sociológicos, econômicos e da ciência da computação. Cotia: Editora Revoar, 2016.
[108] Disponível em: <https://coinmarketcap.com/historical/20170903>. Acessado em 02.09.2017.

num paralelo naquele mesmo país, é como se o fisco requeresse judicialmente o acesso a todos os dados bancários de correntistas do J.P. MorganChase ou do Bank of America – uma problemática violação do sigilo bancário.

No Brasil não há ainda uma discussão tão arraigada quanto ao tema, mas tem se testemunhado a relativização do sigilo mais amplamente considerado, em espaços que não o virtual. Em seu artigo 145, parágrafo 1ª, a Constituição Federal determina que, sempre que possível, os impostos terão caráter pessoal e serão graduados segundo a capacidade econômica do contribuinte, facultado à administração tributária, especialmente para conferir efetividade a esses objetivos, identificar, respeitados os direitos individuais e nos termos da lei, o patrimônio, os rendimentos e as atividades econômicas do contribuinte, o que acabou por gerar grande mudança na relação jurídica do Fisco com os contribuintes, sobretudo após a edição da Lei Complementar nº 105/2001, trazida ao mundo jurídico com o fim de atender ao comando constitucional, cujo texto franqueou o acesso direto do Órgão Fiscalizador aos dados bancários dos fiscalizados, desde que observados os procedimentos descritos na norma.

Em fevereiro de 2016 foram analisadas as Ações Diretas de Inconstitucionalidade nº 2.390, 2.386, 2.397 e 2.859, bem como o RE 601.314 (este com repercussão geral) e a questão foi objeto de longos debates, sendo definida a tese de que o artigo 6º da Lei Complementar é compatível com a Constituição Federal, não havendo a quebra do sigilo bancário ao fisco, mas, tão somente, a sua transferência, o que afastaria a necessidade de autorização judicial prévia.[109]

Não se olvida que a Lei Complementar nº 105/2001 e seu decreto regulamentador elencam taxativamente as hipóteses de *disclosure* das informações, não tendo deferindo ao fisco "carta branca" ou liberdade plena para a escolha do contribuinte cuja vida bancária irá acessar. Nem se desafia aqui o dever geral de pagar impostos do contribuinte brasileiro, mas pela especificidade da questão e pela novidade que as criptomoedas representam, como novas barreiras para a observação das atividades dos detentores de valores, parece-nos prudente que as autoridades estudem novas vias de tributação. Ter acesso aos dados bancários dos *marketplaces* que operam as transações de criptomoedas no Brasil, como quer o órgão estadunidense equivalente – pode fragilizar seletivamente a intimidade de alguns usuários de criptomoedas e ceifar o desenvolvimento de um mercado que pode ser bastante

[109] Disponível em http://www.stf.jus.br/arquivo/informativo/documento/informativo814.htm Acessado em 02.09.2017

promissor ao país – a tomar pela força do setor bancário no Brasil, um dos mais bem-sucedidos no mundo.

Todavia, para além de questões de política fiscal, o problema das *bitcoins* desperta também debates de destacada natureza penal. E isso porque, não obstante essa criptomoeda não seja por si só um ilícito, tampouco tenha sido criada visando fins delitivos, é também verdade que o mercado de *bitcoins* tem sido utilizado com propósitos criminais de múltiplas possibilidades – desde formas sofisticadas de evasão e sonegação fiscal, até para a consolidação de um mercado online de drogas conhecido como Rota da Seda (*Silk Road*). A desregulamentação e o caráter relativamente anônimo das transações acabam por fornecer um meio razoavelmente seguro para a realização de operações obscuras, em espaços virtuais menos fiscalizados que conjuntamente formam a chamada *deep web.*[110] A necessidade de apuração de crimes praticados por meio dessa nova forma de relação social e econômica pode culminar em novas manifestações do conflito entre o sigilo de dados e o justificável interesse estatal na investigação e persecução penal. Com isso, criam-se novos desafios para a acomodação destes interesses persecutórios às necessidades de preservação da intimidade, especificamente daqueles que se utilizam das *bitcoins* – ou mesmo da *deep web* – sem transpassar os limites de legalidade.

É importante que o Brasil comece a se preocupar com a atividade das criptomoedas em todos os seus aspectos. Ao que importa para o presente estudo, é notável que os *marketplaces* de criptomoedas detêm consideráveis volumes de informação. Apesar dos maiores *players* nesse mercado contarem com termos de uso claros, não há quem os regule especificamente na detenção dessas informações. Aqui seria auspiciosa a aprovação, como se verá adiante, de uma Lei Geral de Dados para o país.

A exegese dos problemas jurídicos em torno das criptomoedas é mais um exemplo de desafio para a intimidade na *Sociedade em Rede*. Saber como operá-la pode constituir importante marco referencial para o resto do mundo. O Brasil detém as condições necessárias para avançar no tema e tornar-se eventual protagonista (tem mercado relevante, *players* capacitados na operação, setor bancário bem organizado e volume de investimentos condizente). Contudo, falta especialmente definir um marco legal que demarque os espaços de liberdade dos usuários, com vistas a deixar os investidores mais seguros e, ao mesmo tempo,

---

[110] SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. *Repatriação e crime...* cit., p. 219-226.

minimizar os riscos penais advindos desta nova modalidade de relação negocial. Em todo caso, a questão passa inexoravelmente pela definição dos limites impostos pelo direito à privacidade nas operações com criptomoedas que guardem relação com o território brasileiro.

### 1.2.4 Inteligência Artificial

A inteligência artificial fascina há um bom tempo a humanidade. O conceito de Inteligência Artificial (AI na sigla em inglês) é atribuído ao cientista da computação John McCarthy, que cunhou o termo em 1955. O termo é extremamente amplo e complexo, mas pode ser resumido como a inteligência da máquina projetada para executar um conjunto definido de ações e aprender com a experiência.[111]

O aumento dos estudos e aplicações a respeito da inteligência artificial tem levantado questões éticas a respeito dos limites do uso da tecnologia. As máquinas têm sido capazes de "aprender" os comportamentos dos usuários e até de mimetiza-los. Há variados debates quanto a formas de proteger a intimidade dos usuários em meio ao avanço desse campo da tecnologia.[112]

Devido à própria natureza da inteligência artificial, nossos dados estão menos seguros do que nunca, e as empresas de tecnologia agora estão colecionando ainda mais informações pessoais sobre cada um de nós em escala global – o *Big Data*. Há alertas quanto ao potencial de ameaça às liberdades civis em decorrência do desenvolvimento desse novo campo[113] e uma guerra geopolítica por seu domínio[114]. Na verdade, o boom da inteligência artificial é tanto sobre a disponibilidade de conjuntos de dados macivos quanto sobre o software

---

[111] Stanford University. AI. Disponível em https://www-cs.stanford.edu/memoriam/professor-john-mccarthy Acessado em 02.09.2017 McCarthy também é referido como o criador, num memorando datado de 01º de Janeiro de 1959, do conceito de compartilhamento de funções de um único computador por uma rede de pessoas. Esse concito, alguns anos depois, foi aplicado por cientistas do MIT para a criação da ARPnet, o embrião da internet que conhecemos hoje. A ideia partiu, portanto, em última análise, de McCarthy.

[112] McMAHAN, H. B [et al.]. *Communication-efficient learning of deep networks from decentralized data. W&CP*, Fort Lauderdale, vol. 54, 2017 e JMLR: e também SHOKRI, R.; SHAMATIKOV, V. Privacy-preserving deep learning. *CCS'15*, 12–16 de outubro de 2015. Disponivel emhttp://www.shokri.org/files/Shokri-CCS2015.pdf Acessado em 03.09.2017.

[113] WIZNER, Ben. Artificial Intelligence at Any Cost Is a Recipe for Tyranny. *ACLU Blog*, online, 23.08.2017. Disponível em: <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/artificial-intelligence-any-cost-recipe-tyranny>. Acessado em 09.09.2017.

[114] VINCENT, James. Putin says the nation that leads in AI 'will be the ruler of the world'. *The Verge*, online, 04.09.2017. Disponível em: <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>. Acessado em 09.09.2017.

inteligente: quanto maior o conjunto de dados, mais inteligentes serão os programas e aplicações.

O uso conjunto de *Big Data* e AI possibilitam a aprendizagem de máquinas (*Machine Learning*). Essa tecnologia está se generalizando nos setores público e privado. Para exemplificar, desde outubro de 2016 a Google deixou de utilizar linguistas para desenvolver seu tradutor instantâneo: as máquinas em AI estavam desenvolvendo o produto de maneira mais rápida e eficiente. Muito mais grave vem sendo o uso desta tecnologia por juízes de alguns estados norte-americanos para sentenciar acusados de crimes. Recentemente o caso *Wisconsin* vs. *Loomis* levou a questão até a Suprema Corte estadunidense [115] quando Eric Loomis questionou o uso de um programa de inteligência artificial (o *Compas*, produzido pela Northpoint Inc.) por parte do Juízo para determinar a sua condenação de seis anos em regime fechado [116]. Loomis queria ter acesso aos critérios que levaram o robô-algoritimico a recomendar a sua pena – a Suprema Corte negou o recurso. A Northpoint venceu a demanda sob o argumentou que o algorítimo do *Compas* é segredo industrial.

Em outro estado nos EUA, a Virgínia, a utilização de algorítimos mas estabelecer condenações já acontece há mais de dez anos. CALISKAN-ISLAM, BRYSON, e NARAYAAN já demonstraram o perigo no uso de inteligência artificial para estabelecer penas[117]: algoritmos são necessariamente programados e essa programação pode conter um erro de viés ideológico [118]. Os pesquisadores demonstraram que sentenças produzidas por robôs-algorítmicos com nomes geralmente atribuídos a pessoas de descendência africana são comumente mais duras do que aquelas que contêm nomes tradicionalmente europeus[119]. A

---

[115] U.S. Supreme Court. Wisconsin vs. *Loomis.* Disponível em: https://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/16-6387.htm Acessado em 10.09.2017

[116] Disponível em https://harvardlawreview.org/2017/03/state-v-loomis/ Ver também http://www.nytimes.com/2005/01/02/magazine/sentencing-by-the-numbers.html, https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html e https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html Acessado em 10.09.2017.

[117] CALISKAN-ISLAM, A. BRYSON, J.J, NARAYAAN, A. *Semantics derived automatically from language corpora necessarily contain human biases.* Princeton University. Disponível em: http://randomwalker.info/publications/language-bias.pdf. Acesso em 06/09/2017.

[118] "Bias should be the expected result whenever even an unbiased algorithm is used to derive regularities from any data; bias is the regularities discovered." (CALISKAN-ISLAM, A. BRYSON, J.J, NARAYAAN, A. *Semantics derived automatically from language corpora necessarily contain human biases.* Princeton University. p. 01)

[119] "We have shown that machine learning can acquire prejudicial biases from training data that reflect historical injustice. (…) We show for the first time that if AI is to exploit via our language the vast knowledge that culture has compiled, it will inevitably inherit human-like prejudices. In other words, if AI learns enough about the

inteligência artificial nesse caso aplica, a partir de um conjunto de dados, uma fórmula a tentar evitar novos casos semelhantes. Assim, se a máquina "aprende" que nomes atribuídos geralmente a pessoas de uma etnia se envolvem mais em práticas delitivas, ela automaticamente endurece as futuras penas de pessoas com esse fator em comum, resultando em inaceitável viés racial reflexo que acaba por provocar uma abominável política criminal higienista e racista. É preciso, portanto, tomar bastante cuidado com a aplicação da Inteligência Artificial[120] no campo jurídico.

A par disso, as principais características da grande análise de dados ainda representam uma mudança gradual no processamento de dados comuns. Por isso, as maiores implicações para a intimidade da população em geral envolvem a aplicação não previamente autorizada da Inteligência Artificial com dados coletados – mesmo que a coleta tenha acontecido sob autorização. Essas implicações surgem não só do volume dos dados, mas das formas em que são gerados, a propensão a encontrar novos usos para isso, a complexidade do processamento e a possibilidade de consequências inesperadas para indivíduos no futuro.

A privacidade por design (*privacy by design*) pode ser um caminho para evitar a coleção indiscriminada de dados dos usuários da rede para criação de algorítimos de inteligência artificial. Ela é uma abordagem de segurança internacional que foi criada em 1995 numa parceria entre as autoridade de dados do Canadá e a da Holanda e será minuciosamente abordada no próximo capítulo. Sob a privacidade por design, as empresas de tecnologia devem dar conta de valores humanos ao criar seus sistemas e garantir que eles tenham projetado a máxima privacidade individual em cada etapa do processo. O ponto é sabermos qual é esse limiar da "mínima privacidade".

---

properties of language to be able to understand and produce it, it also acquires cultural associations that can be offensive, objectionable, or harmful. These are much broader concerns than intentional discrimination, and possibly harder to address. (…) Our results show that European-American names have more positive valence than African-American names in a state-of-the-art word embedding. That means a sentence containing a European-American name will have a higher sentiment score than a sentence with that name replaced by an African-American name. In other words, the tool will display a racial bias in its output based on actor and character names. We picked this example because the argument follows directly from our experiments on names. But our results suggest that other imprints of human racial prejudice, not confined to names, will also be picked up by machine-learning models." Ibid., p. 10-11

[120] MONAHAN, J; SKEEM, J. Risk Assessment in Criminal Sentencing. *Virginia Public Law and Legal Theory Research Paper*, n.. 53. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662082 Acessado em 12.09.2017.

A aprendizagem automática de máquinas envolve um estágio de pré-processamento para melhorar a qualidade dos dados de entrada[121]. Esse pré-processamento, também chamado de rotulagem, é, na maior parte das vezes, humano. A rotulagem humana de um conjunto de dados de treinamento pode criar uma nova oportunidade de imprecisões ou tendências. Em todos os casos, há aplicações para os resuultado que podemos ainda desconhecer.

Em termos gerais, o aprendizado da máquina pode ser dividido em dois tipos de aprender: supervisionado e não supervisionado por inteligência artificial. Na aprendizagem supervisionada, os algoritmos são desenvolvidos com base em conjuntos de dados rotulados. Neste método, os algoritmos são treinados para mapear dados de entrada e fornecê-los para uma saída “tratada” com valores "corrigidos", ou seja, aplicáveis a uma determinada situação. Esta fase inicial de "formação" cria modelos do mundo em que previsões podem então ser feitas na segunda fase de "predição". Por outro lado, na aprendizagem sem supervisão os algoritmos não são treinados e encontraram regularidades em dados de entrada sem instruções sobre o que procurar, fornecendo, ao final, apenas os padrões encontrados nos dados de entrada.

Essencialmente, se os dados de entrada contiverem erros e imprecisões, o “jogo” do aprendizado pela máquina estará viciado – como no caso concreto do viés racista acima demonstrado.

É preciso, portanto, tratar a inteligência artificial como uma tecnologia não-neutra e ainda em evolução. É um erro pensar que robôs-algoritmicos poderão resolver questões essenciais de maneira equanime e sem qualquer viés. As máquinas, mesmo em inteligência artificial, são ainda criadas pelo homem e obedecem comandos pré-estabelecidos. Ainda que se pense em criação de movimentos e reações automatizadas da máquina, é necessário ter em mente que ela foi, em algum momento, ao menos exposta a um volume de dados de treinamento.

No que importa a este trabalho, é urgente estabelecer, como se tratará adiante, uma Lei Geral de Dados no Brasil para regular as possibiidades de treinamento e uso dessa nova habilidade dos computadores. Basta dizer que é impossível saber para o que os nossos dados, constantemente coletados em todos os tipos de dispositivos eletrônicos, serão utilizados no futuro – mas, por outro lado, é seguro dizer que a coleta massiva está ocorrendo constantemente (e de forma cada vez mais econômica). A intimidade dos usuários de quaisquer dispositivos

---

[121] KOTSIANTIS, S. B.; KANELLOPOULOS, D; PINTELAS, P. E. Data preprocessing for supervised leaning. *International Journal of Computer Science* vol. 1, no. 2, 2006, p. 111-117.

eletrônicos corre, por esse prisma, eminente e constante risco de violação, se não agora, num futuro cada vez mais próximo e com possíveis aplicações na computação preditiva e iteligente.

### 1.2.5 Neurociências e computação preditiva

A computação preditiva pode ser mais uma via a contribuir na discussão quanto à liberdade do querer. A neurociência e a computação preditiva têm pelo menos dois caminhos que se cruzam: há as tentativas de predição do pensamento, que combinam estimulos cerebrais com uma varredura de ressonância magnética funcional (fMRI, na sigla em inglês), e o estudo, por meio dos algorítimos de aprendizado das máquinas, para entender a arquitetura e o funcionamento do cérebro. Ambos importam na questão desde a muito debatida acerca da liberdade da vontade[122]

Máquinas de inteligência artificial e cérberos trabalham num sistema parecido, de "custo" zero, em trocas que devem chegar ao equilíbrio (o *gradiente básico de equilíbrio*, segundo MARBLESTONE, WAYNE e KORDING[123]). As máquinas com inteligência artificial embarcada se concentraram em encontrar formas cada vez mais rápidas de "fechar" essa conta. Uma boa resposta para isso pode (e, ao que tudo indica, *deve*) estar nas redes neurais.

A neurociência pode contribuir com o aprendizado das máquina em diversos níveis e vice e versa. Já há desde exemplos de pesquisas utilizando a computação preditiva para estabelecer os caminhos de estimulos no cérebro[124] até outras, que encontram respostas que as neurociências e a medicina ignoravam[125].

Os "algoritmos" de otimização no cérebro humano – as nossas redes neurais – são resultado de centenas de milhões de anos de evolução natural. O nosso cérebro pode ter

---

[122] Quanto a isso e a possibilidade do desenvolvimento da dogmática penal independente de um posicionamento acerca do livre arbítrio, ver RODRÍGUEZ, Víctor Gabriel de Oliveira. *Livre arbítrio e direito penal e direito penal*: revisão frente aos aportes da neurociência e à evolução dogmática. 321p. Tese (Livre-docência em Direito Penal) – Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2015.

[123] MARBLESTONE, A. H.; WAYNE, G.; KORDING, K.P. Toward an integration of deep learning and neuroscience. *Frontiers in Computacional Neuroscience*. Revista eletrônica. 14.09.2016. Disponível em https://www.frontiersin.org/articles/10.3389/fncom.2016.00094/full#h9. Acessado em 22.09.2017

[124] Massachusetts Institute of Technology – Technology Review. *How Machine Learning is helping neuroscientists crack our neural code.* Disponível em https://www.technologyreview.com/s/608604/how-machine-learning-is-helping-neuroscientists-crack-our-neural-code/ Acessado em 22.09.2017.

[125] BAKAR, N. [et al.]. *ALS and artificial inteligence:* IBM Watson suggests novel RNA binding proteins altered ALS. Disponível em https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=HLW03040USEN Acessado em 23.09.2017.

encontrado formas de usar funções de custo que interagem e chegam ao equilibrio sobre o desenvolvimento, de modo a simplificar os problemas de aprendizagem, orientando e moldando os resultados da aprendizagem não supervisionada.[126] A descoberta de ponto de inflexão seria a epifania da inteligência artificial, quando uma rede deixa de precisar de dados pré programados de treinamento para "aprender" sozinha.

Nesse sentido, é possível que o estudo aliado das neurociências com Inteligência Artificial, *Big Data* e *Machine Learning* consigam ser mais uma via para debater a questão do livre arbítrio do ser humano, estudando os meandros que cercam a questão.

Nesse ponto, a computação preditiva pode oferecer novas técnicas e caminhos experientais para a questão da autonomia da vontade. Os caminhos fornecidos pelas máquinas dotadas de inteligência artificial podem ser num futuro próximo uma via alternativa ou mesmo auxíliar aos estudos médicos na área, por exemplo. Se, um dia, as máquinas lograrem exito em emular o cérbro humano, poderemos descobrir – ou ao menos ter a *possibilidade de* – se as experiências de Libet e seus sucessores[127] estavam corretas, com a prova em dados empíricos extraidos de um cérebro mimetizado por um computador.

É certo, pois, que uma descoberta desse tipo impactará gravemente a intimidade dos indivíduos. Como narra RODRÍGUEZ

> a finalidade de conhecer o cérebro e sua função será conseguir manipulá-la (...)parece bastante evidente que os estudos médicos visam sempre à possibilidade de interferência no objeto estudado. Se essa interferência ocorre para uma saudável cura de casos gritantemente patológicos ou se podem impor uma normalização de comportamento humano, a tangenciar a eugenia, trata-se de questão a ser decidida no campo ético.[128]

Essa exata conclusão parece amoldar-se como uma luva ao uso da computação preditiva para descobrir os caminhos do cérebro e da autonomia da vontade humana: uma vez descoberta a trilha, parece bastante plausível que apenas o liame ético a separe do uso para controle social e, logo, como na possibilidade de experiência médica, possa também "ser utilizado para consertar personalidades voltadas ao crime"[129].

---

[126] MARBLESTONE, A. H.; WAYNE, G.; KORDING, K.P. Toward an integration of deep learning and neuroscience. *Frontiers in Computacional Neuroscience*. Revista eletrônica. 14.09.2016. Disponível em https://www.frontiersin.org/articles/10.3389/fncom.2016.00094/full#h9. Acessado em 22.09.2017.
[127] Aqui incluída a de Haynes, Fried, entre outros, narradas por RODRÍGUEZ, Víctor Gabriel de Oliveira. *Livre arbítrio...* cit., p. 20 e ss.
[128] RODRÍGUEZ, Víctor Gabriel de Oliveira. *Livre arbítrio*... cit., p. 28.
[129] Ibid. p. 29.

Diante dessa realidade, é importante que os estudiosos da intimidade e da privacidade de dados preocupem-se com os avanços – necessários – da computação preditiva e do desafio da predição e da liberdade do querer do homem.

### 1.2.6 Internet das Coisas – IoT (*Internet of Things*)

Quando os primeiros componentes eletrônicos dotados de microprocessadores de comando surgiram na década de 1980, a humanidade não poderia prever que em tão pouco tempo eles fossem diminuir tanto de tamanho e aumentar tanto a sua capacidade de processamento. A industria do ramo é uma das mais inovadoras e disruptivas desde a Revolução Industrial. A vida como conhecemos hoje passa essencialmente pelo uso de dispositivos com processadores. A chegada da internet aos aparelhos de uso diário levou a importancia desse objetos, que, até então, não ofereciam risco à intimidade dos usuários, para um novo nível de importância de estudo.

O desenvolvimento da Internet das Coisas possibilita a criação de dispositivos com acesso à internet e a venda de aparelhos "remodelados" que nunca antes precisaram de uma conexão – como um controlador de irrigação de jardins ou uma máquina de fazer sucos. Chega a ser irônico chamar determinados produtos de "inteligentes". A Internet das Coisas está presente hoje em nossas vidas de uma maneira que não nos damos conta – e será cada vez mais – em muitos caso, fragilizando a intimidade e a vida privada dos seus usuários.

Para ilustrar com alguns exmplos, o aspirador-robô Roomba está, desde 2015, criando mapas dos ambientes que aspira e enviando, via internet, para a sua fabricante, a iRobot[130]; a fabricante de aderaços sexuais WeVibe, fechou um acordo multimilionário com os reguladores estadunidenses depois de revelar que os seus produtos enviavam para a fabricante até os horários em que eram utilizados. [131]; a fabricante de carros elétricos Tesla liberou remotamente para os donos de modelos da marca que estavam próximos da área atingida pelo

---

[130] IEEE Spectrum. *Robots iRobot Brings Visual Mapping and Navigation to the Roomba 980.* Disponível em https://spectrum.ieee.org/automaton/robotics/home-robots/irobot-brings-visual-mapping-and-navigation-to-the-roomba-980 Acessado em 15.09.2014

[131] FREYTAS-TAMURA, Kimiko. Maker of "smart" vibrators settles data collection lawsuit for $3.75 million. The New York Times, online, 14.03.2017. Disponível em: <https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html>. Acessado em 15.09.2017.

furacão Irma, na Flórida, uma carga extra de 40 milhas, levantando questões éticas sobre como a fabricante poderia ainda controlar – e monitorar – os veículos de clientes seus, que pagaram pelo produto e são os legítimos proprietários[132]. Cada aparelho, por menor e mais inofensivo que possa parecer, desde que ligado à rede, pode ser controlado remotamente por alguém que não o seu dono. Quando se imagina a quantidade de dispositivos com câmeras e microfones, a dimensão do problema começa a se desenhar.

A internet das coisas está nas onipresentes câmeras – quase todas já com tecnologia de reconhecimento facial, muitas com biometria -, nos locais de trabalho, lazer e nas nossas casas. Ela permite o "rastreamento" perfeito de qualquer um de nós, do momento em que acordamos ao local em que dormimos.

Os desafios para a intimidade nesse campo são, portanto, os maiores possíveis. Basta dizer que quase todos os planos de saúde têm aplicativos para telefones. Esses aplicativos coletam constantemente os dados dos usuários, a pretexto de fornecer sempre a localização de médios e hospitais próximos. O acúmulo a longo prazo desses dados permite ao detentor – a operadora do plano – conhecer detalhadamente o comportamento e os hábitos de uma pessoa, dos lugares que ela frequenta ao número de horas de sono em média. Esse dado pode subsidiar o oferecimento futuro de um novo plano – ou a negativa na renovação do existente. Para ficar no setor de seguradoras, boa parte dos carros novos são "conectados", contêm sistemas embarcados de navegação. Há opções de seguro com rastramento constante do veículo. A seguradora conseguirá, sem o menor esforço, auferir se os dados constantes na apólice estão sendo cumpridos pelo proprietário do veículo ou se, em caso contrário, vier a ser acionada, poderá, no futuro, negar o pagamento do prêmio, diante das provas, por dados, do descumprimento das condições do contato.

Os defensores da tecnologia argumentam que a IoT pode contribuir decisivamente para a implementação de "cidades inteligentes" (*smart cities*), com a integração entre todos os dispositivos[133]. É preciso ponderar, porém, que o custo disso não pode ser a intimidade do

---

[132] FUNG, Brian. As Hurricane Irma bore down, Tesla gave some Florida drivers more battery juice. Here's why that's a big deal. *The Washington Post*, online, 11.09.2017. Disponível em https://www.washingtonpost.com/news/innovations/wp/2017/09/11/as-hurricane-irma-bore-down-tesla-gave-some-florida-drivers-more-battery-juice-heres-why-thats-a-big-deal/?utm_term=.10a8ef857fb4 Acessado em 15.09.2017.

[133] CISCO. *A IoT conecta objetos à Internet, gerando dados e informações aos quais nunca tivemos acesso antes.* Disponível em: <https://www.cisco.com/c/pt_br/solutions/internet-of-things/overview.html?stickynav=1>. Acessado em 15.09.2017.

cidadão: onde está a opacidade numa monitoração constante, até mesmo pelo aspirador de pó em casa?As empresas precisam se conscientizar acerca do problema.

Quando as empresas coletam dados do usuário, eles devem assumir a responsabilidade de proteger seus usuários; se não aceitarem a responsabilidade no trato da nova – e grande – questão, devem abster-se de coletar esses dados – o que não parece interessante para os negócios.

A política de privacidade em camadas pode ser, por exemplo, um *standard* viável para a internet das coisas. Prática adotada para as licenças Creative Commons[134], pode servir como modelo util. Essas licenças têm um design de três camadas: a camada legal, a camada "legível por humanos" e a camada "legível por máquina". A camada legal seria a política jurídica para o tratamento dos dados. A camada "legível por humanos" seria um resumo conciso e simplificado da política de privacidade em linguagem simples que um consumidor médio poderia ler. A camada "legível por máquina" seria o código que o software, os mecanismos de busca e outros tipos de tecnologia podem entender e permitiria apenas que os dispositivos conectados na internet das coisas tenham acesso a informações permitidas pelo consumidor. É um modelo possível de normatização simples para o setor.

É impossível saber ao certo o número de dispositivos conectados na internet das coisas – algumas estimativas dão conta de até 24 bilhões de dispositivos em 2020, mas o número é pouco preciso[135] – o certo é que um número abisal de equipamentos coleciona, e colecionará cada vez mais, dados sobre todos nós. A segurança desse monitoramento constante – quem pode garantir, por exemplo, que um hacker mal intencionado não está espionando agora mesmo o leitor pela câmera do computador mais próximo? – é questão de primeira grandeza no futuro da humanidade.

Pesquisadores das Universidades de Helsinki, Aalto e do Max Planck Institute for Informatics, conduziram um interessante estudo de longa duração (seis meses) com 12 participantes que tiveram câmeras e gravardores de voz instalados em todo tipo de dispositivo eletrônico, de eletrodomésticos a computadores, e que ficaram ligadas o tempo todo. Esse

---

[134] CREATIVE COMMONS. *Sobre as licenças:* a função das nossas licenças. Disponível em: <https://creativecommons.org/licenses>. Acessado em 16.09.2017

[135] BUSINESS INSIDER. *There will be 24 billion IoT devices installed on Earth by 2020*. Disponível em http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5 Acessado em 16.09.2017.

estudo, com as pessoas conscientes de que não experimentavam um simples assistente doméstico por voz, como a Siri da Apple, a Cortana da Microsoft ou o Watson da IBM, mas uma coleção constante de todos os dados gerados, demonstrou que, para os participantes "o sistema de vigilância provou ser um causa de irritação, preocupação, ansiedade e até raiva"[136].

O Brasil terá, em breve, um plano nacional de ação para a Internet da Coisas[137]. Diante do cenário que se apresenta, será preciso investiga-lo a fundo para saber em que medida atenderá a proteção da intimidade dos nossos cidadãos.

### 1.2.7 Armazenamento de dados em nuvem

A computação em nuvem refere-se à capacidade de acessar e manipular informações armazenadas em servidores remotos, usando qualquer plataforma habilitada para Internet, incluindo smartphones. As instalações e aplicações de computação serão cada vez mais entregues como um serviço, pela Internet – nos tópicos que discutimos acima, vale notar o explosivo desenvolvimento da Blockchain as a Service (BaaS), por exemplo.

Nós já utilizamos a computação em nuvem quando, por exemplo, usamos aplicativos como o o Microsoft Office, o Google Docs, o Google Drive, o One Drive, o iCloud, o Dropbox e o SpiderOak. No futuro, governos, empresas e indivíduos cada vez mais se voltarão para a nuvem. O hardware como conheciamos há cinco anos atrás deixará completamente de existir nos próximos cinco anos.

É bastante importante, então, que os mecanismos e aplicações a que confiamos a guarda de arquivos na nuvem prezem pela não aderencia dos dados as suas plataformas e evitem, ao máximo, a leitura do conteúdo depositado – inclusive pelo uso de mecanismos de inteligência artificial. Há até um *standard* internacional para guiar esses *holders* de dados, o ISO/IEC 27018:2014, que propõe diversas diretrizes.

---

[136] OULASVIRTA, A. [et al.] *Long-term Effects of Ubiquitous Surveillance in the Home.* UbiComp '12: Proceedings of the 2012 ACM Conference on Ubiquitous Computing: Pittsburgh, EUA, 2012. p. 41-50 Disponível em https://people.mpi-inf.mpg.de/~oantti/pubs/ubicomp2012-oulasvirta.pdf. Acessado em 16.09.2017.

[137] BNDES. Internet das coisas: um plano de ação para o Brasil. Disponível em http://www.bndes.gov.br/wps/portal/site/home/conhecimento/estudos/chamada-publica-internet-coisas/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil Acessado em 16.09.2017.

Ao que interessa para este trabalho, é provável que o futuro imediato da armazenagem de dados em nuvem esteja na Blockchain. Portanto, como discutimos longamente o assunto acima, não há aqui a necessidade de maior aprofundamento.[138]

### 1.2.8 Redes Sociais

As redes sociais são, provavelmente, a mais nova fronteira para a intimidade e um dos maiores desafios já experimentados em toda a história da humanidade. Em primeiro lugar, cumpre estabelecer que jamais na um agente, público ou privado, deteve tantos e tão detalhados dados sobre um volume tão assustador de pessoas como tem hoje o Facebook.

Trata-se provavelmente da maior e melhor coleção de dados que já se viu: os usuários, por vontade própria e diante de poucos estimulos, cedem para a rede social todos os tipos possíves de dados, recebendo em troca apenas o acesso gratuito a plataforma.

Esses dados, depois de tratados, são oferecidos em larga escala para anúnciantes. O problema está justamente na tutela desse grande volume de dados e na falta de fiscalização ou regulação para o uso de uma ferramenta tão importante. Em 2014, por exemplo, o Facebook se retratou por autorizar e apoiar o estudo de KRAMER, GUILLORY e HANCOCK com relação ao comportamento de seus usuários. Os três pesquisadores manipularam durante uma semana o *feed* de notícias de 689.003 usuários em língua inglesa para testar suas reações a uma avalanche de notícias positivas ou negativas de seus amigos. Concluíram que "as emoções expressas por outras pessoas no Facebook influenciam nossas próprias emoções, constituindo o estudo evidencia experimental de que existe contagio por redes sociais"[139]. Simultaneamente, há fragilização da privacidade em geral. MAGALHÃES resume bem o conflito em comento:

> Não há nada de natural ou neutro na maneira como esses dados são produzidos e analisados, ou na definição de o que é relevante. Todos seus elementos são resultado de decisões subjetivas e, mesmo que indiretamente, também ideológicas. Nos últimos anos, uma quantidade crescente de críticos têm se debruçado sobre o tema. Em geral, eles apontam para os riscos que esses sistemas representam para ao menos quatro valores democráticos fundamentais. O primeiro, claro, é a privacidade. Há décadas, empresas que negociam nossos dados afirmam que as pessoas não se importam de serem constantemente monitoradas. Anos de pesquisa sugerem o contrário. A maior

---

[138] Vale constar, no entanto o interessante tratamento do tema na Alemanha. Para isso, ver WEICHERT, T. *Cloud Computing and Data Privacy*. The Sedona Conference, 2011. Disponível em https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf Acessado em 18.09.2017.

[139] KRAMER, A.; GUILLORY, J.; HANCOCK, J. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS Review*, Vol. 111, n. 24. Jun. 2014. Disponível em http://www.pnas.org/content/111/24/8788.full.pdf

> parte das usuários simplesmente não sabe que esse monitoramento ocorre. Dentre as que sabem, a sensação tende a ser de resignação. Se elas não podem negociar as cláusulas do contrato, qual é a solução? Uma ruptura unilateral (sair de uma rede social, por exemplo) tem enormes custos sociais para as pessoas. É necessário levar em consideração a extrema desigualdade entre empresas e usuários antes de concluir que as pessoas não querem ser monitoradas — especialmente quando governos utilizam os dados e expertise das empresas para nos espionar, como Edward Snowden revelou. O segundo é a diversidade. Cientistas políticos e filósofos parecem concordar que uma democracia depende de exposição à diferença. Se experimentamos apenas o que já conhecemos, acreditamos ou gostamos, teremos dificuldade em compreender o outro, com quem, num sistema democrático, temos que lidar e chegar a algum tipo de acordo. Sistemas de algoritmos que objetivam nos dar apenas o que já mostramos que queremos tornam essa experiência mais rara e tendem a radicalizar posições políticas. Que esses sistemas criam, em alguma medida, bolhas de filtragem é algo que mesmo cientistas pagos pelo Facebook atestaram. Mas a dimensão exata dessas bolhas, e a responsabilidade sobre elas é algo ainda incerto entre pesquisadores.[140]

É possível que a intimidade dos usuários do Facebook tenha sido afetada em seu âmbito informacional com tal experiência não consentida. As atitudes de preocupação com o usuário, contudo, quando partem dessas redes, são em geral, fruto de demandas públicas, como no caso das últimas eleições majoritárias nos EUA. A partir dali, o Facebook e o Twitter engendraram esforços para diminuir a propagação de notícias falsas.

Apesar da importância que essas empresas representam hoje na difusão de informações, mimetizando verdadeiros conglomerados de mídia, é preciso deixar claro que o real papel que desempenham: são essencialmente a nova indústria de dados. O "conectar" de pessoas e a difusão de opiniões em 140 caracteres são, na verdade, métodos de aumento de tempo de permanência de conexão e de diminuição da taxa de rejeição na coleta de dados. É, por exemplo, bastante mais eficiente que o mero rastreio de buscas porque entrega um raio-x completo do comportamento do usuário.

O controle de *bots* nesse tipo de rede pode, de fato, representar ameaça real para a democracia, tanto maior quanto mais pessoas estiverem "conectadas". As redes criam bolhas comportamentais que, muito ao contrário da prometida conexão, isolam os usuários em seus próprios padões de comportamentos. É notável que os algoritmos dessas redes são segredos industriais, mas é preciso discutir com a sociedade em que medida o isolamento criado contribui para o desenvolvimento da democracia.

---

[140] MAGALHÃES, João Carlos. Democracia... cit.

### 1.3 Possíveis violações da privacidade em ambiente digital relacionadas à política

É necessário viabilizar um modelo de respeito aos dados pessoais em que cidadãos e Estado estejam protegidos, com regras de coleta de dados permitidas, regulamentadas e fiscalizadas de modo que a privacidade dos dados do usuário seja preservada, não comprometendo sua autodeterminação. Por isso, o encontro dos novos limites da privacidade na rede e a intersecção dos novos comportamentos com a política são tão significativos. O direito penal precisa estar preparado para os novos desafios nessa área, garantindo o respeito aos direitos fundamentais.

No campo das ciências políticas, pode representar perigo, por exemplo, a coleta e armazenagem massiva de dados com fins de estudo de cenários de votação – ainda mais sem a autorização dos indivíduos que "cedem" tais dados.

Uma relação desse tipo pode ferir o princípio da confiança[141] do usuário, a ponto de ameaçar gravemente a privacidade em seu aspecto decisional – que será estudada adiante -, e sua capacidade de acreditar na democracia como um sistema justo de governo. Não estamos muito longe desse ponto[142].

Para JUTH e LORENTZON, nossas decisões são resultado "causado por nosso caráter, nossa memória, nosso humor, bem como pela nossa percepção da situação em que atuamos (e, em última análise, talvez, todos esses eventos mentais são causados por estados (emocionais) em nossos cérebros)" (trad. livre)[143]. Tanto os estados emocionais quanto a nossa percepção da

---

[141] Segundo André Luís Callegari "O princípio da confiança significa que, apesar da experiência de que outras pessoas cometem erros, se autoriza a confiar — numa medida ainda por determinar — em seu comportamento correto (entendendo-o não como acontecimento psíquico, senão como estar permitido confiar)" (CALLEGARI, André Luís. Imputação objetiva: lavagem de dinheiro e outros temas de direito penal. *Boletim IBCCRIM*, São Paulo, n. 78, v. 7, 1999. p. 3.)

[142] De acordo com Lima "É evidente que adulterações de dados eletrônicos põem em risco a necessária confiabilidade das comunicações e negócios eletrônicos. Porém, o momento é propício ao incremento de medidas penais que produzam efeitos em todos os campos afetados pela informática, trazendo, com isso, normas que de forma efetiva atendam à necessária proteção a todos os bens jurídicos ofendidos por intermédio de computadores." (LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança computacional*. Campinas: Millennium, 2007. p. 21.)

[143] No original: "our will is free: the will is caused by our character, our memories, our mood, as well as by our perception of the situation in which we act (and ultimately, perhaps, all these mental events are caused by states in our brains). Our will, like everything else, is an integral part of an all-encompassing causal web, and even though we did what we did because we wanted to, we could not have wanted what we did not want" (JUTH, N.; LORENTZON, F. The concept of free will and forensic psychiatry. *International journal of law and psychiatry*, Quebéc, vol.33, n.1, 2013.)

situação em que atuamos passam atualmente pelos relacionamentos digitais.

BECHARA observa que para ROXIN as normas apenas podem perseguir a finalidade de assegurar aos cidadãos uma coexistência livre e pacífica, garantindo respeito aos direitos humanos de todos. Segundo essa linha de pensamento, se essa tarefa não pode ser cumprida por outros instrumentos de controle social, o Estado deve garantir penalmente não apenas as condições individuais necessárias para coexistência (como a vida, a integridade física e o patrimônio) mas também as instituições estatais que sejam imprescindíveis a tal fim, que, no caso desse estudo, julgamos ser a intimidade e a autodeterminação informativa[144].

É na internet que definimos hoje boa parte das nossas emoções e é essa mesma rede que tem sido um campo de batalha política importante no Ocidente nos últimos anos. Sem nos darmos conta, estamos diante de um novo – e importante – fator comportamental a atingir a democracia.

REALE JÚNIOR expõe bem a interiorização do aprendizado social pelo qual o indivíduo passava desde o berço no século passado.[145] Assim como a criança descrita por ele é receosa da aprovação de seus pais, os indivíduos na sociedade da informação o são em relação aos seus pares. A interação social e as tomadas de decisão que antes eram pautadas, como descreve o antigo decano, pela família, pela escola, pela igreja, pelo sindicato[146] – estão hoje, em boa parte, adstritas aos aspectos comportamentais e interações sociais digitais dos indivíduos. Os agentes de socialização mudaram[147]. Por isso, os agentes privados detentores de coleções de dados dos indivíduos têm um papel fundamental nos rumos das democracias ocidentais.

---

144 BECHARA, Ana Elisa Liberatore Silva. *O rendimento da teoria do bem jurídico no direito penal atual*. Revista Liberdades, São Paulo, n. 1, p. 16-29., mai./ago. 2009. P. 24 (citando ROXIN, Claus. Es la proteción de los bienes jurídico una finalidade del derecho penal? In *La teoria del bien jurídico. Fundamento de legitimación del dercho penal o juego de abalorios dogmático?* Roland Hefendehl (ed.). Barcelona: Marcial Pons, 2007. P. 447).

145 REALE JÚNIOR, Miguel. *Instituições de direito penal.* 2.ed. Rio de Janeiro: Forense, 2006. p.05.

146 Ibid. p.04.

147 "Consumers should not be expected to understand the privacy dimensions of a "custom targeting" system that uses wide-ranging data sets to determine "the absolute value of each impression" for an advertiser. How and why should any user have to know how a data-targeting "demand-side platform" operates and will affect their privacy and consumer decision-making?" (CHESTER, J. Cookie Wars: how new profiling and targeting techniques threaten citizens and consumers in the "Big Data" era. In: GUTWIRTH, Serge, LEENES, Ronald, De HERT, Paul. *European data protection*: in good health? Bruxelas: Springer, 2012. p. 55.)

Há necessidade de um diálogo profundo entre as empresas e a sociedade, como meio de atribuir legitimidade a um processo de tutela adequado aos dados atinentes à intimidade.[148] ROSENDAAL notou isso[149] complementando que como está, a convivência social por meios digitais pode mesmo moldar a personalidade das pessoas, afetando gravemente a formação da vontade dos indivíduos[150]. Segundo o autor é possível que os processos políticos e de tomada de decisões na sociedade sejam afetados por esse novo meio de convivência[151].

CASTELLUCCIA vai além e anuncia como real o risco a integridade da pessoa humana na criação de perfis de comportamento[152]. Segundo ele o recolhimento de dados informáticos afeta diretamente a privacidade dos usuários, podendo levar a criação de uma sociedade de vigilância[153].

De fato, com operações de *Big Data* e Inteligência Artificial, é posível que em pouquíssimo tempo as pesquisas eleitorais sejam substituidas por técnicas de *profiling*, que dirão como vota cada eleitor. Já há consultorias especializadas no estabelecimento de perfis dos eleitores. A Privacy International, uma ONG britânica que estuda o respeito à privacidade no

---

[148] "Businesses are expected to dialogue with society and acknowledge the legitimacy of the stakeholfers requests" (DEL GIUDICE, M.; PERUTA, M.R.D.; CARAYANNIS, E.G. *Technological*… cit., p. 98.)

[149] ROOSENDAAL, A. We are all connected to Facebook… by Facebook! In: DE HERT, Paul [et al.]. *Reinventing data protection?* Bruxelas: Springer, 2014.

[150] "Making choices and defining wishes and desires is closely to identify. Identify is who you are as an individual an how you want to be seen by others, so it has an internal and an external element. The internal can be described as how human beings acquire a sense of self. The external element relates to social interaction with others. This information, however, is not always similar. When an individual wants to express himself and wants to present himself differently in different roles or contexts, control over data concerning him is a necessary condition. This is where privacy comes in." (Ibid., p. 11.)

[151] "The problem is that, in the information age, individual self-determination itself is shaped by the processing of personal data. How personal data are used determines the terms under which an individual participates in social and political life." (Ibid., p. 14.)

[152] "The concept of *Behavioural Profiling* (also known as "targeting") consists of collecting and analyzing several events, each attributable to a single originating entity, in order to gain information relating to the originating entity (…) Behavioural profiling involves collecting data (recording, storing and tracking) and searching it for identifying patterns (with the help of data mining algorithms). The data collection phase is often referred to as *Behavioural Tracking.*" (CASTELLUCCIA, Claude. Behavioural Tracking on the internet: a technical perspective. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014. p. 21.)

[153] "It can be argued that the customizations resulting from profiling are also beneficial to the users that only receive information relevant to their interest. However, it creates serious privacy concerns since it allows some companies or institutions to gather and concentrate a huge amount of information about their customers, and about Internet users in general. The danger is to move into a surveillance society or Internet, where all our online or physical activities are recorded and correlated. Some companies offer various services that gather different types of information from users. The combination and concentration of all this information provides a powerful tool." (Ibid. p. 34.)

mundo, relatou o uso da técnica nas eleições do Quênia de 2017[154]. Mas o seu uso é mais antigo e sofisticado em outros lugares: nos EUA, segundo estudo do MIT, o estabelecimento de perfis dos eleitores com base nos seus dados informáticos é utilizado pelo menos desde as eleições de 2006, tendo sido decisivo tanto na eleição quanto na reeleição de Barack Obama[155].

É igualmente possível que as já existentes *Fake News* sejam direcionadas por robôs-algorítimicos para decidir o voto de eleitores indecisos. Isso, aliás, já ocorre num cenário maior, conforme estudamos. Mas o avanço da tecnologia e a lentidão das leis na proteção dos dados pessoais pode permitir que a técnica seja cada vez mais personalizada e eficiente, a um custo cada vez menor. Em outras palavras, se os algorítimos que acessam a intimidade dos usuários da rede hoje já são capazes de *influenciar* nas eleições, é possível que em pouco tempo eles sejam capazes de *decidi-las* e é papel do direito penal previnir isso.

## 1.4 A Coleção de dados Nos EUA e na União Européia: diferenças fundamentais

### 1.4.1 Estados Unidos

Os EUA discutiram por quase três anos (entre 2011 e 2013) a aprovação do seu *Cyber Intelligence Sharing and Protection Act*, que regularia as invasões, por órgãos do governo, de dados de seus próprios cidadãos sem prévia autorização judicial, com base no *Patrioct Act*, expondo desde conversas online até acessos a contas e movimentações financeiras.

Os opositores da proposta argumentam que a lei quebraria não apenas a privacidade do cidadão como sua própria dignidade ao exibir uma radiografia de seus atos no mundo digital. Com o projeto de lei ainda tramitando à época no Congresso estadunidense, em maio de 2013, Edward J. Snowden, então funcionário de uma empresa privada contratada para prestar serviços à *National Security Agency* – a NSA, possivelmente a mais poderosa agência de espionagem do mundo –, revelou ao jornal The Washington Post a existência de um Programa Nacional de Segurança e Vigilância, conhecido como "Planning Tool for Resource Integration, Synchronization, and Management" – o PRISM. O então presidente americano, Barack Obama,

---

[154] PRIVACY INTERNATIONAL. Voter profiling in the 2017 Kenyan election. Disponível em: <https://www.privacyinternational.org/node/1462>: Acessado em 20.09.2017.

[155] ISSENBERG, Sasha. How Obama's team used Big Data to rally voters. *Massachusetts Institute of Technology* – Technology Review. Dezembro de 2012. Disponível em https://www.technologyreview.com/s/509026/how-obamas-team-used-big-data-to-rally-voters/ Acessado em 20.09.2017.

admitiu a existência do PRISM, em funcionamento pelo menos desde 2007, mesmo sem uma legislação para regular seu uso.

Segundo os dados obtidos por Snowden, o PRISM é capaz de monitorar em tempo real informações de redes sociais, ligações por voz ou vídeo, e-mails e cartões de crédito e, cruzando essas informações, é capaz de fornecer um relatório completo do "alvo". O alvo, no entanto, não é especificado e pode ser qualquer pessoa, a qualquer momento, em qualquer lugar do planeta. Isto significa, na prática, que todo cidadão no mundo, que utilize a internet, um telefone, ou um cartão de crédito, pode ser monitorado em tempo real pelo governo norte-americano. Pior: o governo dos EUA contrata empresas privadas para fornecerem a mão-de-obra, os analistas que cuidam do monitoramento.

Informações passadas pelo ex-agente mostrariam diversas empresas (a exemplo de Yahoo!, Google, Microsoft, Facebook, PalTalk, YouTube, Skype, AOL e Apple) como "colaboradores" do governo dos EUA no fornecimento de dados. Snowden declarou que resolveu revelar as informações porque o modo com a NSA está operando coloca, segundo sua opinião, em risco a intimidade de qualquer pessoa na Terra[156].

Snowden, era um contratado da *Booz Allen Hamilton*, uma empresa de Tecnologia da Informação que presta serviços para o governo americano, fugiu do Havaí, onde trabalhava num laboratório de análise de dados da NSA, para Hong Kong levando com ele dados e relatórios suficientes para comprovar que a agência que deveria cuidar da segurança dos americanos fazia muito mais do que isso, espionando inclusive telefones celulares de líderes de países aliados, a exemplo da Chanceler alemã Ângela Merkel e a ex-Presidente brasileira Dilma Rousseff.

As denúncias do ex-agente evidenciaram questões a respeito do tratamento de dados até então pouco discutidas. A primeira e mais óbvia é o limite que uma agência de espionagem pode alcançar: não é crível acreditar que qualquer outro país que detenha os meios de espionar quem quer que seja vá deixar de utilizar-se de tal ferramenta no cenário atual, com pouca ou nenhuma regulação para o tema. Mas é menos razoável ainda que líderes de países (aliados, inclusive) ou cidadãos comuns tenham sua privacidade exposta ao gosto de um agente americano. Pior: Snowden nem sequer era agente governamental, trabalhava sob contrato para

---

[156] GREENWALD, Glenn. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, online, 11.06.2013. Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acessado em 30.09.2017.

uma empresa privada, que tem, em última análise, acesso irrestrito aos dados de qualquer pessoa, em todo o globo.

Os norte-americanos mantiveram durante 15 anos um acordo com a União Europeia para a troca de dados de cidadãos e residentes, o *Safe Harbor Treaty*[157] que permitia a companhias americanas arquivarem dados provenientes de consumidores europeus em território estadunidense e autocertificarem a segurança da informação. Em 2015, a Corte Europeia de Justiça declarou invalidou o acordo. A intensa coleta de dados pelas autoridades dos EUA, ao que se pode compreender com as revelações de Snowden, começou logo depois dos ataques de 11 de Setembro de 2001. Em 26 de Outubro de 2001 o então Presidente George W. Bush assinou o *Ato Patriota*[158], estabelecendo novos limites de investigação pelas autoridades daquele país. Dentro destes novos limites, entrou em vigor, um mês depois, o *Aviation and Transportation Security Act* que, entre outras determinações, obrigava todas as companhias aéreas a abrirem o *Passager Name Record* para as autoridades estadunidenses (logo em seguida Austrália, Japão, Canadá e Rússia alinharam-se ao exemplo americano com atos parecidos ou idênticos[159]

Com a mesma proteção jurídica, os americanos colocaram em validade ainda naquela época o *Terrorist Finance Tracking Program*, que rastreava, a pretexto de bloquear transferências de dinheiro entre terroristas, todas as operações bancárias de transferência internacional de valores que envolvessem a SWIFT, a *Society for Worldwide Interbank Financial Telecommunication*, uma cooperativa financeira baseada na Bélgica que operadora de mais de 90% das transferências financeiras internacionais[160]. Em 2010 o Parlamento

---

[157] ROSENBACH, Macel. Prism Exposed: Data Surveillance with Global Implications. *Spiegel*, online, 10.06.2013. Disponível em: http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761.html>. Acesso: 09.09.2017.

[158] La Patriot act es uma ley extensa y compleja que introduce modificaciones sustanciales em 15 leyes federales y que confiere inusuales poderes ejecutivos a estruturas operativas de control y a los servicios de intelligence. No obstante, pese a la complejidad de muchas de sus normas y su incidência sobre valores constitucionales, fue aprobada por el congresso a través de um procedimento de urgência, sin debate ni enmiendas dignas de destacar. Aunque el documento incorporo propuestas anteriores al 11 de septiembre, éstas asumieron um rol claramente marginal em el debate del Congreso, ante todo porque uma amplia mayoría las consideraba letales para los derechos civiles e incluso ponían em duda su compatibilidade com la Constituición." (VERVAELE, J.A.E. *La legislación…*, cit., p. 12.)

[159] Ver mais em http://www.statewatch.org/news/2003/dec/apis_en.pdf e http://www.cov.com/files/Publication/8aa81e95-460a-4d30-a901-28b14757ec00/Presentation/PublicationAttachment/37f11b14-ff49-4e95-a5ce- 2ee016f94329/oid23778.pdf

[160] Quanto a isto, vale ressaltar o anotado por John Vervaele "Los Bancos Centrales de Canadá, Alemania, Francia, Italia, Japón, Holanda, Reino Unido, Suecia, la Reserva Federal (Banco Central) de Estados Unidos y el Banco entral Europeo (BCE son las diez entidades encargadas de supervisar la actividad de SWIFT. La implicación de

Europeu rejeitou uma proposta que previa a entrega obrigatória destas transações sempre que a autoridade estadunidense indicasse uma situação de investigação de terrorismo. Essa decisão só foi possível porque os servidores da SWIFT estão sob jurisdição europeia.

As implicações destes atos de espionagem posteriores ao Ato Patriota são muito sérias: o governo dos EUA passou desde então a monitorar boa parte dos deslocamentos, transações financeiras e transmissões de dados de cidadãos do mundo todo, sem qualquer respeito às leis de outras nações, à intimidade, um dos direitos humanos fundamentais garantido na Declaração Universal dos Direitos Humanos da ONU, e ao direito fundamental à proteção de dados, consagrado na União Europeia nas últimas décadas[161]

O PRISM, principal programa de monitoramento conhecido daquele país deveria monitorar, segundo os mandados concedidos pela *US Foreign Intelligence Surveillance Court* (uma corte criada em 1978 especialmente para autorizar missões de segurança de agências especializadas do governo), apenas pessoas fora dos EUA. O principal supedâneo legal para a implementação da vigilância pela Corte é a Section 702 do *Foreign Inteligence Surveillance Amendments Act*, que deve ser renovada pelo Congresso dos EUA a cada dez anos.

Documentos obtidos por Snowden, no entanto provam que a NSA abriu o acesso ao PRISM (pelo menos parcialmente) para seus aliados do programa FIVE EYES, a saber: Reino Unido, Canadá, Austrália e Nova Zelândia. Por mais de uma vez, quando a NSA queria obter acesso aos dados de residentes nos EUA, para manobrar sua jurisdição, a agência pediu para seus aliados deste programa, por via do próprio PRISM, consultarem e lhe repassarem o que fosse preciso. Em pelo menos uma ocasião, documentada pelo *New York Times*, a NSA quebrou o sigilo advogado-cliente por este caminho, em favor do governo americano[162]. Ou

---

ocho bancos centrales europeos – además del próprio BCE – em la entrega secreta de información bancária a Washington supone um nuevo caso de colaboración transatlântica de dudosa legalidade surgida bajo la conmoción de los atentados del 11 de septiembre. La comisión belga de protección de datos há juzgado que SWIFT há violado el derecho europeo y belga, y critica a SWIFT por no haber informado a la Comisión Europea y a las autoridades belgas sobre el conflito legal entre las obligaciones legales de Estados Unidos, de Europa y Bélgica." (VERVAELE, J.A.E. *La legislación…* cit., p. 48.). O autor faz referência à Opinión nº37/2006 de 27 setembro de 2006. O caso SWIFT pode ser encontrado em http://www.statewatch.org/news/2008/may/eu-us-swift-doc.pdf e https://www.privacyinternational.org/projects/swift. Acesso em: 06/09/2017.

[161] Article 12: .No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." United Nations (UN) Universal Declaration of Human Rights (UDHR) – Disponvel em: http://www.un.org/en/documents/udhr/index.shtml

[162] Cf. POITRAS, Laura; RISEN, James. Spying by N.S.A. Ally Entangled U.S. Law Firm. The New York Times, online, 15.02.2014. Disponível em: https://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-

seja, nesse caso, o poder tecnológico foi capaz de driblar até regras autoimpostas pelos agentes de poder.

Países menos democráticos e com restrições à atividade da imprensa, a exemplo de China e Rússia, pelo poder que demonstram na rede, certamente têm a capacidade de operar sistemas semelhantes.

Apesar da bandeira de combate ao terror, a verdade é que os dados obtidos pela NSA ou por outras agências e governos têm muito mais importância estratégica e econômica. OS EUA, por exemplo, espionaram, via PRISM, todas as conversações da Conferência das Nações Unidas para mudança climática em Copenhagen, segundo documentos obtidos pelo *The Guardian*[163].

Há alguma proteção à privacidade na quarta emenda da Constituição dos EUA, que garante o direito a "personalidade, domicílio, escritos e dados", mas que como relata BOEHM[164] é realmente relativizada em nome do interesse público.

O *Privacy Act*, de 1974, garante o processamento justo de dados dos cidadãos americanos e residentes permanentes naquele país. De todo modo, a normativa está desatualizada frente aos desafios atuais e foi bastante relativizada no contexto de combate ao terrorismo.

O uso de modernas técnicas de investigação[165] pode ajudar efetivamente agentes governamentais na busca por suspeitos e criminosos na Sociedade em rede, mas é preciso

---

law-firm.html. Acessado em 22.02.2014. Além disso, John Vervaele anota que "It goes without saying that all these transformations affect the position of the defence lawyer in the criminal process. His legal privilege is under pressure. In certain countries, when dealing with secret evidence in cases of organized crime and terrorism, the defence lawyer has no full access to the file (limited disclosure) or only special security screened bar lawyers can act on behalf of the suspect. The defence lawyer's role and his duties and responsibilities are redefined." (VERVAELE, J.A.E. Survillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system? In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014. P. 25)

[163] VIDAL, John. Snowden revelations of NSA spying on Copenhagen climate talks spark anger. The Guardian, online, 30.01.2014. Disponível em: http://www.theguardian.com/environment/2014/jan/30/snowden-nsa-spyingcopenhagen-climate-talks. Acessado em 22.08.2017.

[164] BOEHM, Franziska, *A comparison between US and EU data protection legislation for law enforcement purposes.* Directorate general for internal Policies, European Parliament: Bruxelas, 2015. p. 51

[165] Segundo John Vervaele "proactive criminal investigation includes the situation in which there is not yet any reasonable suspicion that a crime has been committed, is about to be committed or that specific preparatory acts have taken place and in which, of course, there can be no suspect(s) legally speaking. The objective of proactive investigations is to reveal the organizational aspects in order to prevent the preparation or commission of a serious crime and to enable the initiation of criminal investigation against the organization and/or its members." (VERVAELE, J.A.E. *Survillance*… cit., p. 121.)

estabelecer diretrizes ao uso da técnica. Os softwares de vigilância eram capazes, até o final da década de 1990, de entregar aos agentes do Estado trocas de mensagens, interceptações telefônicas e movimentações bancárias dos alvos de investigações. O que vivenciamos agora está muito além disso e os EUA são protagonistas nas violações nesse campo.

Este tipo de atividade é capaz de ameaçar as garantias de um suspeito, que vigiado eletronicamente, tem seu sigilo de dados quebrado. Segundo VERVAELE, o Estado utiliza-se deste aparato de vigilância como mecanismo de administração do risco, mesmo que isto consagre a adoção do *ius puniendi* contra toda a sociedade[166], o que de maneira alguma pode ser encarado com normalidade.

Quando nos confrontamos com a realidade que a reunião desses dados é realizada por agentes terceirizados, portanto particulares, e que o fluxo de informação que abastece esse tipo de iniciativa é todo ele de origem de outros agentes privados – plataformas, redes sociais etc – temos uma vaga percepção da gravidade e extensão do problema.

### 1.4.2 União Europeia

A intimidade, preocupação constante de alguns países na sociedade da informação, viu nascer, nos últimos anos um direito fundamental equiparável: a proteção ao sigilo de dados. A União Europeia é protagonista na criação desse direito e vem dedicando-se a estabelecer princípios para a coleta, armazenamento e uso de dados pessoais por indivíduos, organizações e pessoas desde o início da década de 1980, com a *Convenção 108*.[167]

Pela sensibilidade do que a coleção de dados de um indivíduo pode fornecer para quem tem a habilidade para estuda-los, em 2006 a UE adotou a *Directive on retention of communication traffic data*, promovendo a uniformização das regras para provisão de dados

---

[166] "We are living in a setting of time in which many reforms of the criminal justice system are the result of a political instrumentalisation and mediatisation of crime and the fear of crime. These reforms are being justified by the criminal policy paradigms of combating drugs, organized crime and terrorism. The result is that the ius puniendi of the state (being one of the most repressive interferences in liberty on behalf of the state), is being instrumentalised and put at service of danger and risk management. When prevention of dangerousness becomes the triggering mechanism for the use of very intrusive investigative techniques, as secrete surveillance or systematic targeted surveillance and criminal punishment, the criminal justice system is risking perverting into a security system." (VERVAELE, J.A.E. *Survillance*… cit., p..126).

[167] Disponível em http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acessado em 22.09.2017.

por parte dos provedores às autoridades do bloco e para regular os limites de armazenagem destes dados. Ainda assim, o alcance do uso dos dados para investigações criminais continuou a critério de cada Estado Membro. Em 08 de abril de 2014, a *European Court of Justice* considerou que este tipo de armazenamento viola dois direitos fundamentais – o respeito a vida privada e a proteção de dados pessoais. Segundo a Corte "ao exigir a retenção desses dados e permitir que as autoridades nacionais competentes tenham acesso a eles, a diretiva interfere de uma forma particularmente grave com os direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais"[168].

A UE adotou um novo *Charter of Fundamental Rights* em 2009 para revisar, entre outras coisas, a proteção aos dados pessoais, que ganhou caráter de direito fundamental, equiparando-se à liberdade de expressão e à garantia a um julgamento isento. Pode-se entender o novo caráter protetivo da lei como uma evolução do direito à privacidade: a proteção dos dados pessoais é um novo campo de proteção, originado da proteção à privacidade.

Antes de tudo isso, em 1995, pela diretiva 95/46/EC, a União Europeia já tinha sua primeira legislação geral de dados. A diretiva foi complementada em 2002 pela diretiva 2002/58/EC *on Privacy and Electronic communications.* Recentemente, em 2016, depois de quatro anos de negociações, o bloco europeu logrou aprovar a seu Regulamento Geral de Proteção de Dados – GDPR na sigla em inglês. A nova legislação entrará em vigor apenas em 25 de maio de 2018 e é a mais moderna do tipo no ocidente. Ela prevê avanços como o consentimento justo no uso dos dados (o que quer dizer que os contratos, que são praticamente de adesão, de uso de plataformas deverão ser inteligíveis e diretos), o aviso em 72 horas ao usuário em caso de vazamentos de informações; os usuários europeus têm a partir da lei o direito de saber dos provedores e aplicações como os seus dados pessoais estão sendo utilizados, onde e com qual propósito, o direito ao esquecimento – no aspecto da desindexação, como veremos adiante -, a portabilidade dos seus dados na rede, a adoção do *privacy by design* como *standard* e a imposição da figura do *Data Protection Officer* (DPO). [169] Trata-se de uma legislação avançada, que poderia servir de modelo para uma Lei Geral de Dados no Brasil.

---

[168] "By requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data" Disponível em: http://www.bbc.com/news/worldeurope-26935096

[169] Disponível em www.eugdpr.org e http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

A *European Court of Human Rights* - ECtHR – também deu mostras de avanços nos últimos anos. A Corte se dedica a regulação do tema antes mesmo da UE, desde a década de 1980. Com base no artigo 8º de sua Carta, a ECtHR passou a entender que a proteção de dados pessoais eletrônicos goza do mesmo status da proteção à "vida privada", *por analogia"*[170]. No ano 2000 no caso *Rotaru* v. *Romenia*, a Corte deixou bastante claro o *standard* que adota para a proteção de dados: dados referem-se à "qualquer informação relacionada a identificar ou a tornar identificável um indivíduo*"*[171]. Estão, portanto, além da simples esfera de "vida privada" dos indivíduos, configurando proteção maior, a exemplo do que também adota a Lei de Acesso à informação brasileira.

O que está em jogo é a dignidade dos indivíduos e organizações. Há dois caminhos: um sob o discurso da segurança pública, que parece o adotado pelos EUA e fragiliza a intimidade dos cidadãos, criando possíveis detentores de dados sob os quais não se pode ter controle – ainda mais com um belicoso governo Trump; e um segundo caminho, sob o signo da proteção de direitos, que parece ser o adotado pela UE. Neste último, é preciso fazer cumprir as leis que protegem a intimidade e avançar sempre na direção das proteções. Se aplicado eticamente, é este segundo o único caminho a possibilitar o desenvolvimento da sociedade.

Em ambos os casos importa que a intimidade, enquanto valor fundamental para o desenvolvimento da personalidade, esteja bem protegido – inclusive por noras penais, se for o caso, como veremos adiante. Quanto a isso, DE LA CUESTA nota que:

> "En realidade, lo importante no es tanto aferrare a las reglas y mecanismos tradicionales, que el uso de as TIC puede facilmente rodear y evitar, sino caminhar hacia un mundo virtual en el que las garantias y derechos fundamentales de los indivíduos, en particular, el derecho a la inmidad y la libre expresión, queden igualmente garantizados en el marco de los procedimentos de investigación y enjuiciamiento de carácter penal que han de seguir respectando los estândares de un juicio justo. (...)En la actualidad, es preciso dar passos eficaces para que la

[170] ECtHR, Copland v. the United Kingdom, § 41.

[171] ECtHR, Rotaru v. Romania, § 43: "The Court has already emphasised the correspondence of this broad interpretation with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is 'to secure . . . for every individual . . . respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him' (Article 1), such personal data being defined in Article 2 as 'any information relating to an identified or identifiable individual." Consultar também o artigo 2(a) da Convenção de 1981 e o artigo 2(a) da Diretiva de 1995.

> incapacidade por parte de los Estados de aplicación en el mundo virtual no lleve a la desprotección de los derechos humanos en el ciberespacio."[172]

Concordamos com a posição do Professor e notamos que os exemplos tanto dos EUA quanto da UE devem servir para inspirar o legislador brasileiro a buscar caminhos para proteger cada vez mais a intimidade no nosso país.

## 1.5 Coleções de dados no Brasil

### 1.5.1 O Marco Civil do Ciberespaço brasileiro

A internet chegou ao Brasil em 1988, por iniciativa da FAPESP (a Fundação de Amparo à Pesquisa do Estado de São Paulo). Mas foi apenas em 1995, por iniciativa do Ministério das Comunicações (hoje Ministério da Ciência, Tecnologia, Inovações e Comunicação – MCTIC), que se estabeleceu a primeira regulamentação da rede no país, com a criação do CGIbr – o Comitê Gestor da Internet no Brasil.[173]

Desde então, já experimentamos mais de uma onda legislativa com condão de regular aspectos penais da rede. A primeira lei expressiva nesse sentido foi a nº 11.829/2008, que trouxe arcabouço jurídico para o combate a disseminação de pornografia infantil na internet. O passo seguinte foi dado apenas em 2012, quando a atriz Carolina Dieckmann teve fotos intimas divulgadas amplamente na rede sem seu consentimento. O Congresso Nacional aprovou em velocidade incomum a Lei nº 12.737/2012 para disciplinar os casos de invasão de dispositivos informáticos. Típica lei de ocasião, a Lei Carolina Dieckmann perdeu conveniente oportunidade de trazer satisfatória disciplina jurídico-penal para o ciberespaço brasileiro[174].

A última mudança significativa deu-se com o estabelecimento do Marco Civil da internet. A par de ser uma legislação moderna quanto ao estabelecimento de princípios para a rede, não existem ali quaisquer tratamentos para possíveis delitos informáticos ou relacionados à privacidade, à intimidade e suas violações na rede. O Marco legal, enquanto regulação do

---

[172] DE LA CUESTA ARZAMENDI, José Luis. Sociedad de la información y derecho penal: a la luz del XIX *congreso internacional de derecho penal*. Revista Brasileira de Ciências Criminais, São Paulo, v. 23, n. 112, p. 79-106., jan./fev. 2015. P. 102.

[173] ZANIOLO, Pedro A., *Crimes modernos*: o impacto da tecnologia no direito. Curitiba: Juruá, 2007. p. 103-104.

[174] "A Lei n. 12.737/2012 tramitou durante uma década no Congresso Nacional, o que não impediu que surgisse com recurso exagerado a elementos normativos com imprecisões técnicas palpáveis" REALE JÚNIOR, Miguel (org.), *Código penal comentado.* São Paulo: Saraiva, 2017.

ciberespaço brasileiro, poderia ter estabelecido normas gerais para todos os agentes que constroem hoje a internet no Brasil, elencando condutas e estabelecendo tipos penais.

Num contexto mais genérico, o Marco Civil estabeleceu uma série de princípios a partir dos quais devemos desenvolver modulações que busquem levar ao papel o cenário virtual. São várias as evoluções necessárias, notadamente ligadas a proteção ao desenvolvimento da personalidade (enunciada no art. 2, II do Marco) ainda por vir.

Em 1990, a ONU já havia estabelecido um guia de princípios a serem respeitados para que o sigilo comunicacional esteja assegurado, com relação aos dispositivos eletrônicos, são eles: princípio da legalidade e equidade, princípio da precisão, princípio do uso justificado, princípio do acesso exclusivo a pessoa interessada, princípio da não discriminação, princípio do poder de fazer exceções em relação aos dados acessados, princípio da supervisão, fiscalização e sanção e princípio do respeito ao fluxo transfronteiriço de dados[175].

O Marco Civil da Internet brasileira é eminentemente principiológico. Ele segue o formato da Resolução 2009/003 do CGIbr, que ficou conhecida como "*Decálogo de princípios para a governança e o uso da internet no Brasil*". Estão lá, além da privacidade, uma série de princípios frente aos quais o uso do ciberespaço brasileiro deve ser regulado, dentre eles: liberdade, observância dos direitos humanos, governança colaborativa, universalidade, diversidade, inovação, neutralidade da rede, funcionalidade, segurança, estabilidade e interoperabilidade.

Seja qual for a base adotada, é certo que a capacidade de um indivíduo para controlar os termos em que suas informações pessoais são adquiridas e utilizadas é o ponto de empoderamento da proteção da privacidade de seus dados na rede[176]. Tal habilidade está diretamente condicionada ao que será oferecido ao usuário. O raciocínio mercadológico é bastante simples: quanto mais dados a aplicação reúne de um usuário, maior será sua capacidade de oferecer produtos e serviços para esse potencial cliente. O da autodeterminação do uso de dados também: quanto melhor a regulação sobre as aplicações, maior será a independência na

---

[175] UN Guidelines Concerning Computerized Personal Data Files, Nova York: Assembléia Geral da ONU, 14 de Dezembro de 1990. Disponível em: http://www.un.org/documents/ga/res/45/a45r095.htm Acesso em 28.05.2016 (Trad. livre).

[176] "The ability of an individual to control the terms under which their personal information is acquired and used' is often presented as the hallmark of data protection." (POULLET, Yves; ROUVROY, Antoinette. *The right*… cit., p. 68.)

tomada decisória.

Esta capacidade está, portanto, no cerne do problema da proteção da privacidade na sociedade da informação. Pode-se afirmar, com isso que, a par do conjunto protetivo disposto nos princípios que regem a internet no Brasil – contido no Marco regulatório –, é preciso que estabeleçamos limites mais claros. Precisamos achar soluções aplicáveis aos novos injustos a partir do conjunto de princípios postos – que já parecem ser pilar suficiente.[177]

Apesar dos fundamentos não se pode dizer que a Lei já tenha tratado de todas as novas situações. Em seus 32 artigos, mesmo que sejam louváveis a garantia da privacidade e da intimidade (art. 7, I), da inviolabilidade e sigilo das comunicações (art. 7, II e III), do não fornecimento a terceiros de dados pessoais (inclusive dos registros de acesso a aplicações – art. 7, VII) e de informações claras quanto ao uso, armazenamento, tratamento e proteção de dados – com finalidade destinada apenas ao quanto previsto em contratos ou termos (art.7, VIII, *c* ), e que tudo isso não possa ser objeto de contrato de adesão que não ofereça foro brasileiro (art. 8, II), neste ponto da história, por mais improvável que possa parecer, boa parte das aplicações – e notadamente as redes sociais – conseguem driblar, um a um, todos esses direitos.

Não é que o Marco Civil seja completamente ausente na proteção dos dados pessoais e da intimidade, mas também não é que seja assente: a Lei toma conhecimento da discussão ao elencar que "qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais (...)em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros*"* (art. 11, caput), mas depreca ao Decreto regulatório o procedimento de apuração de infrações a esse ponto (art. 11, § 4º ). O Decreto nº 8. 771, por sua vez, repassa ao CGI a responsabilidade.

---

[177] Citando o REsp 1.168.547/RJ, da 4a Turma do STJ, j. 11.05.2010, v.u., rel. Min. Luis Felipe Salomão, DJe 07.02.2011, "[i]n recent years, issues concerning data protection on the Internet have entered the courts and compel the courts to find adequate solutions within the existing framework. A recent decision of the Superior Court of Justice, concerning a disclosure of a picture on a website, indicates how the problem of data protection on the Internet is increasingly gaining relevance in the Brazilian legal system. In this case, the court decided that the company that controlled the website was liable for the misuse of the image and had to pay compensation for material and moral damages. Central to the decision was the opinion of the rapporteur, which discussed the new challenges posed by the Internet to the legal system and recognized that technological innovations gave rise to the development of a new concept of privacy, based on the control of personal information by the individual." (DONEDA, Danilo; MENDES, Laura S. Data protection in Brazil: new developments and current challenges. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014.)

O Marco Civil considera o ciberespaço como uma ferramenta fundamental para a liberdade de expressão. Segundo o conteúdo dele, a internet deve permitir ao brasileiro que se comunique e se manifeste como bem entender, nos termos da Constituição. O texto aponta que "*o acesso à internet é essencial ao exercício da cidadania*", com a garantia de que a privacidade não será violada, a qualidade da conexão estará em linha com o contratado e que dados do cidadão só serão repassados a terceiros se o titular deles aceitar.

Há ainda questões polêmicas que merecem maior investigação da Lei por parte dos agentes públicos. Os diversos bloqueios do WhatsApp são exemplos disso. A aplicação, que pertence ao Facebook, foi bloqueada por mais de uma vez, como medida coercitiva para que entregasse dados de usuários para autoridades brasileiras. O WhatsApp tem mais de 100 milhões de usuários ativos no Brasil[178] e seu bloqueio é o equivalente a retirada do ar de um dos principais meios de comunicação em nosso território, um evidente equívoco.

O CGI pronunciou-se para esclarecer, acertadamente, que, segundo sua visão,

> [o] art. 12 da Lei nº 12.965/2014 (Marco Civil da Internet) autoriza tão somente a suspensão temporária das atividades que envolvam os atos elencados expressa e taxativamente no art. 11 do mesmo diploma legal: "a operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet". Nesse sentido, o teor do art. 12 do Marco Civil da Internet não se refere à aplicação extensiva da lei para que se determine a suspensão total e irrestrita das atividades de empresas prestadoras de serviços e aplicações de Internet.[179]

Muito mais eficaz seria, portanto, que fosse aplicada uma outra sanção ao aplicativo ou à rede social que o detém, como a imposição de multa. Em verdade, as sanções precisam ser aplicadas da menos grave à mais grave, desde a advertência até a proibição da empresa exercer a atividade no país.

De fato, o WhatsApp utiliza a criptografia de ponta a ponta, método consagrado de proteção de dados pessoais e mais recomendável medida nesse sentido hoje – inclusive consagrada tanto no Marco Civil quanto no seu Decreto regulamentador. É fato, porém, que o artifício protetor pode voltar-se contra a sociedade, na medida em que criminosos podem

---

[178] COSSETTI, Melissa Cruz. Facebook revela dados do Brasil na CPBR9 e WhatsApp 'vira ZapZap'. *TechTudo*, online, 28.01.2017. Disponível em: http://www.techtudo.com.br/noticias/noticia/2016/01/facebook-revela-dados-do-brasil-na-cpbr9-e-whatsapp-vira-zapzap.html. Acesso em 22.05.2017.

[179] RIBEIRO, Gabriel. Bloqueio do WhatsApp fere o Marco Civil da Internet? Veja a posição do CGI. TechTudo, online, 19.12.2015. Disponível em: http://www.techtudo.com.br/noticias/noticia/2015/12/bloqueio-do-WhatsApp-fere-o-marco-civil-da-internet-veja-posicao-do-cgi.html Acesso em 28.05.2016.

utilizar-se da opacidade para cometer atos criminosos. Há até quem defenda que o caminho correto para a obtenção dos diálogos de usuários do WhatsApp seria o da cooperação internacional, a exemplo do que ocorrem nos vultuosos casos de crimes financeiros[180].

Não parece ser o caso. Se nos crimes financeiros as autoridades brasileiras acionam as autoridades de outros países para obter informações de alguns milhares de correntistas brasileiros em bancos estrangeiros, na requisição de conversas pelo WhatsApp o volume parece mais próximo a casos de informações advindas de operadoras de telefonia móvel, quando entregam para as autoridades conversas via SMS, só que criptografadas – diferença essencial.

Empresas que atuam com aplicações do tipo poderiam, porém, estabelecer métodos de cooperação legítimos e claros com as autoridades. Isto não está nem perto de dizer que a empresa deva deixar de adotar a criptografia nas conversas de seus usuários ou que deva fornecer uma *backdoor* para as autoridades – ambas alternativas vedadas pelo texto do Decreto Regulamentador do Marco Civil, além de comprometedoras da privacidade. É que, como visto, parece impossível que o país ignore o potencial de uma aplicação com 100 milhões de usuários em seu território que adota criptografia de ponta a ponta.

Não existe ainda uma via exatamente adequada, precisamos rediscutir o próprio acesso das autoridades aos dados. Não se trata de impor a entrega da chave criptográfica[181] mas

---

[180] Nesse sentido a opinião de Ronaldo Lemos, apontado como um dos principais idealizadores do Marco Civil da Internet. Disponível em: http://veja.abril.com.br/tecnologia/suspensao-do-WhatsApp-mostra-fragilidade-da-internet-brasileira-diz-idealizador-do-marco-civil/ Acesso em: 28.05.2016.

[181] Aqui vale apontar a recente polêmica entre as autoridade norte-americanas e a Apple quanto à entrega da chave criptográfica do sistema iOS da empresa para que o FBI investigasse um dos terroristas responsáveis pelos ataques de San Bernardino, Califórnia. No começo de 2016 a Apple enfrentou uma batalha judicial e de opinião pública com o FBI ao se negar a entregar a chave de criptografia de seu sistema, o que equivaleria a construir um sistema para burlar suas próprias regras de ambiente seguro. O FBI argumentava que precisava da chave para investigar o terrorista. A Apple argumentou que uma equipe de 10 engenheiros levaria 10 dias para quebrar toda a criptografia daquele aparelho específico e que o que o FBI queria na verdade era a criptografia de todo o sistema, dando livre acesso a todos os Iphones no mundo. Depois de alguns meses, o FBI desistiu da ação contra a empresa e divulgou que tinha obtido a chave de criptografia. A Apple está processando o Departamento de Estado Norte-americano para que o Estado seja obrigado a revelar seu método. Mesmo diante dessa situação, a empresa não se furtou a disponibilizar os dados que detinha em backup do terrorista. Disponível em: http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0, http://g1.globo.com/tecnologia/noticia/2016/02/apple-x-fbi-disputa-e-mais-dificil-diz-diretor-da-policia-federal-dos-eua.html, http://g1.globo.com/tecnologia/noticia/2016/03/fbi-desbloqueia-iphone-de-terroristas-e-encerra-processo-contra-apple.html, Acesso em: 28.05.2016. É esse o ponto defendido aqui com relação ao WhatsApp: a empresa precisa ser obrigada a manter acesso a backups de conversas de seus usuários para, quando instada, entregar esses dados para as autoridades.

de estabelecer ao menos um canal permanente de diálogo, em que as autoridades possam requisitar, ao invés do conteúdo das conversas, os dados de localização, por exemplo.

Numa analogia com a obrigação dos provedores de manterem por um tempo determinado os registros de acesso de seus usuários, poderia se estabelecer a obrigação de aplicações como o WhatsApp de manterem os registros dos participantes em uma conversa, por um certo período.

Ao contrário de estimular investigações proativas[182], esta via poderia estabelecer uma alternativa para ao menos esclarecer entre quais usuários e quando comunicações ocorreram – jamais disponibilizando métodos obscuros de acesso para as autoridades em nome do interesse público[183]. Na sociedade do risco, apenas bradar pela opacidade sem entregar alternativas aos agentes responsáveis pela segurança é ignorar os novos desafios.

Há ainda outros exemplos da necessidade de rediscussão das normas penais que não estão abarcados no Marco Civil. É o caso do compartilhamento não autorizado na rede de imagens inapropriadas com conteúdo de tortura ou estupro ou com nudez ou conteúdo sexual.

Esse procedimento de apuração é importante não apenas porque pode desvendar os meandros das coleções de dados, mas porque pode estabelecer *standards* de limites de influência das redes no conteúdo disponibilizado para os seus usuários. Trata-se de um ponto

---

[182] "Proactive criminal investigation includes the situation in which there is not yet any reasonable suspicion that a crime has been committed, is about to be committed or that specific preparatory acts have taken place and in which, of course, there can be no suspect(s) legally speaking. The objective of proactive investigations is to reveal the organizational aspects in order to prevent the preparation or commission of a serious crime and to enable the initiation of criminal investigation against the organization and/or its members." (VERVAELE, J.A.E. *Survillance*… cit., p. 121.)

[183] Para que fique claro, deve-se observar o que ensina VERVAELE: "We are living in a setting of time in which many reforms of the criminal justice system are the result of a political instrumentalisation and mediatisation of crime and the fear of crime. These reforms are being justified by the criminal policy paradigms of combating drugs, organized crime and terrorism. The result is that the ius puniendi of the state (being one of the most repressive interferences in liberty on behalf of the state), is being instrumentalised and put at service of danger and risk management. When prevention of dangerousness becomes the triggering mechanism for the use of very intrusive investigative techniques, as secrete surveillance or systematic targeted surveillance and criminal punishment, the criminal justice system is risking perverting into a security system. (…)Due to the secrecy of the modus operandi of surveillance techniques the basics of natural justice, such as equality of arms, disclosure between the parties and open confrontation are being adapted to shield surveillance agents, their modus operandi and part of the evidence. Investigative surveillance does contribute to inquisitorial secret proceedings. Equality of arms and fair trial are not absolute human rights. Legitimate aims (such as the protection of security) can justify restrictions. However, there is a bottom line for fairness: the procedure must be fair as a whole. This means that the defendant must be able to prepare his defence and challenge the evidence at trial. It also means that the judiciary must have full access to the file in order to balance the rights of the defence and security. Without judicial supervision (justiciability) surveillance is a potential undermining factor of the thresholds and guarantees in the criminal justice system." (VERVAELE, J.A.E. *Survillance*… cit., p. 126-127.)

fundamental na proteção da privacidade, na intimidade e na proteção do sigilo de dados na rede que não pode deixar de ser discutido.

A proteção de dados deve envolver um conjunto de leis e práticas político-sociais capazes de transformar o fluxo de dados em algo adequado e seguro, dentro de limites éticos e apenas para fins estritos, devolvendo ao indivíduo o controle da formação de suas opiniões[184]. Neste Sentido, a Corte Constitucional Alemã explicitou que "é um pré-requisito para o livre desenvolvimento da personalidade sob condições modernas de processamento de dados que o indivíduo necessite de proteção contra a coleta, armazenamento e transmissão ilimitada de seus dados"[185] Apesar de todos os esforços, o Marco Civil ainda não é capaz de estabelecer esse tipo de proteção. Mesmo que estabeleça a guarda da privacidade enquanto um princípio da rede, a Lei deixa um salto normativo quanto ao estabelecimento de limites da privacidade de dados online[186].

A aquisição de tamanho poder por parte dos atores privados passou, em boa medida, desapercebida pelo legislador. O Marco Civil não trata em momento algum do monitoramento por *cookies*, histórico de cliques e marketing comportamental – e deixa igualmente de lado a penalização dos excessos nessas condutas[187].

---

[184] Neste sentido, Poullet e Rouvroy "According to the [German] Constitutional Court's opinion the development of the data processing technologies obliged the State to revise and adapt the guarantees it provides to individuals in order to protect and foster the capabilities needed to implement their right to freely self-determine their personality. In the circumstances of the day, the legal protections offered to the individuals' capabilities for self-development would probably need to address the specific threats accompanying the development of ubiquitous computing and ambient intelligence". (POULLET, Yves; ROUVROY, Antoinette. *The right*… cit., p. 55.)

[185] "The German Constitutional Court therefore explicitly acknowledged that "it is a prerequisite of free development of the personality under modern conditions of data processing; the individual needs protection against unlimited collection, storage and transmission of his personal data." (POULLET, Yves; ROUVROY, Antoinette. *The right*… cit., p. 56.)

[186] É o que também pensam Danilo Doneda e Laura Mendes: "problems related to data protection in the Internet need a special attention of the regulators. Problems concerning data protection in social networks, cookies, behavioral advertising, cloud computing as well as problems related to privacy on smart phones demand a specific approach. It is clear that these are all transnational problems, and as such they need a supranational response. Nonetheless, it is important to address these questions, in order to solve the problems and demands in the national level. The proposed law 2126 of 2011 commonly referred to as the Civil Framework for the Internet, deals, among many issues, also with data protection on the Internet. It aims to establish a set of rights to all Internet users in Brazil and announces as guiding principles both the "protection of privacy" and "protection of personal data, under the terms of the law." In this context, both the Civil Framework for the Internet and the Data Protection draft bill are certainly important steps in this direction, although they don't address all these specific questions regarding online privacy." (DONEDA, Danilo; MENDES, Laura S. Data protection in Brazil: new developments and current challenges. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014._

[187] Segundo Jeff Chester "While the debate on privacy and online marketing has focused on behavioral profiling—so called Online Behavioral Advertising (OBA)—such practices are only a part of the overall data collection

É possível afirmar que a coleção de históricos informáticos dá ao detentor a exata medida de como nos comportamos na internet. Sendo assim, é razoável supor que ao detentor dessas coleções de dados sejam impostas regulações e tipos penais pelo abuso no uso da privacidade de quem lhe forneceu tais dados.

DANILO DONEDA e LAURA MENDES argumentam que essa situação é na verdade prejudicial tanto para os usuários da rede quanto para os empresários – que ficam expostos a um vazio regulatório, o que, ao invés de significar maior liberdade da rede, se traduz em incertezas negociais para o futuro. Exemplo disso é a falta de diretrizes para o desenvolvimento nacional de computação em nuvem[188], campo desregulamentado no país. Para os autores, é necessário um entendimento setorial para que seja aprovada uma regulação desses vazios.

A importância desse novo meio relacionamentos não comporta mais o tratamento de um simples produto com o qual se concorde ou não com os termos de uso. A liberdade na rede passa, necessariamente, pela regulação dos agentes detentores de dados relacionados à privacidade do usuário no ciberespaço. Esses dados significam hoje um poder que merece atenção do direito penal.

O Marco Civil e o seu decreto regulamentador, mesmo que dignos de reconhecimento no esforço para a garantia da privacidade das comunicações, não resolveram os problemas ligados ao tema. É preciso ir além, talvez com o estabelecimento de uma Lei Geral de Dados e de uma autoridade de Dados. Um ou outro caminho precisam dar subsídios

---

apparatus. From social media surveillance tools and "in-game" advertising tracking, to online video measurement and location tracking, a bevy of increasingly inter-connected user data services are deployed to track us throughout the interactive landscape. Our Internet experiences are also shaped, invisibly, by technologies that "optimize" how we interact with Web pages, to help manage our online journeys so we will "convert" to whatever the digital marketer desires us to do (such as buying a product or filling out a form). A growing range of "immersive" and neuromarketing-based applications, designed to convince us to accept the enjoyable pleasures of much of contemporary online marketing-based content, has added new forms of "subliminal persuasion" to the data collection equation" (CHESTER, J. *Cookie Wars*… cit., p. 55.)

[188] "In Brazil, the lack of a broad regulation in this field has increasingly been considered as a problem both by citizens and by companies: on the one hand, citizens are more and more aware of the risks of an uncontrolled data flow, as issues such as identity theft and commercial abuse of personal data have gained visibility; on the other hand, compliance with international standards concerning the international transfer of personal data and a strong set of rules governing data protection in general are considered a necessity for the development of new businesses in the country, such as cloud computing. In this context, a comprehensive data protection act is seen at the same time as a way of ensuring more protection to the citizens, concerning the processing of their personal data, and increasing legal certainty to the companies, regarding how to process and use personal data within the legal framework. Furthermore, analyzing the current data protection framework in Brazil, we see that there are some challenges to be faced, which would need a sectorial approach." (DONEDA, Danilo; MENDES, Laura S. *Data protection*… cit. p. 16-17.)

para a solução da contínua coleta de dados no país.

### 1.5.2 Direito ao esquecimento

O Direito ao esquecimento vem ganhando novas arenas de debate no Brasil nos últimos anos. Exemplo disso são os casos *Aida Curi* e da *Chacina da Candelária*, ambos já julgados no STJ e aguardando julgamento no STF. No julgamento do *Recurso Especial* no caso Aida Curi, o Ministro Luis Felipe Salomão asseverou em seu voto que:

> Com efeito, no conflito entre a liberdade de informação e direitos da personalidade - aos quais subjaz a proteção legal e constitucional da pessoa humana -, eventual prevalência pelos segundos, após realizada a necessária ponderação para o caso concreto, encontra amparo no ordenamento jurídico, não consubstanciando, em si, a apontada censura vedada pela Constituição Federal de 1988.[189]

Aviva-se, então, a necessidade e urgência na regulação do uso de dados que podem afetar a intimidade e a privacidade do indivíduo por meios de comunicação e buscadores de internet. O direito de informar não pode sobrepor-se a outros, igualmente constitucionais. Cumprida a pena, os fatos que cercam um ato criminoso precisam ser superados.

É da nossa Constituição Federal a vedação expressa às penas de caráter perpétuo – art. 5º, inciso XLVII – e do nosso Código Penal a imposição de um marco temporal para os efeitos das penas, de cinco anos a contar da data de seu cumprimento ou extinção – art. 64, inciso I. Superado o lapso dos cinco anos, não há critério material apto a valorar o delito cometido.

Por isso mesmo que o art. 93 do Código Penal prevê o instituto da reabilitação, que "alcança quaisquer penas aplicadas em sentença definitiva, assegurando ao condenado o sigilo dos registros sobre seu processo e condenação". Aplicado em combinação ao art. 748 do Código de Processo Penal, que afirma que, concedida a reabilitação: "[a] condenação ou condenações anteriores não serão mencionadas na folha de antecedentes do reabilitado, nem em certidão extraída dos livros do juízo, salvo quando requisitadas por juiz criminal", temos que é absolutamente ilegal a lembrança de condenações passadas, por quem quer que seja.

Nada disso significa dizer, ressalve-se, que a história deve ser esquecida: a trajetória da humanidade é envolta por atos criminosos que jamais podem deixar de ser rememorados –

---

[189] STJ, REsp nº 1.335.153 – RJ, Rel. Min. Luis Felipe Salomão. 04.09.2013

mas os envolvidos em qualquer crime precisam ver preservada a chance de superar os malfeitos, sob pena de, na *sociedade em rede*, jamais terem o direito de reconstruírem as suas vidas. O direito de informar e a curiosidade pública não podem se confundir. Foi também nesse sentido o voto do Ministro Luis Felipe Salomão no *Recurso Especial* supracitado, a conferir:

> Com efeito, a historicidade de determinados crimes por vezes é edificada à custa das mencionadas vicissitudes, e, por isso, penso que a historicidade do crime não deve constituir óbice em si intransponível ao reconhecimento de direitos como o vindicado nos presentes autos. Na verdade, a permissão ampla e irrestrita a que um crime e as pessoas nele envolvidas sejam retratados indefinidamente no tempo – a pretexto da historicidade do fato – pode significar permissão de um segundo abuso à dignidade humana, simplesmente porque o primeiro já fora cometido no passado. Por isso, nesses casos, o reconhecimento do "direito ao esquecimento" pode significar um corretivo – tardio, mas possível – das vicissitudes do passado, seja de inquéritos policiais ou processos judiciais pirotécnicos e injustos, seja da exploração populista da mídia. Portanto, a questão da historicidade do crime, embora relevante para o desate de controvérsias como a dos autos, pode ser ponderada caso a caso, devendo ser aferida também a possível artificiosidade da história criada na época.[190]

Cremos que, passados cinco anos do cumprimento ou extinção da pena, os fatos criminosos e os agentes envolvidos não podem ser alvo de novas reportagens jornalísticas ou documentais, devendo os buscadores da rede mundial de computadores serem instados a manter apenas aqueles *links* carregados até o atingimento desse marco temporal.

Aliás, é bom que se diga: não há um *direito ao esquecimento* puro e simples. O que se denomina "direito ao esquecimento" parece ter mais com a facilidade da comunicação de uma ideia que com o direito em si. O que está abarcado nesse verdadeiro guarda-chuvas são os direitos de reabilitação, de desindexação de conteúdo, de resposta (mesmo sem uma Lei de Imprensa ou de Meios de Comunicação) e etc. A posição esposada aqui refere-se especificamente à vedação às penas de caráter perpétuo e a preservação da intimidade de pessoas condenadas, vez que, na sociedade em que vivemos, parece impossível que o Estado obrigue alguém a "esquecer" o que quer que seja. Vítima, ofensor e familiares têm o direito, contudo, de, cumprida a pena, serem deixados em paz.

Nesse ponto, curial que se faça uma consideração: o eventual não acolhimento do direito ao esquecimento significará efetiva relativização do direito à superação dos efeitos da pena na *sociedade em rede* e estará a reafirmar postulados do positivismo penal, que, mesmo que de forma residual, constituem grave ameaça à democracia. Nesse sentido, a melhor doutrina

---

[190] STJ, REsp nº 1.335.153 – RJ, Rel. Min. Luis Felipe Salomão. 04.09.2013.

anota que:

> Ao tratar o criminoso como inimigo, constata-se uma desconsideração expressa do indivíduo como cidadão (...)e a sanção a ser a ele imposta adquire um sentido de instrumento de segurança. É sob essa perspectiva, também, que se compreende – embora seja inadmissível – o modo absolutamente atentatório a direitos e garantias individuais pelo qual o processo penal tem sido posto em prática. O que pode ser observado é uma verdadeira confusão entre os conceitos de processo penal e guerra.[191]

É preciso rediscutir a matéria a luz dos princípios penais, para que não signifique o mero casuísmo de um debate dessa ou daquela causa. A nossa Constituição e as Leis são claras.

Ainda que não se vislumbre o direito ao esquecimento, é necessário reconhecer que outros direitos, consagrados infra constitucionalmente e constitucionalmente precisam ser observados. Do ponto de vista penal, o estabelecimento de um direito desse tipo pode dar aos apenados a possibilidade de, na sociedade em rede, verem superadas as suas penas, podendo de fato reinserir-se na sociedade sem a mácula constante de um apontamento para o seu nome e o seu delito.

---

[191] GOMES, Mariângela G. M. Periculosidade no Direito Penal contemporâneo. In: MENDES, Gilmar Ferreira; BOTTINI, Pierpaolo Cruz; PACELLI, Eugênio. (Org.). *Direito Penal Contemporâneo*: Questões Controvertidas. Vol. 1. São Paulo: Saraiva, 2011. p. 536-537.

## 2. INTIMIDADE E COLEÇÕES DE DADOS: CONCEITOS E CAMINHOS

### 2.1. Privacidade, intimidade, dados e liberdade

É preciso entender a intimidade frente à revolução tecnológica digital da Sociedade em rede. Nesse sentido, COSTA JÚNIOR entende que o processo que vivemos levou à corrosão das fronteiras da intimidade. Segundo ele, o fenômeno pode levar a deformação progressiva dos direitos fundamentais[192].

Em que pese concordarmos em parte, é necessário investigar as interações atuais dos atores privados na internet para auferir em que medida os usos dos dados pessoais constituem, de fato, violações à intimidade e em que passo o direito penal deve intervir nessa dinâmica, sempre observando a ressalva de DE LA CUESTA de que

> "Particular llamada de atención merece la evitación de toda suerte de hiperregulación y sobrepenalización de ciberespacio, que hipotecando la liberdad de comunicación acaban atacando e interfiriendo con derechos tan fundamentales como la liberdad de expressión y la recepción, procesamiento y revelación de información, los cuales merecen igualmente pleno respeto y garantia en un estado de derecho"[193]

É o que se passa a discutir nesse capítulo.

#### 2.1.1 O Conceito de dados pessoais

Estabelecido o cenário de debates atuais e de desafios iminentes, o estudo das violações da privacidade e da intimidade por atores privados na internet pressupõe também alguns marcos conceituais importantes, como se fará nesse capítulo, a começar pelo conceito de dados pessoais.

Em relação a eles, há duas vertentes: a reducionista – que prevê que só são pessoais os dados que podem ser associados diretamente a uma pessoa[194] – e a expansionista – que prevê que dado pessoal pode ser qualquer tipo de informação que permita a identificação do

---

[192] COSTA JÚNOR, P.J. *O direito de estar só: tutela penal da initimidade*. 2. ed. São Paulo: Revista dos Tribunais, 1995. p. 22.

[193] DE LA CUESTA ARZAMENDI, José Luis. Sociedad de la información y derecho penal: a la luz del XIX *congreso internacional de derecho penal*. Revista Brasileira de Ciências Criminais, São Paulo, v. 23, n. 112, p. 79-106., jan./fev. 2015. P. 85.

[194] SOLOVE, Daniel. J. *The digital person:* technology and privacy in the informaion age. New York University Press: New York, 2004.

indivíduo, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta[195].

A Lei de Acesso a Informação (Lei nº12.527/2011) prevê, no art. 4º, IV, que é "informação pessoal: aquela relacionada à pessoa natural identificada ou identificável". Mesmo com a divergência ao entorno da definição "identificados" ou "identificáveis", pode-se apontar que as duas correntes apontam para um mesmo norte, qual seja o da capacidade do dado em identificar o indivíduo.[196] O conceito de dado pessoal está atrelado, portanto, ao dado que possa, direta ou indiretamente, identificar uma pessoa.

Na internet, o dado pessoal é coletado continuamente para os mais diversos fins. O cuidado com a coleta, a tutela e o uso e os limites éticos aplicados nessas etapas são cruciais para que se evite a violação da privacidade e da intimidade dos usuários da rede. De acordo com RODRÍGUEZ, o direito de controlar o destino dos dados pessoais é um dos aspectos da intimidade, sendo possível a sua tutela penal para coibir condutas que levem ao seu uso, armazenamento ou combinação indevida[197]. Tal noção é lapidar para este estudo.

### 2.1.2 Conceitos de intimidade, vida privada e privacidade

São antigas as discussões quanto ao direito à privacidade, data pelo menos do século XVI a inviolabilidade do domicílio na Inglaterra, mas foi apenas em 1890 que a obra mais referenciada sobre o tema, o artigo *The Right to privacy*, foi publicada por WARREN e BRANDEIS. Segundo ele o direito de privacidade (*the right of privacy*) é o direito de ser deixado em paz (*the right to be let alone*)[198]. As discussões em seu entorno desde então – quanto a vida

---

[195] SCHWARTZ, Paul M. SOLOVE, Daniel J. *The PII Problem*: Privacy and a New Concept of Personally Idenifiable Information. Disponível em: http://scholarship.law.berkeley.edu/facpubs/1638. Acessado em 29.09.2017

[196] Sobre isto, BIONI, Bruno Ricardo. *Autodeterminação informacional:* paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

[197] "O direito à intimidade tem uma vertente de Direito de Terceira Geração (ou até de Quarta Geração, na expressão de alguns autores), na medida em que nasce como reação ao progresso tecnológico. Nesse sentido, assume um caráter difuso, relacionado ao interesse de que os dados da coletividade não sejam colhidos e combinados indevidamente. Não se pode reconhecer, entretanto, o direito à autodeterminação informativa como desvinculado da intimidade, pois a violação à autodeterminação informativa somente passa a ser relevante quando menoscaba a intimidade. O direito de controlar o destino dos dados pessoais de um determinado titular é, portanto, aspecto da intimidade, e sua tutela penal pode ocorrer para coibir condutas que impliquem o uso, armazenamento e combinação indevida de dados pessoais." (RODRÍGUEZ, Víctor Gabriel de Oliveira. *Tutela...* cit., p. 236.)

[198] "(…) the most comprehensive of the rights and the right most valued by civilezed men". Ibid.

privada, a intimidade, a reserva, ou a mais de uma esfera de intima – como já afirmamos, têm sido intensas.[199] Diversas evoluções do conceito se seguiram, inclusive com desdobramentos e a divisão dele em esferas até a evolução para a autodeterminação informacional, que será tratada no capítulo seguinte.

COSTA JÚNIOR[200], adotando a doutrina alemã, aduz que a privacidade pode ser dividida em esferas. Na mais externa (*Privatsphare*) está aquilo que o indivíduo deseja resguardar para que não se torne de domínio público. Numa segunda (*intimsphare*) estão as informações compartilhadas apenas com quem o indivíduo estabelece relações de confiança. Na esfera mais concêntrica (*Geheimsphare*) é que estão os segredos que devem ser mantidos em sigilo ou contados apenas aos indivíduos extremamente íntimos. Para RODRÍGUEZ[201], a vida privada contém a intimidade, sem se ignorar, como aduz ele, que o termo *privacy* "abarca um e outro e se encontra traduzido, pela doutrina como intimidade"[202].

Ao que indica a doutrina, a privacidade está no direito do indivíduo de controlar acesso de terceiros aos dados de sua vida de maneira ampla, estabelecendo um primeiro nível de autorização para ser adentrada. A vida privada fica adstrita a um segundo nível, do âmbito familiar, mas imbricada à intimidade. A intimidade é o âmbito em que o indivíduo reserva os seus pensamentos e emoções - em nossa opinião, o que ORTEGA Y GASSET denomina de ensimesmamento*[203]*.

O artigo 12.º da Declaração Universal dos Direitos do Homem reforça expressamente à proteção da privacidade – segundo ele: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei".

---

[199] MATA BARRANCO, Norberto J. de la; BARINAS UBIÑAS, Desirée. *La protección*… cit., p. 35.
[200] COSTA JÚNIOR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. 4.ed. rev. e atual. São Paulo: Revista dos Tribunais, 2007. p. 34.
[201] RODRÍGUEZ, Víctor Gabriel de Oliveira. *Tutela*... cit., p. 33. Ver também FERREIRA, Ivette Senise. *A intimidade...* cit., p. 96-106.
[202] Ibid. Idem.
[203] ORTEGA Y GASSET, J., Obras Completas. Madrid: Alianza Editorial, 1994, Tomo 5, P. 301

De acordo com SARMENTO E CASTRO[204], a mesma proteção genérica da vida privada resulta do artigo 8.º da Convenção Europeia dos Direitos do Homem (Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais) que prevê que "qualquer pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Segundo ela[205], esta proteção, que foi sendo adotada gradativamente por toda a UE, pode ser encontrada na Constituição Portuguesa (artigo 26), da Bélgica (artigo 22.º), da Espanha (artigo 18.º), da Finlândia (artigo 8.º), da Grécia (artigo 9.º) e da Holanda (artigo 10.º). A Alemanha (artigo 10), a Dinamarca (artigo 72), a Irlanda (artigo 40.5), a Itália (artigos 14 e 15) e o Luxemburgo (artigo 28.º) apenas garantem nas suas Constituições a inviolabilidade do domicílio e/ou da correspondência.

O que se chama mais genericamente de privacidade, que contém a vida privada e a intimidade, é, portanto, um dos mais importantes direitos de personalidade e tem indistinta relação com a dignidade humana. Diante da nova realidade de monitoramento ininterrupto dos dados, é indispensável o estudo das formas de evitar as violações à privacidade e à intimidade.

### 2.1.2 Relação entre intimidade e coleta de dados

No caso dos dados, a privacidade não é capaz de explicar todos os aspectos da necessidade de proteção deles, como a qualidade desses dados, a limitação de finalidade e a segurança a que estão expostos. Melhor será dizer que a proteção de dados depende tanto do princípio da privacidade quanto do princípio da proporcionalidade em seu uso[206].

Isto significa que empresas e organizações devem utilizar-se do acesso privilegiado aos dados – e portanto, no mínimo à privacidade, mas possivelmente também à intimidade –

---

[204] CASTRO, Catarina Sarmento. *Direito da informática, privacidade e dados pessoais.* Coimbra: Edições Almedina, 2005. p. 25-27.
[205] Ibid. Idem.
[206] De acordo com De Hert e Gutwirth 'Never does an individual have an absolute control over an aspect of his or her privacy. If individuals do have freedom to organise life as they please, this will only remain self-evident up to the point that it causes social or inter-subjective friction. At that stage, the rights, freedoms and interests of others, as well as the prerogatives of the authorities come into play. The friction, tension areas and conflicts create the need for a careful balancing of the rights and interests that give privacy its meaning and relevance. This shows clearly that, although quintessential for a democratic constitutional state, because it refers to liberty, privacy is a relational, contextual and per se social notion which only requires substance when it clashes with other private or public interests.' ('Privacy, Data Protection and law enforcement. Opacity of the individuals and transparency of the power', in Privacy and the Criminal Law, E. Claes et alii (ed.), Interscientia: Antwerpen-Oxford, 2006, p.74

com a devida moderação[207] e com a adequada aplicação dos princípios da proporcionalidade e da limitação de propósito[208]. É crucial que se limite ao mínimo possível o volume de dados utilizados para oferecimento de serviços e produtos.

Conquanto o debate em relação ao volume ainda seja necessário, um ponto é certo: é preciso que os detentores de coleção de dados sejam instados a observar limites de uso dos dados de modo que não vulnerem – ainda mais – a privacidade dos usuários. A implementação de padrões claros de consentimento com a coleta, processamento e exposição ao conteúdo gerado com base no perfil de um usuário é fundamental para a proteção da privacidade e já foi alvo inclusive de recomendação da AIDP.

RODOLFO ULRICH vai além: para ele os dados obtidos pela utilização desproporcional das coleções podem causar consequências sérias para a vida dos indivíduos, que vão da antecipação de perfis de candidatos a um emprego a exclusão de programas de seguro (inclusive de saúde e vida)[209].

O autor argentino salienta que muitas empresas estão se valendo da atmosfera de liberdade vigente na rede para aprender os hábitos e costumes de seus usuários e, com isso, escolher seus clientes. A privacidade do usuário é invadida por várias ferramentas das aplicações que, sem aviso – ou com muito pouco –, utilizam alguns dos dados de seus usuários,

---

[207] Até porque, de Acordo com Poullet e Rauveoy, a privacidade está mais ligada a um "direito à opacidade", de manter a vida privada protegida do escrutínio alheio, o que, sejamos sinceros, é impossível de maneira absoluta em relação à privacidade de dados. Neste sentido: "Even in the traditional villages, the role played by the walls of the private home included the protection of a sphere of intimacy where individuals felt allowed to give up, for the time of the private encounter, the role he or she endorses in public. In that sense, the 'right to opacity' is a precondition to the very existence of the 'authenticity' of the self and to the implementation of the ability we have, as human beings, to develop our personal identity. Our 'inviolate personality' may only grow in the shadow of partial opacity.42 The 'right to opacity' protects the individual from others watching, scrutinizing or spying on his or her private realm (…) Privacy as 'seclusion' or as the 'right to be left alone' suggested a geographical scope of application: the 'private sphere' to which the right to privacy applied was bordered by the house's walls or by the private letter's material envelope." (POULLET, Yves; ROUVROY, Antoinette. *The right*… cit., p. 63-64.)

[208] Nesse sentido, uma das resolusções adotas pela AIDP: "The purpose limitation principle should be respected in general, and, as a rule, when transferring electronic personal data to law enforcement authorities. The purpose limitation principle means that personal data can only be collected for an explicit, specified and legitimate purpose, and not further processed in a way incompatible with those purposes." Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

[209] "Los datos obtenidos por internet, o por la indebida utilización de una base de datos, son manipulados de las más imaginativas maneras que ocasionan molestias, en algunos casos y graves perjuicios en otros, y provocan hasta la muerte civil de una persona. Así los datos son utilizados para: 1) El marketing directo, (…) 2) Exclusión de cobertura médica, 3) Exclusión de asegurados, 4) determinación de perfil de futuros empleados." (UICICH, Rodolfo Daniel. *El derecho a la intimidad en internet y en las comunicaciones electrónicas*. Buenos Aires: Ad-Hoc, 2009. p. 81.)

extraídos diretamente de redes sociais, para determinar seus costumes na rede e, eventualmente, vender esta informação[210] - o que, em nossa opinião, representa a mercancia da privacidade alheia, quase sempre não autorizada.

Os novos direitos, surgidos dessas novas interações na rede, demandam desafios não apenas no campo jurídico, mas moral, social e, sobretudo, tecnológico. É necessário, portanto que se observe a devida proporcionalidade na utilização dos dados frente às possíveis violações de direitos.

### 2.1.3 Privacidade, Intimidade e vida privada: evolução diante da internet

Há diversos trabalhos a tratar da intimidade no último século[211]. Nos últimos dez anos, contudo, a intimidade experimentou novos contornos diante do desenvolvimento dos meios de comunicação, notadamente da internet. Os dados dos usuários da rede são agora comumente armazenados em servidores e enviados a terceiros com autorizações restritas de uso. O usuário da internet, ao entrar em sítios eletrônicos ou utilizar aplicações experimenta vulnerabilidades inimagináveis.

Diante desse cenário, SARA COSTA defende que os dados pessoais, alvo da proteção associada à intimidade, são aqueles que permitem alcançar informações acerca da vida de uma pessoa, de modo que as suas atitudes se tornem identificáveis, sendo esse direito inerente a preservação da vida privada[212]. A evolução da privacidade no campo digital seria a autodeterminação informacional, que garante ao indivíduo o controle da utilização de seus dados. COSTA entende que tal proteção já consta, por exemplo, no art. 35, I da Constituição Portuguesa, que prevê que o cidadão daquele país tem, inclusive o direito de conhecer o

---

[210] En este ambiente de libertad, donde la información circula fluidamente sin restricciones, muchas empresas recurren a la tecnología para averiguar los hábitos y costumbres de los navegantes, se entrometen en la vida privada del 97suario a través de diversas herramientas como las cookies, y sin advertir al navegante que se utilizarán ciertos datos suyos, es decir sin requerir consentimiento alguno utilizan los datos personales extraídos en beneficio propio directo, a veces, y en otras oportunidades los venden a terceras personas o empresas" (Ibid., p. 79.)

[211] Segundo Rodríguez "O conceito de intimidade é recente e tem relação direta com a novas tecnologias. No mundo antigo, a intimidade, tal e qual conhecemos hoje, praticamente inexistia. O pensamento cristão deu grande impulso ao tema, com a ideia de reserva, mas foi somente após a Revolução industrial que se formulou a noção de intimidade como um direito" (RODRÍGUEZ, Víctor Gabriel de Oliveira. Tutela..., cit., p. 235)

[212] COSTA, Sara. A proteção de dados pessoais na internet. *Revista juridica*, Maputo, v. 6, set. 2004. p. 288. Vida privada aqui em sentido amplo, o mesmo adotado anteriormente por Rodríguez. Vale também a leitura de MATA Y MARTIN, Ricardo Manuel. La protección penal de datos como tutela de la intimidad de las personas: intimidad y nuevas tecnologías. *Revista Penal***,** Valencia, n. 18, p. 217-235, jul. 2006 quanto a situação na Espanha.

processo de tratamento do dado informático que lhe é disponibilizado[213] e de recusar que seus dados sofram qualquer tipo de tratamento[214]. Em âmbito europeu, há jurisprudência da Corte Europeia de Direitos humanos equiparando a proteção da integridade dos dados eletrônicos à proteção da privacidade[215].

BROWNSWORD aduz que o direito ao processamento justo de dados é "vital num mundo onde as informações pessoais são automaticamente processadas numa extensão jamais sonhada".[216] Quando as atuais normas foram pensadas, o processamento de dados encontrava-se em estágios muito anteriores de desenvolvimento. Hoje, com a proliferação no número de injustos cometidos pela rede, o paradigma mudou. RODRÍGUEZ nota que a internet teve papel fundamental nessa mudança. Para ele:

> No momento atual, a Internet não é apenas um campo novo de trabalho, sobre o qual se pode profetizar e prognosticar um destino de sucesso econômico e social. Faz-se uma realidade: uma rede mundial, sem donos, de terminal hipertextual, em que cada usuário é ao mesmo tempo consumidor e provedor, e que permite armazenamento, acesso e troca de dados em tempo real, em escala global, sem limites de acesso. Num ambiente como esse, a falta de limites, de fronteiras e de um governo central traz ao tema da intimidade alguns problemas muito peculiares, em especial em relação à possibilidade de intervenção jurídica. De fato, pouco adiante conhecer aprofundadamente o problema da intimidade e garantir a sua existência como direito fundamental, se um dos seus principais ofensores passa ao largo de qualquer regulação, ou seja, não é atingido por nenhum tipo de norma.[217]

Na nossa opinião, a intimidade deve ser o fio condutor e guia necessário para a proteção do sigilo de dados e consequentes violações na rede. De acordo com BOADA:

> la intimidad individual es una manifestación necessaria para la vida moral del ser humano, ya que todos los hombres tienen, por necesidad, algo que reservan para sí. La intimidad, entonces, consiste en el domínio exclusivo y reservado que la persona tiene de su fuero interno proprio y personal.[218]

---

[213] Ibid., p. 299.
[214] Ibid., p. 304.
[215] CONSELHO DA EUROPA. Corte Européia de Direitos Humanos. *Copland v. the United Kingdom*, § 41. Disponível em http://194.242.234.211/documents/10160/10704/1531450 Acesso em 29.06.2016.
[216] "I believe that a dedicated rightsbased protection of the interest in fair processing of personal data is vital in a world where personal information is automatically processed to an extent not dreamed of when the need for data protection law was first accepted." (BROWNSWORD, Roger. Consent in data protection law: Privacy, Fair Processing and Confidentiality. In: DE HERT, Paul [et. al]. *Reinventing data protection?* Bruxelas: Springer, 2014. p. 99.)
[217] RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit., p. 85.
[218] GUTIÉRREZ BOADA, John Daniel. *Los límites entre la intimidad y la información.* Bogotá: Universidad Externado de Colombia, 2001. p. 37.

A discussão toma novo folego quando introduzida a possibilidade de que a formação dos juízos de valor dos indivíduos, diante das trocas comunicacionais na internet, possam ser afetados, necessitando de novo campo protetivo. RODRÍGUEZ leciona ser "possível afirmar que a intimidade corre graves riscos diante do arsenal tecnológico controlado por indivíduos e grandes corporações que têm interesse imediato na detenção de informações complexas e recombinadas sobre toda a sociedade". [219]

A personalidade hoje também é formada pelas interações nesse ambiente de redes, sendo certo que só com a garantia da intimidade que o indivíduo se sente pleno de suas capacidades associativas para a tomada de decisões nesse ambiente e, possivelmente nas relações com algum vínculo a ele.

Também a vida privada tem encontrado crescentes desafios diante da rapidez dos novos meios comunicacionais. Há um verdadeiro estímulo a exposição pública de atos e fatos da vida privada. Tudo que se possa imaginar é registrado em fotos e vídeos compartilhados com agentes estranhos, sobre os quais se perde o controle no momento em que ganham publicação na rede.

Mas, ao mesmo tempo, os indivíduos passaram a clamar por direitos ligados a intimidade e à vida privada, como o do esquecimento na internet e as discussões a respeito do tempo e da legitimidade de armazenamento de dados por servidores. Em todos os casos deve valer a autonomia dos indivíduos, em estrita relação aos seus próprios dados e direitos de imagem e personalidade.

Essa convergência entre a valorização da personalidade, da dignidade humana e da intimidade já foi bem explorada pelo Tribunal Constitucional Federal da Alemanha. Em 25 de dezembro de 1983, aquela Corte julgou a Lei de recenseamento da população alemã, aprovada no ano anterior pelo parlamento do país. A sentença desse julgamento projetou o conceito da autodeterminação informativa que se verá adiante.

É evidente que os conceitos de privacidade, intimidade e vida privada vêm sofrendo graves modificações diante dos avanços no uso de aplicações da rede. É também papel do direito penal acompanhar essa mudança para que, se violado o bem jurídico da intimidade, exerça o seu papel. A pena também é uma forma de demonstração de que um valor é

---

[219] RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit., p. 2.

protegido.[220] Por isso, somos da opinião de que cabe o estudo de medidas penalizantes em relação aos agentes que abusam do poder computacional que detêm – seja no processamento de dados, na sua combinação, na indexação, no abuso da confiança do usuário ou na subtração.

O agente que detém dados alheios deve ter em conta que o usuário da sua aplicação depositou em sua confiança *bens imateriais intangíveis evidentemente vulneráveis*[221]. Na União Europeia, como visto no capítulo anterior, as empresas serão inclusive instadas a adotar um responsável para esse depósito – a figura do *Data Protection Officer*. É preciso estar atento às evoluções da rede para que novas aplicações e usos não fragilizem ainda mais a intimidade dos usuários no Brasil.

### 2.1.4 Direito constitucional v. falta de proteção infraconstitucional

Não parece demais reforçar em tópico próprio o aspecto constitucional da intimidade. O constituinte fez da Carta cidadã um livro de proteções, é preciso revisitá-lo todos os dias. Em tempos de fragilização de direitos fundamentais, cumpre ao direito penal contribuir nessas revisitas.

No Brasil, a inviolabilidade da intimidade é constitucionalmente assegurada, sendo certo que a vida privada encontra proteção no art. 21 do Código Civil, como direito de personalidade intransmissível e irrenunciável (art. 11 do mesmo diploma).

Ao penalista cumpre dizer que a intimidade dá supedâneo aos artigos 153, 154 e 154-A do nosso Código Penal, mas verdadeira reafirmação da democracia, vez que é ela que

---

[220] "O Direito penal deve defender bens jurídicos, mas também tem função de comunicar à sociedade que determinado bem jurídico é positivamente valorado. Nesse sentido, a previsão de pena aos delitos contra a intimidade tem a função de mostrar que ela é um valor a ser protegido, até mesmo ante o interesse social de persecução penal, que não pode sacrificar desmedidamente um direito de personalidade" (RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit., p. 238)

[221] "Não pode ser desprezado pelo direito penal que os dados eletrônicos, matéria-prima para as operações computacionais, são bens imateriais intangíveis, que não podem facilmente ser transportados de um lado para o outro pelas formas tradicionalmente reconhecidas, trazendo evidente vulnerabilidade a esses. Uma das principais características dos dados eletrônicos é essa imaterialidade, proporcionando com isso uma certa fragilidade, considerando essa separação entre o seu conteúdo e o campo em que foi gerado. Por tudo isso, por seu caráter etéreo, deve ser criado e mantido algum sistema de proteção penal, com a finalidade de desenvolver cuidados jurídicos específicos ao material informático."
LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. Campinas: Millennium, 2007. p. 17.

permite o livre desenvolvimento da personalidade e que dá ao cidadão brasileiro a garantia à opacidade dos momentos que não dizem respeito ao restante da sociedade.

Não é mero acaso que a proteção da intimidade e da vida privada conste justamente do artigo 5º da nossa Constituição Federal – onde estão as demais proteções fundamentais. SAMPAIO FERRAZ entende que esse direito é

> um direito subjetivo fundamental, cujo titular é toda pessoa, física ou jurídica, brasileira ou estrangeira, residente ou em trânsito no país; cujo conteúdo é a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por só a ele lhe dizerem respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão; e cujo objeto é a integridade moral do titular.[222]

O direito à intimidade é também parte da Declaração de Direitos Humanos da ONU, que estabelece em seu art. 12 que "ninguém será sujeito a interferências em sua vida privada, na sua família, no seu lar, ou na sua correspondência, nem a ataques à sua honra e reputação. Todo homem tem direito à proteção da lei contra tais interferências ou ataques". A Corte Interamericana de Direitos Humanos também já definiu que o art. 11 da Convenção tem proteção semelhante[223].

SENISE relata que esse direito "não encontrou ainda uma formulação à altura da modernidade dos nossos preceitos constitucionais e da evolução da nossa doutrina"[224]. De fato, a intimidade, apesar de tutelada constitucionalmente e de bem jurídico básico para a aplicação de alguns tipos penais, não encontrou até hoje uma lei ordinária que a proteja *stricto sensu*. Há, no máximo, a proteção reflexa ao domicílio, correspondência e, foco desse trabalho, a algumas situações envolvendo dispositivo informático. Essa proteção parece ainda bastante aquém do que um direito fundamental merece.

Alguns projetos de Código Penal já apresentaram sugestões de imposição de um tipo específico para proteger a violação da intimidade, nunca concretizado, porém. Nova sugestão nesse sentido precisaria dar protagonismo à questão da intimidade e sua relação com os dados pessoais inseridos na internet. Lei do tipo precisaria, aliás, descer à minúcia das

---

[222] FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, vol. 88, 1993. p. 439-440.
[223] CIDH. Sentença do caso Escher v. Brasil. "O art. 11 da Convenção príbe toda ingerência arbitrária ou abusiva na vida privada das pessoas"
[224] FERREIRA, Ivette Senise. *A intimidade*... cit., p. 103.

diversas formas de violação – novamente, o processamento de dados, a combinação indevida, a indexação indesejada, o abuso da confiança do usuário ou mesmo a subtração.

A Espanha passou por uma reforma legislativa sobre o tema em 2015. A mudança tornou qualificado (art. 197, inc. 4) o crime de divulgação de revelação de segredos quando praticados por responsáveis pela guarda de arquivos, inclusive informáticos ou se envolverem a divulgação não autorizada de dados pessoais.[225] Introduziu-se ainda o inc. 7 no mesmo art. 197 para tornar crime a conduta de "revelar ou ceder a terceiros, sem autorização da pessoa afetada, imagens e gravações audiovisuais realizadas com a sua anuência se a gravação prejudicar gravemente a sua intimidade pessoal" – o que pode inibir os casos de *revange porn*. A mesma reforma endureceu ainda o tratamento contra os delitos de invasão de dispositivos (art. 197 bis), os delitos de *hacking*.

[225] ESPANHA. Código Penal y legislación complenetária. Artículo 197. "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando: a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior. 5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior. 6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años. 7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.".

Esses tipos penais introduzidos no ordenamento espanhol são ainda vagos e mereciam melhor apuração antes de tornarem-se Leis.[226] Conquanto seja imperfeita, a iniciativa ao menos levantou o debate para os novos crimes envolvendo a intimidade, os dados e a internet naquele país.

O Brasil, realizado um extenso debate ao entorno da questão, pode adotar o modelo espanhol, criminalizando condutas que fragilizem a intimidade diante dos novos paradigmas de relacionamentos e compartilhamentos de dados estabelecidos pela rede. A discussão aprofundada e prévia a acontecimentos fáticos que levam ao assoamento na aprovação de um diploma penal do tipo pode eviar ainda que surjam nessa questão os chamados gestores atípicos da moral[227], a pressionar, como no geral, por penas duríssimas e desproporcionais a invasõesa ou a má gestão de dados.

É possível que, nesse ponto da história, a penalização de algumas condutas com base no bem jurídico da intimidade sejam recomendadas. No próximo capítulo são oferecidas algumas sugestões nesse sentido.

## 2.2 Autodeterminação informativa

Longe dos prognósticos otimistas de alguns anos atrás, a internet vem demonstrando nos últimos tempos que o ambiente anárquico-idealista desejado pelos ciberpunks[228] tem sido superado em nome dos interesses do capital. Basta checar a lista das 500 empresas mais lucrativas do mundo no último ano para ver que as companhias petrolíferas e os bancos perderam seus postos para empresas de tecnologia baseadas na rede. Estamos, isso sim, diante de um importante ponto de mudança na história, em que não só a informação representa alta influência e poder monetário, mas também dita os rumos da sociedade de acordo com a forma que é entregue.

---

[226] COLLANTES, Tàlia González. Los delitos contra la intimidad tras la reforma de 2015: luces y sombras. *Revista de derecho penal y criminología*, Madrid, 3a. época, n. 13, p. 51-83., jan./jun. 2015.

[227] Segundo Renato de Mello Jorge Silveira: "Os gestores atípicos da moral são um fenômeno característico das sociedades pós-industriais. Os tradicionais gestores da moral coletiva no Estado capitalista, normalmente, eram oriundos das classes burguesas conservadoras. Atualmente, com o ganho da participação das demais classes sociais, o panorama mudou, sendo patente que entidades várias, como organizações ecológicas, feministas, de consumidores, pacifistas, étnicas ou raciais, exerçam influência junto ao Estado, impondo e defendendo seus interesses, mesmo em termos penais. Essa influência, diga-se, não se mostra de forma científica, mas, tão-só, política" SILVEIRA, Renato de Mello Jorge. Direito penal supra-individual. São Paulo: RT, 2003, p. 32, nota 50

[228] Qaunto ao tema, ver a trilhogia do *Sprawl*, de William Gibson (*Neuromancer*, *Count Zero e Mona Lisa Overdrive*).

Nesse sentido, os novos atores privados do ciberespaço, notadamente as redes sociais surgidas na última década, detêm muito mais relevância na vida dos indivíduos do que a imprensa tradicional. Se antes era preciso escolher qual notícia seria lida nas tantas páginas de um periódico, hoje ela é entregue de maneira direcionada e seletiva, com base em *cookies* que monitoram o comportamento do usuário ininterruptamente. Se por um lado isso pode representar certa facilidade, por outro pode submeter a um determinado nível de sugestividade indesejado.

De acordo com RODRÍGUEZ, "intimidade e vida privada são conceitos que mudam de acordo com as alterações sociais e tecnológicas, que ultimamente têm sido muitas e velozes."[229]. Ao julgar a lei de recenseamento nacional aprovada em 1982, a Corte Alemã impediu que os dados dos cidadãos alemães fossem utilizados para outro fim que não o de recensear. Foi essa sentença que forjou o direito de autodeterminação informativa[230] defendido por COSTA, sob o signo da valorização do direito a personalidade em combinação com a dignidade da pessoa humana[231]. O Tribunal garantiu a proteção contra a coleta, difusão, armazenamento e utilização ilimitados de dados pessoais[232-233]. Ao fazer isso, a sentença projetou[234] as bases modernas para a adequada proteção à intimidade do indivíduo[235].

---

[229] RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit., p. 93

[230] DESIMONE, Christian. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, v, 11, n, 3. 2003. p. 61.

[231] COSTA, Sara. *A proteção*... cit., p. 56.

[232] Quanto a esse ponto, apesar de divergir da autora quanto a não diferenciação adequada entre privacidade e intimidade, vale a leitura do comentário a decisão do tribunal em LIMBERGER, Têmis. A informática e a proteção à intimidade. *Revista do Ministério Público do Rio Grande do Sul*, Porto Alegre, n. 43, jul./out. 2000.

[233] A Corte estabeleceu o direito à autodeterminação informativa (Grundrecht auf informationelle Selbstbestimmung) no julgamento de causa (BVerfGE 65, 1). Referente a coleta de dados pessoais pelo poder público, autorizada pela Lei do Censo (Volkszählungsgesetz), coleta de dados esta que não conferia adequadas garantias de uso das informações às únicas finalidades da lei e de anonimato dos indivíduos participantes. Aplicando em conjunto as normas dos artigos 1.º e 2º da Lei Fundamental Alemã, o Tribunal declarou a existência desse direito como emanado dos princípios da dignidade da pessoa humana e do livre desenvolvimento da personalidade. Ver mais em https://freiheitsfoo.de/files/2013/10/Census-Act.pdf

[234] Rodríguez cita a lição de Erhard Denninger, para quem o direito de autodeterminação informativa na verdade teria sido lançado em 1971 pelo Ministério Federal do Interior da Alemanha. Por isso a escolha do vocábulo "lançou" aqui. Barranco Mata relata que a Suprema Corte estadunidense já teria abordado o *informational privacy* em 1977 em *Whalen vs. Roe*, quando tratou da proteção da revelação de dados de uma pessoa sem o seu consentimento. Mesmo assim, de se salientar que quase toda a doutrina ao falar de tal direito lembra apenas da sentença referida, ao que parece justo atribuir a ela a projeção que o direito a autodeterminação informativa alcançou. (Cf. RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit. p. 61 e MATA BARRANCO, Norberto J. de la; BARINAS UBIÑAS, Desirée. *La protección*… cit., p. 53).

[235] Segundo Ivete Senise Ferreira a intimidade tem origem mais remota, apontando a jurisprudência inglesa do séc. XVIII como seu berço. Cf. FERREIRA, Ivette Senise. *A intimidade*... cit., p. 96-106.

Entendemos que essa proteção passa necessariamente pelo fortalecimento da autodeterminação do indivíduo nas esferas mais intimas, que levam a formação de seus pensamentos. MATA BARRANCO, ao dissertar sobre as esferas intimas propostas por HUBMAN e aperfeiçoadas por HENKEL na Alemanha – a *Spharentheorie*, esfera maior da privacidade atribuída a proteção do conhecimento de terceiros aspectos da pessoa, a *Intimsphare*, com aspectos mais próximos da intimidade em si e a *Geheimsphare*, uma esfera ainda mais íntima, que protegeria aspectos atinentes ao sexo e à religião – admite que os marcos entre privacidade e intimidade podem ser, em certas ocasiões, imprecisos, mas entende que esse âmbito de intimo em que o indivíduo toma decisões deve ser acima de tudo preservado – trata-se, segundo seu postulado, de fazer valer a soberania pessoal do indivíduo.[236]

Além da Alemanha, O direito à autodeterminação informativa já encontra ressonância nas constituições de diversos países. Espanha[237] e Portugal[238], por exemplo, que já o incorporaram.

RODRÍGUEZ [239] enuncia as três gerações de direitos humanos reconhecidas atualmente pelos juristas. A primeira, os direitos de defesa, impondo salvaguardas à personalidade frente as ameaças estatais, como é o caso da intimidade; a segunda, surgida dos movimentos sociais do século XIX, de direitos de natureza econômica, social e cultural, como são os casos da seguridade social e da saúde; e a terceira, dos direitos baseada nos progressos tecnológicos, na qual se insere a autodeterminação informativa.

---

[236] MATA BARRANCO, Norberto J. de la; BARINAS UBIÑAS, Desirée. *La protección*… cit., p. 36-37.
[237] Espanha. Constituição de 1978. artigo 18. 4. "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"
[238] Portugal. Constituição de 1976. Artigo 35.º Utilização da informática. 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.
[239] RODRÍGUEZ, Víctor Gabriel. *Tutela…* cit., p. 59.

Nos parece adequado afirmar que a autoderminação informativa referida pela Corte Alemã deriva tanto dos direitos a personalidade quanto da proteção à intimidade. Trata-se, aos nossos olhos, de um direito de terceira geração, porque nascido justamente do progresso tecnológico. Sem ele, os indivíduos na sociedade em rede sofreriam constante ameaça à intimidade, posto que são, o tempo todo, inseridos em contextos fragilizantes desse direito fundamental.

Na União Europeia, a autodeterminação afirmativa está consagrada no art. 8º do Capítulo de direitos fundamentais; no Brasil, segundo RODRÍGUEZ, não merece ainda *status* de direito fundamental.[240] Ainda que não seja equiparável à intimidade, mas é certo que constitui direito[241] – carente de tutela adequada, em nossa opinião.

Diante da evolução do cenário na última década, entendemos que, com a geração de direitos relacionados à tecnologia e a emergência de um debate quanto ao tema das novas violações da intimidade, cabe – e é mesmo essencial – o estabelecimento desse direito em nosso país de maneira clara, expressa, ainda que não com o status de direito fundamental[242].

Importa observar que o espaço em que o indivíduo reserva sua soberania decisória tem sido afetado decisivamente por esse novo mundo digital. O ser humano passou a depender de seus dados para a tomada de decisão, há uma verdadeira simbiose entre o espaço físico e o digital que pode afetar seus desejos e decisões. Se trata nesse caso, segundo MATA BARRANCO, de tutelar, quanta e qual informação sobre determinados assuntos e pessoas queremos receber e de que maneira essa própria informação pode ser utilizada[243]. De acordo com o Catedrático da Universidade do País Basco, essa é a continuação da autodeterminação informativa, a que se dá o nome de autodeterminação decisional – o direito de livre desenvolvimento em âmbito privado, sob a salvaguarda da soberania pessoal, desde uma perspectiva na qual a proteção

---

[240] Idem. p.66.

[241] Na nossa Carta Constitucional não existe dispositivo que faça referencia expressa a este direito, mas se pode considerar, de maneira reflexa, que a inscrição da palavra "dados" no inciso XII do art. 5º, em combinação com o inciso X do mesmo artigo, podem oferecer tal proteção.

[242] O que aqui se faz é especificamente compreender que a intimidade, em seu conceito mais amplo, atento aos novos perigos que a informática lhe traz, compreende também a autodeterminação informativa, ou seja, a liberdade de não fornecer dados pessoais sem necessidade absolutamente comprovada, de não os ver combinados por nenhum meio informático sem autorização de lei e de ter acesso imediato aos próprios dados na esfera pública ou privada, bem como ter a capacidade de corrigi-los complementá-los e, principalmente, apaga-los quando necessário" (RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit., 94.)

[243] MATA BARRANCO, Norberto J. de la; BARINAS UBIÑAS, Desirée. *La protección*… cit., p. 46.

informacional do direito à vida privada permite a pessoa tutela seu aspecto decisional[244]. Sequer logramos alcançar a proteção adequada do primeiro, a que se trata esse tópico, já há um esboço – legítimo – de sua evolução. De fato, o direito precisa acompanhar de perto os avanços da tecnologia.

Segundo MATA BARRANCO "não se trata de navegar protegido, mas de navegar seguro: seguros de nossas eleições, seguros que elas representam nossos direitos, que não se violará nossa privacidade, da nossa autodeterminação pessoal e do respeito ao nosso espaço privado"[245]. Há discussões no mesmo sentido no Canadá com Cavoukian[246] e na Holanda com Hustinx.[247]

A nova realidade de riscos na internet reclama novos direitos específicos a resguardar a personalidade do indivíduo. De acordo com RODRÍGUEZ, "com a tecnologia informática, há uma nova realidade, diversa da existente quando a possibilidade de controle da informação pessoal ocorria apenas pelo suporte em papel. Não se trata, portanto, de uma mera intensificação da capacidade de controle da informação pessoal, mas de algo qualitativamente diverso, que é a possibilidade de combinação automática de dados, próximos ou remotos."[248]

No exercício da autodeterminação informativa, entendemos que o indivíduo pode exercer controle sobre a legitimidade do recolhimento, da divulgação e da utilização dos seus dados pessoais, falta uma Lei específica para viabilizar isso. Há latente fragilidade do direito à autodeterminação informativa com os avanços da tecnologia. Uma Lei Geral de Dados poderia suprir esse *déficit*, esclarecendo os princípios aplicáveis ao tratamento de dados, os direitos dos titulares desses dados, as medidas de gestão necessárias e etc.

Como ensina BOBBIO "os direitos não nascem todos ao mesmo tempo. Nascem quando devem ou podem nascer"[249]. Esse, ao que tudo indica, será um direito que logo será exatamente delimitado e consagrado.

---

[244] Ibid. p.59
[245] MATA BARRANCO, Norberto J. de la. La privacidad en el diseño y el diseño de la provicidad, también desde el derecho penal. *Cuaderno del Instituto Vasco de Criminología,* San Sebastian, n. 28, pp. 253-274, 2014.
[246] CAVOUKIAN, A. *Privacy by design...take the challenge.* Washington: Privacy and Information Comission, 1997. p. 7.
[247] HUSTINX, P., *Privacy by design: delivering the promises.* Artigo digital: Springer, 2010. Disponível em: http://link.springer.com/article/10.1007/s12394-010-0061-z. Acesso em 14.07.2016.
[248] RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit., p. 67.
[249] BOBBIO, Norberto. *El tiempo de los derechos*. Madrid: Editorial Sistema, 1991. p. 18

## 2.3 Intimidade como bem jurídico na internet

Há farto debate a respeito do bem jurídico. BECHARA relata que o surgimento da teoria do bem jurídico insere-se num movimento de reação à ideologia iluminista, a partir de uma preocupação com a insegurança jurídica e de um despertar positivista[250]. Segundo ela o bem jurídico aparece pela primeira vez com Binding, com a da atribuição por aquele autor de um sentido formal à infração ao dever de obediência do cidadão em relação ao Estado[251].

Diante do novo cenário de possível danosidade social provocada pela miríade de atores privados que, de alguma forma, detêm coleções de dados dos usuários da internet – notadamente as redes sociais – é de se verificar a existência ou não de um aporte de direitos que tornem pertinentes a existência de infrações a intimidade na rede, com a consequente fragilização, em um novo nível, da intimidade.

É desaconselhável adicionar a existência de uma proteção rasa ou indevida, colocando-a sob a égide do Direito Penal para causar a (falsa) sensação de segurança. O cenário da legítima penalização de condutas que ameaçam direitos fundamenteais está, porém, distante disso. No caso da intimidade, como visto até aqui, princípio que deriva diretamente da dignidade da pessoa humana, a proteção da norma penal é possível. As mudanças da última década na internet parecem justificar uma investigação quanto aos novos limites de sua aplicação. A tutela da autodeterminação informativa, tendo como base as novas fragilizações da intimidade, tem sido até mesmo negligenciada no âmbito da política criminal e, em certa medida, pelas ciências criminais. Este pode ser um direito – não fundamental – derivado da intimidade.

Há, no entanto, alguns marcos internacionais específicos a tratar do tema da intimidade e da vida privada e desses direitos com a expansão da internet. A Convenção sobre cibercrime de Budapeste é um bom exemplo disso. Trata-se de um dispositivo com as assinaturas de quase 70 países e mais de 40 ratificações[252], no âmbito do Conselho da Europa. Ele propõe robusto e universal conjunto protetivo para evitar práticas que façam com que as

---

[250] BECHARA, Ana Elisa Liberatore Silva. *Bem jurídico-penal***.** São Paulo: Quartier Latin, 2014. p. 93.
[251] Ibid., p. 100.
[252] Council of Europe, Treaty 185. Budapest 23.11.2001. Disponível em https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=6i3Tdf7z. Acesso em 27.09.2017

redes informáticas sejam utilizadas para o cometimento de infrações, ligando as violações do sistema informático à quebra do quanto inscrito no Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas. O texto reafirma o:

> "direito à liberdade de opinião sem qualquer ingerência, o direito à liberdade de expressão, incluindo a liberdade de procurar, de receber e transmitir informações e ideias de qualquer natureza sem considerações de fronteira, e, ainda, o direito ao respeito pela vida privada"[253].

Precebe-se, portanto, que tanto a liberdade de expressão quanto a intimidade são direitos derivados da própria dignidade do homem e, por isso, merecem o maior nível de proteção possível.

BOTTINI argumenta no sentido de que as tecnologias atuais potencializam a probabilidade de crises, exigindo medidas de precaução e prevenção[254]. O autor preocupa-se com a complexidade das relações sociais, sendo certo, segundo ele, que também elas são objeto de criação de novos riscos.[255]

Parece possível que as violações da privacidade e da intimidade que ocorrem na internet por parte de atores privados sejam suficientes para embasar sua normatização.

Ainda para BOTTINI, a caracterização dos tipos penais deve necessariamente passar por um bem jurídico a ser protegido digno do *ius puniendi*. Segundo ele a construção de um critério sólido para a identificação de bens jurídicos passíveis de proteção penal passa precisamente pela fundamentação na dignidade da pessoa humana, no conjunto de condições necessárias para a autodeterminação do individuo. Para SYDOW é possível que entre esses direitos subjetivos esteja o de conservação do meio ambiente íntimo em que se vive e que, mais recentemente, o ambiente informático seja indissociável disso[256]. CANTO argumenta que o cerne

---

[253] Idem. Preâmbulo. Expõe ainda que "Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável;"

[254] BOTTINI, Pierpaolo C. *Crimes de perigo abstrato e princípio da precaução na sociedade de risco*. São Paulo: Revista dos Tribunais: São Paulo, 2007. p. 35.

[255] BOTTINI, Pierpaolo C. *Crimes*... cit., p. 96.

[256] SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. 2.ed. São Paulo: Saraiva, 2015. p. 84.

do bem jurídico nesse caso está na informação.[257] Em todos, há uma convergência de direitos em que a intimidade é fator fundamental.

SILVA SANCHEZ reconhece que vivemos numa época de complexidade das interações, asserta que "la actual revolución de las comunicaciones da lugar a un vértigo derivado de la falta – sentida y probablemente assimismo real – de domínio del curso de los acontecimentos, que no puede sino traducirse en términos de inseguridad"[258], constando que existe um contexto de crescente desorientação pessoal diante da realidade. Para o autor podem ser considerados bens jurídicos todos os objetos que o ser humano necessite para a sua completa e livre autorrealização. SILVEIRA admite a formatação até de novos bens jurídicos, supra-individuais na sociedade pós-industrial, lembrando que eles devem ser lastreados nos interesses da vida social da pessoa[259].

ANA ELISA BECHARA, assevera que o direito penal protege apenas os valores consagrados na lei fundamental[260], mas aduz que a Constituição não oferece as garantias necessárias para erigir-se em instrumento exclusivo para o estabelecimento de interesses que devem ser protegidos pelo direito penal[261]. Para a autora no caso brasileiro o problema do estabelecimento de um norte constitucional está no caráter aberto e analítico da Carta Cidadã. Ela pondera que esse caminho tem contribuído para legitimar a ampliação da via penal, "sob pretexto de ofensa a bens de caráter coletivo"[262].

Adentrando o problema específico dos desafios impostos pelas novas formas de sociabilidade advindas da internet, SYDOW postula a construção de um bem jurídico da "*segurança informática*", justamente como sendo derivado do quanto elencado como direito na

---

[257] "Em tales términos, sostengo como principal bien jurídico protegible la información, y, secundariamente los datos informáticos em sí mismos o los sistemas de o los sistemas y redes informáticos y de telecomunicaciones, pues los primeiros no constituyen más que la representación electrónica, incluso digital, de la primera, com um valor variable, y los segundos los mecanismos materiales de funciones automáticas de almacenamiento, tratamento, transferência y transmisión de aquélla, cuya afectación o no, de cualquiera de ellos, datos o elementos, pueden servir, normalmente mas no necessariamente, para la configuración de algunas modalidades o tipos de delitos informáticos." (DEL CANTO, Enrique Roviera. *Delincuencia informática y fraudes informáticos.* Granada: Comares, 2002. p. 72.)

[258] SILVA SÁNCHEZ, Jesús María. *La expansión del derecho penal*: aspectos de la política criminal en las sociedades postindustriales. 2.ed. rev. Madrid: Civitas, 2001. p. 33.

[259] SILVEIRA, Renato de Mello Jorge. *Direito penal supra-individual:* interesses difusos. São Paulo: Revista dos Tribunais, 2003. p. 57.

[260] BECHARA, Ana Elisa Liberatore Silva. Bem jurídico..., cit., p. 122.

[261] Ibid. p. 129.

[262] Idem.

Convenção de Budapeste. Ele subdivide esse novo bem em (i) integridade, (ii) confidencialidade e (iii) disponibilidade, sendo que a integridade protegeria a incolumidade das criações intelectuais e a inteireza dos arquivos; a confidencialidade seria a proteção do acesso às informações dos usuários  e sua intimidade; à disponibilidade caberia a parte da proteção do acesso a qualquer momento pelo titular dos dados.[263]

Com a devida licença, discordamos. Nos parece que a penalização de algumas – novas – condutas, fruto das interações geradas na sociedade a partir do desenvolvimento da internet de acesso quase universal, tendo como base a fragilização da intimidade dos indivíduos é razoável e possível.

Contudo, ao menos no que concerne às interações sociais virtuais que colocam em risco a intimidade dos indivíduos, talvez não seja o caso de se buscar a fundamentação de uma regulação jurídico-penal com base em novos bens jurídicos. Entendemos aqui que a intimidade já é caminho suficiente para a proteção, notadamente em relação aos dados, sendo possível a sua tutela penal com o estabelecimento de tipos que a violem de novas maneiras, fruto das novas formas de interação em rede.

Parece possível o estabelecimento de um novo campo do estudo, cujo objeto passa pela proteção da autodeterminação informativa – todavia, em estrita ligação com a intimidade, esta já abrangida pelo direito penal há tempos. Essa possibilidade não é proposta para que exista algum tipo de proteção aos dados em si, como objetos autônomos e independentes dos interesses humanos, mas sim como fatores indispensáveis ao indivíduo – usuário da internet –, enquanto elemento necessário da sua intimidade e formador de sua personalidade.

Mesmo diante de tantas e tão velozes evoluções no tema, parece precipitada a adoção de um novo bem jurídicco de uma pretensa "segurança informática" na tutela das violações da intimidade na internet. Algo do tipo não passa de tutela da própria intimidade, tendo em vista que a segurança, nesse caso, protegeria justamente a intimidade dos indivíduos que depositaram os seus dados em dispositivos informáticos.

A par de em alguma medida se aproximarem às iniciativas punitivas que adentram um certo "direito de precaução", como descrito por BOTTINI[264], os possíveis novos injustos

---

[263] SYDOW, Spencer Toth. O bem jurídico nos crimes informáticos. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 23, n. 113, p.193-212, mar./abr. 2015. p. 208. Ver também a exposição mais extensa em SYDOW, Spencer T. *Crimes informáticos*... cit., p. 70-88.

[264] BOTTINI, Pierpaolo C. *Crimes de perigo*... cit., p. 109.

praticados na rede, a partir das novas violações da privacidade e da intimidade, desempenhariam o papel de definir a periculosidade de certas condutas para a sociedade e para os sujeitos, tornando legitima a possibilidade de sanção estatal. Para os delitos informáticos como um todo e, especificamente, da tutela da autodeterminação informativa, há, ao que parece, subsidio suficiente para eventuais tutelas penais.

Contudo, resta o desafio dos limites e da adequação das técnicas pelas quais as condutas socialmente danosas no âmbito da internet podem ser alcançadas pelo direito penal. Retorna-se, portanto, à ressalva já antes realizada por RENATO DE MELLO JORGE SILVEIRA, no sentido de que a delimitação daquilo que é punível deve ser baseado em princípios materiais sólidos[265]. BECHARA, por sua vez, ao comentar as sucessivas mudanças legislativas impostas pelas transformações sociais modernas, salienta que tal necessidade não pode servir de pretexto para a tentação do abandono ao princípio da legalidade, sendo certo que "o legislador não pode surpreender os destinatários da norma sem expor claramente o que e como pune"[266]. A autora lembra que não basta a ofensa à legalidade para a caracterização do injusto, é preciso que se perceba também ofensa ao princípio da ofensividade. Para ela: "toda infração penal requer a exteriorização e materialidade de um fato, o qual deve lesionar ou expor a perigo um bem juridicamente tutelado"[267]. Diante da necessidade de maior da proteção da intimidade em tempos de sociedade em rede com compartilhamento constante de dados e do reconhecimento da autodeterminação informativa, parece possível o estabelecimento de novas penalizações.

Tais comportamentos danosos à sociedade, especialmente no que tange à violação da intimidade – e da autodeterminação informativa, naquilo que guardar relação com a vida privada –, constituem novas formas de agressão ao livre desenvolvimento das subjetividades, possuindo, a depender de sua intensidade e abrangência, ofensividade para refletir um injusto penal materialmente compreendido. Daí a necessidade de se pensar, portanto, um conjunto normativo adequado aos novos tempos e formas de sociabilidade, mediante uma tipificação condizente com os injustos próprios do ambiente digital, naquilo que for idôneo e necessário à proteção das individualidades frente a novas formas de agressão.

---

[265] SILVEIRA, Renato de Mello Jorge. *Fundamentos da Adequação Social em direito penal.* São Paulo: Quartier Latin, 2010. p. 78

[266] BECHARA, Ana Elisa Liberatore Silva. Bem jurídico..., cit., p. 151.

[267] Ibid., p. 152.

Destarte, constatada a possibilidade da initimidade figurar como bem jurídico a ser tutelado frente às novas violações ocorridas no ambiente da rede, parece ser cabível a instituição de tipos penais para regular esses novos delitos.

## 2.4 Intimidade como direito de defesa

A intimidade tem espectro amplo de proteções e pode ser vista como verdadeiro direito de defesa. O artigo 5º da Constituição Federal, dispõe exatamente sobre os direitos e garantias e assegura como direito fundamental, de forma expressa, a proteção da intimidade e da vida privada. Também em convenções internacionais erigidas para a contemplação de direitos humanos essenciais, o tema relativo à proteção do sigilo é objeto de específico tratamento, como no exemplo do artigo 11 da Convenção Americana de Direitos Humanos (Pacto de San José da Costa Rica), a qual passou a integrar o ordenamento jurídico nacional, com a promulgação do Decreto nº 678/1992.

Há, ainda, no artigo 5º da Carta da República o inciso XII, que protege os sigilos nas comunicações, vedando a mitigação do sigilo de dados e das comunicações telefônicas e telemáticas dos indivíduos sem a existência de fundamentada decisão judicial.

Pode-se entender, portanto, que o direito à intimidade surge no nosso ordenamento como um verdadeiro direito de defesa em relação a qualquer intromissão na vida privada e na intimidade, por parte do Estado ou de particular, sendo um direito ativo de controle das informações que dizem respeito ao indivíduo e apenas a ele[268].

As penalizações aventadas a seguir não vão justamente nessa linha, posto que alicerçadas justamente na proteção da privacidade e da intimidade dos usuários da rede enquanto direito de opacidade. A defesa da intimidade dos cidadãos parece ser o único caminho a garantir o livre desenvolvimento da personalidade face ao Estado e aos demais cidadãos.

---

[268] Para Péres Luño o primeiro aspecto, de proteção à intromissão, é um direito com dimensão negativa enaunto o segundo aspecto, de controle de acesso a informações da vida privada e da intimidade, constitui direito de dimensão positiva. Ver mais em PÉRES LUÑO, António-Enrique. El derecho a la intimidad en el Âmbito de la Biomedicina. In: LA CUESTA, Antonio Ruiz de (coord.). *Bioética y derechos humanos*: implicaciones sociales y jurídicas. Sevilha: Universidade de Sevilha, 2005. p. 109.

## 2.5 Novos limites da intimidade: estabelecimentos de tipos

### 2.5.1 Tipos penais para a proteção da intimidade

A tipicidade, em brevíssima síntese apresentada por REALE JÚNIOR, consiste na congruência entre a ação e o paradigma legal, sendo o tipo de crime parte de um modelo, uma formulação geral.[269] SILVEIRA ensina que a tipicidade assume relevos importantes mostrando-se como instrumento metodológico de compreensão das estruturas normativas, desempenhando a função de seleção de comportamentos humanos[270].

A internet, quando se trata da devida regulação, precisa ainda de um modelo geral de proteção a vida privada e a intimidade, com formulação específica de tipos para condutas que as fragilizam sobremaneira. Não parecem mais, diante de tantas novas modalidades de injustos que têm na rede seu insumo, satisfatórias as criminalizações analógicas. Ressalve-se que, apesar da velocidade dos avanços na rede, um tipo deve ser taxativo e claro, não dando margem a possíveis avanços tecnológicos.

Segundo TIEDEMAN:

> A expressão criminalidade por computador se alude a todos os atos, antijurídicos segundo a lei penal vigente (ou socialmente prejudiciais, e por isso, penalizáveis no futuro), realizados com o emprego de um equipamento automático de processamento de dados. Por um lado, dito conceito abarca pois o problema da ameaça da esfera privada do cidadão mediante a acumulação, arquivo, associação e divulgação de dados obtidos por computadores.[271]

De fato, compreendemos que há hoje mais delitos que são praticados pelos computadores do que a legislação tem sido capaz de acompanhar. É função ético-social do direito penal a proteção dos valores fundamentais para a sociedade, ainda que nem todo bem jurídico requeira tal tutela.[272] A intimidade, contudo, parece carecer de tal tutela específica na sociedade em rede.

---

[269] BOTTINI, Pierpaolo C. *Crimes de perigo...* cit., p. 37.
[270] SILVEIRA, Renato de Mello Jorge. *Direito penal...* cit., p. 73-74.
[271] TIEDEMANN, Klaus. Criminalidad mediante computadoras. In: TIEDEMANN, Klaus. *Poder económico y delito* - Introducción al Derecho Penal Económico y de la Empresa. Barcelona: Editorial Ariel S.A., 1985. p. 38.
[272] MIR PUIG, Santiago. Bien jurídico y bien jurídico-penal como límites del Ius puniendi. *Estudios penales y criminológicos***,** Santiago de Compostela, n. 14, 1991. p. 205

A Espanha, como já visto nesse estudo, adota tipo penal específico, desde 2015, para a proteção da intimidade na rede. Ainda que genérica, a penalização espanhola pode servir para demonstrar que há sim necessidade de adoção de parâmetro semelhante.

A falta de debates na área pode contribuir para a criação excessiva de tipos, além de, pela falta de precisão, gerar o risco de tipos genéricos. Parece-nos pertinente, portanto, que se discuta a penalização de condutas que fragilizam a intimidade na internet.

### 2.5.2 **O estabelecimento de tipos penais para detentores de dados**

No que diz respeito aos detentores de dados, quase sempre pessoas jurídicas, as alternativas de responsabilização penal estão muito mais concentradas na atribuição de responsabilidade a figura do garante, que ao descumprir eventual Lei Geral a ser estabelecida para regular a matéria incidiria na conduta do artigo 13, § 2, do Código Penal.

Além desse agente responsável, eventuais condutas poderiam atingir os indivíduos que violarem, pelo acesso privilegiado aos dados pessoais contidos em sistemas informáticos, a privacidade e a intimidade de usuários da rede. Neste caso, é importante que se individualize a responsabilidade penal dos indivíduos.

É possível também, para evitar uma onda de penalidades desnecessárias e a consequente indesejada inflação de normas do tipo, que as violações mediante acesso privilegiado constituam qualificadoras de eventual tio por abuso de confiança.

O dano para uma empresa que não cuida adequadamente dos dados depositados em sua confiança é hoje, inegavelmente, muito maior sob o aspecto reputacional. È bastante dificil imaginar que alguém confiasse hoje nos Yahoo – que recentemente admitiu que em 2013 fora inteiramente *hackeado,* perdendo o controle sobre as informações de 3 bilhões de contas[273] ou a Equifax, que perdeu o controle sobre os cadastros de 143 milhões de clientes[274].

---

[273] Disponível em: https://www.tecmundo.com.br/mercado/122657-problemao-ataque-2013-afetou-3-bilhoes-contas-yahoo.htm Acessado em 02.09.2017

[274]Disponível em https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/ Acessado em 02.09.2017.

De qualquer maneira, há que se estabelecer, como veremos adiante, uma figura de responsabilidade pela gestão dos dados de uma organização. Há inclusive recomendção da AIDP nesse sentido[275]:

> ICT network users and system providers should be encouraged to protect the safety of networks, including by self-regulation of providers. Neglect of safety measures should not lead to criminal liability on the part of users. Legislatures may, however, make punishable the violation of specific obligations to ensure the security of other persons' data.

O legislador brasileiro deve, portanto, se conscientizar acerca dessas novas formas de violação, inclusive no que diz respeito aos deveres de cuidado, estabelecendo, quando couber, tipos penais específicos para os detentores de dados alheios.

### 2.5.3 **O estabelecimento de penais para invasores**

A par de da mudança legislativa de 2012 que trouxe a lume uma Lei para criminalizar a invasão de dispositivo informático (Lei nº12.737 – Lei Carolina Dieckmann), não há no Brasil um tipo semelhante a inibir as invasões de dados – e consequente violação da privacidade e da intimidade.

É preciso conscientizar o legislador de que os dados, apesar de, na maior parte das vezes, estarem contidos em dispositivos informáticos, nem sempre são violados mediante "invasão do dispositivo" ou "mediante violação indevida de mecanismo de segurança". De fato, as imprecisões do diploma atual decorrem da emergência na aprovação, decorrente de um esforço pouco usual e momentâneo em face a uma situação fática envolvendo uma figura pública.

A mera conduta de "hackear" ou "crackear" (este segundo o termo mais correto)[276] pode, até dispensar o elemento subjetivo do tipo, subsumindo-se na mera quebra do código, mas há ainda que se investigar as invasões com elementos bem definidos. Nesse sentido,

---

[275] Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

[276] O Hacker é propriamente o sujeito aficionado por tecnologia que estuda as fragilidades do sistema. O é um hacker que dedica-se a invadir maldosamente sistemas.

envolvendo invasões ou indo além delas, um diploma específico mereceria investigar, por exemplo, o *data mining* (estabelecimento de perfis para venda a terceiros), a *porn revenge* (a divulgação de vídeos íntimos de ex-parceiros), o *ciberstalking* (perseguição por redes sociais), *cibergrooming* (aliciamento sexual pela internet), *data phishing* (obtenção de dados, semelhante a um estelionato), entre outras condutas[277]. Não é que todas essas condutas mereçam tratamento necessariamente penal (a AIDP já ofecereu recomendação inclusive quanto a isso[278]) mas, se fragilizarem, em medida sufiente a intimidade, a norma extrema pode ser uma das alternativas.

Invasores que violam coleções de dados e, consequentemente, a intimidade e a vida privada alheias, pelo uso da internet podem violar, por vias impossíveis de se prever há apenas alguns anos, o bem jurídico intimidade. De acordo com RODRÍGUEZ,

> O Direito penal (...) tem função de comunicar à sociedade que determinado bem jurídico é positivamente valorado. Nesse sentido, a previsão de pena aos delitos contra a intimidade tem a função de mostrar que ela é um valor a ser protegido, até mesmo ante o interesse social de persecução penal, que não pode sacrificar desmedidamente um direito de personalidade[279].

Conquanto existam no nosso código os crimes de Divulgação de segredo (art. 153), de violação de segredo profissional (art. 154), de invasão de dispositivo informático (art. 154-A) e, sob outro prisma, de dano (art. 163), esses tipos não são suficientes para inibir a criminalidade informática.

SYDOW classifica os delitos desse tipo em próprios e impróprios. Segundo ele, os impróprios são os delitos comuns, aqueles que poderiam ter sido praticados por outros meios; enquanto os próprios são aqueles que visam atingir um sistema informático ou os seus dados[280].

---

[277] Quanto a isso, ver o interessante artigo de Emilio Viano. VIANO, Emilio C. The "online" world and cybercrime: a new reality for criminal law and criminology. **Direito e Cidadania,** Praia, Cabo Verde, v. 9, n. 27, p. 29-41., 2008.

[278] "Given the growing concern about the frequency and seriousness of cyber stalking, cyber bullying, and cyber grooming, special attention shall be given to effectively respond to the problem, emphasizing positive approaches, prevention, public education and awareness, and alternative sanctions, rather than only applying criminal law protection." Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

[279] RODRÍGUEZ, Víctor Gabriel. *Tutela*... cit., p. 238.

[280] SYDOW, Spencer T. *Crimes informáticos*... cit., p. 88 Apesar de discordarmos da posição esposada por este autor quanto a eventual consagração de um novo bem jurídico do sistema informático, entendemos a classificação delitiva bastante acertada.

No caso dos delitos impróprios, entendemos que é até possível a aplicação dos tipos já vigentes – embora uma tipificação específica contribuísse sobremaneira para eventuais analogias precárias. No caso dos delitos próprios a falta de legislação especifica é flagrante. Não há, por exemplo, como penalizar com as normas atuais adequadamente a prática de Malware, a inserção de código malicioso que pode ser utilizada para a cópia ou subtração de dados de usuários da rede.

É auspicioso que se ofereça tratamento penal adequado e específico, pelo menos para as violações mais comuns nesse campo. Ao balancear a realidade dos novos possíveis delitos cometidos pela internet e a necessidade de segurança cibernética, o sistema de justiça criminal deve equilibrar interesses individuais, coletivos, do setor privado e público. Ainda que seja recomendável, como ensina Roxin, que o direito penal intervenha apenas como ultima medida, e que medidas de prevenção robusta mereçam ser privilegiadas na defesa ativa da intimidade, como a educação pública, a conscientização, a imposição de sanções alternativas e a adoção de programas de integridade de dados por gestores, em casos extremos é preciso que o legislador considere o estabelecimento de tipos específicos.

Nesses casos, como se viu, é necessário o extenso e atento debate para a imposição de normas penais. O assodamento no debate ou a imposição de Leis de ocasião – como, após quase uma década de tramitação, acabou sendo o caso da Lei Carolina Dieckmann – são desrecomendadas – ainda mais nesse caso, em que se propõe aqui a norma extrema para penalização rara de violações à intimidade.

Se este for o caminho adotado, ainda que se reconheça aqui a sua legitimidade e, em certa medida, diante dos avanços das condutas e da tecnologia, até a necessidade de inovações legislativas nesse sentido, impõe-se a moderação nas penas[281].

---

[281] Vale o magistério de DOTTI "As alternativas para o sistema de penas constituem meios, métodos e formas de reação ao delito que atuam em todos os momentos do dinamismo penal. Através da cominação, quando o ordenamento positivo consagra novas modalidades de sanção; da aplicação, quando ao juiz se possibilitam meios para a melhor escolha e medição da pena; e da execução, quando os regimes dispõem de condições formais e materiais que atendam aos objetivos gizados pelas diversas medidas de prevenção e repressão à criminalidade. DOTTI, René Ariel. Bases e Alternativas para o Sistema de Penas. 2ª edição. São Paulo: Editora Revista dos Tribunais, 1998, p. 475

A invasão de redes e dispositivos merece proteção específica. O ato de hackear essas redes pode tanto funcionar como elemento subjetivo de possíveis tipos penais quanto ser ele a conduta em si, dispensando elementos subjetivos.

Nesse sentido, parece legítimo o estabelecimento tanto de uma conduta de invasão de redes quanto outras, com a invasão de redes para determinados fins – como a alteração ou subtração de dados. Nesse caso, o direito penal pode desempenhar importante proteção à intimidade dos titulares desses dados e, ao mesmo tempo, servir de elemento disuasório.

# 3. ALTERNATIVAS PARA A EVOLUÇÃO DA QUESTÃO

## 3.1 O futuro da gestão dos dados no Brasil

Até esse ponto da pesquisa estabelecemos (i) as questões controversas e os novos desafios, apresentando o cenário atual de desafios – e são muitos – (ii) o marco normativo brasileiro para a internet, (iii) os conceitos que permeiam as questões estudadas (iv) um panorama comparativo de proteções e (v) aquilo que, imaginamos, poderia contribuir para a mitigação dos riscos associados às violações da privacidade e da intimidade na internet diante dos novos desafios que se apresentam.

Pois bem. Ao pisar nesse ponto, cumpre desvendar as novas alternativas para mitigar os riscos de violações da privacidade e da intimidade no Brasil. O novo Regulamento Geral de dados da União Europeia, uma legislação moderna que entrará em vigor em 2018, pode contribuir como caminho possível para ser seguido. Abordaremos a seguir os aspectos de uma Lei Geral de Dados no Brasil bem como a viabilidade e conveniência do estabelecimento de uma Autoridade de Dados para o país. Ao final, apresentamos nossa tomada de posição quanto a todos esses temas.

## 3.2 Privacy by design e Privacy by default

Antes de adentrarmos nas possibilidades de normatização das questões relacionadas ao direito fundamental a intimidade de modo a prevenir as possíveis violações a esse direito por atores privados na internet, convém apresentar o que pode ser uma alternativa – a adoção da privacidade por design e por padrão (*privacy by design and default*) para a diminuição da fragilidade da privacidade e da intimidade na rede. Tal caminho não exclui, contudo, a adoção de uma Lei Geral de Dados.

A *Privacy by design* nada mais é que o empoderamento dos usuários frente as aplicações na rede, pela formulação de um conjunto de requisitos técnicos de segurança para cada camada da aplicação que está sendo criada, desde o seu projeto, com a elaboração de um modelo de avaliação e certificação de requisitos mínimos, quando possível, dando ao usuário o controle das permissões de coletas de dados seus. A adoção desse padrão tornaria mais equânime a relação entre fornecedores e consumidores de conteúdo da rede. Privacidade por design significa, ainda, coletar e processar o menor número possível de dados pessoais (com a aplicação do princípio de minimização de dados).

Na prática, isso significa que todas as empresas que processam dados pessoais devem garantir que a privacidade seja incorporada ao seu sistema durante todo o processo de disponibilização do seu produto, primando pela autonomia do indivíduo que é alvo da aplicação.

Na Alemanha, a implementação da nova cédula de identidade eletrônica (*neuer eletronischer Personalausweis –nPa*) e do novo cartão de seguro saúde (*elektronische Gesundheitskarte – eGK*) adotam a privacidade por design. Isso pode impossibilitar a gravação de dados de eventos e localização, de modo que nenhum perfil relacionado a dados possa ser criado a partir do uso desses cartões eletrônicos. Nem as verificações anteriores de dados biométricos realizados por funcionários do governo nem contatos comerciais usando a função de verificação de identidade podem ser recuperadas da zona relevante do chip e certamente não poderão ser recuperadas e armazenadas pela parte que estará utilizando o cartão para identificar o titular. Isso evita que os dados sejam usados para compilar perfis de movimento ou comportamento dos cidadãos daquele país, fortalecendo a intimidade[282].

A *privacy by default*, ou privacidade por padrão, por sua vez, significa que os detentores de um produto ou uma aplicação devem garantir ao público a adoção dos padrões mais altos de proteção dos dados como regra-geral.

Além disso, todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto, serviço ou aplicação devem ser mantidos somente durante o tempo necessário para fornecer o produto, serviço ou aplicação. No exemplo das redes sociais, se o usuário se inscrever para uma nova conta, deve saber exatamente quais informações serão compartilhadas no seu perfil por padrão, não poderá a rede social dali em diante compartilhar mais informações que o assentido na adesão. Para uma conta de redes sociais, a informação mais essencial seria seu nome e seu endereço de e-mail – mas não a sua idade e localização, por exemplo. Somente as informações mais básicas devem ser compartilhadas.

A AIDP já recomendou a adoção da *privacy by design* e da *privacy by default*[283]*:*

> Commercial personal data processors, like Internet and telecommunications providers, social media platforms, and application developers, should be required to

---

[282] SHAAR, P. Privacy by design. *Identity in the information Society*, vol.3, n.2, ago. 2010.

[283] Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

> adopt privacy by design and by default policies, if necessary by compelling measures. The violation thereof should be redressed through non-criminal or criminal sanctions.

A partir de 2018, tanto a *privacy by design* quanto a *privacy by default* se tornarão parte integrante do desenvolvimento tecnológico e do processamento de dados na União Europeia, com a entrada em vigor do GDPR[284]. O instrumento, é bom que se diga, não é específico sobre como os detentores de algorítimos e aplicações implementarão essas mudanças, mas fala na implementação de uma certificação[285] comum de segurança da

---

[284] Conselho Europeu. General Data Protection Regulation (GPDR) .Artigo 25 " Data protection by design and by default: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article."

[285] Conselho Europeu. General Data Protection Regulation (GPDR) Artigo 42: "Certification: The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

The certification shall be voluntary and available via a process that is transparent.

A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means."

informação, o que certamente levará a uma mudança de cultura significativa nas operações de empresas naquele continente. Será auspicioso se a mudança refletir-se numa mudança de paradigma mundial.

### 3.3 O novo Regulamento Geral de dados da União Europeia: um modelo possível

O Parlamento Europeu e o Conselho da União Europeia aprovaram em 2016, depois de mais de quatro anos de debates, o Regulamento Geral sobre Proteção de Dados (GDPR, na sigla em inglês para *General Data Protection Regulation*), que pode ser apontado como a mais importante e moderna legislação de proteção de dados na atualidade.

A novel legislação tem o propósito claro de padronizar o tratamento dos dados nos países do Bloco. O GDPR entrará em vigor em 25 de maio de 2018. O âmbito de aplicação material do GDPR é bastante extenso, abrangendo praticamente toda e qualquer operação de "tratamento" de dados pessoais — ambos os termos dotados de definição ampla na norma. Isso inclui a coleta, o registro, a organização, a conservação, a utilização, a divulgação e destruição de qualquer informação relativa a uma pessoa física identificada ou identificável – aqui numa adoção de padrão parecida a do caso brasileiro, como visto anteriormente. Pessoas físicas e jurídicas que de alguma forma façam operações de tratamento de dados pessoais deverão adequar as suas práticas para não correrem o risco de sofrerem sanções severas por parte das autoridades da UE.

Convém anotar que a legislação é imposta ao tratamento de dados de qualquer pessoa ou empresa de originem no bloco. Para exemplificar, se uma empresa brasileira faz o tratamento de dados pessoais de um indivíduo que está no território da União Europeia, de forma relacionada à oferta de bens ou serviços, ainda que fornecidos gratuitamente, ela estará sujeita às normas do GDPR e potencialmente obrigada a designar um representante no respectivo Estado-Membro, sob pena de arcar com sanções que podem incluir multas e até a proibição do tratamento de dados advindos da União Europeia.

A nova legislação estabelece uma série de direitos para os titulares de dados pessoais e de deveres para os atores privados que dão tratamento a esses dados. Segundo ela, quando fundado no consentimento, o ato de consentir deve corresponder a uma manifestação de vontade induvidosa, livre, específica, informada e explícita, pela qual o titular aceita, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento. O titular tem o direito de retirar o seu consentimento a qualquer momento, com a

mesma facilidade com que o tenha consentido – as recomendações da AIDP vão exatamente nesse sentido, aliás[286].

Do ponto de vista das atividade de investigação, as autoridades de controle europeias passam a ter amplos poderes sobre os agentes de tratamento de dados pessoais, incluindo as prerrogativas de requisitar informações, obter acesso às suas instalações e ordenar a adoção de medidas para o cumprimento dos deveres e obrigações previstos no GDPR.

Do ponto de vista sancionador, também passam a poder impor limitação temporária ou definitiva e até a proibição do tratamento de dados, bem como aplicar multas em valores que podem chegar a 20 milhões de euros ou, no caso de empresas, a 4% do seu faturamento anual em nível mundial — o que for maior.

A legislação é, portanto, bastante dura com os coletores, armazenadores e processadores de dados pessoais.

Para além da garantia de processamento justo dos dados, das adoções da privacidade por design e por padrão, há também outros direitos relevantes previstos no GDPR, assegurados ao titular dos dados pessoais independentemente de o tratamento ser realizado com base no seu consentimento ou sob outra circunstância prevista na norma. Entre eles, pode-se citar (i) o direito de acesso, pelo qual o titular pode pleitear e obter do agente a confirmação de que os seus dados pessoais são ou não objeto de tratamento e, em caso positivo, pode acessar esses dados e receber informações como as categorias de dados pessoais tratados, as finalidades do tratamento, os terceiros para os quais foram ou serão divulgados e a existência de decisões automatizadas, incluindo para a criação de perfis; (ii) o direito de retificação, pelo qual o titular pode pleitear e obter do agente de tratamento, sem demora injustificada, a correção dos dados pessoais inexatos que lhe digam respeito; (iii) o direito de desindexação, pelo qual o titular pode pleitear e obter do agente o apagamento dos seus dados pessoais quando deixarem de ser necessários para a finalidade que motivou sua coleta ou tratamento, bem como (sendo o caso) se o titular retirar o seu consentimento, entre outras circunstâncias; (iv) o direito de restrição do tratamento, que pode ocorrer, por exemplo, quando o tratamento for ilícito e o titular se opuser

---

286 "Consumer protection, informed consent, purpose limitation, right to erasure, correction and notification, shall be paramount values in guiding the formulation of laws and regulations on data collection, selling and buying on the Internet, financial transactions and investments, and marketing and promotional campaigns." Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

à desindexação dos seus dados pessoais, solicitando ao agente, em vez disso, a limitação da sua utilização – direito este até então não previsto na legislação da União Europeia; e (v) o direito de portabilidade dos dados, pelo qual o titular pode pleitear e receber do agente de tratamento os dados pessoais que lhe tenha fornecido, em formato estruturado, de uso corrente e de leitura automática, bem como transmiti-los livremente a outro agente.

Além do dever de observância dos direitos assegurados aos titulares de dados pessoais, a nova legislação impõe aos agentes de tratamento diferentes obrigações, tais como (i) a manutenção de registro de todas as atividades de tratamento sob a sua responsabilidade, com informações como o nome e os contatos do agente de tratamento, as finalidades do tratamento, as categorias de destinatários a quem os dados pessoais foram ou serão divulgados etc.; (ii) a adoção de medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco decorrente da atividade de tratamento; e (iii) a notificação da autoridade de controle competente ou dos próprios titulares em caso de violação de dados pessoais, a depender da gravidade do risco resultante do evento.

Como um todo, o Regulamento deve servir de exemplo para países que ainda não adotaram uma Lei Geral de Proteção de dados, como é o caso do Brasil e até para aqueles que já têm uma legislação do tipo em vigor. De fato, o *enforcement* de uma norma do tipo pode contribuir para a segurança dos dados, diminuindo a precariedade no armazenamento e os abusos no processamento.

No passo que estamos hoje no Brasil, por exemplo, o processamento, coleção e compartilhamento de dados por indivíduos e organizações, apesar da garantia de proteção da privacidade e da proteção dos dados pessoais, de acordo com o Marco Civil da Internet[287], é um campo aberto e desregulado, dando todo tipo de acesso à violações por parte de agentes privados. Diante da necessidade de regulação, passamos a discuti-la.

### 3.4 Uma Lei Geral de Dados para o Brasil

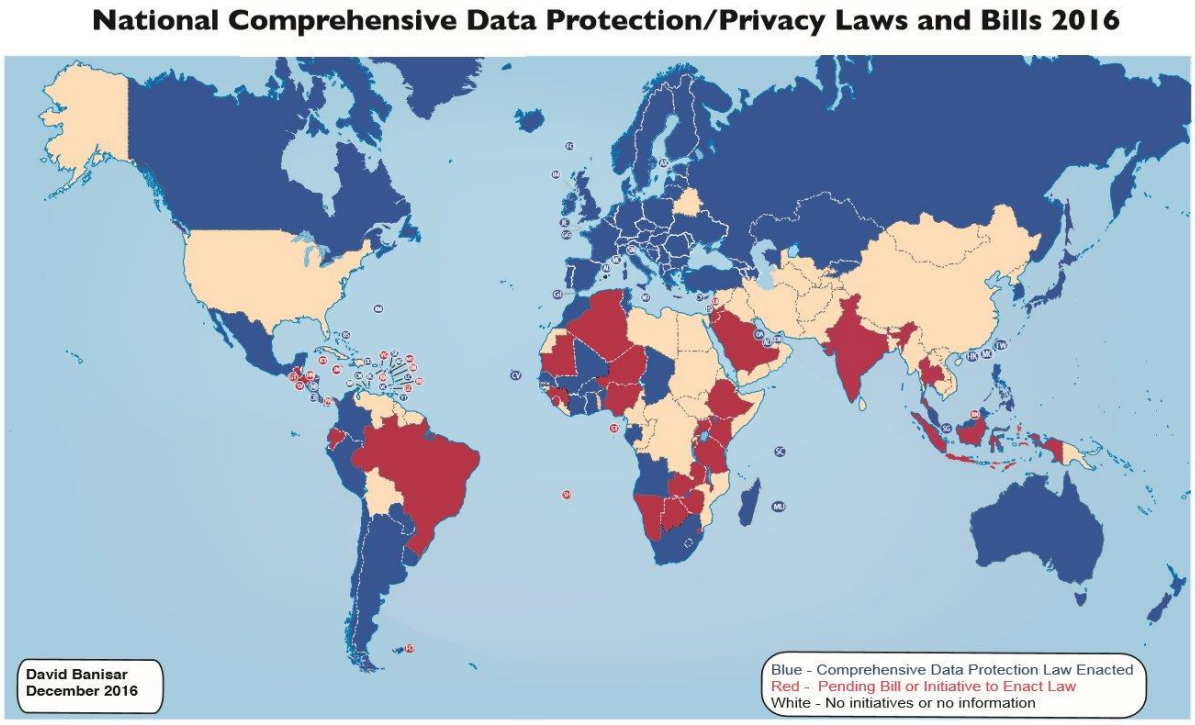
Novas descobertas e aplicações da tecnologia desgastam a intimidade todos os dias. O Brasil, contudo, está, a cada dia mais, atrasado no estabelecimento de um *standard* que regule

[287] Brasil. Lei nº 12.965/2014. Art. 3º, II e III.

a coleta, o armazenamento, o compartilhamento, a indexação, a mixagem e a fraude dos dados pessoais. Urge que o legislador pátrio adote rapidamente uma normativa geral de dados.

Há, nesse sentido, pelo menos três projetos de lei em tramitação no Congresso nacional, o PL/Esx 5276/2016, o PL/Sen nº330/2014 e o PL/Cam nº 4060/2012, que propõem uma Lei Geral de Dados.

O nosso país é, aliás, um dos poucos países que não tem em vigor uma Lei do tipo, conforme demonstra a figura a seguir:




Dos três projetos em tramitação, pode-se apontar como mais adequados o PLS nº 330/2014, que é na verdade um substitutivo do Senador Relator Aluysio Nunes Ferreira, e o PL/Exe nº 5276/2014. Nenhum deles conta com sanções penais diretas para a coletores, armazenadores e processadores de dados.

No primeiro caso, há a interessante definição e diferenciação ente dados pessoais e pessoais sensíveis, além da correta definição de figuras e autorizações em relação a estes dados. Reforça ainda a inviolabilidade da intimidade e da vida privada. O PL prevê os princípios que devem reger o tratamento dos dados, os direitos dos titulares desses dados, - como o importante consentimento expresso para a coleta e o conhecimento da lógica de tratamento

automatizado dos seus dados[288], dá tratamento para as tutelas específicas dos dados e as figuras de responsabilidade e impõe regras para transferências internacionais de dados. As sanções previstas são eminentemente administrativas.

No segundo caso, o PL/Exe nº5276/2014, há uma aproximação maior da nova normativa europeia, inclusive com definições semelhantes em relação aos agentes e objetos dos processos de tratamentos de dados, um verdadeiro *checklist* para o tratamento dos dados pessoais[289] e disposições mais objetivas quanto aos direitos do titular dos dados[290]. Há a previsão de sanções no caso de infração por agentes públicos, nos termos da Lei nº 8.112/ 1990 e Lei nº 8.429/1992. Por fim, o projeto logra trazer a lume a figura do Conselho Nacional de Proteção de Dados e da Privacidade, que ficaria responsável pela implementação e fiscalização da Lei. O PL defende a privacidade das pessoas tanto em relação ao poder público, cuja atuação pode violar garantias individuais, quanto contra as práticas de atores privados que queiram lucrar com os dados dos usuários brasileiros. Impede, por exemplo, que empresas coletem, comprem ou vendam dados dos cidadãos sem seu consentimento livre e informado. Trata-se da melhor iniciativa em tramitação.

Entendemos que ambos os Projetos de Lei ainda merecem alguns ajustes. O que importa salientar nesse item, contudo, é a urgência de uma legislação que estabeleça princípios e critérios para a coleta e o processamento dos dados, de modo a evitar que sejam utilizados indiscriminadamente para fins comerciais, contra a vontade dos indivíduos e rompendo diuturnamente barreiras éticas.

Em nossa opinião, uma Lei Geral de Dados deve prever como princípios o livre acesso do titular aos seus dados e as normas de segurança que criaram o produto ou aplicação (*privacy by design* e *by default*), a finalidade expressa de uso dos dados, as vias de transparência, a justificativa de necessidade da coleta, a qualidade de coleta e dos dados coletados, a segurança do armazenamento e do processamento e a não discriminação.

É preciso, também, assegurar direitos básicos ao titular dos dados, como o acesso a qualquer tempo, a retificação de informações, o cancelamento, apagamento e desindexação a qualquer tempo, o bloqueio de usos, a dissociação e não adesão, por último, a possibilidade de oposição a políticas e termos de uso da aplicação, produto ou serviço – o "dizer não", por

---

[288] Senado Federal. PLS nº330/2014. Art. 6º, IV e VI.
[289] Ministério da Justiça. PL/Exe nº5276/2014. Art. 7º e seguintes.
[290] Idem, art. 17 e ss.

exemplo, a uma política do Facebook, sem ser completamente excluído da rede social por conta disso.

Ainda, concordamos com a necessidade e criação de uma Autoridade de Dados e o formato de um conselho nacional, com a participação de agentes do governo, agentes de notório saber e da sociedade civil organizada parece o formato mais acertado – a via de composição do CGI.br pode servir de importante modelo, contanto que, no caso de uma nova Autoridade tão ligada a um direito fundamental, seja dado maior peso à participação de membros de notório saber.

É conveniente, ainda, abordar as possíveis sanções: uma Lei do tipo precisa levar em consideração que a intimidade é bem jurídico suficiente para a criação de tipos, como se estudará adiante.

Não se quer, por óbvio, impor penalizações desnecessárias, e, na linha com o recomendado pela AIDP, é auspicioso que se privilegie a imposição de sanções alternativas[291], mas reafirmamos nossa posição de que o reconhecimento da intimidade enquanto bem jurídico que vem sendo fragilizado diante de novas condutas na internet é supedâneo suficiente para a imposição de tipos próprios.

Ainda, a figura de um agente responsável – e penalizado por eventual omissão – parece razoável. A criação de um *Data Protection Compliance Officer* para organizações que processem dados não é desarrazoada. A divisão de riscos e fiscalização entre o poder público e os agentes privados será o caminho mais recomendado para que a gestão dos dados não se torne um problema nos próximos anos e o direito penal não pode negar o seu papel nessa dinâmica. É o que trataremos no próximo item.

### 3.5 Aspectos penais de uma Lei Geral de Dados no Brasil

A aprovação de um diploma Geral de Dados toca muito mais nas regulações para corporações do que para agentes privados. Nessa medida, a gestão de riscos precisa chegar aos detentores de dados pessoais alheios no Brasil, inclusive nas responsabilização dos agentes. No

1. [291] "In addressing the threat and reality of cybercrime and the necessity of cyber security, the legal and criminal justice system should balance individual, collective, private sector and public interests. Over reliance on criminal law protection should be avoided in favour of robust prevention, active defence, public education and awareness, and alternative sanctions." Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

cenário de riscos que aflora, exsurge, com notória importância, a figura de um agente responsável pela gestão desses dados.

Tal figura poderá ser o agente garante por eventuais condutas lesivas de organizações, nos termos do artigo 13, § 2, do Código Penal. Cometerá, em casos de violação de direitos dos titulares de dados pessoais, a omissão penalmente relevante desde que arrogará a responsabilidade pela manutenção dos preceitos éticos e do estado da arte das boas práticas informáticas gerindo os dados sob sua tutela. Tomará, portanto, o dever de cuidado, proteção e vigilância, assumirá a responsabilidade de impedir o resultado lesivo. Um executivo encarregado desse papel, que, em função de contrato, ou mesmo por situação de fato no âmbito da corporação, coloca-se, efetivamente, na posição de garantidor da não ocorrência dos resultados lesivos[292], a exemplo do que alude a Lei anticorrupção.

Posto que em muitas organizações já há inclusive um agente desse tipo para as práticas de integridade, notadamente em aspectos financeiros – muito em virtude da tendencia inaugurada justamente pela Lei anticorrupção nos últimos anos -, a missão desse profissional de integridade pode ser complementada para um espectro mais amplo, passando a, além de contemplar a proteção da Administração Pública contra a própria companhia, não apenas em face de ações institucionais, mas também diante de ações individuais impróprias que advenham dos integrantes dela ou em seu benefício, tomar a exata mesma postura com relação à gestão dos dados pessoais.

Aproveita-se, com isso, a função que passou a gerir o risco nos últimos anos para agregar a ela a gestão do risco computacional, pela assunção efetiva dos deveres de cuidado também nesse campo. O *Compliance Officer,* que já tem o dever de tudo fazer ao seu alcance para impedir a prática daquelas condutas associadas à corrupção, à subvenção da prática de atos ilícitos, às fraudes nos procedimentos licitatórios, e outras correlatas, especialmente por meio da implementação de um programa de integridadce efetivo, poderá somar às suas atribuições o combate aos abusos ou desvios relacionados aos dados, também com a implementação de um

[292] Segundo Manuel Gómez Tomillo, quando a lei exige que a pessoa encarregada desse papel aja no nome ou por meio da pessoa jurídica, requer-se que o sujeito atue ou omita-se, em requisito alternativo, mas desde que em seu âmbito de responsabilidades. TOMILLO, Manuel Gómez, *Introducción a la responsabilidad penal de las personas jurídicas en el sistema español*. Valladolid: Lex Nova, 2011. P. 83.

programa de diretrizes de tratamento dos dados e o estabelecimento de marcos éticos para o uso dos dados. Ao se omitir, poderá ser igualmente envolvido no cenário das apurações para avaliar-se a relevância de sua omissão diante das eventuais violações à privacidade e à intimidade de outros agentes por parte da organização que tutela.

Trata-se de uma proposição simples e não utilitarista para fazer cumprir uma eventual Lei Geral de Dados. Outros caminhos podem também ser aventados, como a criação de tipos específicos para tutelar a intimidade, em especial em relação aos dados colocados em computadores, notadamente no tratamento de condutas de particulares. No caso das pessoas jurídicas, todavia, a solução pela integridade parece caminho menos traumático e com ambientação conhecida, pela adoção da figura dos *Compliance Officers* nos últimos anos, para as organizações.

### 3.6 Uma autoridade de Proteção de Dados

Como visto no tópico 3.4, o PL/Exe nº5276/2014 prevê a figura do Conselho Nacional de Proteção de Dados e da Privacidade, o embrião de uma Autoridade de Dados para o país.

Autoridades desse tipo já existem em diversos países e na União Europeia[293] e são responsáveis pelo controle do tratamento dos dados, a fim de assegurar o cumprimento das regras de respito à privacidade e à intimidade; pelo aconselhamento de instituições e organismos no tratamento dos dados; pela condução de investigações para apurar desvios em relação à privacidade e à intimidade; pelas cooperações internacionais nesse campo; e no monitoramento das evoluções tecnológicas que possam, de aguma maneira, fragilizar a privacidade, a vida privada e a intimidade.

Na União Europeia, a Autoridade Europeia de Dados já é tradicional e nomeada para um mandato de cinco anos renovável por outros cinco. O texto do GDPR inclusive consagrou a adoção de autoridades com essa função naquele continente e a AIDP incluiu em

[293] UNIÕA EUROPEIA. Autoridade Europeia para a Proteção de Dados (AEPD). Disponível em: <https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_pt>. Acesso em 09.09.2017.

suas recomendações quanto ao tema justamente o controle de dados sensíveis por uma autoridade independente[294]

Entendemos que o estabelecimento de uma autarquia ou conselho com poderes para regular a coleta, armazenamento e processamento de dados no Brasil, além dos aspectos éticos e a aplicação de sanções administrativas específicas, representaria um avanço importante na medida em que estabeleceria um canal de comunicação entre a sociedade e o poder público nesse novo campo de estudos, a exemplo do que aconteceu em outras áreas do direito nas últimas décadas.

[294] "Adequate technical means should be used to control the access to data for the purpose of building information positions. An independent authority should control the access to sensitive data." Resolutions of the Congress of the International Association of Penal Law (1926-2014). International Association of Penal Law. Disponível em http://www.penal.org/sites/default/files/RIDP86%201-2%202015%20EN.pdf Acessado em 01.09.2017.

## 4. CONCLUSÃO

1) As novas fronteiras do uso da tecnologia têm afetado as relações humanas de maneira inédita na história. Há uma transformação social em curso, a história da comunicação da humanidade jamais se deparou com um ponto de mudança tão paradigmático quanto a popularização da internet de banda larga e o desenvolvimento das redes sociais. Os detentores dos algoritmos que controlam as aplicações que estão a coletar continuamente os dados dos usuários da internet detêm um poder inédito na história da humanidade: o controle das emoções de seus usuários. É preciso regulá-los.

2) A privacidade se expandiu, tornando-se uma nova expressão da liberdade e abarcando novos ramos do direito. Uma dessas evoluções está associada diretamente à tecnologia: a proteção ao sigilo de dados. Na internet, o dado pessoal é coletado continuamente para os mais diversos fins. O cuidado com a coleta, a tutela e o uso e os limites éticos aplicados nessas etapas são cruciais para que se evite a violação da privacidade e da intimidade dos usuários da rede.

3) Ficou evidente que o "estado atual da arte" na matéria de proteção às modernas formas de violação da privacidade e da intimidade na internet recomenda maior participação do indivíduo na tutela dos seus próprios dados. Nesse sentido, parece fundamental, inclusive diante das recomendações da AIDP, a obrigatoriedade da aplicação de técnicas de *privacy by design* e *privacy by default* . É preciso que empresas e organizações *saibam* dizer como estão gerindo os dados a elas confiados.

4) O consentimento na coleta, processamento e utilização de dados pessoais na internet é fato determinante para a própria colheita dessas informações. O usuário deve poder expressar consentimento livre, inequívoco, específico. É preciso que os detentores de tais coleções estabeleçam mecanismos de gestão dos dados que minimizem a extensão da coleta.

5) Para Roxin as normas apenas podem perseguir a finalidade de assegurar aos cidadãos uma coexistência livre e pacífica, garantindo respeito aos direitos humanos de todos. Segundo essa linha de pensamento, se essa tarefa não pode ser cumprida por outros instrumentos de controle social, o Estado deve garantir penalmente não apenas as condições individuais necessárias para coexistência (como a vida, a integridade física e o patrimônio) mas

também as instituições estatais que sejam imprescindíveis a tal fim[295]. No presente estudo, entendemos que a initimidade pode ser analogicamente aplicada a tal ensimanento, vez que é gundamental para a formação da personalidade e que vem sofrendo novas formas de fragilização.

6) Não é necessário o estabelecimento de um bem jurídico do sistema informático. A intimidade já é direito fundamental suficiente a embasar eventual tutela. Percebemos que a intimidade não é estática: ela evolui afetando e sendo afetada pela sociedade e, por isso, pode ensejar proteções até então inéditas.

7) Entendemos que o Marco Civil da Internet e o seu Decreto regulamentador não dão proteção suficiente para a intimidade, assim como não o fazem os diplomas penais a tratar do tema, notadamente o art. 154-A.

8) A gestão de riscos precisa chegar aos detentores de dados pessoais alheios no Brasil, inclusive nas responsabilização dos agentes. Nesse cenário de riscos que aflora, exsurge, com notória importância, a figura de um agente responsável pela gestão desses dados. Essas organizações, ao que propomos, deverão indicar um *Data Compliance Oficer* para gerir o acesso aos dados que foram a elas confiados. Esse agente terá o papel de garante.

9) Os conceitos de privacidade, intimidade e vida privada vêm sofrendo graves modificações diante dos avanços no uso de aplicações da rede. É também papel do direito penal acompanhar essa mudança para que, se alcançado o bem jurídico da intimidade, exerça o seu papel.

10) Entendemos que, com a geração de direitos relacionados à tecnologia e a emergência de um debate quanto ao tema das novas violações da intimidade, cabe o estabelecimento do direito a autodeterminação informativa no ordenamento pátrio, de maneira clara, expressa, ainda que não com o status de direito fundamental.

11) Adotamos a posição de que a penalização de algumas – novas – condutas, fruto das interações geradas na sociedade a partir do desenvolvimento da internet de acesso quase universal, tendo como base a fragilização da intimidade dos indivíduos é razoável e possível.

---

[295] BECHARA, Ana Elisa Liberatore Silva. O reconhecimento..., cit., p. 75.

12) As Leis atuais são insuficientes para tutelar, do ponto de vista penal, as diversas condutas que surgiram nos últimos anos a vulnerar a initmidade na internet. Urge a aprovação de diplomas mais modernos e específicos a coibir essas condutas.

13) O estabelecimento de tipos protetores da intimidade em debate adiantado e bem conectado com os preceitos mais modernos da dogmática pode evitar a consagração de diplomas penais precários, amparados em pressões de gestores atípicos da moral.

14) Ao tratar das novas ameaças à intimidade na rede, deve-se balancear os interesses dos diversos agentes. A Lei Penal é a medida extrema e, apesar de recomendarmos a confecção e aprovação de tipos específicos, eles devem conter penalizações moderadas. Medidas diversas, como as sanções alternativas devem ser privilegiadas.

15) As eventuais penalizações não devem, jamais, atigir a as liberdades de pensamento e de expressão. O direito penal, nesse caso, deve limitar-se a proteger direitos fundamentais, nunca o contrário.

16) O Regulamento Geral sobre Proteção de Dados pode ser apontado como a mais importante e moderna legislação de proteção de dados na atualidade e pode servir de modelo para uma eventual legislação no Brasil. Ele, contudo, não supera a necessidade do estabelecimento de diplomas penais para regular os delitos próprios.

17) O ato de invadir uma rede deve ser consiredo enquanto conduta delitiva, mas há condutas ainda mais específicas que necessitam igual normatização.

18) Uma Lei Geral de Dados deve prever como princípios o livre acesso do titular aos seus dados e as normas de segurança que criaram o produto ou aplicação (*privacy by design* e *by default*), a finalidade expressa de uso dos dados, as vias de transparência, a justificativa de necessidade da coleta, a qualidade de coleta e dos dados coletados, a segurança do armazenamento e do processamento e a não discriminação.

19) Entendemos que o estabelecimento de uma autarquia, conselho ou autoridade com poderes para regular a coleta, armazenamento e processamento de dados no Brasil, além dos aspectos éticos e eventuais sanções administrativas, representaria um avanço importante na medida em que estabeleceria um canal de comunicação entre a população e o poder público nesse novo campo de estudos.

20) O direito penal tem papel fundamental na prevenção às violações a privacidade e à intimidade na rede, na medida em que precisa tomar definitiva posição na

criminalização específica e bem dosadas de novas condutas que fragilizam o direito fundamental insculpido no artigo 5º, inciso X da nossa Constituição Federal.

**BIBLIOGRAFIA**

ALCOTT, H.; GENTZKOW, M. Social Media and Fake News in the 2016. *Journal of Economic Perspectives,* vol. 31, n. 2, primavera 2017. Disponível em https://web.stanford.edu/~gentzkow/research/fakenews.pdf. Acesso em: 05/08/2017.

ANDERSON, D. L.; SHAPIRO, L. *Introduction to chain codes.* The mind Project – Consortium on cognitive Science Instruction. Disponível em http://www.mind.ilstu.edu/curriculum/chain_codes_intro/chain_codes_intro.php. Acessado em 20.08.2016.

ARAÚJO, Ana Cristina. The Lisbon Earthquake of 1755 – Public Distress and Political Propaganda. *E-JPH,* Brown University, vol. 4, n.1, verão 2006. Disponível em https://www.brown.edu/Departments/Portuguese_Brazilian_Studies/ejph/html/issue7/html/araaujo_main.html. Acessado em 20.07.2017.

ASIA-PACIFIC ECONOMIC COOPERATION. *APEC Privacy Framework*. Singapore: APEC Secretariat, 2005.

BAKAR, N. [et al.]. *ALS and artificial inteligence:* IBM Watson suggests novel RNA binding proteins altered ALS. Disponível em https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=HLW03040USEN Acessado em 23.09.2017.

BARBOSA, T. C. B. M. (coord.). *A revolução das moedas digitais:* aspectos jurídicos, sociológicos, econômicos e da ciência da computação. Cotia: Editora Revoar, 2016.

BAUMAN, Z. *Liquid Modernity*. Cambridge: Cambridge Polity Press, 2000.

BECHARA, Ana Elisa Liberatore Silva. *Bem jurídico-penal*. São Paulo: Quartier Latin, 2014.

BELOQUE, Juliana Garcia. *Sigilo Bancário* – Análise Crítica da LC 105/2001. São Paulo: Revista dos Tribunais, 2003.

BESSI, A.; FERRARA, E. Social bots distort the 2.016 U.S. Presidential election discussion. *First Monday*, vol. 21, n.11. Disponível em http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653a#p4 Acessado em 08.08.2017.

BIONI, Bruno Ricardo. *Autodeterminação informacional:* paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

BOBBIO, Norberto. *El tiempo de los derechos*. Madrid: Editorial Sistema, 1991.

BOEHM, Franziska, *A comparison between US and EU data protection legislation for law enforcement purposes.* Directorate general for internal Policies, European Parliament: Bruxelas, 2015.

BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 12, n. 47, mar./abr. 2004.

BOND, R. [et al.]. *A 61-million-person experiment in social influence and political mobilization. Nature Magazine,* Nova York, n. 489, p. 295–298, 2012.

BOTTINI, Pierpaolo C. *Crimes de perigo abstrato e princípio da precaução na sociedade de risco*. São Paulo: Revista dos Tribunais, 2007

BOYD, D. M.; Ellison, N. B. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication,* n. 13, p. 210–230, 2007.

BROWNSWORD, Roger. Consent in data protection law: Privacy, Fair Processing and Confidentiality. In: In: DE HERT, Paul [et. al]. *Reinventing data protection?* Bruxelas: Springer, 2014.

CALISKAN-ISLAM, A. BRYSON, J.J, NARAYAAN, A. *Semantics derived automatically from language corpora necessarily contain human biases.* Princeton University. Disponível em: http://randomwalker.info/publications/language-bias.pdf. Acesso em 06/09/2017.

CALLEGARI, André Luís. Imputação objetiva: lavagem de dinheiro e outros temas de direito penal. *Boletim IBCCRIM*, São Paulo, n. 78, v. 7, 1999.

CASTELLS, Manuel. *Communication Power*. New York: Oxford University Press, 2013.

CASTELLS, Manuel. *Internet Galaxy*: reflections on the internet, business and society. Oxford: Oxford University Press, 2001.

CASTELLUCCIA, Claude. Behavioural Tracking on the internet: a technical perspective. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014.

CASTRO, Catarina Sarmento. *Direito da informática, privacidade e dados pessoais.* Coimbra: Edições Almedina, 2005.

CAVOUKIAN, A. *Privacy by design...take the challenge.* Washington: Privacy and Information Comission, 1997.

CHAN, Melanie. *Virtual reality:* representations in Contemporary Media. London: Bloombury Academic, 2014.

CHESTER, J. Cookie Wars: How new profiling and Targeting techniques threaten citizens and consumers in the "Big Data" era. In: GUTWIRTH, Serge, LEENES, Ronald, De HERT, Paul. *European data protection*: in good health? Bruxelas: Springer, 2012.

COLLANTES, Tàlia González. Los delitos contra la intimidad tras la reforma de 2015: luces y sombras. *Revista de derecho penal y criminología*, Madrid, 3a. época, n. 13, p. 51-83., jan./jun. 2015.

COLLI, Maciel. A problemática detrás da responsabilização penal (objetiva) pela prática de um cibercrime. In: FAYET JÚNIOR, Ney; MAYA, André Machado (Org.). *Ciências penais*: perspectivas e tendências da contemporaneidade. Curitiba: Juruá, 2011.

COLLI, Maciel. Cibercrimes: da teoria cibernética aos crimes cometidos através da rede mundial de computadores. In: MAYA, André Machado (Org.); FAYET JÚNIOR, Ney. *Ciências penais e sociedade complexa II*. Porto Alegre: Nuria Fabris, 2009.

COSTA JÚNIOR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. 4.ed. rev. e atual. São Paulo: Revista dos Tribunais, 2007.

COSTA, Sara. A proteção de dados pessoais na internet. *Revista juridica*, Maputo, v. 6, set. 2004.

COUNCIL OF EUROPE. *Treaty 185*. Budapest 23.11.2001.

DALLARI, Dalmo de Abreu. *El Hábeas Data en Brasil*. Talca: Ius et Praxis, 1997.

DE HERT, Paul [et al.]. *Reinventing data protection?* Bruxelas: Springer, 2014.

DE HERT, Paul [et. al]. *Reinventing data protection?* Bruxelas: Springer, 2014.

DE HERT, Paul; GUTWIRTH, Serge. *Privacy and criminal law* – privacy, data protection and law enforcement: opacity of the individual and transparency of power. Oxford: Intersentia, 2006.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto [coord.] *Direito & Internet – aspectos jurídicos relevantes*. 2 ed. v. 1. São Paulo: Quartier Latin, 2005.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto [coord.] *Direito & Internet – aspectos jurídicos relevantes*. 2 ed. v. 2. São Paulo: Quartier Latin, 2005.

DEL CANTO, Enrique Roviera. *Delincuencia informática y fraudes informáticos.* Granada: Comares, 2002.

DEL GIUDICE, M. From informational Society to Network Society: the challenge. In: DEL GIUDICE, M.; PERUTA, M.R.D.; CARAYANNIS, E.G. *Social Media and Emerging Economies*: technological, cultural and economic emplications. Springer: Nova York, 2014.

DE LA CUESTA ARZAMENDI, José Luis. Sociedad de la información y derecho penal: a la luz del XIX *congreso internacional de derecho penal*. Revista Brasileira de Ciências Criminais, São Paulo, v. 23, n. 112, p. 79-106., jan./fev. 2015.

DESIMONE, Christian. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, v, 11, n, 3. 2003.

DION, Michel. *Financial crimes and existential philosophy*. Londres: Springer, 2014.

DONEDA, Danilo, MENDES, Laura S. Data protection in Brazil: new developments and current challenges. In: GUTWIRTH, Serge, LEENES, Ronald, De HERT, Paul. *Reloading data protection:* multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014

EUROPEAN COMISSION *Charter of Fundamental Rights*. Bruxelas: Secretaria do Comissariado, 2009. Disponível em: <http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm>. Acesso em 20.04.2016

FAIDEN, Ruth; BEUCHAMPS, Thomas Beauchamps. *A History and Theory of Informed Consent*. Oxford: Oxford University Press, 1986.

FERRARA, E. [et. al]. The rise of social bots. *Communications of the ACM*, vol. 59, n. 7, 2016. Disponível em https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext Acessado em 14.08.2017

FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, vol. 88, 1993.

FERREIRA, Ivette Senise. A intimidade e o direito penal. *Revista Brasileira de Ciências Criminais*, São Paulo, vol. 2, n. 5, p.96-106, jan./mar. 1994.

GARIBALDI, Gustavo E. L. *Las modernas tecnologías de control y de investigación del delito:*

su incidencia en el derecho penal y los principios constitucionales. Buenos Aires: Ad-Hoc, 2010.

GOMES, Mariângela G. M. Periculosidade no Direito Penal contemporâneo. In: MENDES, Gilmar Ferreira; BOTTINI, Pierpaolo Cruz; PACELLI, Eugênio. (Org.). *Direito Penal Contemporâneo*: Questões Controvertidas. Vol. 1. São Paulo: Saraiva, 2011.

GRECO FILHO, Vicente. *Interceptação Telefônica:* Considerações sobre a Lei nº 9.296 de 24 de julho de 1996. São Paulo: Saraiva, 1996.

GUSTIN, Miracy Barbosa de Sousa; FONSECA DIAS, Maria Tereza. *(Re)pensando a pesquisa jurídica:* teoria e prática. 2 ed. Belo Horizonte: Del Rey, 2006.

GUTIÉRREZ BOADA, John Daniel. *Los límites entre la intimidad y la información.* Bogotá: Universidad Externado de Colombia, 2001.

GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul. *Reloading data protection:* multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014.

HUSTINX, P., *Privacy by design: delivring the promises.* Artigo digital: Springer, 2010. Disponível em: http://link.springer.com/article/10.1007/s12394-010-0061-z Acesso em 14.07.2016

JUTH, N.; LORENTZON, F. The concept of free will and forensic psychiatry. *International journal of law and psychiatry*, Quebéc, vol.33, n.1, 2013.

KEYNES, Edward. *Liberty, property and privacy*. Harrisburg: Pennsylvania State University Press, 1996.

KOTSIANTIS, S. B.; KANELLOPOULOS, D; PINTELAS, P. E. Data preprocessing for supervised leaning. *International Journal of Computer Science* vol. 1, no. 2, 2006.

KRAMER, A.; GUILLORY, J.; HANCOCK, J. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS Review*, Vol. 111, n. 24. Jun. 2014. Disponível em http://www.pnas.org/content/111/24/8788.full.pdf

KRAMER, A.; GUILLORY, J.; HANCOCK, J. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS Review*, vol. 111, n. 24., jun. 2014. Disponível em: <http://www.pnas.org/content/111/24/8788.full.pdf>. Acesso em: 06/09/2017.

LEAL, Luziane de F. S. *Crimes contra os direitos da personalidade na Internet*: violações e reparações de direitos fundamentais nas redes sociais. Curitiba: Juruá, 2015.

LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança computacional*. Campinas: Millennium, 2007.

LIMBERGER, Têmis. A informática e a proteção à intimidade. *Revista do Ministério Público do Rio Grande do Sul*, Porto Alegre, n. 43, jul./out. 2000.

LISZT, F.V. *Tratado de direito penal alemão*. Trad. José Higino Pereira. Campinas: Russel, 2003.

LYON, David. *The electronic eye*. Mineapolis: University of Minnesota Press, 1994.

LÓPEZ ORTEGA, J. J. *Intimidad informática y Derecho Penal (La protección penal de la intimidad frente a las nuevas tecnologías de la información y comunicación)*. In: Derecho a la intimidad y nuevas tecnologías. Centro de Documentación Judicial del Consejo General del Poder Judicial. Cuadernos de Derecho Judicial IX. Madrid, 2004, pp. 110-111.

MAJKIC, Zoran, *Big data integration theory* - Theory and methods of database mappings, programming languages, and semantics. Tallahasee, FL, EUA: 2014.

MARBLESTONE, A. H.; WAYNE, G.; KORDING, K.P. Toward an integration of deep learning and neuroscience. *Frontiers in Computacional Neuroscience*. Revista eletrônica. 14.09.2016. Disponível em https://www.frontiersin.org/articles/10.3389/fncom.2016.00094/full#h9. Acessado em 22.09.2017

MARÍN, Fernando Rodríguez. Los delitos de escuchas ilegales y el derecho a la intimidad. *Anuaria de Derecho Penal y Ciências Penales*, Madrid, t. XLIII, jan-abr., 1990, p. 207.

MATA BARRANCO, Norberto J. de la. Armonización europea y previsión de responsabilidad de las personas jurídicas en el Código penal español. *Revista Penal*, Valencia, n. 33, p.32-65, jan. 2014.

MATA BARRANCO, Norberto J. de la. La privacidad en el diseño y el diseño de la provicidad, también desde el derecho penal. *Cuaderno del Instituto Vasco de Criminología,* San Sebastian, n. 28, pp. 253-274, 2014.

MATA BARRANCO, Norberto J. de la; BARINAS UBIÑAS, Desirée. La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redeginir el objeto de tutela? *Revista de Derecho Penal y Criminología*, Madrid, 3ª Época, n. 11, p.13-92, jan./jun. 2014.

MATA Y MARTIN, Ricardo Manuel. La protección penal de datos como tutela de la intimidad de las personas: intimidad y nuevas tecnologías. *Revista Penal***,** Valencia, n. 18, p. 217-235, jul. 2006.

McMAHAN, H. B [et al.]. *Communication-efficient learning of deep networks from decentralized data. W&CP*, Fort Lauderdale, vol. 54, 2017.

MIR PUIG, Santiago. Bien jurídico y bien jurídico-penal como límites del Ius puniendi. *Estudios penales y criminológicos***,** Santiago de Compostela, n. 14, 1991.

MIRÓ LLINARES, Fernando. *El cibercrimen:* fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons, 2012.

MOLES PLAZA, R., *Derecho y Control en Internet.* Barcelona: Ariel, 2003.

MONAHAN, J; SKEEM, J.. Risk Assessment in Criminal Sentencing . *Virginia Public Law and Legal Theory Research Paper*, n.53. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662082 Acessado em 12.09.2017.

NAKAMOTO, Satoshi. *Bitcoin: a peer-to-peer Eletronic Cash System.* Disponível em: https://bitcoin.org/bitcoin.pdf Acessado em 15.08.2017.

NARAYANAN, Arvind [et al.]. *Bitcoin and Cryptocurrency* Technologies. Draft, 2015.

ORWELL, George. *1984.* 29.ed. São Paulo: Cia Editora Nacional, 2005.

OULASVIRTA, A. [et al.] *Long-term Effects of Ubiquitous Surveillance in the Home.* UbiComp '12 : Proceedings of the 2012 ACM Conference on Ubiquitous Computing: Pittsburgh, EUA, 2012. p. 41-50 Disponível em https://people.mpi-inf.mpg.de/~oantti/pubs/ubicomp2012-oulasvirta.pdf. Acessado em 16.09.2017.

PAESANI, Liliana Minardi. *Direito e internet:* liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2013.

PALAZZI, Pablo A. *Los delitos informáticos en el código penal*: analisis de la ley 26.388. Buenos Aires: Abeledo Perrot, 2009.

PÉRES LUÑO, António-Enrique. El derecho a la intimidad en el Âmbito de la Biomedicina. In: LA CUESTA, Antonio Ruiz de (coord.). *Bioética y derechos humanos*: implicaciones sociales y jurídicas. Sevilha: Universidade de Sevilha, 2005.

POULLET, Yves; ROUVROY, Antoinette. The right to informational self-determination and the value of self-development: Resseassing the importance of privacy to democracy. In: DE

HERT, Paul [et al.]. *Reinventing data protection?* Bruxelas: Springer, 2014.

REALE JÚNIOR, Miguel. *Instituições de direito penal.* 2.ed. Rio de Janeiro: Forense, 2006.

REALE JÚNIOR, Miguel (org.), *Código penal comentado.* São Paulo: Saraiva, 2017.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade de hoje. Rio de Janeiro: Renovar, 2008.

RODRÍGUEZ, Víctor Gabriel de Oliveira. *Fundamentos de Direito Penal Brasileiro:* Lei penal e Teoria Geral do Crime. São Paulo: Atlas, 2008.

RODRÍGUEZ, Víctor Gabriel de Oliveira. *Livre arbítrio e direito penal e direito penal*: revisão frente aos aportes da neurociência e à evolução dogmática. 321p. Tese (Livre-docência em Direito Penal) – Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2015.

RODRÍGUEZ, Víctor Gabriel de Oliveira. *O Ensaio como Tese*: estética e narrativa na composição do texto científico. 1. ed. São Paulo: Martins Fontes WMF, 2012.

RODRÍGUEZ, Víctor Gabriel de Oliveira. *Tutela da Penal da Intimidade*: perspectivas da atuação penal na sociedade da informação. São Paulo: Atlas, 2008.

ROOSENDAAL, A. We are all connected to Facebook… by Facebook! In: DE HERT, Paul [et al.]. *Reinventing data protection?* Bruxelas: Springer, 2014.

ROXIN, Claus. Las formas de intervención en el delito: estado de la cuestión. In: ROXIN, Claus et al. Sobre el estado de la teoría del delito: Seminario en la Universitat Pompeu Fabra. Madrid: Civitas, 2000. p. 155-178.

ROXIN, Claus. A teoria da imputação objetiva. Trad. Luis Greco. *Revista Brasileira de Ciências Criminais,* São Paulo, vol. 38, 2002.

ROXIN, Claus. Finalismo: um balanço entre seus méritos e deficiências. *Revista Brasileira de Ciências Criminais - IBCCRIM*, São Paulo, vol. 65, 2007.

ROXIN, Claus. O conceito de bem jurídico como padrão crítico da norma penal posto à prova. *Revista Portuguesa de Ciência Criminal*, Coimbra, v. 23, n. 1, p.7-43, jan./mar. 2013.

SAAD-DINIZ, Eduardo. Fronteras del normativismo: a ejemplo de las funciones de la información en los programas de *criminal compliance*. *Revista da Faculdade de Direito da Universidade de São Paulo,* vol. 108, jan-dez 2013, São Paulo: USP, 2013.

SAN MARTÍN, Cristos Velasco. *La jurisdicción y competencia sobre delitos cometidos a*

*través de sistemas de computo e internet*. Valencia: Tirant lo Blanch, 2012.

SCARANCE FERNANDES, Antonio; ALMEIDA, José R. G.; MORAES, Maurício Z. *Sigilo no Processo Penal*: eficiência e garantismo São Paulo: Revista dos Tribunais, 2008.

SCHMIDT, Éric, COHEN, Jared. *A nova era digital* – reformulando o futuro das pessoas, das nações e da economia. Lisboa: Alfragide, 2013.

SCHWARTZ, Paul M. SOLOVE, Daniel J. *The PII Problem*: Privacy and a New Concept of Personally Idenifiable Information. Disponível em: http://scholarship.law.berkeley.edu/facpubs/1638 Acessado em 29.09.2017

SHAAR, P. Privacy by design. *Identity in the information Society*, vol.3, n.2, ago. 2010.

SHOKRI, R.; SHAMATIKOV, V. Privacy-preserving deep learning. *CCS'15*, 12–16 de outubro de 2015. Disponivel emhttp://www.shokri.org/files/Shokri-CCS2015.pdf Acessado em 03.09.2017.

SILVA SÁNCHEZ, Jesús María. *La expansión del derecho penal*: aspectos de la política criminal en las sociedades postindustriales. 2.ed. rev. Madrid: Civitas, 2001.

SILVA, Rita de Cássia Lopes da. *Direito Penal e sistema informático*. São Paulo: RT, 2003.

SILVEIRA, Renato de Mello Jorge. *Fundamentos da Adequação Social em direito penal.* São Paulo: Quartier Latin, 2010.

SILVEIRA, Renato de Mello Jorge. *Crimes sexuais*: bases críticas para a reforma do direito penal sexual. São Paulo: Quartier Latin, 2008.

SILVEIRA, Renato de Mello Jorge. *Direito penal supra-individual*: interesses difusos. São Paulo: Revista dos Tribunais, 2003.

SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. *Repatriação e crime*: aspectos do binômio crise econômica e direito penal. Belo Horizonte: Editora D'Plácido, 2017.

SILVEIRA, Renato de Mello Jorge. "A imprensa e a lei da mordaça". In: Boletim do IBCCrim, Setembro, 2000

SMART, Nigel Paul. *Cryptography*: an introduction. 3.ed. New York: McGraw-Hill, 2003.

SOLOVE, Daniel. J. *The digital person:* technology and privacy in the informaion age. New York University Press: New York, 2004.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. 2.ed. São Paulo: Saraiva, 2015.

SYDOW, Spencer Toth. O bem jurídico nos crimes informáticos. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 23, n. 113, p.193-212, mar./abr. 2015.

SZASZ, Thomas. *Psychiatric Justice*. Nova York: Macmillan, 1965.

TAPSCOOT, D.; TAPSCOOT, A. *Blockchain Revolution:* How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Nova York: Penguin, 2017.

TELLES, André. *A Revolução das mídias sociais*: cases, conceitos, dicas e ferramentas. São Paulo: M. Books do Brasil, 2011.

TERWANGNE, Cécile de. Is a Global Data Protection Regulatory Model Possible? In: DE HERT, Paul [et al.]. *Reinventing data protection?* Bruxelas: Springer, 2014. p. 181

TIEDEMANN, Klaus. Criminalidad mediante computadoras. In: TIEDEMANN, Klaus. *Poder económico y delito* - Introducción al Derecho Penal Económico y de la Empresa. Barcelona: Editorial Ariel S.A., 1985.

TOMILLO, Manuel Gómez, *Introducción a la responsabilidad penal de las personas jurídicas en el sistema español*. Valladolid: Lex Nova, 2011

TROTTIER, Daniel; FUCHS, Christian. Theorising social media, politics and the State: na introduction. In: TROTTIER, Daniel; FUCHS, Christian (ed.). *Social media, politics and the State:* protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and Youtube. Nova York: Routledge, 2015.

UICICH, Rodolfo Daniel. *El derecho a la intimidad en internet y en las comunicaciones electrónicas*. Buenos Aires: Ad-Hoc, 2009.

VACIAGO, Giusepppe. *Privacy v. Security? A dilemma of the digital era* Turim: Unicri, 2014.

VAN DIJK, J. *The network society*. Londres: SAGE, 2006.

VERDELHO, Pedro. A reforma penal portuguesa e o cibercrime. *Revista do Ministério Público de Lisboa*, Lisboa, v. 27, n. 108, pp. 97-124, out./dez. 2006.

VERVAELE, J.A.E. *La legislación antiterrorista en Estados Unidos*. Inter arma silente leges? Buenos Aires: Del Puerto, 2007.

VERVAELE, J.A.E. Survillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system? In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (ed.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014.

VERVAELE, J.A.E. Survillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system? In: GUTWIRTH, Serge, LEENES, Ronald, De HERT, Paul, *Reloading data protection*: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, 2014

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, vol. IV, nº5, 1890.

WEICHERT, T. *Cloud Computing and Data Privacy*. The Sedona Conference, 2011. Disponível em https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf Acessado em 18.09.2017.

WEISBURD, A., WATTS, C., BERGER, JM., *Trolling for Trump: how Russia is trying to destroy our democracy.* War on Rocks. Disponível em https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/ Acessado em 07.08.2017

ZAFFARONI, Eugenio Raul; OLIVEIRA, Edmundo. *Criminology and Criminal Policy Movements*. Lanham: University Press of America, 2013.

ZANIOLO, Pedro A. *Crimes modernos*: o impacto da tecnologia no direito. Curitiba: Juruá, 2007.