CONSENTIMENTO

BIG DATA

DADOS PESSOAIS

ANONIMATO

PRIVACIDADE
EM PERSPECTIVAS

DADOS GENÉTICOS

ESQUECIMENTO

CAMPANHAS ELEITORAIS

FILTROS BOLHA

MODELOS REGULATÓRIOS

Lumen Juris Editora

www.lumenjuris.com.br

Filiais

Sede: Rio de Janeiro
Rua Octávio de Faria, n° 81 – Sala
301 – CEP: 22795-415 – Recreio dos
Bandeirantes – Rio de Janeiro – RJ
Tel. (21) 3933-4004 / (21) 3249-2898

São Paulo (Distribuidor)
Rua Sousa Lima, 75 –
CEP: 01153-020
Barra Funda – São Paulo – SP
Telefax (11) 5908-0240

Minas Gerais (Divulgação)
Sergio Ricardo de Souza
sergio@lumenjuris.com.br
Belo Horizonte – MG
Tel. (31) 9-9296-1764

Santa Catarina (Divulgação)
Cristiano Alfama Mabilia
cristiano@lumenjuris.com.br
Florianópolis – SC
Tel. (48) 9-9981-9353

CONSENTIMENTO

BIG DATA

DADOS PESSOAIS

ANONIMATO

PRIVACIDADE
EM PERSPECTIVAS

Organizadores: Sérgio Branco e Chiara de Teffé

DADOS GENÉTICOS

ESQUECIMENTO

CAMPANHAS ELEITORAIS

FILTROS BOLHA

MODELOS REGULATÓRIOS

ITS Instituto de Tecnologia & Sociedade do Rio

Editora Lumen Juris
Rio de Janeiro
2018

Categoria: Direito Civil

Produção Editorial
Livraria e Editora Lumen Juris Ltda.

Diagramação: Rômulo Lentini
Capa: Thiago Dias

Livraria e Editora Lumen Juris Ltda.

Impresso no Brasil
Printed in Brazil

CIP-BRASIL. CATALOGAÇÃO-NA-FONTE

Privacidade em perspectivas / organizadores Sérgio Branco, Chiara de Teffé. – Rio de Janeiro : Lumen Juris, 2018.
256 p. : il., tabelas ; 23 cm.

ISBN 978-85-519-0542-5

1. Direito fundamental. 2. Direito individual. 3. Privacidade. I. Branco, Sérgio. II. Teffé, Chiara de. III. Título.

CDD 342.0858

Ficha catalográfica elaborada por Ellen Tuzi CRB-7: 6927

Apresentação

A privacidade pode ser analisada a partir de múltiplas perspectivas. Desde sua concepção mais tradicional – como o direito de ser deixado só –, até a contemporânea visão de que a privacidade diz respeito ao controle de dados pessoais, muita coisa mudou. O incremento definitivo para a discussão atual do tema foi o avanço tecnológico das últimas décadas, que teve como consequência a necessidade de se compreender a privacidade de modo interdisciplinar.

O debate, amplo e de interesse coletivo, extrapola o campo do Direito para atingir também as ciências sociais, a ética, a filosofia e a cultura popular. Quem acompanha a série *Black Mirror*, disponível no Brasil pela plataforma Netflix, sabe que a privacidade perpassa diversos episódios, mais notadamente aquele que encerra a primeira temporada, *The Entire History of You*. Não à toa, a análise da série é objeto do texto de Arthur Bezerra, que compõe esta coleção.

A propósito, diversos textos do livro tratam de assuntos urgentes. Em ano eleitoral, o impacto do *big data* e dos algoritmos nas eleições é o assunto fundamental do artigo de Andréia Santos. A privacidade de dados genéticos, que vem sendo discutida inclusive no Supremo Tribunal Federal, é abordada por Cláudio Barbosa. Daphnee Iglesias, por sua vez, trata do instigante e pouco debatido conceito de *nudge privacy*, que se relaciona com as teorias comportamentais e a influência na livre escolha dos indivíduos.

A regulação da privacidade na internet aparece na discussão sobre os conhecidos filtros bolha, proposta por Fernando Schincariol, na análise dos projetos de lei para regulação de dados pessoais no Brasil, conforme os modelos apresentados por Guilherme Guidi, e na proteção da privacidade pela própria tecnologia e pelo seu *design*, de acordo com o artigo de Jonas Valente.

Naturalmente, a ética é uma preocupação constante nesse cenário de incerteza causado pela contemporaneidade. Assim, Kátia Lima e Luiz Peres-Neto apresentam questões que relacionam a ética e a comunicação no mundo digital.

O direito ao esquecimento, outro assunto cujo debate vem se avolumando nos últimos anos, é tratado por Lívia Helayel. Boa parte da relevância do tema se deve a uma decisão proferida pela Corte Europeia em 2014 sobre um caso envolvendo o Google na Espanha. A respeito ainda do Google, seu modelo de negócio e do uso de *big data*, temos o artigo de Marcela Mattiuzzo.

Em meio à maioria de artigos que tratam da privacidade sob uma perspectiva privada, Márcio Ricardo Ferreira traz uma relevante abordagem criminal do uso de dados pessoais. Também partindo de uma perspectiva de direito público, Mariana Cunha e Melo trata da privacidade levando em conta aspectos processuais. Fechando a coletânea, temos o texto de Rodrigo Gomes sobre a fundamental questão do consentimento para uso de dados pessoais em um mundo marcado pela coleta de dados em prol do *big data*.

Todos esses trabalhos exemplares são fruto do primeiro grupo de pesquisa do Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS.

O ITS é um centro de pesquisa multidisciplinar totalmente independente, que trabalha em parceria com diversas instituições brasileiras e estrangeiras, na interseção do uso tecnológico e o interesse público. Suas atividades se dividem em quatro áreas principais: direitos e tecnologia; democracia e tecnologia; inovação e tecnologia; e educação. Você encontra mais informações sobre o ITS em seu site: itsrio.org.

Os grupos de pesquisa do ITS são projetos anuais cujos participantes são selecionados por meio de edital público. Podem participar pesquisadores de qualquer lugar do mundo, uma vez que os encontros são todos ao vivo, porém online, e são conduzidos em português. Após o primeiro ciclo do grupo de pesquisa, cujo resultado você encontra aqui, o segundo grupo de pesquisa do ITS teve como tema **cidades inteligentes** e outra publicação ocorrerá em breve com os novos trabalhos de conclusão.

Esperamos que, nos próximos anos, mais temas sejam acrescidos e que possamos promover um debate de alto nível sobre questões de interesse público relacionadas à tecnologia e aos desafios que ela nos impõe.

Finalmente, é importante lembrar que os textos aqui reunidos se encontram disponíveis na área de publicações do site do ITS e estão licenciados por meio da licença *Creative Commons* na modalidade **atribuição, uso não comercial, compartilhamento pela mesma licença** (CC-BY-NC-SA). Para saber mais sobre as licenças *Creative Commons* e suas permissões, visite o site do ITS.

Os organizadores

Sumário

O Impacto do Big Data e dos Algoritmos nas Campanhas Eleitorais

Andréia Santos[1]

Introdução

O presente artigo tem como finalidade demonstrar que as novas ferramentas tecnológicas têm grande valia para as agências de marketing político e podem ter forte impacto nas campanhas eleitorais: uma, porque o *big data* contribui para que as pesquisas de opinião sejam mais efetivas; duas, haja vista que os provedores influenciam na formação da opinião pública e podem propiciar a mudança no comportamento político dos eleitores por meio de seus algoritmos, sendo, pois, mais eficientes e direcionados que as mídias tradicionais de massa.

Edward Bernays, conhecido como o "pai das relações públicas", em seu artigo "*Engineering of Consent*"[2] (engenharia do consentimento – tradução literal), alerta que as novas ferramentas, ao mesmo tempo que podem contribuir para um fim social comum, podem ser utilizadas para fins não democráticos.

Quando do surgimento das mídias de massa tradicionais (rádio, televisão, jornal e revista), a ética foi um elemento que precisou ser desenvolvido e englobado ao segmento, haja vista a função essencialmente social dessas instituições – ou seja, viabilizar o acesso à informação. Como será visto nos próximos tópicos, é a partir dela (mídia) que o indivíduo tem a percepção de mundo.

As notícias elaboradas pelas mídias tradicionais passam por um processo de editoração antes delas serem enfim veiculadas. Inicia-se com a escolha de um fato, da elaboração do texto e da editoração deste, ou seja, averiguar linguagem, intenções e

1 Advogada, pós-graduada em Direito Digital e das Telecomunicações pela Universidade Presbiteriana Mackenzie e em Mídia, Política e Sociedade pela Fundação Escola de Sociologia e Política de São Paulo. Possui extensão em Direitos Autorais na Harvard Law School em parceria com a UERJ e ITS Rio e formação na Escola de Governança da Internet do CGI.br. Coordenadora do iStart – instituto voltado à Ética e Educação Digital.

2 BERNAYS, Edward L. **The engineering of consent**, 1947. Disponível em: <http://classes.dma.ucla.edu/Fall07/28/Engineering_of_consent.pdf> Acesso em: 21.01.17.

veracidade. E, por essa razão, códigos de ética e regulamentos específicos foram desenvolvidos para a imprensa, sendo ela responsável pelos conteúdos que veicula.

Como exemplo, pode-se citar a Declaração de Chapultepec[3], documento adotado pela Conferência Hemisférica sobre Liberdade de Expressão, realizada em Chapultepec, na cidade do México, em 11 de março de 1994. Apesar de não ser um tratado, os chefes de Estado de alguns países se comprometeram a cumprir suas disposições, dentre eles, os Estados Unidos e o Brasil[4].

Um dos princípios elencados nessa declaração diz que:

> IX – A credibilidade da imprensa está ligada ao compromisso com a verdade, a busca de precisão, imparcialidade e equidade e a clara diferenciação entre as mensagens jornalísticas e as comerciais. A conquista desses fins e a observância desses valores éticos e profissionais não devem ser impostos. São responsabilidades exclusivas dos jornalistas e dos meios de comunicação. Em uma sociedade livre, a opinião pública premia ou castiga.

Diante da então debatida parcialidade das mídias de massa e da própria característica desses meios em que a informação é lançada de forma unilateral, ou seja, a mensagem é veiculada de "um para todos", a descentralização permitida, *a priori*¸ pela Internet surge como uma alternativa para a sociedade.

Contudo, com o monopólio e a concentração da informação por parte das grandes empresas de Internet, como Google e Facebook, e de seus respectivos modelos de negócios criados, os quais têm sido pautados na veiculação de notícias, sobretudo no desenvolvimento de algoritmos que selecionam e personalizam o conteúdo para o usuário, torna-se relevante e necessário o debate sobre a função social dos provedores perante essa "transferência" de curadoria outrora realizada pelos editores e, agora, pelos algoritmos.

Sendo assim, o primeiro tópico é destinado a trazer um arcabouço teórico acerca dos meios de comunicação social, sobretudo acerca do conceito de opinião pública, bem como de seu processo de formação. Concomitantemente, é essencial discorrer sobre o comportamento político do eleitor, apontando os fatores que influenciam em seu processo de decisão de voto.

---

3 Declaração de Chapultec. Disponível em: <http://www.abjornalistas.org/legislacao_-_declaracao_chapultec.php> Acesso em: 20.01.17

4 Países que assinaram a Declaração de Chapultec: Argentina, Bolívia, Belize, Brasil, Chile, Colômbia, Costa Rica, Equador, El Salvador, os Estados Unidos, Granada, Guatemala, Honduras, Jamaica, México, Nicarágua, Panamá, Porto Rico, a República Dominicana e Uruguai. Disponível em: <http://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=533&lID=4#_ftn7> Acesso em: 20.01.17

Nesse mesmo tópico, são abordados o monopólio e a concentração da informação nas grandes empresas de Internet, demonstrando, por meio de dados estatísticos, que essas são utilizadas, pela maioria das pessoas, como fonte de notícias e, portanto, podem influenciar a opinião pública do eleitor.

Por conseguinte, tratar-se-á da evolução das pesquisas de opinião diante das novas ferramentas tecnológicas, principalmente com o *big data,* que propiciou a coleta de maior quantidade e qualidade de dados dos eleitores, permitindo mensurar praticamente em tempo real as intenções de voto. Nessa oportunidade, *big data* e algoritmos serão desenvolvidos a partir do conceito de política computacional apontado pela socióloga Zeynep Tufecki.

Seguindo o raciocínio, e para fins didáticos, apresentar-se-á como *case,* para demonstrar o impacto do *big data* nas eleições, a campanha à presidência de Barack Obama, em 2008. E, no que tange aos algoritmos, as problemáticas quanto ao fenômeno do *filter bubble* (filtro-bolha), a veiculação de notícias falsas e as ferramentas de checagem lançadas pelo Google e pelo Facebook.

Por fim, far-se-á um panorama legislativo sobre a proteção de dados pessoais no Brasil, com o objetivo de demonstrar que os provedores não são transparentes com seus usuários quanto à coleta, ao tratamento e à finalidade do uso de seus dados, ensejando assim violação ao direito constitucional à privacidade.

Opinião Pública e Comportamento Político

Antes de adentrar no objeto de estudo deste artigo – o uso do *big data* e dos algoritmos nas campanhas eleitorais – faz-se necessário, ainda que brevemente, em se tratando de tema relacionado à mídia e à política, apresentar algumas reflexões sobre os meios de comunicação social e como eles impactam na formação da opinião pública e contribuem para a modificação do comportamento político.

A imprensa e, posteriormente, os denominados meios de comunicação social sempre tiveram (e ainda têm) como principal função viabilizar à população o acesso à informação, seja por meio de livros, revistas, jornais, rádio ou televisão. Por esta razão, na década de 1940[5], iniciaram-se diversos estudos – sob ótica multidisciplinar, por meio da ciência política, antropologia, economia e/

5 RUMMERT, Sonia Maria. **Os meios de comunicação de massa como aparelhos de hegemonia.** p. 66-67. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/9109> Acesso em: 20.01.17.

ou psicologia, a fim de averiguar o papel e o poder de influência desses meios na construção da opinião pública e da cultura da sociedade[6].

Para McLuhan[7], os meios de comunicação é que constituem as mensagens, de forma que uma mesma mensagem, quando transmitida por meios diferentes, produzirá efeitos sociais diferentes, isso porque cada meio possui suas especificidades. Além disso, acredita o autor que "a evolução dos meios de comunicação determina a evolução da própria humanidade (a etapa pré-tecnológica ou primitiva; a época tipográfica, marcada pela Revolução Industrial e a época atual, de entrada na era eletrônica, na qual o mundo se transforma em uma aldeia global"[8]. Por fim, entende que nós, consumidores desses meios, não podemos controlar os respectivos efeitos influenciadores que recaem sobre nós. Somente esses meios é que têm o poder de controle[9].

Quando partimos para o estudo da ciência política, essa ideia desenvolvida por McLuhan, no final da década de 1970, muito se assemelha à tese de Walter Lippmann (1922), que versa sobre como as mídias contribuem para a construção da opinião pública (seja em seu sentido positivo, possibilitando o acesso à informação, seja em seu sentido negativo, manipulando a sociedade de acordo com interesses políticos, ideológicos e/ou econômicos).

De acordo com Walter Lippmann, parafraseado por Maxwell McCombs, "os veículos noticiosos, nossas janelas ao vasto mundo além de nossa experiência direta, determinam nossos mapas cognitivos daquele mundo. A opinião pública [...] responde, não ao ambiente, mas ao pseudoambiente construído por veículos noticiosos"[10]. Ou seja, as imagens, os estereótipos e os conceitos que criamos em nossas cabeças são reflexos do meio de comunicação:

> Aqueles aspectos do mundo exterior que têm a ver com o comportamento de outros seres humanos, na medida em que o comportamento cruza com o nosso, que é dependente do nosso, ou que nos é interessante, podemos

6 RUMMERT, Sonia Maria. **Os meios de comunicação de massa como aparelhos de hegemonia**. p. 66-67. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/9109> Acesso em: 20.01.17.

7 MARSHALL, McLuhan. **Os meios de comunicação como extensão do homem**. São Paulo, Cultrix, 1979. p. 36.

8 RUMMERT, Sonia Maria. **Os meios de comunicação de massa como aparelhos de hegemonia**. p. 66-67. Disponível em: < http://bibliotecadigital.fgv.br/dspace/handle/10438/9109> Acesso em: 20.01.17.

9 RUMMERT, Sonia Maria. **Os meios de comunicação de massa como aparelhos de hegemonia**. p. 66-67. Disponível em: < http://bibliotecadigital.fgv.br/dspace/handle/10438/9109> Acesso em: 20.01.17.

10 MCCOMBS, Maxwell. **A Teoria da Agenda – A mídia e a opinião pública**. Ed. Vozes, Rio de Janeiro, 2004. p. 19

> chamar rudemente de opinião pública. As imagens na cabeça desses seres humanos, a imagem de si próprios, dos outros, de suas necessidades, propósitos e relacionamento, são suas opiniões públicas. Aquelas imagens que são feitas por grupos de pessoas, ou por indivíduos agindo em nome dos grupos, é Opinião Pública com letras maiúsculas[11].

Por conseguinte, o mesmo autor frisa quais fatores que limitam o acesso aos fatos:

> são eles as censuras artificiais, as limitações do contato social, a relativa falta de tempo disponível diariamente para prestar atenção nos assuntos públicos, a distorção emergente devido aos eventos que precisam ser comprimidos em mensagens muito breves, as dificuldades em fazer um pequeno vocabulário expressar um mundo complicado, e finalmente o temor de enfrentar aqueles fatos que parecem ameaçar a rotina estabelecida das vidas humanas[12].

Como mencionado, alguns fatores limitam o nosso acesso aos fatos. Sendo assim, importante mencionar, nessa fase, que os veículos noticiosos passam por um processo denominado como *gatekeeping* (seleção de conteúdo). Esse processo, bem como o de editoração de uma notícia, faz parte da organização de conteúdo de uma mídia. Contudo, o que se questiona é a falta de transparência desses veículos ao afirmar suposta neutralidade ideológica – apartidários. Como será visto ao longo desse artigo, essa crítica perpassa aos provedores de Internet, mesmo não sendo esses ditos, explicitamente, como imprensa.

Ao analisar as características das mídias sociais de massa, observa-se que as tradicionais (televisão, rádio, jornal e revista) possuem uma relação de "um" para "todos"; ou seja, a informação é unilateral. Porém, transpondo-se para a Internet, verifica-se um fluxo de dados inimaginável e inesgotável (de "todos" para "todos"). É o que os pesquisadores denominam como "*information overload*", em que a quantidade de informação supera a capacidade do indivíduo de processá-las, implicando dificuldade na filtragem dos dados[13].

Sendo assim, nas mídias tradicionais, a mensagem é elaborada de acordo com o entendimento e a ideologia da respectiva organização, sem qualquer ingerência

---

11 MCCOMBS, Maxwell. **A Teoria da Agenda – A mídia e a opinião pública.** Ed. Vozes, Rio de Janeiro, 2004. p. 19

12 MCCOMBS, Maxwell. **A Teoria da Agenda – A mídia e a opinião pública.** Ed. Vozes, Rio de Janeiro, 2004. p. 19

13 MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático**. Juruá: Rio de Janeiro, 2014. P.114-15. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/14106> Acesso em: 20.01.17.

da sociedade. Não há troca de informações ou prévia discussão. Por isso, seu poder de persuasão e influência sobre a população é latente, podendo moldar a opinião pública e, como será visto a seguir, o comportamento político do eleitor.

Muito embora a Internet apareça, para os pensadores otimistas, como Pierre Levy, como "espaço do saber" e "inteligência coletiva" – uma esfera em que os indivíduos podem compartilhar informações, ideias, projetos e engajar-se politicamente por meio de debates democráticos –, observa-se que as grandes empresas de Internet têm a capacidade técnica de, assim como as mídias tradicionais, influenciarem sutilmente na formação do conhecimento e no processo decisório eleitoral.

De acordo com Iara Vianna, o comportamento político de um eleitor pode ser influenciado por diversas variáveis, as quais são aduzidas e fundamentadas por três grandes teorias clássicas: Sociológica, Psicossociológica (ou Psicológica) e Escolha Racional:

> As duas primeiras correntes trabalham com os chamados fatores de longo prazo para explicação do voto, sendo exemplos de algumas de suas variáveis de estudo a classe social, a escolaridade, a religião (no enfoque sociológico) e a identificação partidária e o posicionamento ideológico (no psicológico). A Teoria da Racionalidade, por outro lado, se centra em analisar fatores de curto prazo, como a avaliação do desempenho do governo, sobretudo através de suas políticas econômicas. Em alguns casos, ao se tratar do voto racional, trata-se também da imagem dos candidatos e os temas debatidos durante as campanhas eleitorais[14].

Observa-se, assim, que a decisão de voto do eleitor se dá por intermédio de fatores determinantes, como um amigo, algum familiar ou até mesmo superior hierárquico, fator econômico, fator ideológico e descrença e ineficiência no governo. E, diante disso, a mídia tem um papel fundamental, pois é por meio dela que a sociedade é informada sobre os fatos que lhe permitem entender a situação atual de determinado espaço-tempo. Embora as teorias citadas não tenham sido desenvolvidas com o olhar para a Internet, os conceitos podem ser transpassados e rediscutidos frente ao ambiente digital.

As redes sociais são constituídas de pessoas que se reúnem em razão de suas afinidades e comportamento (*clusters*). A título exemplificativo, cita-se que, em 2010, o Facebook incluiu na conta de 60 milhões de usuários americanos o botão "estou votando" ("*I'm voting*"). De acordo com a assessoria de imprensa da empresa,

14 VIANNA, Iara Lima. **Eleição presidencial de 2014**: contexto, racionalidade e sentimentos partidários. Dissertação de Mestrado apresentada ao Programa de Pós Graduação em Ciência Política da Universidade Federal de Minas Gerais, 2015.

tratava-se de um estudo a fim de averiguar a influência dos "amigos" em prol do engajamento político, conforme nota oficial lançada na própria página do Facebook[15].

O referido estudo foi publicado com o seguinte título: "*A 61-million-person experiment in social influence and political mobilization*"[16], na revista *Nature*, em 2012, mesmo ano em que outro botão foi incluído na época das eleições (*voter megaphone*), o qual foi visto por aproximadamente 2,4 milhões de brasileiros, durante as eleições nacionais do referido ano.

Aliás, esse estudo foi tratado por Jonathan Zittrain, professor da Faculdade de Direito de Harvard, em seu artigo "*Facebook could decide an election without anyone ever finding out",* publicado no *The New Republic*, em 2014[17], o qual apontou três pontos importantes para o debate: (a) o parâmetro para a escolha dos usuários participantes do estudo; (b) o "efeito cascata" produzido pelo botão "*I´m voting*"; e (c) o fenômeno denominado como "*gerrymandering*" (manipular a favor de um partido ou classe – tradução literal).

Apesar da rede social (Facebook) informar que os usuários foram escolhidos aleatoriamente, Zittrain indica que, diante da quantidade e especificidade dos dados sensíveis (como, por exemplo, opção sexual, religiosa e política) sob custódia das grandes empresas de Internet, os indivíduos participantes poderiam, em uma situação hipotética, ser selecionados de acordo com os interesses da empresa. Frisa-se que a desconfiança acerca dos parâmetros se sobressai, haja vista que o estudo foi realizado sem que os respectivos participantes fossem previamente informados.

O efeito cascata se consubstancia justamente na influência que os "amigos" exercem na decisão de voto dos indivíduos. O estudo consistia basicamente no seguinte: no dia das eleições, apareceu para alguns usuários um gráfico indicando os locais de votação, o botão "*I´m voting*" para que o usuário apertasse assim que votasse e as fotos de até 06 amigos que haviam feito a mesma coisa.

Os resultados demonstraram que os usuários notificados da votação de seus amigos eram 0,39% mais propensos a votar do que aqueles no grupo de controle (que receberam apenas uma mensagem de "*get-out-the-vote*" – saia para votar) e as decisões resultantes de votar também pareciam ondular com o comportamento

15 Election Day 2012 on Facebook. Nota oficial. Disponível em: <https://www.facebook.com/notes/us-politics-on-facebook/election-day-2012-on-facebook/10151076006385882> Acesso em: 20.01.17.

16 A 61-million-person experiment in social influence and political mobilization. Disponível em: <http://fowler.ucsd.edu/massive_turnout.pdf> Acesso em: 20.01.17.

17 ZITTRAIN, Jonathan. Facebook Could Decide an Election Without Anyone Ever Finding Out. **New Republic**. Publicado em: 01 jun. 2014. Disponível em: <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> Acesso em: 20.01.17.

de amigos próximos do Facebook, mesmo que essas pessoas não tivessem recebido a mensagem original, ou seja, não receberam o botão de "I´m voting", mas conseguiam visualizar em sua linha do tempo a atividade de amigos próximos.

Esse pequeno aumento nas taxas de participação contribuiu para o aumento do número de votos. Os pesquisadores concluíram que seu gráfico do Facebook mobilizou diretamente 60.000 eleitores e, graças ao efeito cascata, acabou por gerar 340.000 votos adicionais naquele dia. Como indicam, George W. Bush venceu na Flórida e, portanto, a presidência, por 537 votos – menos de 0,01% dos votos emitidos nesse estado.

Por fim, há que se mencionar sobre o fenômeno "*gerrymandering*", que, para Zittrain, ocorre quando um site distribui informações de forma a beneficiar sua própria agenda ideológica. E, aqui, encontra-se a mesma crítica realizada em face das mídias de massa tradicionais – o monopólio e a concentração da informação e, por conseguinte, o poder de influência na formação da opinião pública do usuário.

Em janeiro de 2017, a Quartz, em parceria com a Mozilla, publicou o relatório final de uma pesquisa apontando que 55% dos brasileiros acham que o Facebook é a Internet[18]. Além disso, alguns pontos levantados merecem ser destacados:

a. a maioria das pessoas não entende o que é internet, em seu nível básico;

b. não conseguem distinguir notícias falsas das verdadeiras, bem como notícias de propaganda;

c. há um grande monopólio e concentração de informações – o Google é a empresa responsável por mais de 75% das pesquisas feitas na internet, e por 95,9% das pesquisas feitas de smartphones;

d. o Facebook é outro enorme concentrador da internet – além de ser a rede social com maior número de usuários no mundo (com 1,7 bilhão), a empresa também é dona das outras duas redes sociais que compõem o pódio: WhatsApp e Messenger, com 1 bilhão cada.[19] Pode-se citar aqui, inclusive, o Instagram.

---

18 SUMARES, Gustavo. 55% dos brasileiros acham que o Facebook é a internet, diz pesquisa. **Olhar Digital**. Publicada em: 17 jan. 2017. Disponível em: < http://olhardigital.uol.com.br/noticia/55-dos-brasileiros-acham-que-o-facebook-e-a-internet-diz-pesquisa/65422> Acesso em: 20.01.17.

19 SUMARES, Gustavo. 55% dos brasileiros acham que o Facebook é a internet, diz pesquisa. **Olhar Digital**. Publicada em: 17 jan. 2017. Disponível em: <http://olhardigital.uol.com.br/noticia/55-dos-brasileiros-acham-que-o-facebook-e-a-internet-diz-pesquisa/65422> Acesso em: 20.01.17.

Observa-se que esse dado é preocupante, principalmente quando conjugado com os resultados apresentados pela Pew Research Center, em 2015, informando que 63% das pessoas se utilizam do Facebook para se informar[20] – ou seja, os sites oficiais de notícias e, até mesmo as mídias tradicionais, tornaram-se secundárias, proporcionando, assim, um grande poder de influência para as redes sociais.

No início de maio de 2016, o jornalista Michael Nunez, do portal Gizmodo, publicou uma matéria relatando sobre o processo de "curadoria" de notícias realizada pelo Facebook[21]. Conforme informações de ex-funcionários, desde 2014, a rede social estava contratando jornalistas para exercerem funções de curadores, a fim de monitorar as notícias e evitar que pautas conservadoras ou que remetessem à própria rede social estivessem entre os chamados "*trending news*" (principais notícias). Logo, as notícias que supostamente apareciam como as principais poderiam não ser.

Embora a rede social (Facebook) tenha informado que essa curadoria de notícias por intermédio de humanos não mais exista, a reflexão impera quando um provedor que não se denomina como imprensa, mas sim como um espaço público, tem a capacidade técnica de programar suas ferramentas tecnológicas com o objetivo de atender seus próprios interesses sem qualquer transparência a seus usuários.

Campanhas Eleitorais, pesquisas de opinião e ferramentas tecnológicas

As campanhas eleitorais estão cada vez mais envoltas por estratégias criadas por agências de marketing político, principalmente no tocante à pesquisa de mercado e/ou à pesquisa de opinião pública – ou seja, aquela que permite averiguar junto aos eleitores seus interesses, valores, ideais, sobretudo se determinado candidato é "bem visto" pela população.

As pesquisas de opinião, em sua essência, são custosas e demoradas, uma vez que envolvem esforço humano, conhecimento técnico e demandam tempo. É necessário mobilizar uma equipe especializada ou, ao menos, treinada e

20 Pesquisa: mais de 60% das pessoas usam o Facebook para se informar. **Olhar Digital**. Publicado em: 15 jul. 2015. Disponível em: <http://olhardigital.uol.com.br/noticia/pesquisa-mais-de-60-das-pessoas-usam-o-facebook-para-se-informar/49810> Acesso em: 22.01.17.

21 NUNEZ, Michael. Former Facebook Workers: We Routinely Suppressed Conservative News. **Gizmodo**. Publicado em: 09 mai. 2016. Disponível em: <http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006> Acesso em: 20.01.17.

empenhada em fazer com que cidadãos participem e respondam a formulários presencialmente ou por telefone.

Entretanto, atualmente, os provedores são capazes de armazenar, sobretudo, extrair informações dos indivíduos sem a necessidade de que respondam quaisquer perguntas ou formulários. Esses dados vão além de "idade, sexo e raça", pois coletam características pessoais, comportamentais e opiniões[22].

Durante as campanhas eleitorais, as equipes de marketing político criam sites e aplicativos com o intuito de informar sobre os projetos, as ideias dos candidatos e doações e promover certa aproximação com o eleitorado. Contudo, essas mesmas ferramentas permitem obter diversos dados dos indivíduos, como número de celular, localização, preferências, dentre outros.

Apesar de serem considerados dados "anônimos", por supostamente não identificarem o usuário, há que se destacar, como bem delineado pela socióloga Zeynep Tufecki, que o cruzamento de todos os dados adquiridos permite não somente a identificação do indivíduo em si, mas também a opinião política da região em que determinado eleitor se encontra, propiciando que o candidato "personalize" seu discurso para esse local.

Em julho de 2014, a socióloga Zeynep Tufekci, publicou um interessante artigo – "*Engineering the public: Big data, surveillance and computational politics*[23]" – alertando sobre as seis novas ferramentas de persuasão, vigilância e engenharia social, denominadas como políticas computacionais, e como elas impactam diretamente nas campanhas eleitorais.

De acordo com a pesquisadora, as ferramentas correspondem: ao *big data* (informalmente denominado como um grande conjunto de dados armazenados); aos emergentes métodos computacionais (que permitem a verificação da semântica); à modelagem (possibilita o acesso às características psicológicas do usuário e fornece conteúdo específico); à ciência comportamental (para persuasão); à experiência científica em tempo real (as redes sociais permitem estudos em tempo real); e ao poder das plataformas e da governança algorítmica. Para fins desse artigo, atentar-se-á ao *big data* e aos algoritmos.

---

22 MIRANDA FILHO, Renato. Um arcabouço para pesquisas de opinião em redes sociais. Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais – Departamento de Ciência da Computação. Disponível em: <https://www.dcc.ufmg.br/pos/cursos/defesas/1779M.PDF> Acesso em: 20.01.17.

23 TUFEKCI, Zeynep. Engineering the public: big data, surveillance and computational politics. **First Monday**, Volume 19, n. 7, 7 July 2014. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097> Acesso em: 20.01.17.

Big Data

Conforme delineado pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro, *big data*:

> (...) é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores[24].

De acordo com o McKinsey Global Institute, *big data*:

> (...) é um termo utilizado para descrever um grande volume de dados, em grande velocidade e grande variedade; que requer novas tecnologias e técnicas para capturar, armazenar e analisar seu conteúdo; e é utilizado para abrilhantar a tomada de decisão, fornecendo introspecção e descobertas, e suportando e otimizando processos[25].

Partindo desses conceitos, o *big data* apresenta três características relevantes, conhecidas como os "3 V´s": (i) volume – a sociedade atual é altamente conectada e tecnológica, todos os dias milhões de transações e comunicações são realizadas *online,* seja troca de e-mails, mensagens por comunicadores instantâneos, fotos, vídeos, digitalização de documentos, cadastros; (ii) velocidade – esses dados são criados de forma acelerada e praticamente instantânea, portanto, atualizadas; e (iii) variedade – os dados coletados são aleatórios, variados e advém das mais diversas ferramentas – mídias sociais, celular, gps, sistemas integrados etc[26].

Transpondo-se ao cenário das campanhas eleitorais, tendo como fundamento tudo o que já foi desenvolvido nos tópicos anteriores, o *big data* revoluciona as pesquisas quantitativas e qualitativas de opinião pública. Foi exatamente a estratégia e os mecanismos adotados pela campanha à presidência de Barack

---

24 ITS – Instituto de Tecnologia e Sociedade. **Big Data no projeto sul global**. Rio de Janeiro, 2016. p.09. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf> Acesso em: 20.01.17.

25 DEL PRÁ NETTO, Adriana Sodré; PIOLI MORO, Evandro; FOLLY FERREIRA, Fernanda. Universidade Federal do Rio de Janeiro. Disponível em: <http://www.gta.ufrj.br/grad/15_1/bigdata/intro.html> Acesso em: 20.01.17.

26 MCAFEE, Andrew; BRYNJOLFSSON. Big data: the management revolution. **Harvard Business Review**. Publicado em: out. 2012. Disponível em: <https://hbr.org/2012/10/big-data-the-management-revolution> Acesso em: 20.01.17.

Obama, em 2008. A equipe de marketing captou diversos dados pessoais e sensíveis, a ponto de obter um histórico de preferências, interesses e comportamento de seus eleitores, a fim de viabilizar o envio de e-mails personalizados.

O documentário "Obama Digital #obamadigital"[27] traça um panorama demonstrando a efetividade das mídias digitais ao propiciar uma articulação de redes e a mobilização dos eleitores para participarem ativamente dos debates públicos, inclusive, para o desempenho de funções nos comitês políticos.

De acordo com o relatado no documentário, o candidato atuou em dezesseis redes sociais, a fim de se aproximar dos diversos grupos sociais; criou um site para propiciar a arrecadação de doações e o debate sobre as propostas apresentadas e outro para que as informações consideradas falsas fossem desmentidas; e, concomitantemente, realizou a compra de links patrocinados para que seus conteúdos estivessem no topo dos resultados das pesquisas realizadas no Google.

Interessante notar que os eleitores cadastrados nos sites oficiais do então candidato recebiam e-mails personalizados conforme seu histórico de participação na campanha eleitoral (se era ou não voluntário, se era ou não doador ou se já havia realizado doações nas campanhas passadas), ou seja, um verdadeiro banco de dados relacionados ao histórico político dos usuários.

Claro está que esses dados eram coletados de forma variada – redes sociais, sites, serviços de localização (gps), plataformas de doações. Acrescenta-se que a obtenção desses dados foi facilitada pela transferência indevida dessas informações entre provedores e empresas de marketing e publicidade, bem como demais parceiros comerciais, como instituições financeiras.

Algoritmos

Atualmente, fala-se muito sobre a chamada inteligência artificial, principalmente em relação àquela imagem dos robôs nos filmes científicos. Contudo, faz-se necessária conceituá-la para que se entenda a abrangência do tema e, por conseguinte, a definição de algoritmo.

Didaticamente, o professor Marcelo Crespo explica que se trata da:

> (...) realização, por uma máquina, de tarefas geralmente ultimadas por um humano. Pode-se até mesmo entender que ela se divide em quatro categorias: a) aprendizagem mecânica; b) processamento da linguagem natural; c)

27 Vídeo disponibilizado na plataforma Vimeo <https://vimeo.com/7870206>. Acesso em: 20.01.17.

> visão; e d) fala. A aprendizagem mecânica nada mais é que um sistema que processa dados para melhorar continuamente o desempenho na realização de uma tarefa. Já o processamento da linguagem natural é a possibilidade de um computador compreender a linguagem humana, interpretando o que as pessoas realmente transmitem nas suas interações, decifrando suas intenções e fornecendo respostas cada vez mais precisas nos resultados de uma pesquisa. Já a visão é a habilidade de interpretar imagens, identificá-las e descrevê-las, o que geralmente é feito de forma automática pelos humanos. Por fim, a fala é o sistema que permite uma máquina interpretar a linguagem oral e propiciar interação entre os humanos e as máquinas[28].

Os algoritmos, como uma subárea da inteligência artificial, podem ser definidos como um método para resolver um problema específico se utilizando de operações computacionais[29]. Em síntese, são eles que reconhecem padrões e traduzem a linguagem dos humanos para as máquinas.

Em 2016, os algoritmos (juntamente com as empresas Google e Facebook) foram tema central nas campanhas eleitorais dos Estados Unidos, haja vista o efeito "filtro-bolha" (tido como um método de monitoração e segregação da rede), a propagação de notícias falsas nas redes sociais e o uso de *bots* (programa de computador criado para automatizar procedimentos[30]) para viabilizar a propagação de conteúdos em maior quantidade e alcance.

O fenômeno do filtro-bolha

Como mencionado anteriormente, a quantidade de informações compartilhada na Internet supera a capacidade do indivíduo de processá-las, dificultando na filtragem do conteúdo que circula. É o que os pesquisadores denominam como "*information overload*" [31].

---

28 CRESPO, Marcelo; ALMEIDA CAMARGO, Coriolano. Inteligência artificial, tecnologia e o Direito: o debate não pode esperar!. **Direito Digit@al – Migalhas**. Publicado em: 30 nov. 2016. Disponível em: <http://www.migalhas.com.br/DireitoDigital/105,MI249734,41046-Inteligencia+artificial+tecnologia+e+o+Direito+o+debate+nao+pode> Acesso em: 20.03.17.

29 US Congress, Office of Technology Assessment, SDI: Technology, Survivability and Software, OTA-ISC-353 (Whashington, DC: U.S. Government Printing Office, May 1988). p. 188.

30 LOUREIRO, Rodrigo. Entenda de uma vez por todas o que é um bot e como ele funciona. **Olhar Digital**. Publicado em: 11 abr. 2016. Disponível em: < https://olhardigital.uol.com.br/noticia/entenda-de-uma-vez-por-todas-o-que-e-um-bot-e-como-ele-funciona/57075> Acesso em: 20.03.17.

31 MAGRANI, Eduardo. **Democracia conectada**: a internet como ferramenta de engajamento político-democrático. Juruá: Rio de Janeiro, 2014. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/14106> Acesso em: 20.01.17.

Nesse cenário, surgem as grandes empresas de aplicações para internet que, por meio de seu alto conhecimento tecnológico, ofertam serviços de "filtragem" de informações, os quais correspondem a algoritmos que facilitam o referido filtro, a fim de propiciar ao usuário as "principais" informações conforme as palavras-chave fornecidas pelo próprio interessado.

E, a partir disso, podem derivar duas consequências apontadas por Eduardo Magrani:

> (...) de um lado, a filtragem de conteúdo não intencional, feita pelos provedores, que estamos enquadrando e denominando como *filter bubble*; de outro, a busca dos próprios indivíduos por filtrarem voluntariamente as informações que consomem agravando o problema também desencadeado pelo *filter bubble*, da fragmentação do debate[32].

A teoria do *filter bubble* (traduzida como filtro bolhas), concebida por Eli Pariser, consiste na identificação de padrões, por meio dos algoritmos, com a finalidade de propiciar uma personalização no serviço para o usuário – essa que pode ser traduzida pela expressão "*User Experience*", adotada pelos profissionais de marketing. É a ideia de se utilizar da coleta e análise de dados para reconhecer comportamento e preferências, a fim de viabilizar ao usuário uma "melhor experiência" de navegação e/ou uso de determinado serviço ou produto.

À sociedade, esse mecanismo é passado como uma comodidade, um serviço personificado. Recentemente, o Spotify – aplicativo de música *streaming* – desenvolveu um algoritmo que analisa os padrões musicais do usuário e, assim, cria uma *playlist* personalizada. Ainda, de acordo com o que o usuário escutou no ano, uma *playlist* chamada "Mais tocadas no seu 2016".

Semelhante, pode-se citar o Netflix. Conforme o usuário assiste a filmes, seriados ou documentários, os algoritmos da empresa captam os padrões e passam a sugerir conteúdos parecidos com os já assistidos utilizando chamadas como "porque você assistiu (nome do filme/seriado/documentário)..." ou "principais escolhas indicadas para (nome do usuário)...". Perceba que são formas de se aproximar do usuário e fazer com que ele se sinta satisfeito e "bem atendido" pela empresa.

Entretanto, mesmo que *a priori* esse mecanismo seduza os olhos dos usuários, é nessa conveniência que reside o problema. Esses filtros são segregadores.

---

32 MAGRANI, Eduardo. **Democracia conectada**: a internet como ferramenta de engajamento político-democrático. Juruá: Rio de Janeiro, 2014. p. 119. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/14106> Acesso em: 20.01.17.

A partir do momento em que o padrão do usuário é reconhecido, ele somente terá "contato" com aquilo que o algoritmo filtrou como de seu interesse.

Veja, por exemplo, o Facebook: quanto mais o usuário curte e compartilha determinado tipo de informação, ele acaba por receber somente conteúdos nesse mesmo sentido. Transpondo-se às eleições, observa-se que a polarização não estava apenas nos discursos pessoais, mas, sobretudo, nas redes sociais, impedindo, assim, que o eleitor tivesse uma ampla visão do todo (das ideias, notícias e projetos de todos os candidatos). Como bem colocado por Magrani:

> No entanto, para além da conveniência, o problema reside, no entanto, no excesso da filtragem, tanto por parte das empresas quanto dos próprios indivíduos que sem ter consciência se limitam se afastando de pontos de vista divergentes dos seus e empobrecendo assim o valor do debate na esfera pública virtual. Por isso argumenta-se que os filtros-bolha limitam os usuários ao que desejam (ou desejariam) segundo uma predição algorítmica, dificultando o acesso às informações que devessem ou precisassem ver para enriquecer o debate democrático[33].

Em outubro de 2016, a Pew Research Center publicou um relatório sobre o ambiente político nas mídias sociais[34], que apontou que 39% dos usuários optavam por bloquear, desfazer a amizade ou ocultar a visualização de conteúdos de outros usuários em razão de conteúdos relacionados à política. Desse grupo: (a) 60% assim procede, pois acredita que o conteúdo publicado é ofensivo; (b) 43% afirmam que o outro usuário publica muitos conteúdos relacionados à política; (c) 39% por serem contrários ao conteúdo postado; (d) 38% por considerarem o conteúdo abusivo; e (e) 16% por outros motivos.

Esses dados estatísticos coadunam com a ideia trazida por Magrani ao mencionar que os próprios indivíduos são, de certa forma, responsáveis pela criação dos filtros-bolha. Ou seja, ao bloquearem um perfil, desfazerem uma amizade e/ou ocultarem os conteúdos que são divergentes às suas respectivas opiniões, eles viabilizam, automaticamente, o efeito bolha.

---

33 MAGRANI, Eduardo. **Democracia conectada:** a internet como ferramenta de engajamento político-democrático. Juruá: Rio de Janeiro, 2014. p. 119. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/14106> Acesso em: 20.01.17.

34 DUGGAN Maeve; SMITH, Aaron. **The Political Environment on Social Media**. Pew Research Center, October, 25. 2016. p. 15. Disponível em: < http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/10/24160747/PI_2016.10.25_Politics-and-Social-Media_FINAL.pdf> Acesso em: 06.03.17.

As notícias falsas e os mecanismos de checagem

Um estudo realizado pela Universidade de Stanford com 7.804 estudantes desde o ensino fundamental à faculdade apontou que, aproximadamente, 82% dos participantes não sabem distinguir um conteúdo patrocinado de uma notícia real na internet[35]. O estudo, divulgado em novembro de 2016, demonstrou que a maioria dos estudantes não checa a fonte da notícia, de forma que a credibilidade de uma notícia está relacionada à quantidade de detalhes e ao tamanho da foto anexada.

A pesquisa comprova que, apesar de os participantes serem altamente conectados e entenderem de tecnologia e redes sociais, eles não têm a noção necessária para avaliar a precisão, a veracidade e a confiabilidade das matérias noticiadas[36]. Somada a isso, a compulsiva necessidade de posicionamento, curtidas e compartilhamentos, propicia-se a veiculação de notícias falsas.

Walter Quattrociocchi, pesquisador sobre a propagação de notícias falsas, em entrevista para o The Guardian, em novembro de 2016, afirmou que essas podem não ser tão fáceis de identificar, pois não se tratam de teorias da conspiração ou algo puramente mentiroso. Podem decorrer de títulos (*headlines)* ambíguos – que gerem confusão de sentido – ou meias verdades.[37]

Ainda em 2016, um outro estudo realizado pela Universidade de Warwick comprovou que uma mentira se propaga muito mais rápido que uma verdade e que demora uma média de 12 horas para que um falso rumor seja desmentido online[38]. Isso ocorre justamente diante da ansiedade dos indivíduos em divulgarem/compartilharem informações de forma instantânea sem se valer do tempo de checagem e reflexão do conteúdo.

---

35 Stanford History Education Group; Robert R. McCormick Foundation. **Evaluating information: the cornerstone of civic online reasoning**. Disponível em: <https://sheg.stanford.edu/upload/V3LessonPlans/Executive%20Summary%2011.21.16.pdf> Acesso em: 20.01.17.

36 SHELLENBERGER, Sue. Most Students Don't Know When News Is Fake, Stanford Study Finds. **The Wall Street Journal.** Publicado em: 21 nov. 2016. Disponível em: <http://www.wsj.com/articles/most-students-dont-know-when-news-is-fake-stanford-study-finds-1479752576> Acesso em: 20.01.17.

37 SOLON, Olivia. Facebook's failure: did fake news and polarized politics get Trump elected? **The Guardian**. Publicado em: 10 nov. 2016. Disponível em: <https://www.theguardian.com/technology/2016/nov/10/facebook-fake-news-election-conspiracy-theories> Acesso em: 20.01.17.

38 SILVERMAN, Craig. Recent research reveals false rumours really do travel faster and further than the truth. **First Draft News**. Publicado em: 06 mai. 2016. Disponível em: <https://firstdraftnews.com/recent-research-reveals-false-rumours-really-do-travel-faster-and-further-than-the-truth/> Acesso em: 20.01.17.

Relevante mencionar que há um fator econômico determinante e que propicia a propagação das notícias falsas: a economia digital das curtidas. Durante a campanha eleitoral de 2016, nos Estados Unidos, um estudante de computação de 22 anos, Beqa Latsabidze, pensando em "ganhar dinheiro", criou um site para difundir opiniões partidárias sobre a Hillary Clinton. Ao perceber que nenhum anunciante o contatou, resolveu alterar e misturar notícias reais e outras falsas sobre Donald Trump em meio a discursos anti-Hillary (departed.co)[39].

Em entrevista ao jornal The New York Times, o estudante afirmou que seu único interesse era se beneficiar por meio dos anúncios do Google e fazer com que os usuários do Facebook clicassem nos links e chegassem até o seu site[40]. Para Latsabidze, as notícias veiculadas em seu site não poderiam ser consideradas falsas, mas sim "*infotaiment*" – uma mistura de informação com entretenimento – ou sátira[41].

Essa nova economia digital que beneficia os conteúdos mais acessados e seguidos compactua para que as notícias dúbias, inverídicas e que causem grande comoção sejam veiculadas, a fim de que o portal apareça entre os primeiros nos resultados de pesquisa dos provedores de busca.

Diante de todas as acusações, as empresas Google e Facebook anunciaram, no final de 2016, mecanismos de checagem de notícias. Em outubro de 2016, a Google anunciou o "Google Fact Check", que usará o algoritmo Claim Review para verificar, no próprio Google News, se há marcadores que ratifiquem a veracidade da informação. Conforme publicado no blog oficial, a empresa buscará, concomitantemente, por sites que "sigam critérios comumente aceitos para checagem dos fatos"[42].

---

39 **Folha de São Paulo**. Criador de site de notícias falsas diz que sua motivação é ganhar dinheiro. Publicado em: 28 nov. 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2016/11/1836245-criador-de-site-de-noticias-falsas-diz-que-sua-motivacao-e-ganhar-dinheiro.shtml> Acesso em: 20.01.17.

40 **Folha de São Paulo.** Criador de site de notícias falsas diz que sua motivação é ganhar dinheiro. Publicado em: 28 nov. 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2016/11/1836245-criador-de-site-de-noticias-falsas-diz-que-sua-motivacao-e-ganhar-dinheiro.shtml> Acesso em: 20.01.17..

41 **Folha de São Paulo**. Criador de site de notícias falsas diz que sua motivação é ganhar dinheiro. Publicado em: 28 nov. 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2016/11/1836245-criador-de-site-de-noticias-falsas-diz-que-sua-motivacao-e-ganhar-dinheiro.shtml> Acesso em: 20.01.17.

42 Redação. Google lança recurso que ajuda a checar veracidade de informações. **IDG Now**. Publicado em: 14 out. 2016. Disponível em:<http://idgnow.com.br/internet/2016/10/14/google-lanca-recurso-que-ajuda-a-checar-veracidade-de-informacoes/> Acesso em: 20.01.17.

Dois meses depois, em dezembro de 2016, o Facebook anunciou seu mecanismo de checagem de boatos e notícias falsas[43], o qual novamente envolverá curadoria de notícias. Quando o usuário indicar que determinado conteúdo é falso, o link será enviado para organizações parceiras que farão a checagem da notícia.

Interessante notar que essas organizações "são signatárias do Código de Princípios de Checagem de Dados Poynter. Ele foi criado pelo Instituto Poynter, uma instituição americana fundada na década de 70 com o objetivo de promover boas práticas jornalísticas pelo mundo"[44]. Sendo assim, a ideia de curadoria volta a permear e, com isso, todas as indagações já realizadas nos tópicos anteriores, principalmente no tocante a ser ou não o Facebook um veículo noticioso, e por conseguinte sua respectiva responsabilidade por conteúdos gerados por terceiros.

O debate sobre as notícias falsas é de suma importância. Não é à toa que, no início de março de 2017, em Viena – Áustria, os relatores especiais para a Liberdade de Expressão da ONU, OEA (Organização dos Estados Americanos), OSCE (Organização pela Segurança e Cooperação na Europa) e CADHP (Comissão Africana dos Direitos Humanos e dos Povos) publicaram conjuntamente um documento intitulado "Declaração sobre a Liberdade de Expressão e Notícias Falsas, Desinformação e Propaganda", em iniciativa facilitada pela ARTIGO 19 e pela organização Centre for Law and Democracy[45] com recomendações para o Estados, empresas de tecnologias, meios de comunicação, jornalistas e indivíduos acerca dos desafios em relação ao tema.

O uso de *bots*

Ainda sobre as questões relacionadas à propagação de notícias falsas, imprescindível destacar a polêmica envolvendo o uso dos chamados *bots* (expres-

43 MOSSERI, Adam Mosseri. Vice-Presidente do Feed de Notícias do Facebook. Publicado em: 15 dez. 2016. Disponível em: <http://br.newsroom.fb.com/news/2016/12/combatendo-noticias-falsas-e-boatos/> Acesso em: 20.01.17.

44 CABETTE FABIO, André. Como funcionará o sistema de checagem de notícias falsas do Facebook. **Nexo**. Publicado em: 16 dez. 2016. Disponível em: <https://www.nexojornal.com.br/expresso/2016/12/16/Como-funcionar%C3%A1-o-sistema-de-checagem-de-not%C3%ADcias-falsas-do-Facebook> Acesso em: 20.01.17.

45 ARTIGO 19. "Notícias falsas" é tema de declaração assinada por relatores para a Liberdade de Expressão. Publicado em: 16 mar. 2017. Disponível em: <http://artigo19.org/blog/2017/03/16/noticias-falsas-e-tema-de-declaracao-assinada-por-relatores-para-a-liberdade-de-expressao/> Acesso em: 20.03.17.

são derivada da palavra, em inglês, "*robot*", que significa "robô"[46]) nas eleições presidenciais dos Estados Unidos, em 2016.

De acordo com a Cartilha de Segurança da Informação para Internet publicada pelo Comitê Gestor da Internet no Brasil (CGI.br), em parceria com o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), os *botnets* – uma rede formada por milhares de *bots* – "possibilitam dentre outras ações maliciosas, a coleta de informações de um grande grupo de computadores, envio de *spam* e camuflagem da identidade do atacante"[47].

Para melhor entendimento, cita-se um estudo publicado por Alessandro Bessi e Emilio Ferrara, do Instituto de Ciências Informacionais, da Universidade do Sul da Califórnia, um dia antes das eleições presidenciais americanas de 2016, estimando a atuação de 400.000 (quatrocentos mil) *bots* no Twitter, ou seja, criando *tweets*, bem como *retweetando*[48].

O estudo apontou que, apesar do uso de *bots* em mídias sociais para fins políticos não ser uma novidade, observa-se que os mesmos estão cada vez mais sofisticados, de modo que resta quase impossível averiguar a procedência dos mesmos. Contudo, a pesquisa demonstrou que, aproximadamente, 75% dos *bots* eram em favor do então candidato Donald Trump.

Conforme delineado pelos pesquisadores, o fato de os *bots* produzirem sistematicamente conteúdos positivos a determinado candidato, pode impactar na percepção dos eleitores sobre um suposto apoio orgânico para este candidato quando, na verdade, trata-se de algo artificialmente gerado.

Tal fato ocorre, também, porque muitos dos usuários não verificam a credibilidade das fontes e a veracidade das informações, como delineado no tópico anterior, possibilitando, assim, a propagação de notícias falsas em larga escala, já que os *bots* permitem a publicação de milhares de conteúdos ao mesmo tempo.

Além disso, o uso da inteligência artificial para que os *bots* interajam e conversem com os usuários tem dificultado a identificação dos bots, principalmente porque esses têm "clonado" o comportamento humano. Com o desenvolvimento dessas ferra-

---

46 LOUREIRO, Rodrigo. Entenda de uma vez por todas o que é um bot e como ele funciona. **Olhar Digital**. Publicado em: 11 abr. 2016. Disponível em: <https://olhardigital.uol.com.br/noticia/entenda-de-uma-vez-por-todas-o-que-e-um-bot-e-como-ele-funciona/57075> Acesso em: 06.03.17.

47 CGI.br - Comitê Gestor da Internet no Brasil; NIC.br - Núcleo de Informação e Coordenação do Ponto BR (NIC.br). **Cartilha de Segurança da Informação para Internet.** São Paulo, 2012. p. 26.

48 BESSI, Alessandro; FERRARA, Emilio. Social bots distort the 2016 U.S. Presidential election online discussion. **First Monday**, Volume 21, Number 11 - 7 November 2016. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653> Acesso em: 20.03.17.

mentas, os *bots* não só são capazes de propagar uma quantidade inimaginável de informação, no caso *tweets*, como podem ser programados para atuarem como humanos.

Emilio Ferrara, um dos autores dessa pesquisa, em entrevista à MIT Technology Review, afirmou que realizou um teste para verificar a dificuldade em discernir se determinado perfil no Twitter se tratava de um *bot* ou de um humano. De acordo com o pesquisador, alguns *bots* foram facilmente identificados, tendo em vista que produziam cerca de 1.000 *tweets* por hora. Entretanto, outros pareciam que "iam dormir" (ficavam off-line por um longo período de tempo no dia) e *tweetavam* cerca de 5, 10 ou 15 *tweets* em sequência e, depois, nada por horas[49].

Diante dessas peculiaridades apresentadas, os *bots* apresentam três desafios para o uso democrático das redes sociais: primeiro, o poder de influência pode ser redistribuído para diversos perfis/contas que atuam com fins maliciosos; segundo, o debate político pode se tornar mais polarizado; e, por último, facilidade na propagação de notícias falsas[50].

O princípio da transparência

Frank Pasquale, professor da faculdade de Direito da Universidade de Maryland e pesquisador do Projeto sobre Sociedade da Informação da faculdade de Direito da Universidade Yale, em sua obra "*The Black Box Society – The Secret Algorithms That Control Money and Information*", faz um alerta sobre o desequilíbrio das relações quanto à informação e aos dados.

Ao analisar a dinâmica em que se encontra a sociedade contemporânea, observa-se a facilidade com que as empresas privadas e os governos acessam, coletam e tratam os dados dos cidadãos, enquanto as informações daqueles, em sua grande maioria, estão protegidas por leis, sejam essas de ordem concorrencial (segredo industrial) ou por segurança nacional:

> But while powerful businesses, financial institutions, and government agencies hide their actions behind nondisclosure agreements, ´proprietary methods´, and gag rules, our own lives are increasingly open books. Everything we do online is recorded; the only questions left are to whom the

49 BYRNES, Nanette. How the Bot-y Politic Influenced This Election. **MIT Technology Review**. Publicado em: 08 nov. 2016. Disponível em: < https://www.technologyreview.com/s/602817/how-the-bot-y-politic-influenced-this-election/> Acesso em: 06.03.17.

50 BESSI, Alessandro; FERRARA, Emilio. Social bots distort the 2016 U.S. Presidential election online discussion. **First Monday**, Volume 21, Number 11 - 7 November 2016. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653> Acesso em: 20.03.17.

> data will be available, and for how long. Anonymizing software may shield us for a little while, but who knows whether trying to hide isn´t itself the ultimate red flag for watchful authorities? Surveillance cameras, data brokers, sensor netowrks, and ´supercookies´record how fast we drive, whats pills we take, what books we read, what websites we visit. The law, so aggressively protective secrecy in the world of commerce, is increasingly silent when it comes to the privacy of persons[51].

De acordo com o autor, as ferramentas criadas pelas empresas de tecnologia são verdadeiras "caixas pretas" – os indivíduos têm acesso apenas a uma parte de suas funcionalidades, as quais são descritas como "benefícios". Em contrapartida, não há transparência sobre a respectiva infraestrutura e sua real finalidade, principalmente no que se refere ao uso e transferência dos dados coletados.

Em se tratando de dados, a legislação brasileira é fragmentada, ou seja, a matéria é disciplinada por diversas normas, não havendo uma lei específica que defina e regulamente todas as questões relacionadas. Lembra-se que o Brasil passa por uma discussão intensa sobre a aprovação de uma Lei Geral de Proteção de Dados Pessoais, exteriorizada pelo Projeto de Lei nº 5.276/2016.

O Marco Civil da Internet, apesar de não tratar diretamente sobre proteção de dados pessoais, elenca como princípio para o uso da internet no Brasil, em seu artigo 3º, inciso II, a proteção à privacidade. Seu regulamento, o Decreto nº 8.776/2016, prevê, em seus artigos 13 a 16, padrões mínimos para a segurança dos dados dos usuários.

Dentre os pontos que envolvem o debate, pode-se citar o princípio da transparência, o qual está intimamente atrelado ao direito à informação do consumidor, previsto no artigo 6º do Código de Defesa do Consumidor, remetendo, pois, ao alerta do professor Frank Pasquale acerca da coleta e o uso indiscriminado de dados sem que a sociedade tenha o devido conhecimento de funções e finalidades.

Nesse sentido, desde 1990, é desenvolvida a ideia do "*privacy by design*", originada por Ann Cavoukian[52]. Trata-se de um conceito em que a privacidade deve ser incorporada à própria infraestrutura técnica e nos modelos de negócios permitindo que os usuários decidam sobre respectivas configurações.

---

51 PASQUALE, Frank. The Black Box Society – The Secret Algorithms That Control Money and Information. **Harvard University Press**, 2015. p. 03.

52 Ann Cavoukian é ex-comissária de Informação e Privacidade de Ontário – Canadá – atual Diretora Executiva do Instituto de Privacidade e Big Data da Universidade Ryerson. Mais informações disponíveis em: <http://www.ryerson.ca/pbdi/about/people/cavoukian/> Acesso em: 20.03.17.

Sendo assim, o conceito apresenta três pilares: (a) *IT Systems* – sistemas de tecnologia da informação; (b) *Accountable business practices* – práticas de negócios responsáveis; e (c) *Physical design and networked infraestructure* – projeto (*design*) físico e infraestrutura de rede[53].

Ao analisar o ordenamento jurídico americano, observa-se que em 2011 a Federal Trade Comission (FTC) publicou o relatório "*Protecting Consumer Privacy in an Era of Rapid Change",* o qual recomenda o instituto do *privacy by design* como boas práticas, e em 2014 o relatório "*Data Brokers: A Call for Transparency and Accountability*", trazendo à luz a importância do princípio da transparência nas relações que envolvem coleta e uso de dados.

Na União Europeia, é interessante notar que o novo Regulamento nº 679/2016, sobre Proteção de Dados Pessoais (substituição da Diretiva nº 45/96), que entrará em vigor em 2018, faz alusão ao conceito logo de início[54]:

> (7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. **As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores econômicos e as autoridades públicas**.

Transpondo-se ao cenário brasileiro, esclarece-se que o conceito não é tratado pela legislação. Contudo, alguns princípios que regem o *privacy by design,* como segurança, transparência e consentimento aparecem nos artigos 3º, inciso II, e 7º do Marco Civil da Internet, no artigo 13 do Decreto nº 8.771/2016, bem como no artigo 6º do Projeto de Lei nº 5.276/2016.

Esse breve panorama legislativo é de suma importância, tendo em vista que os provedores e as próprias agências de marketing (político ou não) estão coletando e/ou obtendo dados indiscriminadamente. Aliás, podem, de forma indevida, formar parcerias com empresas terceiras viabilizando a transferência de dados sem o consentimento de seus respectivos titulares.

---

53 SEGALA ALVES, Carla; VAINZOF, Rony. Direito Digital: Privacy by Design e Proteção de Dados Pessoais. **Jota**. Publicado em: 06 jul. 2016. Disponível em: <http://jota.uol.com.br/direito-digital-privacy-design-e-protecao-de-dados-pessoais> Acesso em: 20.10.16.

54 SEGALA ALVES, Carla; VAINZOF, Rony. Direito Digital: Privacy by Design e Proteção de Dados Pessoais. **Jota**. Publicado em: 06 jul. 2016. Disponível em: <http://jota.uol.com.br/direito-digital-privacy-design-e-protecao-de-dados-pessoais> Acesso em: 20.10.16.

Como mencionado no tópico anterior, diversas são as ferramentas computacionais que podem influenciar nas decisões e comportamento políticos, sem que os eleitores sequer percebam, a começar pelo uso de seus respectivos históricos de navegação para direcionar determinadas notícias.

Portanto, resta claro que uma Lei Geral de Proteção de Dados é essencial para regulamentar o tratamento de dados pessoais permitindo aos usuários que tenham o prévio conhecimento da ferramenta e sua real finalidade. Sobretudo, garantindo a proteção dessas informações com padrões mínimos de segurança.

Considerações Finais

O debate sobre o impacto do uso da tecnologia nos processos eleitorais tem sido cada vez mais recorrente nas discussões sobre democracia conectada, ou seja, a importância de plataformas digitais para a promoção de uma participação política mais efetiva, desde o acesso às informações, possibilidade de propostas e exercício da cidadania, até o contato direto com os governantes (ou candidatos), a fim de fiscalizar a implementação das propostas sugeridas durante as campanhas ou sugestões para reparar eventuais necessidades urgentes da sociedade.

Neste cenário, as mídias sociais começam a ser consideradas como um espaço público virtual. As rodas de discussões que outrora ocorriam em praças, instituições e quaisquer outros espaços físicos atualmente desenvolvem-se em redes sociais como Facebook e Twitter. Contudo, imperioso entender que, apesar de promoverem um suposto "espaço público", tais provedores são pessoas jurídicas de direito privado, que possuem interesses próprios que, muitas vezes, não estão claros a seus usuários e à sociedade, em geral.

Conforme analisado neste artigo, os meios de comunicação social têm forte poder de influência na formação da opinião pública. De acordo com pesquisas realizadas pela Quartz em parceria com a Mozilla e outra pela Universidade de Stanford, a maioria dos usuários utiliza o Facebook para se informar, porém não têm capacidade cognitiva para filtrar e reconhecer a veracidade e confiabilidade das informações.

A Internet surge com o ideal de propiciar o fluxo de informações e permitir o compartilhamento do conhecimento. Entretanto, essa descentralização se vê ameaçada diante dos interesses privados e da falta de transparência de grandes corporações e provedores que lideram o mercado das redes sociais por possuírem maior capacidade técnica e humana.

As campanhas eleitorais realizadas nos Estados Unidos, no quesito uso de recursos tecnológicos, são totalmente diferentes das utilizadas no Brasil. Con-

tudo, não se pode negar o poder de influência de provedores, como Google e Facebook, em âmbito brasileiro.

Atualmente, o Brasil se encontra em fase de discussão sobre o Projeto de Lei nº 5.276/2016, o qual dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, em conjunto com o Projeto de Lei nº 4.060/2012 e o Projeto de Lei no Senado nº 330/2013, que também versão sobre o tratamento de dados pessoais, com o objetivo de aprovar uma Lei Geral de Proteção de Dados Pessoais.

Trata-se de um debate de suma importância, uma vez que poderá impedir que empresas coletem e usem indiscriminadamente os dados dos usuários e sem o prévio consentimento deles. Os termos de uso e políticas de privacidade devem ser claros; sem termos genéricos que induzam uma dupla interpretação ou que autorizem o uso arbitrário das informações coletadas. O usuário da Internet deve ter a exata ciência sobre o funcionamento das ferramentas de forma a realizar uma escolha consciente ao aceitar os termos de uso de determinada plataforma.

No que tange às eleições, muito há que se pesquisar acerca do tema, visto que a tendência é a de que o uso do *big data* e mecanismos de inteligência artificial sejam cada vez mais incorporados ao cotidiano dos indivíduos. Faz-se necessário refletir sobre o uso enviesado dos mecanismos tecnológicos para fins não democráticos, como, por exemplo, o uso de *bots* para a criação de milhares de perfis falsos e a consequente propagação de notícias inverídicas distorcendo a percepção do eleitorado.

Não menos importante, essencial é o reconhecimento de que nós, usuários, precisamos ter maior consciência, sobretudo no tocante à prévia averiguação das informações recebidas e compartilhadas, a fim de minimizar os efeitos nocivos do uso inadequado das redes.

Os Reflexos do Grande Irmão no Admirável Espelho Novo de *Black Mirror*

Arthur Coelho Bezerra[55]

Introdução

No repertório de possibilidades filosóficas para a literatura de ficção científica, a representação distópica das sociedades destaca-se como um de seus vetores mais criativos. As distopias, às quais escritores e roteiristas de filmes e séries se dedicam desde o século passado, têm seu principal mote forjado na extrapolação de usos perversos das tecnologias por governos, indivíduos (sejam terrestres ou alienígenas) e organizações, mantendo, por via de regra, a ancoragem em suposições cientificamente plausíveis.

Práticas de vigilância e monitoramento de pessoas, para o exercício de algum tipo de controle individual ou social, são comumente descritas em narrativas distópicas, partindo das possibilidades reais e virtuais dos usos das tecnologias de informação e comunicação. É o caso das três obras sobre as quais este texto irá se debruçar: o livro de George Orwell, *1984*, escrito em 1948 e publicado no ano seguinte; o de Aldous Huxley, *Admirável mundo novo*, lançado em 1932; e a série *Black Mirror*, criada por Charlie Brooker e exibida na TV britânica pela primeira vez em dezembro de 2011[56].

A contribuição que o presente texto procura trazer é sociológica; repousa na reflexão sobre as formas contemporâneas de vigilância e controle que, na mencionada literatura das décadas de 1930 e 1940, poderiam ser lidas como alertas para as sociedades futuras, mas que, ao fim e ao cabo, apresentam-se como profecias cumpridas – não apenas nas histórias de *Black Mirror*, mas no

55 Pesquisador do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) e professor do Programa de Pós-graduação em Ciência da Informação (PPGCI/IBICT-UFRJ). É doutor em sociologia pela Universidade do Rio de Janeiro (UFRJ), com pós-doutorado pela mesma instituição.

56 Atualmente, a série conta com 13 episódios — cada um com sua própria história, produção e elenco, distribuídos em três temporadas (2011, 2013 e 2016) incluindo um episódio especial (2014) — e é re-transmitida internacionalmente por canais de TV e pela Netflix, além de estar amplamente disponível para *download* na Internet.

cotidiano da atualidade. Soma-se, portanto, aos esforços dos autores citados para apontar os riscos que tais expedientes representam para a privacidade dos cidadãos, sendo esta entendida como condição básica para a autonomia dos indivíduos e estrutural para o funcionamento de sociedades democráticas.

Admirável Espelho Preto

Três dias antes da estreia na TV inglesa, o produtor e escritor Charlie Brooker publicou um artigo no jornal The Guardian sobre a sua nova série dramática, intitulada *Black Mirror*. O "espelho preto" do título, escreveu Brooker, "é o que você encontrará em cada parede, em cada mesa, na palma de cada mão: a tela fria e brilhante de uma TV, um monitor, um smartphone"[57]. É o mesmo espelho preto que usamos para assistir a série de Brooker e para ler e escrever textos como este, além de manter contato com outras pessoas e realizar um número incomensurável de atividades pessoais e profissionais.

A principal característica técnica dos espelhos pretos que inundam as grandes metrópoles (e cada vez mais as áreas rurais) é a capacidade de serem, ao mesmo tempo e em tempo real, transmissores e receptores de informação. É importante observar que a circulação de textos, imagens e sons em formatos digitais na rede mundial de computadores ocorre, em muitos casos, independentemente do consentimento dos indivíduos ou mesmo da consciência das pessoas sobre os usos que podem ser feitos dessas informações. A famosa foto divulgada em 2016 por Mark Zuckerberg em sua rede social, Facebook, na qual o computador do bilionário da informática aparece com fitas vedando a câmera e o microfone, deveria servir de aviso, bem como a frase do diretor do FBI, James Comey: "Eu coloquei um pedaço de fita sobre a câmera [do computador] porque vi alguém mais esperto do que eu com um pedaço de fita sobre a câmera dele"[58].

---

57 BROOKER, C. Charlie Brooker: the dark side of our gadget addiction. **THE GUARDIAN**. Publicado em: 01 de dezembro 2011. Disponível em: <https://www.theguardian.com/technology/2011/dec/01/charlie-brooker-dark-side-gadget-addiction-black-mirror>. Acesso em: 12 de janeiro de 2017.

58 HERN, A. Mark Zuckerberg tapes over his webcam. Should you? **THE GUARDIAN**. Publicado em: 22 de junho de 2016. Disponível em: <https://www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook>. Acesso em: 12 de janeiro de 2017. Ainda segundo a matéria, a Electronic Frontier Foundation, uma das principais organizações de ativismo pró-privacidade na internet, vende regularmente adesivos para serem colados nas câmeras de *laptops*.

Somadas às denúncias a respeito da vigilância massiva de cidadãos ao redor do mundo que foram feitas pelo ex-funcionário das agências norte-americanas de inteligência (CIA) e de segurança nacional (NSA), Edward Snowden, não parecem restar dúvidas a respeito da possibilidade de acesso remoto às câmeras e microfones que as pessoas possuem em seus ambientes privados e domésticos. Nesse sentido, vale lembrar das características da chamada "teletela" (*telescreen*), aparelho eletrônico imaginado por George Orwell (pseudônimo do escritor inglês Eric Arthur Blair) que, em muitos aspectos, revela-se similar aos atuais "espelhos pretos":

> A teletela recebia e transmitia simultaneamente. Todo som produzido por Winston que ultrapassasse o nível de um sussurro muito discreto seria captado por ela; mas: enquanto Winston permanecesse no campo de visão enquadrado pela placa de metal, além de ouvido também poderia ser visto. Claro, não havia como saber se você estava sendo observado num momento específico. Tentar adivinhar o sistema utilizado pela Polícia das Ideias para conectar-se a cada aparelho individual ou a frequência com que o fazia não passava de especulação. Era possível que ela controlasse todo mundo o tempo todo. Fosse como fosse, uma coisa era certa: tinha meios de conectar-se a seu aparelho sempre que quisesse. Você era obrigado a viver – e vivia, em decorrência do hábito transformado em instinto – acreditando que todo som que fizesse seria ouvido e, se a escuridão não fosse completa, todo movimento examinado meticulosamente[59].

A teletela foi criada por Orwell para uma de suas mais célebres obras, a ficção distópica *1984*, ambientada em uma realidade na qual um único grupo político (o Partido) exerce um rígido controle sobre a conduta dos indivíduos (à exceção dos "proletas", vistos pelo governo como uma classe inofensiva e sem importância). Nesse universo, a teletela orwelliana encarna o principal instrumento técnico de vigilância, partindo de uma perspectiva panóptica – em que os sujeitos assumem que estão sendo vigiados o tempo todo (conforme o modelo arquitetado por Jeremy Bentham[60] no século XVIII para prisões, hospícios, escolas e asilos) – e ampliando-a para as ruas e os ambientes privados. Assim como HAL 9000, o "computador algorítmico heuristicamente programado" do filme *2001: uma odisseia no espaço*, a teletela é capaz de ler lábios e expressões faciais, a ponto de levar o personagem principal da trama, Winston Smith, a compor a própria fisionomia "de modo a ostentar a expressão de tranquilo otimismo

59 ORWELL, G. **1984**. São Paulo: Cia das Letras, 2009, p.13.

60 A mais conhecida e detalhada análise sobre o panoptismo idealizado por Bentham foi feita por Michel Foucault em sua obra Vigiar e Punir.

que convinha ter no rosto sempre que se encarasse a teletela"[61]. Essa tecnologia, imaginada na ficção de Orwell há 70 anos, está atualmente disponível e já vem integrada aos espelhos pretos que possuímos em nossas mesas, paredes e bolsos.

Depois de 1984

O atual uso de equipamentos eletrônicos para a vigilância da população pode ser lido como uma espécie de profecia orwelliana realizada; o mesmo, entretanto, não poderia ser dito em relação ao controle governamental da informação. Em *1984*, o Partido que vigia tudo e todos também é responsável pela construção da História, forjada segundo os fundamentos do *slogan* "quem controla o passado controla o futuro; quem controla o presente controla o passado". Na prática, o controle do passado na obra de Orwell é realizado pelo Ministério da Verdade (responsável por notícias, entretenimento, educação e belas-artes), por meio de funcionários do Departamento de Documentação cuja principal função é reescrever continuamente qualquer fato histórico, retificando documentos sobre os números de previsões governamentais para a economia (de modo a estarem adequados aos resultados de fato) e destruindo narrativas históricas sobre antigos aliados quando estes se tornam inimigos, além do sumiço de qualquer registro sobre pessoas que tenham sido presas, mortas ou desaparecidas em consequência de traição ao governo.

Apesar da habilidade dos atuais Estados e da grande mídia em exercer formas de controle sobre a circulação de informação, a difusão de canais de comunicação digital tornou hercúlea a tarefa de apagar completamente informações que são compartilhadas na internet, como bem sabem os pesquisadores do chamado direito ao esquecimento. Em *Black Mirror*, o primeiro e o último episódio (respectivamente, *The national anthem* e *Hated in the nation*) narram histórias em que os principais chefes de Estado mostram-se indefesos perante a avalanche de *hashtags* que os colocam em situações de chantagem e ameaça de morte. A desesperada sugestão de ambos os líderes de bloquear a circulação de mensagens em redes sociais é descartada por especialistas por se mostrar inviável. Na vida real, mesmo em países que estabelecem rigorosa censura da internet, não raro os usuários encontram formas de estabelecer comunicação. Um bom exemplo foi o serviço "*speak to tweet*", lançado durante os protestos da Primavera Árabe em 2011, que permitiu que mensagens de voz enviadas para um número específico fossem convertidas em postagens no Twitter (durante o

61 ORWELL, G. **1984**. São Paulo: Cia das Letras, 2009, p.15.

bloqueio da plataforma no Egito). A diferença entre os exemplos citados está nos motivos que ensejam a circulação de tais informações: se no caso da Primavera Árabe trata-se, dentre outras coisas, de defender a liberdade de expressão e denunciar atos violentos das autoridades, nas histórias de *Black Mirror* o fluxo de *tweets* é orientado por motivos bem menos altruístas.

The Big Brother Is Watching You

Se, por um lado, a presença das teletelas entre nós nos aproxima de *1984*, um dos fatores decisivos que distanciam a ficção imaginada por Orwell em 1948 da realidade dos dias de hoje é a participação de outros agentes em práticas de monitoramento e invasão de privacidade, que podem envolver motivações políticas e econômicas ou um grande número de fins pessoais, incluindo ações criminais graves como sequestros, chantagens e assassinatos.

Alguns desses temas são retratados em *Black Mirror. The entire history of you*, o último episódio da primeira temporada, apresenta uma realidade em que as pessoas usam, por livre e espontânea vontade, um implante de memória que permite a gravação de todo o registro audiovisual captado pelos olhos e sua posterior reprodução em telas de TV, o que levanta sérias questões sobre privacidade em situações que envolvem ciúmes e desconfianças em relacionamentos amorosos. Em outro episódio (*Shut up and dance*, o terceiro da terceira temporada), a invasão de privacidade ocorre pelo acionamento remoto das câmeras de computadores pessoais, objetivando o acesso a informações comprometedoras para serem usadas como material de chantagem (se ao menos tivessem seguido o conselho de Zuckerberg e vedado a câmera...). Já nos episódios *Nosedive* e *Hated in the nation* – respectivamente, o primeiro e o último da terceira temporada – a má avaliação de indivíduos feita por outras pessoas em redes sociais pode afetar desde o preço de aluguéis residenciais até o acesso a serviços de transporte, chegando a condenar pessoas à morte.

É interessante observar como a realidade de hoje não está muito distante da ficção de *Black Mirror*, especialmente no caso de *Nosedive*, que extrapola as atuais práticas de avaliação de indivíduos expostas nos perfis profissionais no Facebook e nas contas de prestadores de serviços de aplicativos como o Uber. Os órfãos da rede social Orkut, muito popular no Brasil no início do século XXI, devem se lembrar das avaliações que indivíduos faziam uns sobre os outros utilizando cubos de gelo ("*cool*"), *smiley faces* ("*trusty*") e corações ("*sexy*").

Não estando limitadas aos interesses diretos de um governo totalitário, as práticas individuais de vigilância de pessoas sobre outras pessoas em sociedades consideradas democráticas se alastraram através de outros agenciamentos sociotécnicos, que encontram no *voyeurismo* midiático um estímulo para que uns vigiem os outros[62] [63]. Em *Nosedive*, todas as conversas e demais interações pessoais, tradicionalmente inseridas em uma economia invisível de trocas simbólicas, ganham materialidade em um sistema de avaliações instantâneas por celular, que são computadas para gerar notas para cada indivíduo. Como mencionado, as notas afetam não apenas as relações sociais, mas também as possibilidades de acesso a trabalho e a serviços básicos, levando às últimas consequências a perspectiva deleuziana das sociedades de controle, segundo a qual "os indivíduos tornaram-se 'dividuais', divisíveis, e as massas tornaram-se amostras, dados, mercados ou 'bancos'[64] .

As Portas Da Percepção

A distopia orwelliana, como visto, é baseada em uma realidade totalitária com contornos kafkianos, na qual os indivíduos estão submetidos ao controle constante de teletelas e expostos a cartazes com os dizeres "o Grande Irmão está de olho em você". Outro escritor inglês, Aldous Huxley, havia publicado 17 anos antes a obra *Admirável mundo novo* (1932), que apresentava sua própria distopia futurista na qual o adestramento da sociedade seria feito não por violência e lavagem cerebral, mas por meio de hipnose, uso de drogas e seleção biológica em incubadoras.

Pela proximidade temática, geográfica e histórica, as obras de Orwell e Huxley foram objeto de muitas análises literárias, sociológicas e até tema de músicas e histórias em quadrinhos[65]. Na comparação inevitável, muitos autores argumentam que Huxley teria sido mais profético, ou seja, teria imaginado um futuro mais parecido com o que vivemos hoje do que o criado por Orwell. Segundo Neil Postman, "o que Huxley ensina é que, na era da tecnologia avança-

62 LINS, C.; BRUNO, F. Práticas artísticas e estéticas da vigilância. In: **Vigilância e visibilidade: espaço, tecnologia e identificação**. Porto Alegre: Sulina, 2010.

63 CARDOSO, B. **Todos os olhos: videovigilâncias, videovoyeurismos e (re)produção imagética**. Rio de Janeiro: UFRJ / Faperj, 2014.

64 DELEUZE, G. Post-scriptum sobre as sociedades de controle. **Conversações: 1972-1990.** Rio de Janeiro: Ed. 34, 1992. p.222.

65 Baseada em passagens do livro *Amusing ourselves to death*, de Neil Postman, as comparações entre Huxley e Orwell em formato HQ podem ser vistas em: <http://highexistence.com/amusing-ourselves-to-death-huxley-vs-orwell/>. Acesso em: 12 de janeiro de 2017.

da, a devastação espiritual é mais provável de vir de um inimigo com um rosto sorridente do que de um cujo rosto exala suspeita e ódio"[66].

O próprio Huxley, em carta escrita para Orwell pouco após o lançamento de 1984, vaticina, sem recorrer à modéstia:

> Dentro da próxima geração, acredito que os governantes do mundo descobrirão que as hipnoses infantil e narcótica são mais eficientes, como instrumentos do governo, do que clubes e prisões, e que a ânsia de poder pode ser tão completamente satisfeita sugerindo que as pessoas amem sua servidão quanto por açoitá-los e chutá-los em obediência. Em outras palavras, eu sinto que o pesadelo de 1984 está destinado a modular-se rumo ao pesadelo de um mundo que tem mais semelhança com o que eu imaginava em Admirável mundo novo[67].

Ainda segundo Postman, "nos Estados Unidos as profecias de Orwell são de pequena relevância, mas as de Huxley estão bem encaminhadas para serem realizadas" [68]. A distopia orwelliana, nessas análises, parece aproximar-se da realidade de países com regimes considerados menos democráticos, como os encontrados em regiões do oriente médio e do sudeste asiático. No entanto, como faz questão de destacar a pesquisadora norte-americana Rebecca MacKinnon, que atuou como jornalista tanto em países do ocidente quanto do oriente, "todos os governos, de ditaduras a democracias, estão aprendendo rapidamente a usar a tecnologia para defender seus interesses"; segundo MacKinnon, "a internet é um espaço politicamente contestado, dotado de novas e instáveis relações de poder entre governos, cidadãos e empresas. As batalhas de hoje sobre liberdade e controle estão atravessando simultaneamente democracias e ditaduras; através de linhas econômicas, ideológicas e culturais"[69].

O recém falecido sociólogo polonês Zygmunt Bauman, conhecido pela popularização do conceito de "modernidade líquida", também se aventurou a tecer comentários sobre os dois clássicos da literatura. Para Bauman, embora

---

66 POSTMAN, N. **Amusing ourselves to death: public discourse in the age of show business**. New York: Penguin Books, 2006, p.155. Tradução livre.

67 Tradução livre. Imagem e transcrição da carta (no original, em inglês) podem ser encontradas em: <http://www.lettersofnote.com/2012/03/1984-v-brave-new-world.html>. Acesso em: 12 de janeiro de 2017.

68 POSTMAN, N. **Amusing ourselves to death: public discourse in the age of show business**. New York: Penguin Books, 2006. p.156.

69 MACKINNON, R. **Consent of the networked: the worldwide struggle for internet freedom**. New York: Basic Books, 2013. p.5. Tradução livre, grifo da autora.

as visões futuristas de Orwell e Huxley diferissem, a vigilância revelava-se o principal ponto em comum entre as narrativas, conforme destaca:

> O que elas compartilhavam era o pressentimento de um mundo estritamente controlado; da liberdade individual não apenas reduzida a nada ou quase nada, mas agudamente rejeitada por pessoas treinadas a obedecer a ordens e seguir rotinas estabelecidas; de uma pequena elite que manejava todos os cordões – de tal modo que o resto da humanidade poderia passar toda sua vida movendo-se como marionetes (...). Quando Orwell e Huxley esboçaram os contornos do trágico futuro, ambos sentiram que a tragédia do mundo era seu ostensivo e incontrolável progresso rumo à separação entre os cada vez mais poderosos e remotos controladores e o resto, cada vez mais destituído de poder e controlado[70].

Os argumentos apresentados até aqui nos permitem argumentar que, enquanto a profecia orwelliana mostra como governos podem ter acesso e fazer uso das informações das pessoas como forma de controle social, a distopia de Huxley, por sua vez, revela como esse controle pode ser posto em prática através de mecanismos de dominação simbólica. Tal dominação, para o sociólogo francês Pierre Bourdieu[71], encontra no campo cultural a arena mais propícia para a sua realização, naturalizando comportamentos, gostos e valores socialmente construídos.

Considerações Finais

O avanço tecnológico tem trazido muitas facilidades para os usuários da rede de computadores e o acesso a tais benefícios tem feito com que as pessoas julguem (quando de fato fazem esse julgamento) que dar acesso a suas comunicações e demais informações sobre suas "pegadas digitais" parece ser um preço baixo em troca de segurança e comodidade no consumo[72]. Apesar da inestimável contribuição de Snowden para que a humanidade conheça os usos políticos e econômicos de informações pessoais que podem ser feitos por governos, com a ajuda (voluntária ou não) de empresas bilionárias com amplo acesso a dados e comunicações de metade

70 BAUMAN, Z. **Modernidade líquida**. Rio de Janeiro: Jorge Zahar Editores, 2001. p.64-65.

71 BOURDIEU, P. **A distinção: crítica social do julgamento**. São Paulo: EDUSP, 2007.

72 David Lyon, editor do periódico acadêmico *Surveillance & Society*, acredita que, desde os atentados de 11 de setembro de 2001 nos EUA, as pessoas têm estado mais propensas a aceitar práticas de vigilância como o preço a se pagar pela segurança (2010). Discorro melhor sobre esse assunto em BEZERRA, A. C. Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral. In: **Liinc em Revista**, Rio de Janeiro, v.12, n.2, novembro de 2016, p. 231-242.

da população mundial, como Google, Facebook, Microsoft, Apple e muitas outras, os reflexos de tais denúncias na maneira como as pessoas protegem, divulgam e dão acesso a dados pessoais, infelizmente, não podem ser superestimados.

Os avisos de Snowden e a ficção de *Black Mirror* exprimem, com tintas hiper-realistas, a desconfiança com o progresso científico e tecnológico que caracterizou a citada literatura distópica das décadas de 1930 e 1940, quando os grandes centros desenvolvidos do mundo se engajaram em mais uma guerra mundial. Naquela época, o desapontamento das ciências sociais com os ideais iluministas abria as portas para uma série de críticas reunidas sob o rótulo de "pós-modernidade" – que pode ser melhor entendido como uma forma de descrédito quanto às pretensões modernistas do que como um prenúncio de uma nova era. Em posfácio de 1961 escrito para o livro de Orwell, Eric Fromm comenta: "as utopias negativas expressam o sentimento de impotência e desesperança do homem moderno, assim como as utopias antigas expressavam o sentimento de autoconfiança e esperança do homem pós-medieval. Não poderia haver nada mais paradoxal em termos históricos do que essa mudança"[73].

Orwell faleceu poucos meses após a publicação de *1984*, vitimado pela tuberculose aos 47 anos. Diversos termos criados por ele para o livro se popularizaram, sendo "Big Brother" o mais conhecido por conta do homônimo programa de TV, originalmente transmitido na Holanda em 1999 e posteriormente franqueado a mais de 50 países (no Brasil, é transmitido há 15 anos ininterruptos). Embora o apresentador da edição brasileira refira-se aos participantes como "brothers", o Grande Irmão da atualidade não é apenas quem é vigiado, mas também quem vigia; como o Big Brother orwelliano, os espectadores é que estão "de olho", interessados em "dar uma espiadinha" na privacidade dos confinados. De acordo com Postman, "na profecia huxleyana, o Big Brother não nos observa, por sua escolha. Nós o observamos, pela nossa"[74].

A defesa da privacidade nos dias atuais, portanto, passa não apenas por leis que exijam a prestação de contas (*accountability*) de governos e empresas sobre o uso de dados pessoais dos indivíduos, e tampouco se resume a mecanismos técnicos de proteção de tais dados: seria necessária, também, uma mudança na cultura *voyeur* que, alimentada por sentimentos como ódio, intolerância e sadismo, ajuda, por exemplo, a fazer com que eleitores da maior potência mundial escolham, para presidente, uma figura histriônica e intolerante (que, aliás, muito

73 ORWELL, G. **1984**. São Paulo: Cia das Letras, 2009, p.369.

74 POSTMAN, N. **Amusing ourselves to death: public discourse in the age of show business**. New York: Penguin Books, 2006, p.155.

se assemelha ao personagem *Waldo* de *Black Mirror*). Concordamos com Julian Assange[75] que, no tocante à vigilância que ocorre nas redes digitais, a dimensão cultural é mais difícil de ser alterada do que as leis do homem (com legislação que proteja a privacidade) ou da física (com técnicas como a criptografia). Nesse sentido, para evitar a realização das demais profecias da série, é preciso que haja o reconhecimento de que é nas interações pessoais em redes sociais digitais que são ventilados os valores dos espectadores dos episódios *Hated in the nation* e *The national anthem*. Esse é o primeiro passo para vislumbrar um futuro no qual a sociedade não se torne o White Bear Justice Park de *Black Mirror*, em que a vontade de justiça é substituída por uma sádica sede de vingança.

75 ASSANGE, J. *et. al*.. **Cypherpunks: liberdade e o futuro na internet**. São Paulo: Boitempo, 2013.

Genomics e Privacidade dos Dados Pessoais Genéticos

Cláudio R. Barbosa[76]

Introdução

A coleta e a manipulação de informações genéticas crescem exponencialmente em virtude dos avanços extraordinários das técnicas de sequenciamento dos genomas individuais e redução dos custos envolvidos no tratamento de gigantesca quantidade de dados. Como comparação, se o custo inicial do primeiro completo sequenciamento do genoma humano exigiu aproximadamente três bilhões de dólares, ao longo de uma década, sob a coordenação de quase duas dezenas de instituições de pesquisa, hoje várias empresas investem em técnicas para acelerar e reduzir o custo desse sequenciamento. Basta dizer que a barreira de US$ 1.000,00 para o sequenciamento de um genoma humano foi quebrada em 2014.

Paralelamente à significativa redução de custos do sequenciamento, o aumento da capacidade geral de armazenamento em rede e do poder de processamento de informações genéticas também aumentaram significativamente. Esta nova capacidade permite diversos cruzamentos de fenótipos e genótipos e a identificação individual e prévia de enorme quantidade de doenças, com o que pode ser considerada uma nova medicina individualizada fundamentada em predisposições genéticas individuais.

É sintomático que paralelamente ao Projeto Genoma foi aprovada pela UNESCO a "Declaração Internacional sobre os Dados Genéticos Humanos", ampliando a Declaração Universal sobre o Genoma Humano e os Direitos Humanos de 1997[77], com particular destaque para a natureza sensível dos dados

---

76 Advogado. Sócio de Kasznar Leonardos. Técnico em Informática Industrial. Graduado pela Faculdade de Direito da Universidade de São Paulo (USP) com especialização em direito empresarial. Mestre em Propriedade Intelectual pela The George Washington University (GWU). Mestre em Direito Internacional e Doutor em Direito Comercial pela Universidade de São Paulo (USP). O autor agradece comentários e sugestões de Marcela Mattiuzzo, Aline Ferreira de Carvalho Silva e Priscila Mayumi Kashiwabara.

77 UNESCO. Declaração Internacional sobre os Dados Genéticos Humanos. 2004. Disponível em: <http://bvsms.saude.gov.br/bvs/publicacoes/declaracao_inter_dados_genericos.pdf>. Acesso em: 23.03.17.

genéticos e a indeterminação do impacto futuro da coleta destes dados no titular e na comunidade[78]. Cabe ainda ressaltar que já em 1996 o Congresso norte-americano aprovou uma legislação conhecida como HIPAA[79], a qual determinava a confidencialidade dos dados médicos com a eficácia das regras de privacidade a partir de abril de 2003.

Superado o fundamento técnico, a aceitação internacional sob o prisma ético e político, o avanço no tratamento de informações genéticas levanta questões jurídicas relativas à manipulação destes dados e à privacidade dos participantes[80]. Além da titularidade, o incremento do volume de coleta e manipulação leva ainda à discussão sobre em quais situações poderá ocorrer uma efetiva manipulação das informações genéticas, independentemente das informações estarem mantidas em substrato biológico ou codificadas em um banco de dados[81] sem uma autorização adicional.

A proteção aos dados pessoais antecede a explosão de informações e a administração de gigantescas quantidades de dados, porém é óbvio que a integração digital e a facilidade com que as informações circulam na internet levou a questão dos dados pessoais a um novo patamar. Eis um ponto pragmático: as evoluções terapêutica e de pesquisa baseadas em dados genéticos somente podem ser alcançadas com uma grande base de dados. Nesse sentido, a confiança do paciente na segurança e proteção dos dados é fundamental.

Com esse pano de fundo, investigar-se-á as intersecções entre limites jurídicos e técnicos da proteção aos dados pessoais, qual a orientação normativa que se apresenta, a viabilidade e percalços, traçando um panorama do impacto dos problemas peculiares trazidos pela proteção dos dados pessoais genéticos arquivados em sistemas de informação o que tem sido considerado parte essencial da área denominada como *genomics*, área da ciência que estuda todos os genes (genomas) incluindo a interação desses genes entre si e entre o ambiente no qual o genoma se insere, o que exige uma grande utilização de bases de da-

78 Sobre o impacto da utilização de dados sensíveis, cf. a decisão europeia. Tribunal de Justiça. Caso C—101/01 Bodil Lindqvist [2003] ECR I-12971 de 6 de novembro de 2003.

79 The Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, 110 Stat. 1936, aprovada em 21 de Agosto de 1996.

80 BOHANNON, John. Genealogy databases enable naming of anonymous DNA donors. **Science**, vol. 339, n. 6117, jan. 2013, p. 262.

81 Cabe ressaltar que neste caso deve-se equiparar aos dados genéticos a neutralidade do suporte físico quando se discute direitos autorais e, obviamente, a informação genética mantida em substrato não tem – pela dificuldade de manipulação, custo e volume de armazenamento – o potencial de impacto das bases de dados genéticas.

dos e tratamento informatizado dos mesmos. Em outras palavras, *genomics* se refere ao estudo de sequências e à análise de genomas, enquanto que a genética se preocupa com o estudo das funções dos genes, ainda que também possa se preocupar com processos genéticos (p.ex. interação entre *loci* – locais – e alelos), mas sempre voltado ao genoma como um todo[82].

Dados pessoais genéticos

A proteção aos dados pessoais, ainda que não tenha a mesma envergadura da legislação de outros países, não é uma novidade no direito nacional. A Constituição Federal já em 1988 reconheceu direitos e garantias específicas relativos aos dados pessoais como o princípio da dignidade humana, a proteção aos direitos da personalidade, amparando o direito à liberdade de expressão, o direito à informação, a inviolabilidade da vida privada e da intimidade, a garantia do *Habeas Data*, entre várias garantias à privacidade e à intimidade[83].

Sem adentrar outras normas aplicáveis, o Código Civil ampliou também o reconhecimento e a proteção aos direitos da personalidade, à privacidade e à intimidade. Mais recentemente, o Marco Civil da Internet[84] incorporou como princípio da internet no Brasil a proteção aos dados pessoais[85], destacando que é exigido o consentimento (livre, expresso e informado) do titular de dados pessoais para o fornecimento a terceiros de dados pessoais, incluindo registros de conexão e de acesso a aplicações de internet.

Também é assegurado ao titular de dados pessoais a prestação de:

> informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais, que somente poderão ser utilizados para finalidades que (a) justifiquem sua coleta; (b) não sejam vedadas pela legislação; e (c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet[86].

---

82 Cf. GREELY, Henry T. Ethical issues in Genomics. **International Encyclopedia of the social & behavioral sciences**. 2nd edition, vol. 10. Elsevier, 2015, p. 32. Disponível em: <http://dx.doi.org/10.1016/B978-0-08-097086-8.82011-5>. Acesso em: 23.03.17.

83 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

84 Lei nº 12.965/14. Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: III - proteção dos dados pessoais, na forma da lei.

85 Atualmente, está em trâmite o Projeto de Lei nº 5.276/2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 23.02.17.

86 Lei nº 12.965/2014. Art. 7º, incisos VIII, IX e X.

Além do consentimento expresso para a coleta, bem como a possibilidade de exclusão destes dados.

O uso de dados pessoais genéticos exige claro consentimento do titular e deve submeter-se a todos os requisitos gerais. Tais dados, contudo, pertencem a uma categoria especial: os chamados dados pessoais sensíveis, cujo uso se sujeita a condições mais rígidas e que podem exigir a desvinculação de seu titular. Segundo projeto de lei em discussão [87], são dados pessoais sensíveis aqueles ligados à origem racial ou étnica, referentes à saúde, ou à vida sexual, dados genéticos e biométricos, entre outros. Como apontado na Declaração da UNESCO, estes dados:

> podem indicar predisposições genéticas dos indivíduos e que essa capacidade indicativa pode ser mais ampla do que sugerem as avaliações feitas no momento em que os dados são recolhidos; que esses dados podem ter um impacto significativo sobre a família, incluindo a descendência, ao longo de várias gerações, e em certos casos sobre todo o grupo envolvido[88].

O projeto de lei em discussão prevê requisitos adicionais ao consentimento necessário para o tratamento de dados pessoais sensíveis, ainda que esteja mantida a possibilidade de tratamento destes dados, sem consentimento, para algumas hipóteses previamente definidas[89] cabendo destacar que algumas atividades são excepcionadas, recomendando-se expressamente nesses casos a anonimização dos dados, ou seja, a tentativa de eliminar o vínculo da informação com seu titular por meio da supressão de elementos de identificação, adoção de filtros, técnicas criptográficas, ou outros procedimentos que mascarem a vinculação da informação ao titular dos dados pessoais.

A anonimização é um aspecto definido pelo projeto de lei, que considera dados anonimizados como "dados relativos a um titular que não possa ser identificado". Define, ainda, o processo de anonimização como o "procedimento por meio do qual um dado deixa de poder ser associado, direta ou indiretamente, a um indivíduo". Se o dado pessoal é anonimizado, ele perde sua característica "pes-

87 O PL nº 5.276/2017 determina em seu artigo 11 ("Art. 11. É vedado o tratamento de dados pessoais sensíveis, exceto: I – com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular: (...) II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de uma obrigação legal pelo responsável; b) tratamento e uso compartilhado de dados necessários à execução, pela administração pública de políticas públicas previstas em leis ou regulamentos; c) realização de pesquisa histórica, científica ou estatística, garantida sempre que possível, a anonimização dos dados pessoais sensíveis; (...)").

88 Id. n. 1 *supra*. p. 3.

89 Cf. n. 9 *supra*.

soal" e pode ser utilizado livremente. Se existir dúvida sobre a possibilidade de anonimização, o projeto garante que "os dados anonimizados serão considerados dados pessoais (...) quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido"[90].

Por sua carga ética, pelo absoluto caráter pessoal e por intrinsecamente serem identificadores biológicos, além de serem dados sensíveis, os dados genéticos dificilmente podem ser completamente anonimizados. A comissão de trabalho que discutiu os aspectos de anonimização na União Europeia[91] aponta que a simples remoção de dados específicos é um padrão de anonimização insuficiente ao caso concreto, pois geralmente a simples combinação de dois elementos externos (podendo ser outra base de dados ou outra fonte de informação) permite a individualização do titular previamente anonimizado.

Em resumo, ao mesmo tempo em que os dados pessoais genéticos são sensíveis, existem exceções amplas para sua utilização sem consentimento e, ao mesmo tempo, pela própria natureza dos dados genéticos, o risco de reidentificação é muito alto. Dessa forma, conclui-se que a proteção concedida aos dados pessoais tem eficácia limitada quanto à privacidade que pode ser garantida ao titular dos dados pessoais genéticos. Se a privacidade não pode ser garantida completamente, permanece a investigação quanto a eventuais outros componentes da informação genética.

Titularidade de informações genéticas

Tendo sido abordados a importância e o objeto, convém endereçar a discussão sobre quem controla a informação genética. Os dados pessoais genéticos são informações essencialmente vinculadas ao seu titular e nenhuma outra informação poderia ser mais pessoal para caracterizar biologicamente um ser vivo. Ainda que o ambiente, a história, os relacionamentos e tudo o que vivenciou uma pessoa possam ser considerados para caracterizar e definir uma

90 Cf. n. 7 *supra*. Artigo 13.

91 UE. Opinion 05/2014 on Anonymization Techniques. Adotada em 10 de abril de 2014. Disponível em: <http://www.cnpd.public.lu/de/publications/groupe-art29/wp216_en.pdf> Acesso em: 23.03.17 ("Genetic data profiles are an example of personal data that can be at risk of identification if the sole technique used is the removal of the identity of the donor due to the unique nature of certain profiles. It has already been shown in the literature that the combination of publically available genetic resources (e.g. genealogy registers, obituary, results of search engine queries) and the metadata about DNA donors (time of donation, age, place of residence) can reveal the identity of certain individuals even if that DNA was donated "anonymously".").

pessoa; ainda que pessoas com a mesma carga genética – gêmeos univitelinos, por exemplo[92] – possam ser únicos em seu contexto psicológico e social, as informações genéticas (idênticas e compartilhadas) fazem parte da personalidade de uma pessoa[93], sob o prisma jurídico, ético e, por que não dizer, natural.

Juridicamente, ainda que todos os dados pessoais possam ser caracterizados como direito de personalidade, existe uma questão essencial entre os dados genéticos e os demais dados pessoais ligada à dificuldade de anonimização e, ainda, à dificuldade de aferir que determinado dado genético é essencialmente de um determinado indivíduo, de uma família, ou de uma comunidade ainda maior. Nesse aspecto, titularidade, individualidade e anonimização passam a ser facetas e partes de uma mesma questão. Se existe um valor associado a esse dado genético, além da privacidade, outros interesses passam a estar associados.

Sob um determinado prisma, a possibilidade (e o poder) de decisão sobre material genético passou a ser objeto de discussões jurídicas com o desenvolvimento das fertilizações *in vitro* e o avanço das técnicas de conservação de óvulos, embriões e espermatozoides, adotando-se a visão que o material genético preservado não poderia ser considerado um indivíduo nem tampouco uma coisa

92 SCHILIT, S.L.; SCHILIT, Nitenson, A. My identical twin sequenced our genome. **Journal of Genetic Counsel**. 2016. Disponível em: <doi:10.1007/s10897-016-0046-7>. Acesso em: 23.03.17. Cf. também: AYUSO, C.; MILLAN, J. M.; MANCHENO, M. & DAL-RE, R. Informed consent for whole-genome sequencing studies in the clinical setting. Proposed recommendations on essential content and process. **European Journal of Human Genetics**, 21(10), p. 1054-1059, 2013. Disponível em: <doi:10.1038/ejhg.2012.297>. Acesso em: 23.03.17. Além da identidade genética de gêmeos, populações isoladas (e.g. Islândia) também proporcionam uma uniformidade genética não encontrada em outros locais.

93 A Constituição Federal garante esta proteção ("Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"), o que também é contemplado no artigo 21 do Código Civil e na Lei de Acesso à Informação (Lei nº 12.527/2011). Cf. SOUZA, Capelo de. **O Direito Geral de Personalidade**. Coimbra Editora, 1995, p.318. ("não só o respeito a intimidade da vida privada, em particular a intimidade pessoal, familiar, doméstica, sentimental e sexual e inclusivamente os respectivos acontecimentos e trajetórias, mas ainda o respeito a outras camadas intermédias e periféricas da vida privada, como as reservas de domicílio e de lugares adjacentes, da correspondência e de outros meios da comunicação privada, dos dados pessoais informatizáveis, dos lazeres, dos rendimentos patrimoniais e de demais elementos privados da actividade profissional e econômica, bem como também, last but not the least, a própria reserva sobre a individualidade privada do homem no seu ser para si mesmo ...").

sobre a qual existiria propriedade, devendo ser tratado sob condição especial, sob tutela e decisão das pessoas das quais foram originados[94].

Ao tratar da possibilidade de manipulação das células-troncos, o STF enfrentou questão paralela, decidindo o Min. Carlos Britto que indivíduos seriam apenas as pessoas físicas que sobreviveram ao parto, dotadas de personalidade civil, assentando que a Constituição Federal, quando se refere à "dignidade da pessoa humana", aos "direitos da pessoa humana", ao "livre exercício dos direitos... individuais" e aos "direitos e garantias individuais", estaria falando de direitos e garantias do indivíduo já nascido. A Constituição Federal, portanto, na decisão do STF, limita a consideração de viva à pessoa humana "nativiva". Como consequência, a inviolabilidade do artigo 5º da Carta diz respeito exclusivamente ao indivíduo personalizado[95].

Tal limitação não é exclusiva do sistema jurídico brasileiro. Conhecida decisão nesta área foi a do caso *Davis v. Davis* de 1992[96] na qual a Suprema Corte do Tennessee decidiu que embriões preservados deveriam ser destruídos a pedido de uma das pessoas doadoras, em detrimento do desejo da outra que também contribuiu. A decisão estabeleceu que a vontade prévia das partes em eventual acordo deveria ser preservada e, em sua ausência, deveria ser privilegiada a vontade da parte em evitar qualquer utilização do material genético.

Abordagem diversa da questão, mais orientada na titularidade de dados genéticos, surgiu em decisão da Suprema Corte da Califórnia[97] . John Moore, um paciente, descobriu que seu médico tinha utilizado seu material genético para criar células posteriormente comercializadas para pesquisa de câncer. Em que pese o fato de Moore não ter obtido sucesso em decorrência de questões particulares de seu caso, a decisão levou ao reconhecimento do direito sobre informações genéticas de suas células.

Tais decisões apontam um caminho, mas esbarram em uma dificuldade conceitual ligada ao questionamento da possibilidade de existir um direito exclusivo sobre as próprias células, sobre as informações genéticas e, finalmente,

---

94 SHARPO, Helene S. Matters of Life and Death: Inheritance Consequences of Reproductive Technologies. **Hofstra Law Review**, Vol. 25, Iss. 4, Article 3, 1997. Disponível em: <http://scholarlycommons.law.hofstra.edu/hlr/vol25/iss4/3>. Acesso em: 23.03.17.

95 STF. ADI 3510/DF, Rel. Min. Carlos Britto, 28 e 29.5.2008.

96 Davis v. Davis, 842 S.W.2d 588, 594-97 (Tenn. 1992). Ver também: Chapman, Jennifer E., Zhang, Mark, Davis v. Davis (1992). Embryo Project Encyclopedia (2013-10-17). Disponível em: <http://embryo.asu.edu/handle/10776/6320>. Acesso em: 23.03.17.

97 Moore v. Regents of the University of California (51 Cal. 3d 120; 271 Cal. Rptr. 146; 793 P.2d 479).

sobre a utilização das informações genéticas por terceiros. Em uma extrapolação, este questionamento pode levar a discussões sobre a perpetuação deste direito pela sucessão de titularidade e o impacto econômico desta utilização, seja no âmbito patrimonial seja no impacto ao domínio público[98].

Símbolo maior da possibilidade de utilização permanente de informações genéticas mantidas em suporte biológico e como informação é Henrietta Lacks, norte-americana, afrodescendente que, diagnosticada com um tumor cervical, teve amostras de tecidos retirados durante seu tratamento, sem seu conhecimento, no Johns Hopkins Hospital, e fornecidas à equipe do Dr. George Otto Gey. Gey, então, demonstrou que as células cancerígenas multiplicavam-se em curto intervalo de tempo, mesmo fora do corpo, tornando-se imortais quando cultivadas em condições adequadas. Estas células imortais são hoje denominadas HeLa e têm sido utilizadas em várias pesquisas que permitiram a produção de inúmeros medicamentos biológicos e milhares de trabalhos científicos[99].

Não existe dúvida de que a utilização das células de Henrietta Lacks sem seu consentimento é uma ofensa à visão atual de que todo acesso à informação privada exige um consentimento livre, informado e inequívoco. Em outras palavras, nas esferas ética, jurídica, nacional e internacional, existe uma imposição negativa à coletividade, proibindo o acesso não autorizado aos dados pessoais, protegendo-se as manifestações da personalidade. A preocupação na privacidade dos dados genéticos é demonstrada pela própria família de Henrietta Lacks, particularmente quando considera a exposição destes dados no tempo:

> One of the often voiced concerns regarding genomic data is its potential for discrimination. While, today, certain genome-disease and genome-trait associations are known, we do not know what will be inferred from one's genomic

98 BOYLE, James. **A politics of intellectual property: environmentalism for the net?** Duke L.J., vol. 47, p. 87. ("It is intellectual property, not the regulation of cybersmut, that provides the key to the distribution of wealth, power, and access in the information society. The intellectual property regime could make or break the *educational, political, scientific, and cultural promise of the Net. Indeed, even if our only concern was censorship, it would be perverse to concentrate exclusively on the actions of governments. The digital world gives new salience to private censorship - the control by intellectual property holders of distribution of and access to information. [...] In terms of ideology and rhetorical structure, no less than practical economic effect, intellectual property is the legal form of the information age. It is the locus of the most important decisions in information policy. It profoundly affects the distribution of political and economic power in the digital environment. It impacts issues ranging from education to free speech. The "value" protected (and in a sense created) by intellectual property in the world economy is in the hundreds of billions of dollars and growing all the time.*").

99 SKLOOT, Rebecca. **A vida imortal de Henrietta Lacks**. Trad. Ivo Korytowski. Companhia das Letras: São Paulo, 2011.

> data in the future. In fact, a grandson of Henrietta Lacks expressed his concern about the public availability of his grandmother's genome by saying that "the main issue was the privacy concern and what information in the future might be revealed". Therefore, it is likely that the privacy-sensitivity of genomic data, and thus the potential threats will increase over time[100].

O exclusivo que se origina dos direitos de personalidade não é absoluto. Existe um potencial conflito entre visões privadas e públicas dos direitos da personalidade que sempre acaba sendo exemplificado pelos diversos interesses envolvidos. No episódio de Henrietta Lacks, existe uma tensão entre os direitos de personalidade (que exigem uma conduta negativa de terceiros) e liberdades públicas garantidas constitucionalmente, que particularmente sustentam os direitos de informação e utilização do conhecimento[101].

Os dados pessoais genéticos potencializam mais esta discussão ao tratar parte do próprio indivíduo como informação e potencial de cura própria e de terceiros, ao contrário de criações intelectuais, ou direitos de imagem, habitualmente informações de cunho pessoal e privado. Como elemento complicador, existe o aspecto dos dados genéticos serem compartilhados com sua família, ou seja, são ainda menos exclusivos do que a biografia de um indivíduo e, como forma de incrementar a análise, pode-se partir para a controvérsia da necessidade de autorização das obras biográficas: uma discussão do direito de personalidade que trata das informações sociais, históricas e culturais[102].

Limitações aos direitos da personalidade: informação e saúde

Superada a questão da caracterização como sensível e a necessidade de consentimento, cabe discutir um aspecto teleológico: a importância das informações genéticas, pois o efeito negativo vinculado à titularidade dos dados, ou seja, o direito de impedir terceiros, não é (e tampouco pode ser) um direito absoluto. A

---

100 NAVEED, Muhammad. **Privacy in the genomic era**. Disponível em <https://arxiv.org/pdf/1405.1891.pdf>. Acesso em: 23.03.17.

101 CARVALHO NETO, Inácio de. **Curso de Direito Civil: parte geral**. São Paulo: Atlas, 2006. p. 126. ("os direitos da personalidade são estudados sob a ótica do direito privado, considerados como a garantia mínima da pessoa humana para as suas atividades internas e para as suas projeções ou exteriorizações para a sociedade. Para isso, impõem à coletividade uma conduta negativa, evitando embaraço ao seu exercício. Já as liberdades públicas são condutas individuais ou coletivas realizadas de forma autodeterminada, em face de autorização expressa ou implícita, conferida pelo Estado [...]").

102 Cf. n. 12 *supra*.

possibilidade de utilização por terceiros das informações que compõem a biografia de uma pessoa, dados históricos, pessoais e biográficos, foi discutida com grande destaque recentemente e pode ser usada como paralelo aos dados genéticos.

A controvérsia relativa à limitação dos direitos de personalidade tem origem com a ação proposta por Roberto Carlos visando proibir a circulação da biografia "Roberto Carlos em Detalhes", obra de autoria de Paulo César Araújo, lançada e posteriormente recolhida após decisão determinando a necessidade de autorização prévia do biografado[103]. Como contraponto, o escritor Paulo Coelho criticou, em artigo dirigido a Roberto Carlos, a proibição afirmando estar "extremamente chocado com sua atitude infantil, como se grande parte das coisas que li na imprensa justificando a razão da 'invasão de privacidade' já não fosse mais do que conhecida por todos os seus fãs."[104]. A reação levou a Associação Nacional de Editores de Livros ("Anel") a ajuizar, no Supremo Tribunal Federal, em 2012, ação para permitir a publicação de biografias sem autorização do biografado[105].

A decisão do STF, extensa e bem fundamentada, demonstra a necessidade de ponderação entre os direitos em discussão, com especial enfoque no voto da relatora afirmando que:

---

103 "A biografia de uma pessoa narra fatos pessoais, íntimos, que se relacionam com o seu nome, imagem e intimidade e outros aspectos dos direitos da personalidade. , interpretação que se extrai do art. 5º, inciso X, da Constituição da República, o qual dispõe serem invioláveis a intimidade, a vida privada e a imagem das pessoas. No mesmo sentido e de maneira mais específica, o art. 20, caput, do Código Civil/02, é claro ao afirmar que a publicação de obra concernente a fatos da intimidade da pessoa deve ser precedida da sua autorização, podendo, na sua falta, ser proibida se tiver idoneidade para causar prejuízo à sua honra, boa fama ou respeitabilidade". (Grifou-se). Processo nº 2007.001.006607-2, 20ª Vara Cível do Rio de Janeiro, Juiz Maurício Chaves de Souza Lima, julgado em 24.04.2008. Como decisões anteriores, cabe citar decisão judicial que proibiu exibições públicas do filme "Di", no qual o cineasta Glauber Rocha registra o enterro do seu amigo o artista plástico Emiliano Di Cavalcanti. A proibição foi solicitada por Elizabeth Di Cavalcanti, filha do artista, que considerou profanatória a atitude do cineasta no enterro de seu pai e a obra que dali resultou. Cf. GNASPINI, José Mauro; MACHADO JR., Rubens L. R**. Di-Glauber: filme como funeral reprodutível**. Dissertação de Mestrado. ECA USP. 2003.[s.n.], São Paulo, 2003.

104 COELHO, Paulo. O que é "contexto desfavorável"? **Folha de São Paulo.** 2 de maio de 2007. Disponível em: <http://www1.folha.uol.com.br/fsp/opiniao/fz0205200708.htm>. Acesso em: 23.03.17.

105 "O Tribunal, por unanimidade e nos termos do voto da Relatora, julgou procedente o pedido formulado na ação direta para dar interpretação conforme à Constituição aos artigos 20 e 21 do Código Civil, sem redução de texto, para, em consonância com os direitos fundamentais à liberdade de pensamento e de sua expressão, de criação artística, produção científica, declarar inexigível o consentimento de pessoa biografada relativamente a obras biográficas literárias ou audiovisuais, sendo por igual desnecessária autorização de pessoas retratadas como coadjuvantes (ou de seus familiares, em caso de pessoas falecidas)." STF, ADI 4815-DF, Rel. Min. Cármen Lúcia, DJU 01.02.2016. Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoPeca.asp?id=308558531&tipoApp=.pdf>. Acesso em: 23.03.17.

> [n]ão se admite, na Constituição da República, sob o argumento de se ter direito a manter trancada a sua porta, se invadido o seu espaço, abolir-se o direito à liberdade do outro. No caso do escrito, proibindo-se, recolhendo-lhe a obra, impedindo-se a circulação, calando-se não apenas a palavra do outro, mas amordaçando-se a história. Pois a história humana faz-se de histórias dos humanos, ou seja, de todos nós[106].

Antecipando a ligação com a proteção dos dados pessoais, o voto da Min. Rosa Weber citou o artigo clássico[107] de Samuel Warren com expressa menção à proteção de dados pessoais em redes sociais como um dos grandes desafios futuros. Destacou-se que:

> [n]o caso do direito à privacidade, vale observar, ainda, que os seus maiores desafios contemporâneos nada tem a ver com a imposição de restrições à liberdade de manifestação, relacionados que são aos imperativos da segurança nacional e da eficiência do Estado, à proliferação de sistemas de vigilância e à emergência das mídias sociais, juntamente com a manipulação de dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados[108].

Assim, como a informação é um direito público que pode constitucionalmente sobrepor-se a um direito de personalidade, parece ser claro que o tratamento de dados pessoais genéticos poderá ser excepcionado se o mesmo estiver relacionado a um valor superior como, por exemplo, a solução de saúde individual ou pública.

Essa limitação está refletida no Projeto de Lei de Proteção de Dados Pessoais em discussão[109] quando o artigo 7º determina em seus incisos IV, VII e VIII que o tratamento de dados pessoais é permitido para pesquisa científica, para a proteção da vida ou da incolumidade física do titular ou de terceiros e, ainda, para a tutela da saúde[110]. Tais limitações estão alinhadas à nova regulamentação de dados pessoais que entrará em vigor na União Europeia[111], especialmen-

---

106 Id.

107 WARREN, Samuel D.; BRANDEIS, Luis D. The right to privacy. **Harvard Law Review**, Vol. IV, December 15, 1890. Sobre a origem e critérios adotados no Reino Unido, cf. Prince Albert v Strange (1849), in: Mitchell, Charles/Mitchell, Paul Mitchell (Ed.), Landmark Cases in Equity 2012, p.235–267

108 Id. n. 23 *supra*.

109 Id. n. 9 *supra*.

110 Id.

111 BBMRC-ERIC: **Biobanking and biomolecular resources research infrastructure**. The EU General Data Protection Regulation. May 1st 2016. p. 5. ("Biobanks could be exempted from a number of the

te com fundamento no artigo 89(1) do Regulamento (EU) 2016/679 ("GDRP – General Data Protection Regulation") [112].

A exceção trazida pelo legislador, tanto na norma europeia, quanto no projeto nacional, demonstra a necessidade de flexibilização na identificação das hipóteses em que a regra geral deverá ser limitada. Demonstra-se com isto a impossibilidade de se prever todas as exceções (como ocorre, por exemplo, no artigo 46 da Lei nº 9.610/98, que trata das exceções aos direitos autorais) e harmoniza-se com jurisprudência que tem utilizado a decisão do STF na ADI 4815 como base. É o exemplo do acórdão da Apelação Cível nº 0072597-41.2012.8.26.0100, representando decisão do Tribunal de Justiça de São Paulo em que foi considerada que a exibição de imagem na internet, obtida em evento público, poderia ser utilizada sem autorização expressa da pessoa retratada na imagem, considerando-se os fatos concretos.

Percebe-se, portanto que a exceção para fins de investigação científica prevista no Regulamento da União Europeia não tem exatamente a mesma orientação teleológica que o projeto de lei brasileiro, mas permite uma flexibilização não prevista nos projetos iniciais. Como ponto complementar, o próprio texto que permite a utilização de dados para fins de pesquisa traz uma inovação adicional que é a contrapartida técnica para balancear o risco acessório trazido pela exceção. Se existe a possibilidade de acréscimo de risco com a utilização dos dados pessoais genéticos para fins de pesquisa, o texto normativo exige medidas técnicas adicionais visando atingir (e garantir) a privacidade.

GDPR's general principles, obligations and data subject rights, as, if and when processing personal data for the purpose of scientific research purposes. For example, as a modification of the data storage limitation principle, personal data can be stored for longer periods provided that they will be processed solely for scientific research purposes in accordance with the provisions of article 89(1) of the GDPR and subject to implementation of technical and organisational measures required by the GDPR. Also, the GDPR retains the presumption of compatibility of use for research purposes, thereby enabling further data processing for scientific research purposes of personal data initially processed for a different purpose, provided that a valid legal ground for such initial processing in EU or Member States law exists.").

112 Regulamento (EU) 2016/679 (GDRP – General Data Protection Regulation). Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Acesso em: 23.03.17. ("Artigo 89. Garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos. 1. O tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo. (...)").

Alternativas às proteções puramente jurídicas aos dados pessoais genéticos

Como previsto pelo grupo de trabalho da União Europeia[113], não foi necessário um grande tempo para que a utilização de elementos adicionais permitisse a reidentificação de um banco de dados genético anonimizado. Em 2013, a revista Nature trouxe artigo de Erika Hayden, reportando o fato de Yaniv Erlich ter superado a anonimização da tentativa europeia[114], apenas demonstrando um fato já conhecido da comunidade científica[115].

Recente estudo publicado pela revista Nature[116] apresenta pesquisa sobre possível alternativa para que a privacidade de uma pessoa que seja submetida a um teste genético seja preservada, garantindo-se o sigilo e o resultados dos estudos. Ainda que o resultado seja satisfatório, o próprio estudo aponta que existem riscos de utilização em ataques e/ou utilização de referências externas que permitam individualizar os dados.

A questão é ainda mais ampla e trata da angústia na eventual impossibilidade de superar um receio e recusa de consentimento da população à utilização de dados pessoais genéticos, baseada no medo de que as estratégias de anonimização e/ou exclusivos jurídicos não garantam a privacidade, partindo do pressuposto de que a técnica de criptografia não pode ser a única solução. Estudo publicado por Effy Vayena e de Gassner Urs[117] aponta: (i) que pode ser considerada uma relativização à proteção dos dados pessoais genéticos pois, se a privacidade é entendida como controle sobre informações ou dados, então não precisa atingir níveis máxi-

113 Cf. n. 10 *supra*.

114 HAYDEN, Erika. The genome hacker. Yaniv Erlich shows how research participants can be identified from 'anonymous' DNA. **Nature**. May 9, 2013. p. 172-174.

115 Nils Homer, Szabolcs Szelinger, Margot Redman, David Duggan, Waibhav Tembe, Jill Muehling, John V. Pearson, Dietrich A. Stephan, Stanley F. Nelson and David W. Craig. Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays. Published: August 29, 2008. Disponível em: <http://journals.plos.org/plosgenetics/article?id=10.1371/journal.pgen.1000167>. Acesso em: 29.07.17.

116 MCLAREN, Paul J.; RAISARO, Jean Louis, *et ali.* Privacy-preserving genomic testing in the clinic: a model using HIV treatment, Genetics in Medicine, 18 (8), pp. 814–822, 2016, ISSN: 1098-3600. Disponível em: <http://www.nature.com/doifinder/10.1038/gim.2015.167>. Acesso em: 23.03.17. Cf também DANEZIS, George; CRISTOFARO, Emiliano. Simpler Protocols for Privacy-Preserving Susceptibility Testing. Disponível em <http://seclab.soic.indiana.edu/GenomePrivacy/papers/Genome%20Privacy-paper2.pdf>. Acesso em: 23.03.17.

117 VAYENA, Effy; GASSNER, Urs. Between openness and privacy in genomics. **PLoS Med**. 2016 Jan; 13(1): e1001937. Published online: 2016 Jan 12. Disponível em: <http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001937>. Acesso em: 23.07.17.

mos de controle, mas sim permitir medidas razoáveis de controle; e (ii) o direito à privacidade dos dados pessoais genéticos não é um direito absoluto e pode exigir contrapartidas e atuações dos titulares de direitos, bem como uma flexibilização ainda maior do acesso quando comparado à proteção de outros dados pessoais[118].

Voltando ao estudo de Paul Mclaren[119], a sugestão apresentada – em apertado resumo – é a utilização de camadas criptográficas, dividindo-se os resultados de forma aleatória, acrescentando-se uma etapa de anonimização e, ao final, mantendo as chaves criptográficas públicas com o titular dos dados[120].

Conclusão

Existe inegável avanço na coleta e manipulação de dados genéticos permitindo uma revolução, ainda pouco dimensionada, na medicina preventiva como hoje é conhecida. O tratamento popular do tema desperta fascinação e fantasias (reverberadas em interessantes exercícios em obras de ficção), além de amplificar episódios importantes, reais, que ajudam na orientação e limites das regras éticas e jurídicas que balizam o desenvolvimento do *genomics*. Pela sua natureza, dois aspectos, contudo, devem diferenciar a privacidade no âmbito dos dados pessoais genéticos dos dados pessoais em geral: (i) a possibilidade de reidentificação deve ser minimizada por técnicas combinadas de anonimização e criptografia; e (ii) após a coleta, recusas injustificadas no tratamento dos dados pessoais genéticos para pesquisas terapêuticas pelo titular devem ser balanceadas em função da proteção da saúde humana e de terceiros, particularmente se a informação pessoal genética em questão for considerada essencial.

118 Id.

119 Id. n. 34 *supra*.

120 As explicações técnicas à criptografia e tratamento dos resultados podem ser verificadas no anexo ao artigo (n. 34 *supra*). Disponível em: <http://www.nature.com/gim/journal/v18/n8/extref/gim2015167x7.pdf>. Acesso em: 23.03.17.

Nudging Privacy: Benefits and Limits of Persuading Human Behaviour Online

Daphnee Iglesias[121]

Introduction

Nudge theory is a concept initially used in behavioural science to positively reinforce better decisions by users. It has now become a trend in political science, economics and public policy to promote healthier, smarter choices and to avoid negative externalities – either financial or not. Nonetheless, nudging has also been pointed out as unethical, since it takes away from humans their rationality and autonomy. In this sense, critics believe a "nanny state" is then established[122].

This piece intends to be descriptive-only. The manuscript will delve into the reasons why nudging can be used to enhance privacy in the daily use of social networks and mobile applications, by presenting industry and academia cases where it has either a) been experimented; or b) to which it can be applied. As a general picture, the article will also present some concerns on the legal and ethical aspect of nudge theory, besides bringing up its use as an alternative to privacy notices – pointing out legal limits and its difficulties in ensuring long-term behaviour changes.

---

121 Internacionalista e mestra em Políticas Públicas pela Hertie School of Governance (Alemanha). Atualmente, é técnica-administrativa em educação da Universidade Federal de Goiás (UFG) e pesquisadora independente em privacidade online e dados abertos, realizando estudos comissionados por organizações como World Web Web Foundation e Transparência Internacional. Foi estagiária de pesquisa em segurança internacional e governança web do The Centre for International Governance and Innovation (Canadá) e aluna do Centro de Educação Executiva da Universidade das Nações Unidas para a Paz (UPEACE). / International Relations Analyst, holds a Master in Public Policy by the Hertie School of Governance (Germany). Currently, she is a technical staff at the Federal University of Goiás (UFG) and an independent researcher in online privacy and open data, conducting studies commissioned by organizations such as World Web Web Foundation and Transparency International. She was a research trainee in international security and web governance at The Center for International Governance and Innovation (Canada) and a student at the Center for Executive Education at the United Nations University for Peace (UPEACE).

122 JACHIMOWICZ, J.; MCNERNEY, S. Should the Government Nudge Us to Make Good Choices? , **Scientific American**, September 2015. Available at: <https://www.scientificamerican.com/article/should-governments-nudge-us-to-make-good-choices/#>. Accessed on: 02.03.17.

What is a nudge?

The nudge theory emerged from behavioural science and has found echo in psychology, political science and economics. The concept's general argument is that positive, indirect suggestions can influence a person's decision-making for the better, instead of direct legislation or enforcement on the same matter. The theory's most well-known works are those connected to Richard Thaler and Cass Sunstein, who have popularised the nudge concept and amplified its use. In their words:

> A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not[123].

Nudges have been used as tools to provide better public policies and reduce governmental costs linked to consequences that result from bad choices. Examples in the area of public health are the easiest to be found: providing awareness through the use of pictures that depict illnesses caused by smoking in cigarette packs and displaying salads in larger portions than high-calories snacks in public cafeterias are in place across different countries.

The nudge theory also benefits immensely from how human behaviour deals with default options: most of times, people stick with what it is offered to them. Thus public policy analysts have considered default options that take into account actions leading to positive externalities, whether financial or not.

> (…)Vastly more people in Austria are organ donors than in Germany, simply because the default is set differently in the two countries. Austrians have to opt out of organ donation, Germans have to opt in. (…) Sunstein and Thaler have given the name *libertarian paternalism* to the political philosophy that holds that such empirical findings should be exploited to drive citizens to make better choices[124].

Here, the concept of "good and bad" or "better or worse" choices is always connected to the idea leading to a behaviour that will reflect positively over the course of years, besides granting cheaper solutions to the public administration.

---

123 THALER, R. H.; SUNSTEIN, C. R. **Nudge: Improving Decisions about Health, Wealth, and Happiness**. Yale University Press, 2008, p.8.

124 KAPSER, A.; SANDFUCHS, B. Nudging as a Threat to Privacy. **Rev.Phil.Psych**, 2015, p.455. Available at: <http://link.springer.com/article/10.1007/s13164-015-0261-4>. Accessed on: 02.03.17.

Behavioural science in an online world

With the increased use of social networking websites, smartphones and applications that constantly track users' habits and whereabouts, the concern for privacy in an online world has risen. Despite the amount of personal information voluntarily given away in social media, most internet users are not aware of how much extra personal data is needed to keep applications working silently in the background. Additionally, the privacy issue gains novelty concerns when it comes to online social relations because in this realm, perceptions and interaction behaviours vary from the real world. A new phenomenon, being called as *interpersonal privacy concerns* by field experts, has been studied.

> While individuals are free to decide what personal information they disclose, they often cannot control what others disclose about them, or how others may use the private information that they disclose. Likewise, people may share information that involves others in ways that violate their privacy preferences. This becomes an increasingly significant privacy threat with the emergence of SNSs [social network sites], as the digitized social platform combines an individual's self-disclosure with others' disclosure of information about the individual, records the information in rather permanent fashion, and often presents the information publicly, making it accessible to and beyond one's social circles[125].

Given the privacy challenges brought by the use of new technologies and the subsequent change in interpersonal relations, behavioural science has found room to apply the nudge theory in internet studies. Social experiments conducted by university scholars have demonstrated that different privacy nudges may cause users to review their behaviours and app permissions online.

Applying nudges to enhance online privacy

Research conducted primarily in the United States has pointed out at least five different designs of privacy nudges that could have a positive impact

125 JIA, H.; XU, H. **Interpersonal Privacy Nudges for Promoting Privacy Protective Behaviors on Social Network Sites**. College of Information Sciences and Technology, The Pennsylvania State University, p.2. Available at: <http://cs-sys-1.uis.georgetown.edu/~sz303/PIR2015/pir_submission/pir2015_submission_5.pdf>. Accessed on: 02.03.17.

on how users interact online[126]. Non-profit organisations working around free and open internet access have ventured in this field too. This article will briefly present such strategies now, and what observed impacts they could lead to.

Third-Party Cookie Opt-in Nudge

Starting with the work promoted by open access groups, it is important to shed light on a setup modification promoted by Mozilla, the nonprofit foundation behind the Firefox browser. In February 2013, the organisation released an update patch for its privacy settings, relying on the fact that users generally stick with the default options assigned for their use. The update forbids third-party cookies to be accepted by default while browsing the internet. Third-party cookies are those belonging to different domains than the one currently being visited and are commonly used in online banners and pop-ups. Their default acceptance gives room to tracing users' browsing history on the internet.

While maintaining the choice option – users can, at any given time, modify such configuration –, the update positively increases privacy, since only websites actually visited will have their cookies allowed. The main characteristic of a nudge is then maintained. Needless to say, online advertisers were not happy with this modification and have issued public statements on the matter, besides looking for U.S. legislative support against the action: "Users have the right to decide if they want to utilize third-party cookies. Any browser that blocks third-party cookies by default, as Mozilla intends to do, restricts consumer choice. It is instead the browser that is choosing the user's experience"[127].

Although third-party cookie tracking is anonymous, data can be linked back to the users with the help of data mining tools. Mozilla's intention was pro-privacy, and the patch has not been removed from the browser.

---

126 Studies were put into practice mostly by Carnegie Mellon University, Syracuse University and Pennsylvania State University researchers: WANG, Y. et. al. From Facebook Regrets to Facebook Privacy Nudges. Heinz College Research, Carnegie Mellon University. **Ohio State Law Journal**, 74, 1307-1335. Available at: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1335&context=heinzworks>. Accessed on: 29.03.17. Also check: JIA, H.; XU, H. **Interpersonal Privacy Nudges for Promoting Privacy Protective Behaviors on Social Network Sites**. College of Information Sciences and Technology, The Pennsylvania State University. Available at: <http://cs-sys-1.uis.georgetown.edu/~sz303/PIR2015/pir_submission/pir2015_submission_5.pdf>. Accessed on: 03.03.17.

127 SCHMIDT, K. Privacy Nudge: Cookies and the War of Information. **Inudgeyou – The Applied Behavioural Science Group**, 26 August 2013. Available at: <http://inudgeyou.com/en/archives/4588>. Accessed on: 02.03.17.

Audience Nudge (or Profile Picture Nudge)

Moving on to research developed in academia, the first presented nudge of its kind is the Audience Nudge. Social network users are usually not aware of the reaching limits of what is posted online, nor completely remember who is linked to them as a "friend" or a "follower". Privacy settings are difficult to go through and such options, once again, are kept in default mode (obviously, when dealing with social networking sites, this setup will maximize data collection on behalf of the platform). Due to these reasons, posts and photos might reach unintended audiences. To address regret and compromising situations, researchers at Carnegie Mellon and Syracuse Universities designed a tool to allow users to consider the broad scope of people their online communications might come across to:

> Our profile picture nudge attempts to encourage users to pay attention to their audience by displaying five profile pictures, randomly selected from the pool of people who could view the post being created. These profile pictures serve as visual cues to remind users of the potential audience for their post. (…) [T]he profile pictures are displayed as a user starts typing in the "post" text box. The nudge also displays a notice to the user based on the user's current sharing setting. For example, if the post is to be visible to friends of friends, the notice states, "These people, your friends, AND FRIENDS OF YOUR FRIENDS can see your post[128]".

It is important to highlight how much of personal information humans are aware to give away in social networks considering the effect of instant gratification, measured by interaction with the posts. Therefore, there is plenty of room for regrettable situations to emerge from simple Facebook posts.

When tested in a controlled environment with university students, most of the feedback for this nudging tool was positive: participants have confessed they actually had forgotten who they were friends with. Some of them adjusted their privacy settings while others cleared down their friends' list. This nudge can, consequently, assist users with better decision-making online[129].

---

128 WANG, Y. et. al. From Facebook Regrets to Facebook Privacy Nudges. Heinz College Research, Carnegie Mellon University. **Ohio State Law Journal**, 74, p. 1321. Available at: <http://inudgeyou.com/en/archives/4588>. Accessed on: 02.03.17.

129 Idem, p. 1322.

Timer Nudge

To address possible regrettable situations, Syracuse scholars came up with a second nudge design, one to encourage users to reflect on what has been written on networking platforms. The researchers' goal was to predict angst or negative situations published online to develop into disproportional outcomes.

> When a user starts typing a status update or comment, a message with a yellow background appears stating, "You will have 10 seconds to cancel after you post the update." After the user clicks the "Post" button, the user is given the option to "Cancel" or "Edit" the post during a ten-second countdown before the post gets published on Facebook. There is also an option to circumvent the timer by clicking a "Post Now" button[130].

Results measured for this kind of design were good, but not as promising as the Audience Nudge. Some participants considered it a nuisance, while others reported ignoring the notices after some days. Those acknowledging the 10-second delay used it to correct grammar mistakes or to edit the tone of the message, sometimes even cancelling it overall[131].

Sentiment Nudge

The last tool tailored by Syracuse and Carnegie Mellon researchers was the Sentiment Nudge, designed to intervene with immediate content feedback.

> We designed a sentiment nudge that combines a countdown timer with a notice regarding the content of the post (…). After the user clicks "Post," the timer and a notice highlighted with a yellow background will appear below the text box. We refer to this nudge as the "sentiment nudge."
>
> (…)[W]e used an open-source sentiment-analysis module to analyze the content of each post[132]. This module uses AFINN-111 – a list of 2,477 English words and phrases manually rated as negative or positive, on a scale

130 WANG, Y. et. al. From Facebook Regrets to Facebook Privacy Nudges. Heinz College Research, Carnegie Mellon University. **Ohio State Law Journal**, 74, p. 1321. Available at: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1335&context=heinzworks>. Accessed on: 02.03.17.

131 Idem, p. 1331-1333.

132 SentiMental by GITHUB. Available at: <hhttps://github.com/thinkroth/Sentimental>. Accessed on: 02.03.17.

> between –5 (negative or very negative) and 5 (positive or very positive)[133]. For each post, any words in the wordlist are scored, creating a weighted sum for the entire post. A text message corresponding to this sum is shown to the user. For example, a slightly negative weighted sum would lead to the message, "Other people may perceive your post as *negative*."[134]

After the notice, users would have the option to edit the post, if needed. This design was the least effective, according to the participants. Some of them considered that the sentiment analysis module was taking the sentences out of context by isolating the analysis, word by word. Other users felt a social network site's job was not to be judgemental about feelings or expressions as a real person – which confirms the platforms' use to gain instant gratification as well as to vent frustrations[135].

Data-sharing Awareness Nudge

Another study by a different group of researchers at Carnegie Mellon University demonstrated that people tend to pay more attention to how much personal data is being shared by online applications once they are told such information. Research analysed how efficient permission managers[136] are when combined with privacy nudges. For this experiment, an app called AppOps was used. It released notices about how many times personal data had been shared and how many different third-party companies received such pieces of information.

> The researchers found that app permission managers were helpful. When the participants were given access to AppOps, they collectively reviewed their app permissions 51 times and restricted 272 permissions on 76 distinct apps. Only one participant failed to review permissions.

133 WANG, Y. et. al. From Facebook Regrets to Facebook Privacy Nudges. Heinz College Research, Carnegie Mellon University. **Ohio State Law Journal**, 74, p. 1322-1323. Available at: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1335&context=heinzworks>. Accessed on: 02.03.17.

134 Idem, p. 1322-1323.

135 WANG, Y. et. al. From Facebook Regrets to Facebook Privacy Nudges. Heinz College Research, Carnegie Mellon University. **Ohio State Law Journal**, 74, p. 1329-1333. Available at: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1335&context=heinzworks>. Accessed on: 02.03.17.

136 Once installed in smartphones, permission managers are applications that centralize information on privacy settings for the user.

> But once the participants had set their preferences over the first few days, they stopped making changes. When they began getting the privacy nudges, however, they went back to their privacy settings and further restricted many of them. During this phase, which spanned eight days, users collectively reviewed permissions 69 times, blocking 122 additional permissions on 47 apps[137].

Every participant was alarmed at how much sharing can happen in the background. One piece of location data, for instance, could be linked to several apps, in some cases leading to more than 5,000 data sharing updates within 14 days.

> In interviews, the research subjects repeatedly said the frequency of access to their personal information caught them by surprise.
>
> "4,182 (times) – are you kidding me?" one participant asked. "It felt like I'm being followed by my own phone. It was scary. That number is too high." Another participant's response: "The number (356 times) was huge, unexpected[138]".

The research results have addressed that the ordinary user is unaware of how applications behave in the background – and even for a new technology-savvy user, the overwhelming number of existing functionalities and apps, each demanding its own privacy setting, can certainly become a problem. Nonetheless, once people have the power and information about the real volume of data sharing, they act upon it.

Unfortunately, AppOps operated only for Android users and was discontinued. Apple operating systems do have a privacy manager, but "it does not tell users how often their information is used or for what purpose and does not nudge users to regularly review their settings"[139]. The promising results of such kind of awareness nudge, however, have been embraced.

---

137 SPICE, B. **Study Shows People Act To Protect Privacy When Told How Often Phone Apps Share Personal Information**. CMU News, Carnegie Mellon University, 2015. Available at: <https://www.cmu.edu/news/stories/archives/2015/march/privacy-nudge.html>. Accessed on: 02.03.17.

138 Idem.

139 SPICE, B. **Study Shows People Act To Protect Privacy When Told How Often Phone Apps Share Personal Information**. CMU News, Carnegie Mellon University, 2015. Available at: <https://www.cmu.edu/news/stories/archives/2015/march/privacy-nudge.html>. Accessed on: 02.03.17.

Interpersonal-Privacy Nudge / Comparison-based Privacy Nudge

One last nudge design was proposed by researchers from the Pennsylvania State University. It connects to the studies of interpersonal privacy concerns. Currently, it is very demanding to assess privacy behaviours from an individualistic approach. Thus, this tool was developed to trigger concerns about others' privacy when tagging them in one's own pictures.

> The friend's previous photo-sharing frequency is shown to indicate strict privacy rules and to assist the user in consideration of whether this sharing activity may be conflictive with such rules and if protective behaviors, such as withdrawal of information or communication in private channels, should be taken[140].

Facebook has already implemented a verifying approval tool for tags in posts or pictures – but as an opt-in, not a default option. Hence, some sort of notice as '*Your friend XYZ has tagged herself in 2 photos over the course of 12 months. Are you sure you want to proceed?*' could lead users "to consider the potential conflicts between their own privacy rules and their friends'"[141] and avoid future embarrassing situations.

This nudge design is in tune with recent European research, which promotes the adoption of a comparison-based privacy approach to deal with the matter. It is known paternalism is generally more accepted in the old continent than in the U.S., despite most of the studies on the topic coming from the other side of the Atlantic[142]. Nonetheless, it was on that territory that research grants on the social aspects of privacy behaviours have flourished, apart from legal definitions:

> To enable self-adaptive, user-centric privacy nudges, we make the following three observations. First, comparison is a natural human behavior. People compare themselves to their peer groups every day based on a wide set of criteria ranging from salary to health. Second, comparison does not require ground truth or training data. Instead, self-reflection and decision

140 JIA, H.; XU, H. **Interpersonal Privacy Nudges for Promoting Privacy Protective Behaviors on Social Network Sites**. College of Information Sciences and Technology, The Pennsylvania State University, p.2. Available at: <http://cs-sys-1.uis.georgetown.edu/~sz303/PIR2015/pir_submission/pir2015_submission_5.pdf>. Accessed on: 03.03.17.

141 Idem, p.2.

142 HACKER, P. Nudge 2.0: The Future of Behavioural Analysis of Law in Europe and Beyond. **European Review of Private Law**, 2016, p. 305. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2670772>. Accessed on: 02.03.17.

> making is rather guided by relative values. The aggregated behavior of the peer group dynamically provides individual 'ground truth' for people to evaluate their own decisions. Third, people usually compare not to random strangers. They compare to people from their social environment who they can individually relate to, e.g., people with the same profession, age, or other demographics. In doing so, they harmonize individual and social factors that influence their decision-making process[143].

The use of privacy nudges as a complement to existing regulation on the matter has already been the object of scrutiny by the European Commission. In 2015, it released an extensive policy report acknowledging how nudges are an alternate tool to enhance proper privacy notices and concerns[144].

Ethical implications of the nudging theory

Criticism on behavioural science often revolves around the paternalistic idea that humans are not fully capable of sound judgement and therefore need to outsource their choices to someone or something else. In addition, critics believe that autonomy and rationality, intrinsic human features, are ignored by behavioural science.

On the opposite side of this realm, policy analysts and researchers who defend nudging claim its main characteristic as a way to keep humans aware of their possibilities: choice. It is a choice architecture that it is being developed, and for it to work choices must be presented. Nothing is banned.

Issues of concern about ethics in any study or scientific area will always arise. According to literature, there should be a four-step evaluation on a nudge policy, in order to verify its ethical standards: (A) is there an increase in people's is there an increase in people's well-being?; (B) is autonomy partially/fully affected?; (C) is people's integrity partially/fully affected?; and (D) what are the practical, tangible policy implications of applying such nudge?[145] While

143 ZIEGELDORF, J. H. **Comparison-based Privacy: Nudging Privacy in Social Media (Position Paper).** RWTH Aachen University, 2015. Available at: <https://www.comsys.rwth-aachen.de/fileadmin/papers/2015/2015-ziegeldorf-dpm-cbp.pdf>. Accessed on: 02.03.17.

144 MONTELEONE, S. **Nudges to Privacy Behaviour: Exploring an Alternative Approach to Privacy Notices.** Joint Research Centre, European Commission, 2015. Available at: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96695/jrc96695.pdf>. Accessed on: 02.03.17.

145 SCHUBERT, C. **A note on the ethics of nudges**. VOX, 2016, p.2. Available at: <http://voxeu.org/article/note-ethics-nudges>. Accessed on: 02.03.17.

checking such questions, users and analysts can make a better prediction of long-term scenarios with and without the use of the nudge.

While assuming the best decision for the user, nudge designers need to ponder what is good and bad from the long-term perspective they want to achieve: in public policy, this is often connected to cheaper, safer, healthier choices and programs that will not overload the government's financial or legal capacities. Obviously, such matters are not foreseen in instant gratification tools, such as social networking posts.

Final considerations

Nudges are slowly becoming a mechanism to ensure better protection of online privacy. There is still room for iterating the designs here presented, but it has already become clear to several governments and internet users that such novelty can assist in the protection of personal data. As it is widely expected, lawmaking does not function on the same rhythm as innovation and creativity. Therefore, nudging can enhance protection when combined with governmental regulation and private-sector notices.

It is also important to highlight that the more connected the individual's sphere is to online social interactions, different ways of perceiving privacy must emerge, taking into account risky situations that affect both oneself and others. Nudging has the potential to avoid regrettable sharing, while still keeping options open to the user.

Filtros Bolha, as Escolhas que Fizemos e as que Faremos: Considerações sobre como (Não) Regular a Internet

Fernando Schincariol[146]

Plataformas digitais e os desafios para uma agenda legislativa adequada

A Internet não é regulada apenas por leis[147], mas por meio de interações entre arquiteturas de controle, normas de mercado, normas sociais e leis[148]. A norma jurídica, no entanto, tem a aptidão de influenciar direta ou indiretamente todas estas outras modalidades de regulação, que estão em constante interação[149].

Exatamente por existirem várias modalidades de regulação, nem sempre a ampliação de regras jurídicas e regimes de responsabilidade cada vez mais amplos serão os meios mais adequados para enfrentar fenômenos sociais observados pelo uso da Internet.

A importância desse debate não diminui. Ainda que o acesso à rede infelizmente não seja uma realidade para a maioria dos brasileiros,[150] é inegável que sua regulação afeta a sociedade como um todo.

---

146 Advogado. Bacharel em Direito pela Universidade Presbiteriana Mackenzie; Pós-graduando em Propriedade Intelectual e Novos Negócios na Fundação Getúlio Vargas/SP. E-mail:fernando.schincariol@gmail.com.

147 "Leis" aqui compreendidas em sentido amplo: as normas escritas que traduzem uma proposição prescritiva, assim como proposto por Bobbio em sua Teoria da Norma Jurídica.

148 LESSIG, Lawrence. **Code: Version 2.0.** Nova York: Basic Books, 2016, p. 121. Também disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 23 mar. 2017. "My argument is (...) that we must add one more increasingly salient threat to the list. And to see this new, salient threat, I believe we need a more general understanding of how regulation works—one that focuses on more than the single influence of any one force such as government, norms, or the market, and instead integrates these factors into a single account."

149 Para uma didática explicação sobre o modelo regulatório proposto por Lessig é feita por Marcel Leonardi em: LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2011.

150 Para números brasileiros. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros [livro eletrônico]: TIC domicílios 2015. Núcleo de Informação e Coordenação do

Ao observar que plataformas e serviços *on-line* cooperaram com avanços políticos (e o próprio processo de elaboração e discussão do Marco Civil da Internet mostra isso[151]), com a queda ou enfraquecimento de regimes totalitários e facilitaram sensivelmente o acesso à informação, educação e cultura, sem falar em sua importância para a economia[152], é possível compreender melhor a importância de um tratamento jurídico equilibrado a esse ambiente,[153] que é frequentemente ameaçado.

Informações preliminares de uma pesquisa conduzida por pesquisadores do NIC.br apontam que existem 166 projetos de lei apresentados,[154] alguns visando alterar substancialmente o Marco Civil da Internet. Apesar de não se acreditar na aprovação de todas essas iniciativas, manifestações públicas contrárias a parte delas, inclusive do próprio Comitê Gestor da Internet[155], demonstram a dificuldade em se manter uma agenda positiva para a regulação da rede no Brasil[156]. Entretanto, não é só o legislativo que protagoniza retrocessos.

Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2016. Disponível em: <http://www.cetic.br/media/docs/publicacoes/2/TIC_Dom_2015_LIVRO_ELETRONICO.pdf>. Acesso em: 27.03.17. Não se descuida da notória diferença entre acesso (que, *grosso modo* traduz uma ideia quantitativa apenas) e *acessibilidade* (uma abordagem qualitativa e mais ampla). A esse respeito, confira-se: DE FREITAS, Bruna Castanheira de. Acessibilidade e o Direito de Navegar na Web. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III - Tomo II: Marco Civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 155-167.

151 LEMOS, Ronaldo. Marco Civil como símbolo do desejo por inovação no brasil. In: LEMOS, Ronaldo; George Salomão Leite (coords.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. Bem como: STEIBEL, Fabro. O portal de consulta pública do Marco Civil da Internet. In: LEMOS, Ronaldo; George Salomão Leite (coords.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

152 À título de exemplo, o estudo conduzido pela Deloitte sobre o impacto econômico do Facebook: WILLIAMS, Chris; AGUILAR, Ana. **Facebook's global economic impact**. Deloitte, jan. 2015. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology-media-telecommunications/deloitte-uk-global-economic-impact-of-facebook.pdf> Acesso em: 10.01.16.

153 LEONARDI, Marcel. Marco Civil da Internet, Plataformas Digitais e Redes Sociais. In: **Marco Civil da Internet: Análise Jurídica Sob uma Perspectiva Empresarial**. ARTESE, Gustavo (coord.) Quartier Latin, 2015.

154 CAPELAS, Bruno. Após Marco Civil, crescem projetos de lei sobre internet. **NIC.BR.** Publicado em 10 out. 2016. Disponível em: <https://www.nic.br/noticia/na-midia/apos-marco-civil-crescem-projetos-de-lei-sobre-internet/>. Acesso em: 10.01.16.

155 Nota pública emitida pelo Comitê Gestor da Internet. Disponível em: <http://www.cgi.br/esclarecimento/nota-publica-em-que-expressa-discordancia-sobre-o-projeto-de-lei-que-propoe-criacao-de-cadastro-nacional-de-acesso-a-internet/> Acesso em: 10.01.16.

156 Talvez o exemplo mais recente e emblemático seja o PL 6449/2016 do deputado Marcelo Aguiar, sobre o qual remetemos o leitor aos comentários de: SOUZA, Carlos Affonso e PADRÃO, Vinicius. Sexo e Bloqueios na Internet: uma relação pornográfica. **ITS RIO FEED**. Disponível em: <https://

Apesar de toda a discussão sobre a redação do artigo 19 da Lei 12.965/2014[157], que corrobora o racional do relatório da Comissão Interamericana de Direitos Humanos[158], do Relator Especial para a Liberdade de Expressão da ONU[159], os Princípios de Manila[160], além da jurisprudência do STJ[161], o Tribunal de Justiça do Estado de São Paulo, ignorando tudo isso, condenou[162] um provedor de busca por não ter agido antes de uma ordem judicial[163].

Desde o ponto de vista estrutural, vários atores, cada qual com seu papel - e interesse - compõem o que veio a ser chamado de "ecossistema da Internet"[164]. Este artigo argumenta que para manter o ecossistema equilibrado é necessário que diversas modalidades de regulação sejam pensadas e, a partir da análise da crítica bastante em voga a respeito dos "filtros bolha", defende que este equilíbrio seja alcançado através de uma mudança de hábito na forma com a qual as redes sociais e plataformas digitais são utilizadas.

---

feed.itsrio.org/sexo-e-bloqueios-na-internet-uma-rela%C3%A7%C3%A3o-pornogr%C3%A1fica-4007bd439f1d#.qo7s1ns9m>. Acesso em: 05.0117.

157 Este debate, desde as consultas públicas até o texto final da lei foi descrito por Francisco Brito Cruz em sua dissertação de mestrado. CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital: a experiência de elaboração do Marco Civil da Internet,** 2015. Dissertação (Mestrado em Direito) Universidade de São Paulo.

158 Convenção Interamericana de Direitos Humanos, Relatoria Especial para a Liberdade de Expressão. **Liberdade de Expressão e Internet**. Publicado em: 31 dez. 2013. Disponível em: <http://www.oas.org/pt/cidh/expressao/docs/publicaciones/2014%2008%2004%20Liberdade%20de%20Express%C3%A3o%20e%20Internet%20Rev%20%20HR_Rev%20LAR.pdf> Acesso em: 10.01.16.

159 LA RUE, Frank. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.** Publicado em 15 de maio de 2011. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement> Acesso em: 10.01.16. "The Special Rapporteur believes that censorship measures should never be delegated to a private entity, and that no one should be held liable for content on the Internet of which they are not the author."

160 Uma coalizão da sociedade civil que se uniu para produzir um documento com princípios a serem adotados pelos países na proteção dos intermediários. A "Carta de Manila" como é chamada por alguns é um exemplo do esforço histórico da união de organizações e ativistas pela liberdade de expressão. Para mais, confira-se: <https://www.manilaprinciples.org/pt-br/>. Acesso em: 10.01.16. O texto, na íntegra, está disponível em: <https://www.eff.org/files/2015/07/02/manila_principles_1.0_pt.pdf>. Acesso em: 10.01.16.

161 STJ. Quarta Turma, REsp 1.512.647/MG, Rel. Min. Luis Felipe Salomão. Julgado em: 13 mai. 2015.

162 TJSP. Apelação Cïvel nº 1011391-95.2015.8.26.0005. Rel. Des. Francisco Loureiro. Julgado em: 07 jun. 2016.

163 Para mais detalhes sobre a decisão em questão e os motivos pelos quais ela não parece dar a melhor solução, confira-se os comentários de Bruno Bioni e Paulo Rená no Observatório do Marco Civil. Disponível em: <http://omci.org.br/jurisprudencia/109/site-fraudulento-e-responsabilidade-civil/ >. Acesso em: 27.03.17.

164 INTERNET SOCIETY. **Internet Ecosystem**. Publicado em: jan. 2014. Disponível em: <https://www.internetsociety.org/sites/default/files/bp_Internet%20Ecosystem_032614_en.pdf>. Acesso em: 23.03.17.

A crítica das bolhas de conteúdo

"The Filter Bubble"[165] (traduzido para o português como "O Filtro Invisível - o Que a Internet está Escondendo de Você" por Diego Alfaro e editado pela Zahar) é um livro publicado em 2011 pelo jornalista Eli Pariser. Seus argumentos centrais são muito bem explicados por ele mesmo em um TED Talk[166] e, recentemente, foram incorporados em falas da chanceler alemã Angela Merkel[167] e no último discurso de Barack Obama como presidente dos Estados Unidos[168].

A importância do tema também decorre do crescente número de material que identifica e discute o fenômeno, seja no meio acadêmico, na mídia ou nas próprias redes. Questiona-se muito se as democracias sobreviverão ao *big data* e à inteligência artificial[169], ainda que a área esteja engatinhando e seja demasiadamente mistificada[170].

Confira-se então as principais observações e os principais argumentos feitos por Eli Pariser, que são, sinteticamente, descritos a seguir: a) o conteúdo que vemos nos serviços disponíveis na web (resultados de buscas, feed de redes sociais, a primeira página de determinado site etc) são cada vez mais personalizados, de acordo com os nossos hábitos de uso das ferramentas; b) a mudança do fluxo de informação se deu de forma invisível para os usuários, que não sabem que as informações estão sendo personalizadas para eles; c) grandes corporações tomam decisões com base em seus próprios interesses e, diferentemente da mídia tradicional, elas não seguem a mesma ética dos editores; d) o resultado disso tudo seria a privação de conteúdos e pontos de vistas diferentes aos usuários. Como o filtro tende a priorizar apenas a visão de mundo com a qual o

---

165 Advirta-se que os termos "bolha de conteúdo", "filtro de conteúdo", "bolha de informações" e suas variações em inglês são usados aqui como sinônimos.

166 TED Talk. PARISER, Eli. **Tenha Cuidado com os "Filtros Bolha" online**. Disponível, com legendas em português em: <https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=pt-br>. Acesso em: 23 .03.17.

167 CONNOLLY, Kate. Angela Merkel: internet search engines are 'distorting perception'. **THE GUARDIAN**. Publicado em: 27.10.16. Disponível em: <https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception>. Acesso em 10.01.16.

168 Obama speech: Bubbles are a threat to our democracy. **BBC**. Publicado em: 11 jan. 2017. Disponível em: <http://www.bbc.co.uk/news/world-us-canada-38578839>. Acesso em: 11.01.17.

169 HELBING, Dirk; FREY, Bruno S.; GIGERENZER, Gerd; HAFEN, Ernst et. al. Will Democracy Survive Big Data and Artificial Intelligence? **SCIENTIFIC AMERICAN**. Publicado em: 25.02.17. Disponível em: <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/>. Acesso em: 23.03.17.

170 KAPLAN, Jerry. AI's PR Problem. **MIT TECHNOLOGY REVIEW**. Publicado em: 03.03.17. Disponível em: <https://www.technologyreview.com/s/603761/ais-pr-problem/>. Acesso em: 03.03.17.

usuário concorda, nós não teríamos acesso a informações que desafiam nossos pontos de vista, o que é vital para a democracia.

Pariser também oferece soluções para os problemas que aponta. Atitudes tanto dos indivíduos quanto das empresas e dos governos poderiam contribuir para diminuir o efeito do filtro de conteúdo.

De acordo com o autor, os indivíduos poderiam: a) a partir de uma metáfora com "comida saudável", mudar seus hábitos de consumo de informação; b) usar sites que deem mais visibilidade e controle sobre como seus filtros funcionam; e c) buscar aprender sobre códigos e algoritmos.

Além disso, as empresas poderiam: a) deixar seus filtros mais transparentes aos usuários; b) mostrar quais informações elas possuem sobre as pessoas e como elas são usadas; c) algoritmos que suportam os filtros devem ser desenvolvidos com um senso maior de responsabilidade social, um "filtro colaborativo"; e d) desenhar outros filtros que exponham os usuários a assuntos que estejam fora de sua experiência ou hábitos normais.

Ainda segundo Pariser, os governos e cidadãos poderiam: a) determinar que as empresas deem o controle dos seus dados pessoais aos usuários; b) criar uma agência - ou autoridade - encarregada da fiscalização sobre o cumprimento das normas relativas à proteção de dados; e c) engajar-se nesse debate.

Note-se que a proposta aqui não é nova: desde o início, Pariser vislumbra que ações tanto de cidadãos quanto de empresas e governos poderiam contribuir para solucionar ou atenuar o problema que ele identifica. Nesse aspecto, a tarefa seria apenas discutir as melhores estratégias para "estourar a bolha" e manter a Internet um espaço democrático: deve-se buscar soluções na própria arquitetura das plataformas? Na forma com que as plataformas são utilizadas? Ou, em última instância, é preciso modificar as leis que regem as relações entre usuários e plataformas?

Estourando a bolha pela arquitetura

Regular pela arquitetura é basicamente modular comportamentos positivos ou negativos simplesmente pela forma com a qual as coisas funcionam. Um exemplo bastante claro citado por Marcel Leonardi é o uso da lombada para a diminuição da velocidade[171]. Esse ponto é especialmente importante porque as propostas feitas por Pariser procuram realizar uma alteração direta na arquitetura das plataformas digitais.

171 LEONARDI, Marcel. **Tutela e Privacidade na Internet.** São Paulo. Saraiva, 2011, p. 161.

Mas não só ele. Recente editorial do The Guardian sobre *big data* (entenda-se aqui como "a tecnologia por trás da bolha") argumenta que, se o judiciário e os governos não fizerem alguma coisa, a ruína da privacidade será a ruína da democracia[172].

Curioso notar, porém, que: a) uma das críticas da regulação pela arquitetura é justamente o fato de que ela teria a aptidão para ser invisível ou imperceptível aos usuários[173]; e b) pode ser estranho ou contraditório para americanos e ingleses, mas no Brasil não há liberdade de expressão com anonimato. A condição de anônimo, por disposição constitucional, impediria o exercício da liberdade de expressão[174].

Uma das soluções propostas por Pariser voltada à arquitetura de plataformas é a incorporação de um "senso ético" ou a construção de algoritmos que levem em conta a necessidade das pessoas de estarem expostas a diferentes pontos de vistas.

Não se nega a importância dos serviços *on-line*, principalmente os que possuem alcance global, de perceberem sua responsabilidade social. Contudo, agir diretamente no funcionamento da plataforma pode implicar a mera substituição de um filtro por outro. Vale mencionar, ainda, toda a crítica que poderia seguir sobre a excessiva intervenção estatal, caso a medida decorresse de uma obrigação legal.

Exatamente por terem alcance global e frequentemente estarem intermediando relações (sejam elas entre pessoas e códigos ou pessoas e pessoas), as plataformas digitais dificilmente teriam como contemplar todos os sentidos de "democracia". Em última análise, a demanda seria por uma ferramenta que pudesse criar um "filtro colaborativo" que desse conta de mostrar diversos pontos de vista diferentes e satisfatoriamente incluir a visão de grupos minoritários.

Como apontado por Engin Bozdag e Jeroen Van den Hoven, após análise de diversos algoritmos criados especificamente para diversificar o conteúdo disponível para os usuários, verificou-se que todos eles apresentaram algum tipo de deficiência por não contemplarem todos os sentidos de democracia e reforçarem o discurso de certos grupos[175].

---

172 The Guardian View on big data: the danger is less democracy. **THE GUARDIAN**. Publicado em: 26.02.17. Disponível em: <https://www.theguardian.com/commentisfree/2017/feb/26/the-guardian-view-on-big-data-the-danger-is-less-democracy>. Acesso em: 26.02.17.

173 LEONARDI, Marcel. **Tutela e Privacidade na Internet.** São Paulo. Saraiva, 2011, p. 163.

174 O interessante debate sobre como a vedação ao anonimato pode ser considerado uma ameaça à privacidade e à liberdade de expressão no Brasil foi feito Mariana Cunha e Melo no artigo "Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças ao direito à privacidade no Brasil", que se encontra publicado na presente obra.

175 BOZDAG, Engin; VAN DEN HOVEN, Jeroen. **Breaking the Filter Bubble: democracy and design**. Ethics and Information Technology, 2015, Volume 17, Number 4, p. 249. Disponível em: <https://link.springer.com/article/10.1007/s10676-015-9380-y>. Acesso em: 27.03.17.

Para além do problema das bolhas de conteúdo, a academia convive com o desafio de pensar se e em que medida deve-se modificar a forma com que algoritmos são desenvolvidos e incorporados aos serviços disponibilizados na rede para garantir mais transparência e confiança. Alguns pesquisadores inclusive já desenharam quais seriam os "princípios dos algoritmos compreensíveis"[176]: a) responsabilidade; b) compreensibilidade; c) precisão; d) auditabilidade; e e) justiça[177].

É preciso enfatizar que tal proposta vai além da crítica de Eli Pariser e seria necessário outro artigo para discutir seus aspectos em profundidade. A abordagem citada procura resolver anomalias identificadas em decisões tomadas por algoritmos e não visa exatamente à construção dos algoritmos das plataformas digitais discutidas em "O Filtro Invisível".

O ponto de contato entre as propostas está essencialmente ligado à ideia de transparência, principalmente ao se afirmar que a transparência geraria maior compreensão[178].

Aparentemente, porém, não parece haver uma definição clara sobre o que exatamente precisa ser transparente nos algoritmos de personalização em si. Há "conceitos" de transparência que orientam a atividade empresarial em diversas instâncias, como na coleta, no uso e no tratamento de dados no Marco Civil da Internet, e o dever de informações claras sobre produtos e serviços estipulado no Código de Defesa do Consumidor, além do próprio incentivo de mercado: mais transparência seria traduzida em mais confiança que significaria mais usuários.

Não se descuida também que o próprio conceito de "transparência algorítmica" apresenta limitações: usuários de um algoritmo transparente não necessariamente entendem como ele funciona ou como controlar qualquer tipo de efeito causado por ele. O argumento é defendido por Mike Ananny e Kate Crawford

176 Tradução livre de "Principle for Accountable Algorithms". Apesar da palavra "accountable" ser normalmente traduzida para o português como "responsável", parece que o intuito dos estudos conduzidos até aqui é fazer com que os processos automatizados sejam melhor compreendidos e não simplesmente encontrar novas formas e teorias de responsabilidade civil.

177 Disponível em: <http://www.fatml.org/resources/principles-for-accountable-algorithms>. Acesso em: 27.03.17. É explicado por dois dos pesquisadores em: DIAKOPOULOS, Nikolas; FRIEDLER, Sorelle. How to Hold Algorithms Accountable. **MIT TECHNOLOGY REVIEW**. Publicado em: 17.11.16. Disponível em: <http://www.fatml.org/resources/principles-for-accountable-algorithms>. Acesso em: 27.03.17.

178 PARISER, Eli. **The Filter Bubble: What the Internet is Hiding From You**. The Penguin Press. 2011. Apenas explorando um pouco mais o argumento: o que se sustenta é que a transparência dos algoritmos dos filtros de personalização poderiam permitir que os usuários questionassem resultados ou decisões das quais eles discordam ou que lhes causaram algum dano. "The new filterers can start by making their filtering systems more transparent to the public, so that it's possible to have a discussion about how they're exercising their responsibilities in the first place".

que analisaram o conceito de transparência em diferentes períodos históricos e modelos regulatórios, chegando à conclusão de que transparência não é uma forma adequada para determinar como sistemas algorítmicos são construídos:

> Se a verdade não é uma descoberta positivista, mas uma conquista relacional através de agentes humanos e não-humanos em rede, então o alvo da transparência deve mudar. Isto é, se um sistema deve ser visto para ser compreendido e responsabilizado, o tipo de "ver" que uma teoria ator-rede requer não implica olhar para dentro - mas através de um sistema. Não só a transparência é um modo limitado de conhecer os sistemas, mas ela não pode ser usada para explicar - e muito menos regular - um conjunto distribuído de atores humano e não-humanos cujo significado não reside internamente, mas relacionalmente[179].

Isto não quer dizer que regular pela arquitetura seja impossível ou inútil, mas apenas que possui um custo específico. Quando trata especificamente das arquiteturas de controle, Lessig alerta que "seja lá de que forma o ciberespaço tenha sido feito, não há nenhum motivo para que ele tenha que permanecer desse jeito. A "natureza" da Internet não é a vontade de Deus. Sua natureza é produto do seu *design*. Este *design* pode ser diferente"[180].

Gerar confiança em sistemas "invisíveis" é um desafio recorrente com o qual as empresas de tecnologia conseguiram conviver até agora de forma satisfatória, ouvindo reguladores, usuários e a academia. Veja o *Twitter,* por exemplo: após a introdução de algumas mudanças em sua *timeline*[181], a empresa se reclassificou nas lojas de aplicativos e, atualmente, apresenta-se antes como uma plataforma de notícias e depois como uma rede social[182].

---

179 ANANNY, Mike; CRAWFORD, Kate. **Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability**. Disponível em: <http://journals.sagepub.com/doi/pdf/10.1177/1461444816676645>. Acesso em: 16.01.17. Tradução livre de: "If the truth is not a positivist discovery but a relational achievement among networked human and non-human agents, then the target of transparency must shift. That is, if a system must be seen to be understood and held accountable, the kind of "seeing" that an actor-network theory of truth requires does not entail looking inside - but across a system. Not only is transparency a limited way of knowing systems, but it cannot be used to explain - much less govern - a distributed set of human and non-human actors whose significance lies not internally but relationally".

180 LESSIG, Lawrence. cit., p. 38.

181 PADRO, Jean. Twitter começa a mostrar timeline fora de ordem (mas você pode mudar isso). **TECNOBLOG**. Disponível em: <https://tecnoblog.net/191432/twitter-fora-ordem-cronologica-voltar/>. Acesso em: 13.01.17

182 Entrevista de Evan Davis, "Head" de Notícias e Parcerias para o Twitter UK para a BBC sobre Donald Trump, notícias falsas, filtros bolhas e ser uma plataforma de notícias. Disponível em: <https://www.youtube.com/watch?v=xCAY99HNDfA>. Acesso em 16.0117.

Como se verá adiante, após críticas a respeito de notícias falsas terem modificado os resultados das eleições americanas, diversas iniciativas foram tomadas.

Outro problema associado à regulação pela arquitetura, especialmente em um ambiente tecnológico é que ela pode tornar-se imperceptível para determinadas pessoas, mas facilmente contornáveis por outras. Exemplos são vastos: as regiões dos DVDs, que não impediram a pirataria; bloqueios de sites via DNS, pouco eficazes contra quem sabe configurar um novo servidor; e filtros de acesso com base em IP, facilmente contornáveis através de VPNs. Os dois últimos exemplos podem demonstrar que, além de invisíveis e contornáveis, a solução de regulação pela arquitetura também é facilmente "abusável", ficando mais claro quais são os custos associados a ela.

Sem embargo disso, a intersecção entre arquitetura e direito impõe uma reflexão sobre as formas de desenvolver sistemas para demonstrar o cumprimento de regras jurídicas ou sociais que impactem na confiança e na segurança que são esperadas em serviços *online*.

Deve-se analisar isso a partir de duas configurações/recomendações estruturais. A primeira delas é feita no próprio *Filter Bubble*: defende-se a construção de mecanismos que facilitem o acesso às informações pessoais armazenadas sobre usuários e como elas são usadas, de modo a permitir que eles entendam intuitivamente como o serviço funciona e o quanto ele "sabe" sobre os usuários[183]. Esse ponto é bastante interessante porque, apesar de não estar plenamente explicado no *Filter Bubble*, as leis de proteção de dados de uma forma geral garantem esses direitos. As empresas, por meio dos relatórios de impacto à privacidade, analisam quais seriam as maneiras adequadas de dar controle sobre os dados pessoais aos usuários; os Estados, por meio das autoridades de proteção de dados (ainda ausente no Brasil), têm o papel de fiscalizar o cumprimento dessas regras.

A segunda não está no *Filter Bubble,* mas é uma ideia de regulação por meio da arquitetura adotada na Comunidade Europeia através da GDPR[184], que entrará em vigor

183 Podemos assumir como um desdobramento razoavelmente claro da ideia de "transparência" já comentada.

184 Confira-se o que diz o Artigo 25 da GDPR, inserido no capítulo de "obrigações gerais": "1. 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 organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, 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. 2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default,

em maio de 2018: o conceito de *privacy by design,* que procura determinar que práticas de proteção de dados sejam incorporadas às próprias ferramentas tecnológicas[185].

A legislação europeia procura estimular um sistema de "certificação" através do qual as autoridades de proteção de dados poderiam atribuir "selos" que indicariam que determinada empresa cumpre o que determina a GDPR..

No entanto, o que nem sempre se percebe é que, apesar da determinação de "minimização", refletida também no princípio da finalidade, segundo o qual apenas os dados necessários para cada propósito específico podem ser coletados, não há uma proibição genérica a modelos de negócio baseados em dados: a legislação europeia restringe as formas pelas quais as operações são realizadas, mas não as veda em princípio. Conforme já pontuado por Jules Polonetsky e Omer Tene, a preocupação não deve recair na quantidade de dados obtidos, mas na forma como são usados[186].

Para assimilar como esses conceitos funcionam na prática, tome-se como exemplo o processo de criação de uma conta do Google: após completar os campos (nem todos são obrigatórios), o usuário vê uma janela com os links para os termos de serviço e política de privacidade e 3 grandes avisos sobre "Os dados que processamos quando você usa o Google" (com 4 parágrafos), "Por que os processamos" (um parágrafo e seis tópicos) e "Combinação de dados" (um parágrafo), que foi a forma encontrada pela empresa para obter o consentimento livre, informado e expresso dos usuários[187].

O campo que informa "Por que os processamos" explica que cookies, histórico de pesquisa e dados de geolocalização são usados, entre outras coisas, para aprimorar o serviço de anúncios personalizados. Assim que o usuário concorda com isso, ele é automaticamente levado a uma página na qual ele poderá, em dois cliques, utilizar a conta sem anúncios personalizados se assim desejar.

---

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".

185 Para mais sobre a origem e o debate sobre *Privacy by Design* confira-se o artigo de Jonas Valente nesta mesma publicação: Promovendo a privacidade e a proteção de dados pela tecnologia: Privacy by Design e Privacy Enhancing-Technologies.

186 POLONETSKY, Jules; TENE, Omer. **It's not how much data you have, but how you use it: assessing privacy in the context of consumer data integration**. Disponível em: <https://fpf.org/wp-content/uploads/2012/12/FPF_WP-HowYouUse.pdf>. Acesso em: 27.03.17.

187 Este processo é descrito com base na experiência pessoal de criar uma conta para teste no dia 8 de janeiro de 2017 por meio do link disponível em: <https://accounts.google.com/SignUp?hl=en>. Acesso em: 27.03.17.

Insista-se que a legislação europeia estimula a criação de ferramentas que coletam apenas os dados necessários para determinado fim, mas não impede que uma atividade empresarial se apoie em várias finalidades específicas diferentes. Na realidade, há 6 hipóteses legítimas para a coleta de dados e toda uma sociedade que pode se beneficiar de modelos de negócios baseados em dados[188].

Além disso, a abordagem para fazer com que o consentimento seja removido de modo tão facilitado quanto sua obtenção, de forma granular e endereçando o problema do controle informacional, pode ser identificada através da página "Minha Conta", uma ferramenta que permite, por exemplo, a desvinculação de serviços, a remoção do histórico de pesquisas realizadas (inclusive as feitas por voz) e o apagamento de registros de localização.

Abordar a questão da assimetria informacional e devolver o controle das informações pessoais aos usuários por meio de painéis de controle, como também faz a Microsoft no *Privacy Dashboard*[189], vem se mostrando uma forma eficiente de balancear direitos fundamentais e interesses comerciais legítimos na Internet e um campo fértil para inovações.

Para não estimular a criação de um amontoado de regras que dificilmente passariam no teste de proporcionalidade, recorda-se que avaliar a efetividade dessas ferramentas e criar condições necessárias para que elas floresçam é um compromisso compartilhado e que requer amadurecimento (a diretiva europeia comentada sequer está em vigor), bem como esforços em educação digital. Há muito que os usuários podem fazer para impactar os algoritmos, como será examinado a seguir.

Estourando a bolha pelas normas sociais

Sabe aquela foto que você envia no Instagram mas não no Facebook? Vídeo do Porta dos Fundos no LinkedIn é permitido? Dois minutos de fotos ou vídeos na história do Snapchat: overposting? Mas quem ainda usa Snapchat? Lembra quando era um ultraje pedir para "*add* sem *scrap*"? As regras vão além:

188 ANDRADE, Pedro Less; HEMERLY, Jess; RECALDE, Gabriel; RYAN, Patrick. From Big Data to Big Social and Economic Opportunities: Which Policies Will Lead to Leveraging Data-Driven Innovation's Potential? The Global Information Technology Report 2014: Rewards and Risks of Big Data, Chapter 1.8. INSEAD. Cornell University and the World Economic Forum. Disponível em: < http://www3.weforum.org/docs/GITR/2014/GITR_Chapter1.8_2014.pdf >. Acesso em: 27.03.17.

189 FINGAS, Jon. Microsoft privacy dashboard gives you control over your data. **ENGADGET**. Publicado em: 10.01.17**.** Disponível em: <https://www.engadget.com/2017/01/10/microsoft-privacy-dashboard/>. Acesso em: 23.03.17.

rir com "huahua", repassar corrente de e-mail, fazer indiretas no Facebook, mandar bom dia em grupo do Whatsapp[190].

O conjunto dos usos e costumes do que os usuários coletivamente entendem que seja apropriado ou não dentro de um contexto ou de uma ferramenta é o que caracteriza a regulação pelas normas sociais, que pode ser muito mais efetiva e necessária do que se imagina.

Há um forte caráter complementar à regulação pela arquitetura. Uma vez que boa parte das reivindicações direcionadas às plataformas e redes sociais giram em torno da melhoria e facilitação nos mecanismos de controle pelos usuários, nenhuma mudança significativa do cenário pode vingar sem a sua participação.

Especificamente com relação às bolhas de conteúdo há muito que se pode fazer: como confirmado por uma pesquisa publicada na *Science*, os algoritmos do Facebook importam muito menos para determinar o que nós vemos na timeline dessa rede social do que os amigos com quem escolhemos interagir[191], recordando-se também que é possível inclusive orientar a timeline para mostrar publicações na ordem em que elas são publicadas[192] .

Em outra pesquisa, esta do Pew Research Center[193] foi apontado que a maioria dos americanos acha estressante e frustrante falar sobre política nas redes sociais. Ainda, quando discutem sobre política, a maioria tende a sentir ter menos em comum com o interlocutor do que achava que tinha.

Outra descoberta da pesquisa foi que a maioria dos usuários possui a percepção de que as discussões são mais agressivas e, por isso, tentam ignorar discussões políticas nas redes sociais. Quando isso não dá certo, os usuários tomam atitudes para controlar seus *feeds.*

Há vezes em que o próprio usuário cria a sua bolha e, provavelmente, antes mesmo da Internet existir já fosse assim. De certo modo, filtros sempre existiram, visto que a sociedade sempre consumiu informações filtradas através

---

190 Importante: os exemplos são meramente hipotéticos e não são moralmente condenáveis pelo autor, que não confirma nem nega ter realizado nenhuma das ações descritas.

191 A. Lada; BAKSHY, Eytan; MESSING, Solomon. Exposure to ideologically diverse news and opinions on Facebook. **ADAMIC**. Disponível em: <http://science.sciencemag.org/content/348/6239/1130>. Acesso em: 17 jan. 2017.

192 FACEBOOK. Help Center. Disponível em: <https://www.facebook.com/help/218728138156311?helpref=related>. Acesso em: 17 jan. 2017

193 The Political Environment on Social Media. **PEW RESEARCH CENTER**. Publicado em: Out/2016. Disponível em: <http://www.pewinternet.org/2016/10/25/the-political-environment-on-social-media/>. Acesso em: 30 out. 2016.

de editores. Ora, a escolha entre assinar o jornal X ou Y e assistir o canal A ou B poderia, por si só, indicar justamente isso.

Outrossim, não se pode esquecer que editores podem ser muito menos transparentes do que algoritmos. De certo modo, os debates sobre filtros de conteúdo questionam muito pouco o papel da própria mídia[194].

Há quem observe que a Internet foi tanto responsável pela eleição de Obama em 2008[195] quanto pela eleição de Trump em 2016[196]. Neste último caso, pela divulgação e proliferação de notícias falsas a respeito da candidata opositora Hillary Clinton através das redes sociais, seguindo-se então um grande debate sobre o papel dos intermediários e o que eles poderiam ou deveriam fazer para evitar notícias falsas pela rede, potencializadas pelas bolhas de informação.

O professor Kelly Garrett da Universidade de Ohio tem alguns estudos publicados que contestam a ideia de que o ambiente online tenha efetivamente privado a sociedade de ter contato com pontos de vista diferentes e separa de uma forma bastante interessante o problema do filtro de conteúdo e o de notícias falsas. Segundo ele:

> (...) O software do Facebook aprende com as ações passadas dos usuários, tentando adivinhar quais histórias provavelmente serão mais clicadas e compartilhadas no futuro. Levado ao extremo, isso produz um filtro bolha, no qual os usuários são expostos apenas a conteúdos que reafirmam seus preconceitos. O risco, então, é que os filtros bolha promovem percepções distorcidas ao esconder a verdade. O apelo desta explicação é óbvio. É fácil de entender, então talvez seja fácil de corrigir. Livre-se da personalização dos feeds acabe com os filtros bolha. O problema com a metáfora do filtro bolha é que ela supõe que as pes-

194 Apenas para ficar dentro do exemplo da tecnologia, veja que nenhum senso de "moral jornalística" fez o The Guardian modificar seu editorial. Disponível em: <https://www.theguardian.com/technology/2016/dec/17/holocaust-deniers-google-search-top-spot>, que divulga uma interpretação imprecisa de um artigo escrito por Danny Sullivan, do SearchEngineLand, mesmo depois dos vários pedidos. Disponível em: <http://searchengineland.com/google-holocaust-denial-site-gone-266353>, ou de publicar um artigo, segundo a EFF, sensacionalista sobre uma suposta *backdoor* na criptografia do WhatsApp, disponível em: <https://www.eff.org/deeplinks/2017/01/google-launches-key-transparency-while-tradeoff-whatsapp-called-backdoor>. Todos os links com acesso em: 17 jan. 2017.

195 DUTTA, Soumitra; FRASER, Matthew. Barack Obama and The Facebook Election. **US NEWS**. Publicado em 19.11.2008. Disponível em: <http://www.usnews.com/opinion/articles/2008/11/19/barack-obama-and-the-facebook-election>. Acesso em: 17 jan. 2017.

196 LAPOWSKY, Issie. Here's how Facebook Actually Won Trump the Presidency. **WIRED**. Publicado em: 15 nov. 2016. Disponível em: <https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news/>. Acesso em: 23 mar. 2017.

> soas estão perfeitamente isoladas de outras perspectivas. De fato, inúmeros estudos mostraram que os hábitos dos usuários quase sempre incluem informações e fontes que desafiam suas preferências políticas. Um estudo de dados de usuários do Facebook descobriu que o encontro com informações diversificadas é bastante comum. Em outras palavras, é pouco provável que as notícias falsas (falsas crenças) sejam explicadas pela falta de contato das pessoas com notícias mais precisas. Ao contrário, as identidades políticas preexistentes das pessoas moldam profundamente suas crenças. Assim, mesmo quando confrontados com a mesma informação, seja em um artigo ou um fato confirmado, pessoas com diferentes orientações políticas frequentemente extraem significados dramaticamente diferentes[197].

Não parece haver comprovação ou consenso de que foram notícias falsas que determinaram o resultado das eleições, havendo aqueles que concordam[198] com a ideia, os que discordam[199], os que não sabem dizer[200] e uma teoria mista: ainda que as plataformas não sejam diretamente responsáveis, há algo que precisa ser modificado[201].

---

197 Tradução livre de: "(...) Facebook's software learns from users' past actions; it tries to guess which stories they are likely to click or share in the future. Taken to its extreme, this produces a filter bubble, in which users are exposed only to content that reaffirms their biases. The risk, then, is that filter bubbles promote misperceptions by hiding the truth. The appeal of this explanation is obvious. It's easy to understand, so maybe it'll be easy to fix. Get rid of personalized news feeds, and filter bubbles are no more. The problem with the filter bubble metaphor is that it assumes people are perfectly insulated from other perspectives. In fact, numerous studies have shown that individuals' media diets almost always include information and sources that challenge their political attitudes. And a study of Facebook user data found that encounters with cross-cutting information is widespread. In other words, holding false beliefs is unlikely to be explained by people's lack of contact with more accurate news. Instead, people's preexisting political identities profoundly shape their beliefs. So even when faced with the same information, whether it's a news article or a fact check, people with different political orientations often extract dramatically different meaning". GARRETT, Kelly. **Facebook's problem is more complicated than fake news**. Publicado em: 16 nov. 2016. Disponível em: <https://theconversation.com/facebooks-problem-is-more-complicated-than-fake-news-68886>. Acesso em: 10 jan. 2017.

198 NEWTON, Casey; ROBERTSON, Adi; TIFFANY, Kaitlyn. How social platforms influenced the 2016 election. **THE VERGE**. Publicado em: 14 nov. 2016. Disponível em: <http://www.theverge.com/2016/11/14/13626694/election-2016-trending-social-media-facebook-twitter-influence>. Acesso em: 10 jan. 2017.

199 MASNICK, Mike. If you're blaming Facebook for the presidential election results, you're an idiot. **RECODE**. Publicado em: 9 nov. 2016. Disponível em: <http://www.recode.net/2016/11/9/13578924/trump-blame-facebook-election-results-algorithm-president>. Acesso em: 10 jan. 2017.

200 POOLEY, Jefferson. Why We Can't Know Whether Facebook is to Blame for Trump's Election. **SLATE**. Publicado em: 11 nov. 2016. Disponível em: <http://www.slate.com/blogs/future_tense/2016/11/11/we_can_t_know_whether_facebook_is_to_blame_for_trump_s_win.html>. Acesso em: 10 jan. 2017.

201 CONDLIFFE, Jamie. Regardless of Its Influence on the Election, Facebook Needs to Change. **MIT Technology Review**. Publicado em: 14 nov. 2016. Disponível em: <https://www.technologyreview.com/s/602851/regardless-

A exposição foi tamanha que o Facebook anunciou[202] que iria endereçar o problema através de uma modificação na sua ferramenta: denúncias de usuários (as quais, vale lembrar, já existiam) marcando determinada notícia como falsa colocariam um sinal de "disputado" sobre ela, que a levaria então a um terceiro para comprovar os fatos. Como esperado, já há quem discorde da investida[203] e quem ache que o Facebook não deveria verificar fatos[204].

Do ponto de vista dos provedores de aplicações de internet , a aversão inicial em tomar a frente dessa questão é bastante compreensível. De modo geral, essas plataformas foram desenvolvidas para jogar um jogo com regras bem claras: não monitorar e não censurar[205]. Isto explica porque todas as alternativas encontradas até aqui são razoavelmente minimalistas e envolvem a ação de terceiros: realizar controle editorial nunca esteve nos planos de nenhuma empresa de tecnologia.

Um dos argumentos de Pariser é que "na batalha pelo controle da Internet todo mundo está organizado, menos as pessoas"[206]. Defende-se, por outro lado,

---

of-its-influence-on-the-election-facebook-needs-to-change/>. Acesso em: 15 jan. 2017.

202 MOSSERI, Adam. News Feed FYI: Addressing Hoaxes and Fake News. FACEBOOK's NEWSROOM. Disponível em: <http://newsroom.fb.com/news/2016/12/news-feed-fyi-addressing-hoaxes-and-fake-news/>. Acesso em: 18 dez. 2016.

203 MCGREGOR, Jay. Facebook's Fake News Solution Has Three Big Problems. **FORBES**. Disponível em: <http://www.forbes.com/sites/jaymcgregor/2017/01/16/facebooks-fake-news-solution-has-three-big-problems/#7efc47805d86>. Acesso em: 10 jan. 2017.

204 LESSIN, Jessica. Facebook Shouldn't Fact Check. **THE NEW YORK TIMES**. Publicado em: 29 dez. 2016. Disponível em: <https://www.nytimes.com/2016/11/29/opinion/facebook-shouldnt-fact-check.html>. Acesso em: 29 dez. 2016.

205 Naturalmente isto não significa que nenhum controle deve ou é exercido pelas plataformas. Para compreensão dos deveres dos provedores de serviços, de modo geral. LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez Editora, 2005, sendo importante mencionar que "os provedores de serviços são livres para estabelecer contratualmente qual espécie de conteúdo poderá ser armazenado em seus servidores ou disponibilizado a terceiros, bem como que medidas serão tomadas em caso de violação dos termos do serviço, assim como são livres os usuários contratantes de tais serviços para escolher empresas que permitam ou não a divulgação de conteúdos questionáveis ou potencialmente lesivos, respeitadas sempre as normas de ordem pública." LEONARDI, Marcel. cit., p. 78. A obra está disponível para acesso em: <http://leonardi.adv.br/wp-content/uploads/2011/04/mlrcpsi.pdf>. Acesso em: 27 mar. 2017.

206 "(...) In the fight for control of the Internet, everyone's organized but people. But that's only because most of us aren't in the fight. People who use the Internet and are invested in its future outnumber corporate lobbyists by orders of magnitude. (...) Protecting the early vision of radical connectedness and user control should be an urgent priority for all of us". PARISER, Eli. **The Filter Bubble**, p. 242.

que a sociedade pode não só influenciar os algoritmos[207], mas também decisões corporativas[208] e, inclusive, o cenário legislativo[209].

Um exemplo casuístico de como seria possível influenciar os algoritmos (sem qualquer juízo de valor) pode ser observado no fenômeno que ficou conhecido como "Google bomb", uma tentativa coletiva de milhares de usuários de influenciar os resultados de pesquisa do Google para que determinada expressão direcionasse a uma determinada página. No Brasil, o termo de busca "déspota cachaceiro" levava à página oficial da Presidência quando Lula era presidente. Nos Estados Unidos, o termo "miserable failure" apontava para o site oficial da biografia de George W. Bush[210].

É preciso pensar não só como os algoritmos impactam movimentos sociais[211], mas como os movimentos sociais podem impactar o algoritmo, criar programas de educação digital e debates sobre o funcionamento e a complexi-

---

207 Para um bom cenário dos desafios de se manter uma política de conteúdo coesa e bons exemplos de como é possível *game the system*. BOYD, Danah. **Hacking the Attention Economy.** Disponível em: <_https://points.datasociety.net/hacking-the-attention-economy-9fa1daca7a37#.ows3lhmhk >. Acesso em: 10 jan. 2017.

208 VINCENT, James. Google reverses decision to ban adult content on Blogger. **THE VERGE**. Publicado em: 27 fev. 2015. Disponível em: <http://www.theverge.com/2015/2/27/8119553/blogger-adult-content-ban-reversed>. Acesso em: 10 jan. 2017.

209 Ao comentar as lições aprendidas com esse processo de participação, Carlos Affonso Souza e Ronaldo Lemos ensinam que "Saber quais lições serão aprendidas, quais experiências serão determinantes para o futuro da regulação da rede no Brasil, é um exercício que ainda depende em grande parte de acontecimentos que estão por vir. Até esse ponto, o que pode se afirmar com segurança é que o Marco Civil da Internet produziu um notório impulso na qualidade da participação cidadã na construção de leis. É em si uma conquista, mas não um ponto de chegada. É justamente buscando a diversidade de opiniões e de expertise que se garante que a regulação da rede não seja fruto dos interesses de uns ou outros, dos suspeitos usuais e que toda a coletividade que depende crescentemente da rede para as suas atividades diárias, sejam elas pessoais ou profissionais, não seja prejudicada por debates e decisões regulatórias sobre as quais ela não apenas desconhece como, se conhecesse, jamais poderia participar. Usar a rede para melhorar a regulação e a governança da rede é a mais importante lição ensinada pelo processo de construção do Marco Civil. Que ela seja sempre lembrada quando soluções precisam ser criadas para os desafios que vêm pela frente". In: LEMOS, Ronaldo; SOUZA, Carlos Affonso. **Marco Civil da Internet: construção e aplicação**. Editar Editora Associada: 2016, p. 42.

210 Naturalmente, não estamos endossando a prática. Para mais, confira-se: **WIKIPEDIA**. Bomba do Google. n.d. Disponível em: <https://pt.wikipedia.org/wiki/Bomba_do_Google>. Acesso em: 27 mar. 2017.

211 MOORE, Taylor. How Algorithms Can Impact Online Civil Rights Movements. **CENTER FOR DEMOCRACY AND TECHNOLOGY**. Publicado em: 10 jan. 2017. Disponível em: <https://cdt.org/blog/how-algorithms-can-impact-online-civil-rights-movements/>. Acesso em 10 jan. 2017.

dade da Internet. Muitas coisas estão sendo feitas, valendo ressaltar uma pesquisa do InternetLab que avançou nessa discussão[212].

O Brasil mostrou que é possível construir uma agenda positiva para a regulação da rede que envolva também a sociedade civil com o Marco Civil da Internet. Contudo, talvez seja hora de avançar também no debate sobre o uso que é feito das plataformas. Novamente, a efetividade das medidas apenas o tempo e a experiência poderão atestar, mas, enquanto se espera, talvez seja interessante revermos nossos hábitos, observarmos se nossas *timelines* estão exageradamente parciais através de ferramentas que tentam fazer essa medição, como o , e, se for o caso, voltar a seguir e a interagir com aquela conexão que votou no candidato opositor e seguir mais de um veículo de notícias (Veja e Carta Capital, por exemplo) ao mesmo tempo.

A norma jurídica: eficácia da tutela de direitos através da proteção de dados

Ao final de seu livro, Eli Pariser propõe dois principais pontos de ação para os governos. Em sua concepção, o Estado deveria agir para determinar que as empresas dessem o controle dos dados pessoais de volta aos usuários e criar uma agência específica para fiscalizar se as empresas estão cumprindo as regras. De forma geral, essas obrigações e agências já existem em diversos modelos regulatórios[213], algo até reconhecido pelo autor, que critica o modelo fragmentário americano[214].

A racional utilizada por Pariser parece ser esta: se o "cerne" do problema está na personalização feita através da coleta de dados pessoais, seria preciso então disciplinar essa atividade. Diminuir a personalização seria diminuir o

212 Nos referimos à pesquisa #OutrasVozes, conduzida por Natália Neris e Mariana Valente, que "acompanhou perfis de ativistas de Direitos Humanos a fim de monitorar e registrar semanalmente, durante a última campanha eleitoral, discussões sobre gênero, raça, sexualidade, origem regional e classe social, e sua relação com política e internet". Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2017/02/relatorio_outras_vozes.pdf>. Acesso em 27 mar. 2017.

213 Para mais sobre os modelos regulatórios dos Estados Unidos e da União Europeia confira-se o artigo escrito por Guilherme Berti de Campos Guidi intitulado "Modelos Regulatórios para Proteção de Dados Pessoais", que se encontra publicado na presente obra.

214 "A bigger step would be putting in place an agency to oversee the use of personal information. The EU and most other industrial nations have this kind of oversight, but the United States has lingered behind, scattering responsibilities for protection personal information among the Federal Trade Commission, the Commerce Department, and other agencies. As we enter the second decade of the twenty-first century, it's past time to take this concern seriously". PARISER, Eli. cit. p. 241.

efeito do filtro e o maior controle sobre o uso dos dados resultaria em um maior controle sobre o fluxo de informações.

O problema, como descrito anteriormente, é que o usuário pode ser o principal causador de seu filtro bolha, seja por eliminar quem pensa diferente das *timelines* das redes sociais, seja por não buscar informações de fontes diferentes ou por dar uma preferência muito grande aos seus hobbies ao consumir informação através da Internet.

Nos capítulos anteriores, foi visto que criar plataformas para aumentar as diferentes opiniões sobre determinado assunto ou realizar intervenções diretas nas formas com as quais os algoritmos dos serviços online são criados não necessariamente diminuiria o efeito identificado por Pariser. Do mesmo modo, diminuir o uso de dados para a personalização de serviços (sejam eles quais forem) pela plataforma não necessariamente significaria diminuir os efeitos das bolhas de informação. O que possivelmente se estaria promovendo é a substituição de um filtro por outro; um filtro não personalizado, mas ainda existente. Ou pior: a eliminação de todos os filtros submeteria a coletividade a todas as informações disponíveis.

Pariser defende também a ideia de que dados pessoais devem ser vistos como "um tipo especial de propriedade" do indivíduo, de modo a criar um mercado mais justo. Esta ideia é melhor recebida nos Estados Unidos e defendida, por exemplo, por Lawrence Lessig e Paul M. Schwartz[215], um reflexo da autonomia da proteção de dados frente a privacidade.

Dando alguns passos atrás, percebe-se que a doutrina sempre encontrou dificuldade[216] ou talvez tenha resistido muito à ideia da pouca utilidade prática em definir o conceito de privacidade, que sempre foi vista como uma barreira entre o indivíduo e intromissões externas ou o "direito de ser deixado só"[217].

Danilo Doneda, um dos primeiros a identificar, em âmbito nacional, a autonomia da proteção de dados frente a privacidade, analisando as leis surgidas a partir dos anos 70 e a Diretiva 95/46/CE, afirma que:

---

215 SCHWARTZ, Paul M. Property, Privacy, and Personal Data, 117 **Harvard Law Review** 2055 (2004). Disponível em: <http://scholarship.law.berkeley.edu/facpubs/2150>. Acesso em: 27 mar. 2017.

216 SOLOVE, Daniel J. Understanding Privacy. **Harvard University Press**, 2009, p. 3: "Any attempt to locate a common denominator for all the manifold things that fall under the rubric of "privacy" faces an onerous choice. A common denominator broad enough to encompass nearly everything involving privacy risks being overinclusive or too vague. A narrower common denominator risks being too restrictive".

217 DA SILVA, José Afonso da. **Direito Constitucional Positivo**. 35ª Edição rev. e atual. Editora Malheiros, 2012, p. 206.

> A necessidade de funcionalização da proteção da privacidade faz, portanto, com que ela originasse uma disciplina de proteção de dados pessoais, que compreende pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua "continuação por outros meios". Ao realizar esta continuidade, porém, assume a tarefa de conduzir uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias - especialmente na forma de atuar os interesses que protege, mas também em referência a outros valores e direitos fundamentais. Daí a necessidade de superar a ordem de conceitos pela qual o direito a privacidade era limitado por uma tutela de índole patrimonialista, e de estabelecer novos mecanismos e mesmo institutos para possibilitar a efetiva tutela dos interesses da pessoa[218].

Nota-se, então, que a tutela da privacidade se manifestará contemporaneamente sobretudo através da tutela da proteção de dados por 3 razões: a) a possibilidade de enxergar a proteção de dados como direito fundamental abre espaço para a criação de políticas públicas específicas; b) leis de proteção de dados olharam para o direito negativo de ser deixado em paz e o transformaram no controle dos dados pelo titular; e c) leis de proteção de dados atuais endereçam o problema da assimetria informacional[219].

Com relação aos itens "b" e "c" indicados acima, Alexandre Pacheco observou que as propostas de lei geral de proteção de dados pessoais que vigoram se apoiam no conceito de autogestão ou "*privacy self-management*". Fundamentada na autodeterminação informativa, a "*privacy self-management*" impõe às empresas dentro do ciclo de coleta e tratamento da informação 3 deveres, quais sejam: a) a "notificação" (o usuário precisa saber que os dados estão sendo coletados, similar ao princípio da publicidade); b) o "acesso" (o usuário precisa ter acesso ao banco de dados com suas informações); e c) o "consentimento" (o usuário precisa consentir, de forma livre e informada com a coleta de seus dados) [220].

Esses três princípios básicos (outros existem[221] e estão inclusive nos projetos de lei para uma lei geral de proteção de dados no Brasil) existiriam para que o usuário

---

218 DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro. Renovar, 2006, p. 27.

219 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor.** São Paulo. Saraiva, 2014, p. 26.

220 PACHECO, Alexandre. Se você sabe quem eu sou, eu quero saber quem você é. **Inc. Soc.**, Brasília, DF, v. 5 n. 2, p-165-182, jan/jun, 2012.

221 DONEDA, Danilo. Princípios de Proteção de Dados Pessoais**.** *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III - Tomo I: Marco**

pudesse tomar uma decisão informada e consciente sobre os benefícios e os prejuízos da sua escolha em trocar dados pelos serviços gratuitos disponíveis na web.

Há uma forte crítica sobre a contratualização resultante desse modelo, materializada sobretudo pelos termos de uso e políticas de privacidade[222] e facilitada, entre outras coisas, pela ideia de "propriedade" tratada acima. Ocorre que não é apenas através de arranjos contratuais que negócios baseados em dados são legitimados.

Como comentado no capítulo sobre regulação pela arquitetura, algumas ferramentas precisam ser desenvolvidas e aprimoradas para incorporar a ideia do controle e da autogestão pelos usuários. Além disso, sempre que possível, deve-se buscar legitimar operações de uso de dados em mais de uma hipótese legal, evitando-se o chamado sobrecarregamento do consentimento.

A ideia de que termos de uso e políticas de privacidade são sempre documentos excessivamente longos e difíceis de entender é uma generalização. Nem todos são assim e, como debatido no capítulo sobre regulação pela arquitetura, não são apenas estes documentos que devem legitimar as operações através de usos de dados (a personalização da experiência *online* é apenas um dos vários exemplos). Ademais, diversos instrumentos legais existem para coibir práticas abusivas.

Em que pesem as críticas ao negócio em si,[223] normas para a proteção de dados não proíbem negócios baseados em dados de existirem, ainda que possam coerentemente vedar algumas práticas.[224] Aliás, essa pauta, ao menos no Brasil, sequer foi encampada pelas instituições de defesa do consumidor nos debates sobre os projetos de lei para a criação de uma lei geral de proteção de dados (ainda inexistente, recorde-se), preservando a legalidade da escolha[225] feita pelos usuários.

Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015, p. 369-384.

222 Para uma análise sobre a importância - ou mesmo sobrecarregamento - do consentimento e autogestão para essas operações, defendendo um modelo ambivalente confira-se: 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) Universidade de São Paulo, 2016.

223 ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal of Information Technology**. Publicado em: 4 abr. 2015. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>. Acesso em: 23 mar. 2017.

224 Por exemplo a proibição pelo Marco Civil da Internet do provedor de conexão de armazenar, para qualquer fim que seja, os registros de acesso às aplicações de Internet visitadas pelo usuário.

225 "Pagar com dados é uma escolha válida e precisa ser respeitada. É um modelo que permite a todos os usuários participar do ecossistema online, e não apenas a quem dispõe de recursos para pagar por conteúdos e serviços. Dificultar o tratamento de dados para fins comerciais pode inviabilizar práticas

No caso específico dos filtros de conteúdo, parece um desvio de foco tratar a questão através de um olhar mais rigoroso no cenário legislativo sobre proteção de dados quando, na realidade, diversas outras alternativas podem ser encontradas.

Quanto mais opções existirem para os usuários, mais fácil será para eles escolherem uma plataforma ou serviço de acordo com suas políticas de privacidade e seu histórico de comprometimento (ou não) com boas práticas, bem como pressionar as existentes por mudanças.

A interação entre novas tecnologias e usuários deve garantir a eficácia das normas consumeristas e das normas para a proteção de dados, mas é preciso que exista um ambiente equilibrado para que novos serviços sejam criados e os existentes se desenvolvam. Como pontuado por Hal Varian, é crescente a importância do *small data* e a consciência de que pequenos negócios também possuem hoje a possibilidade de se beneficiarem com a análise de dados sobre seus negócios.[226]

Além de permitir a criação de novas tecnologias e serviços, é preciso também melhorar as já existentes. Apesar da frase "utilizamos as informações que coletamos para melhorar os nossos serviços e criar uma experiência personalizada" parecer um jargão vago do Vale do Silício, é essa noção que vem contribuindo para a significativa melhora dos tradutores e dos sistemas de reconhecimento de voz que usam *machine learning,* para citar apenas duas aplicações[227]. Ainda segundo Varian:

> Estudos observacionais podem descobrir padrões e correlações interessantes em dados. Mas a melhor prática para estabelecer relações causais é a experimentação, e é por isso que empresas como o Google experimentam rotineiramente e continuam a melhorar seus sistemas. Quando as transações são

lícitas consagradas no mercado brasileiro e emperrar a economia digital". LEONARDI, Marcel. Marco Civil da Internet, Plataformas Digitais e Redes Sociais. In: ARTESE, Gustavo (coord.). **Marco Civil da Internet: Análise Jurídica Sob uma Perspectiva Empresarial.** Quartier Latin: 2015.

226 "We hear a lot about "big data" (...) but "small data" can be just as important, if not more so. Twenty years ago only large companies could afford sophisticated inventory management systems. But now every mom-and-pop corner store can track its sales and inventory using intelligent cash registers, which are basically just personal computers with a drawer for cash. Small business owners can handle their own accounting using packaged software or online services, allowing them to better track their business performance. Indeed, these days data collection is virtually automatic. The challenge is to translate that raw data into information that can be used to improve performance." VARIAN, Hal. *Intelligent Technology.* **International Monetary Fund.** FINANCE & DEVELOPMENT, September 2016, Vol. 53, No. 3. Disponível em: <http://www.imf.org/external/pubs/ft/fandd/2016/09/pdf/varian.pdf>.

227 Para exemplos sobre como esses conceitos vêm sendo utilizados na indústria, confira-se: Machine Learning: Solving Problems Big, Small and Prickly, bem como a indicação de pesquisas e outras referências na descrição do vídeo. Disponível em: <https://www.youtube.com/watch?v=_rdINNHLYaQ&t=1s>. Acesso em: 23 mar. 2017.

> mediadas por computadores, é fácil dividir usuários em grupos de tratamento e controle, implementar tratamentos e analisar resultados em tempo real. Atualmente, empresas usam esse tipo de experimentação rotineiramente para fins de marketing, mas essas técnicas podem ser usadas em muitos outros contextos. Por exemplo, instituições como o Laboratório de Ação de Pobreza Abdul Latif Jameel do Instituto de Tecnologia de Massachusetts foram capazes de realizar experiências controladas de intervenções propostas em economias em desenvolvimento para aliviar a pobreza, melhorar a saúde e elevar o nível de vida. Experimentos controlados aleatórios podem ser usados para resolver questões sobre quais tipos de incentivos funcionam melhor para aumentar a economia, educar crianças, gerenciar pequenas fazendas e uma série de outras políticas.[228]

Daí segue que iniciativas legislativas que visam tutelar um "tema da moda" podem não ser a maneira mais adequada de endereçar a questão[229]. É preciso dar espaço para que as instituições e as regulações já existentes cumpram seu papel, mas parece ser ainda mais importante que outras ações sejam colocadas em prática, principalmente aquelas que favoreçam o engajamento e a educação dos usuários.

Considerações Finais

Como observado no primeiro capítulo, a Internet precisa ser vista como um ecossistema cujo equilíbrio é bastante delicado. Abusos do poder legislativo

---

228 VARIAN, Hal. *Intelligent Technology*. **International Monetary Fund.** FINANCE & DEVELOPMENT, September 2016, Vol. 53, No. 3. Disponível em: <http://www.imf.org/external/pubs/ft/fandd/2016/09/pdf/varian.pdf> Tradução livre de: "Observational data can uncover interesting patterns and correlations in data. But the gold standard for discovering causal relationships is experimentation, which is why online companies like Google routinely experiment and continuously improve their systems. When transactions are mediated by computers, it is easy to divide users into treatment and control groups, deploy treatment, and analyze outcomes in real time.

Companies now routinely use this kind of experimentation for marketing purposes, but these techniques can be used in many other contexts. For example, institutions such as the Massachusetts Institute of Technology's Abdul Latif Jameel Poverty Action Lab have been able to run controlled experiments of proposed interventions in developing economies to alleviate poverty, improve health, and raise living standards. Randomized controlled experiments can be used to resolve questions about what sorts of incentives work best for increasing saving, educating children, managing small farms, and a host of other policies".

229 A título de exemplo, cite-se o projeto de lei nº 6812/2017 de autoria do deputado Luiz Carlos Hauly que criminaliza a divulgação e o compartilhamento de informação falsa ou prejudicialmente incompleta na Internet. O projeto não diferencia o autor da notícia de quem a "compartilha" e tem termos excessivamente subjetivos e vagos como "informação prejudicialmente incompleta".

e do poder judiciário foram citados porque são aparentemente mais difíceis de serem solucionados, mas basicamente qualquer "ator" dentro desse ecossistema poderia agir de forma abusiva, ao mesmo tempo em que toda modalidade de regulação terá sempre seu "custo" específico.

A partir do exemplo paradigmático sustentado por Eli Pariser em "The Filter Bubble" e explicado no segundo capítulo, apropriando-se de uma abordagem de regulação proposta por Lawrence Lessig, indagou-se de que maneira seria possível endereçar o problema das bolhas de conteúdo e promover uma regulação adequada da rede.

Seguindo em frente, o primeiro subitem do segundo capítulo buscou analisar a questão da regulação através da arquitetura das plataformas e serviços digitais, ressaltando a crítica bastante recorrente em torno da construção de mecanismos mais transparentes e auditáveis e as dificuldades práticas já debatidas na academia em torno da sua limitação. Argumentou-se então que a regulação pela arquitetura deve ser pautada pela regra da proporcionalidade, mas também de forma estratégica, facilitando o cumprimento das diferentes legislações aplicáveis aos serviços e plataformas que operam pela Internet.

No segundo subitem do segundo capítulo, procurou-se demonstrar que filtros sempre existiram nas formas com as quais consumimos informação (na escolha de determinado canal de TV, de qual jornal ou revista assinar, quais livros ler). Explorou-se também a possibilidade de que mudanças nos hábitos possam ter impactos positivos nas formas com as quais se interage com o conteúdo disponível na web, tentando pensar não só nas formas com que serviços online impactam a sociedade mas também como a sociedade pode impactá-los, reforçando a importância do engajamento dos usuários.

Finalmente, no terceiro subitem do segundo capítulo, analisou-se a regulação pela norma jurídica, em que se explorou a necessidade de se observar os filtros de conteúdo de modo a não se tentar corrigir o problema errado. Por diversos motivos, e pode-se citar a proteção de direitos fundamentais e a criação de segurança jurídica como dois deles, o Brasil precisa de uma lei geral de proteção de dados pessoais, mas ela não pode ser pensada para corrigir os efeitos causados pelas "bolhas de conteúdo".

Deve-se criar condições para que as pessoas efetivamente utilizem as ferramentas de controle de seus dados e para um ambiente favorável à inovação, competição, proteção de direitos e fiscalização de regras sem limitar demasiadamente modelos de negócios.

Há indícios de que vivemos em uma fase de quase negação: uma busca feita por "mulheres bonitas" que reflete padrões estéticos reforçados historicamente tem chocado mais do que suas claras razões sociológicas; termos de busca enviesados procuram demonstrar a parcialidade de motores de busca, como se a pergunta fosse menos importante do que a resposta. A Internet pode tanto amplificar narrativas quanto desconstruí-las e, no fim do dia, somos nós, usuários, que escolhemos qual deve (ou deveria) prevalecer.

Encontrar o ponto de equilíbrio é sim um desafio que precisa ser enfrentado a partir de uma visão ampla, olhando para o que já foi construído. O Marco Civil da Internet se mostrou uma experiência positiva: há que se repetir a dose em uma futura lei geral de proteção de dados pessoais.

Modelos Regulatórios para Proteção de Dados Pessoais

Guilherme Berti de Campos Guidi[230]

Introdução

A privacidade e a proteção de dados pessoais, também chamada de *data privacy*, são temas que têm ocupado espaços cada vez maiores, não mais apenas nos congressos acadêmicos e painéis de discussão, mas também na grande mídia[231]. O cidadão comum, alheio talvez aos grandes debates teóricos, se não tem ainda completa ciência da proteção que pode reclamar para seus dados pessoais, tem no mínimo maiores chances de ser exposto ao assunto.

Tal movimento nos dá importante sinal, pois se mesmo o cidadão comum passa a ter consciência desses seus direitos, ainda que os estudiosos continuem questionando cada vírgula do que foi escrito sobre o assunto, nenhuma dúvida resta sobre a existência de *alguma coisa, algum direito à privacidade e à proteção dos dados.* O presente trabalho não objetiva discutir a existência ou inexistência de um direito à tutela dos dados pessoais nem seus eventuais contornos, mas sim discutir estratégias regulatórias colocadas em prática, tendo como premissa

---

230 Bacharel e Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo - USP, especializado em Direito Digital pela Escola de Direito de São Paulo da Fundação Getúlio Vargas. Pesquisador do grupo de pesquisa "Privacidade na Internet" do Instituto de Tecnologia e Sociedade do Rio de Janeiro e pesquisador colaborador do Grupo de Ensino e Pesquisa em Inovação da Fundação Getúlio Vargas (GEPI/FGV-SP). Membro da Comissão Permanente de Estudos sobre Tecnologia da Informação do Instituto dos Advogados de São Paulo, membro do Comitê de Compliance Digital da *Legal, Ethics and Compliance.* Sócio do escritório Francisco Rezek Sociedade de Advogados.

231 A tal respeito, confira-se, por exemplo: RONCOLATO, Murilo. Por que debater a Lei de Proteção de Dados Pessoais?. **O Estado de São Paulo Online**, 28 jan. 2015. Disponível em: <http://link.estadao.com.br/noticias/geral,por-que-debater-a-lei-de-protecao-de-dados-pessoais,10000029762>. Acesso em 19.01.17. PEDUZZI, Pedro. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. **Agência Brasil EBC**, 19 out. 2015. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet>. Acesso em 19.01.17. ANGWIN, Julia. Protecting Your Digital Privacy Is Not as Hard as You Might Think. **Consumer Reports**, 20 set. 2016. Disponível em: <http://www.consumerreports.org/privacy/protecting-your-digital-privacy-is-not-as-hard-as-you-might-think/>. Acesso em 19.01.17.

a existência de tal direito e seu conteúdo já solidificado, ao menos em princípio, na doutrina sobre o assunto[232]. Dado este enorme passo, deve-se, entretanto, atentar a uma questão relevante e anterior a qualquer discussão sobre direitos e deveres específicos: *como regular?*

O Brasil, chegando atrasado no debate, tenta compensar o tempo perdido, estando o Congresso Nacional pressionado para aprovar algum dos projetos de lei sobre o assunto hoje em trâmite. O que o Congresso discute, no entanto, são propostas que adotam estratégias muito diferentes para abordar a questão[233], pautando o debate nos direitos e deveres que cada projeto promete, sem perceber que a proteção de dados pessoais deve ser pensada antes como política pública, e não como simples objeto passivo para a regulação. Para tanto, é necessário definir, antes de mais nada, qual abordagem regulatória deverá ser adotada, de modo que a tutela da privacidade esteja inserida em um sistema coeso de normas.

Os projetos de lei em discussão no Congresso Nacional, em sua maior parte, adotam modelos legais consolidados, sendo o modelo vigente na União Europeia — ou melhor, o modelo vigente até maio de 2018, dadas as recentes reformas[234] — o mais influente nas propostas. Entretanto, mesmo que as leis brasileiras copiassem o que há de melhor lá fora, nem sempre tais modelos seriam suficientes para garantir direitos e, ao mesmo tempo, incentivar o desenvolvimento tecnológico e econômico, sobretudo nos negócios digitais. A maioria dos modelos atuais tem grande foco em legislação garantista, protetiva, que impõe igualmente diversos deveres aos interessados nos dados alheios. Outros, por sua vez, relegam à autorregulação, ao direito contratual e ao Judiciário a tutela de direitos.

Tal discussão, geralmente, traz um viés essencialmente protetivo ao usuário, sem considerar, por outro lado, os interesses econômicos e o interesse geral no desenvolvimento tecnológico e na inovação. Por essa razão, é necessário justamente dar um passo atrás e pensar em como se pretende fazer para que os titulares tenham seus direitos respeitados, que as empresas cumpram

232 Sobre os fundamentos da proteção dos dados pessoais, confira-se: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006; e LEONARDI, Marcel. **Tutela e privacidade na Internet**, São Paulo: Saraiva, 2012.

233 Entre os projetos de lei mais relevantes, vale destacar: os PLs nº 4.060/2012 e nº 5.276/2016 da Câmara dos Deputados e os PLs nº 181/2014, 131/2014 e 330/2013 do Senado Federal.

234 Como será visto com mais detalhes no item 2, a União Europeia recentemente adotou um modelo aprimorado de proteção de dados, consubstanciado no Regulamento nº 679 de 2016, que substitui a norma anterior, esta que foi fonte de inspiração para outros ordenamentos jurídicos, a Diretiva nº 95/46/CE.

suas obrigações e que a sociedade como um todo considere a privacidade um direito essencial, como efetivamente é.

Para que se possa iniciar tal debate, deve-se primeiro verificar, mapear, o que existe e suas características principais, de modo a revelar a estratégia central de cada modelo para regular a coleta e o uso dos dados pessoais.Serão analisados, para tanto, brevemente os pontos principais de três modelos distintos: o europeu, o norte-americano e o uruguaio. A escolha desses objetos de análise se deve às interessantes variações e contrastes estratégicos entre cada um: um modelo tradicional, de grande influência para outros países e baseado em uma abordagem personalista; um segundo modelo, diametralmente oposto, baseado em valores como propriedade e liberdade contratual; e um terceiro, que buscou adaptar o modelo europeu às exigências da América Latina da virada do milênio.

Espera-se que tal esforço possa evidenciar, em uma análise atenta posterior, quais estratégias regulatórias têm mais sucesso e como elas podem ser combinadas para produzir um paradigma eficiente e prático de modo a garantir a privacidade do indivíduo comum sem descuidar do incentivo à inovação e ao desenvolvimento tecnológico.

O Modelo Europeu

A União Europeia sempre esteve na vanguarda no que diz respeito à proteção de dados pessoais. A Convenção nº 108 do Conselho Europeu, a chamada Convenção de Estrasburgo, inaugurou[235], em 1981, as iniciativas para um modelo robusto de tutela, que hoje é referência em todo o mundo[236].

Antes que se dê mais um passo, é importante esclarecer a natureza jurídica das normas da União Europeia. Regulamentos são normas vinculativas diretamente aplicáveis a todos os países, incluindo-se aí seus cidadãos e pessoas jurídicas, valendo como se direito nacional fosse. Diretivas são normas adotadas pela Comissão e pelo Parlamento Europeu que fixam um objetivo que todos os Estados-Membros devem alcançar, cabendo a cada um decidir os meios exatos para tal, respeitando os preceitos básicos da norma supranacional. Decisões são atos vinculativos apenas para partes específicas, sejam elas Estados ou empresas, sendo diretamente aplicá-

235 Isso sem contar ainda algumas leis anteriores de países daquele continente, por vezes de alcance nacional e por outras leis regionais. Bons exemplos são a Bundesdatenschutzgesetz, de 1977, do Land de Hesse, na Alemanha, e a Loy Informatique et Libertés, de 1978, da França.

236 Países como Uruguai, Argentina e Brasil possuem leis de proteção de dados, ou projetos de leis, inspirados profundamente no modelo europeu da Diretiva nº 95/46/CE, a normativa central em vigor no continente.

veis para os envolvidos. Recomendações e pareceres são atos não vinculativos e podem ser emitidos por diversas instituições europeias, contendo normalmente a recomendação de se adotar ou evitar certa posição ou comportamento, ou a declaração de uma posição quanto à determinada questão[237].

Estrutura normativa e de tutela

O sistema[238] atualmente vigente de proteção de dados pessoais é composto por diretivas, regulamentos, decisões vinculantes e orientações de diversos níveis hierárquicos, criando um quadro legal de diversas camadas que partem sempre de orientações gerais e estabelecem normas cada vez mais específicas sobre os direitos e obrigações relativos aos dados pessoais.

Ainda em vigor[239], a Diretiva 95/46/CE é o texto legal central no sistema europeu de proteção de dados pessoais. A Diretiva centraliza os principais conceitos no campo da proteção dos dados pessoais na União Europeia. Ela traz os princípios básicos da tutela dos dados pessoais, tanto na coleta quanto na manipulação e tratamento de tais dados pelos interessados e por terceiros, direitos básicos dos titulares dos dados tratados, estabelece padrões para as transferências internacionais de dados e cria ainda um aparato de supervisão que sirva como fiscal, árbitro e legislador, nas funções que a Diretiva lhe atribui.

Outras diretivas, de caráter complementar, foram também criadas, buscando a transposição dos princípios da Diretiva 95/46 para outras áreas de controle

237 Os atos jurídicos normativos da União Europeia estão descritos no artigo 288 do Tratado sobre o Funcionamento da União Europeia (TFUE). O TFUE resultou da alteração do Tratado de Roma, de 1957, que estabeleceu a Comunidade Europeia, pelo Tratado de Lisboa assinado em 2007, que reforma os tratados base da União e reorganiza suas instituições.

238 Falou-se aqui de sistema pois o modo de interrelação entre as diversas Diretivas, Regulamentos, Decisões vinculantes regionais e suas contrapartes nacionais enquadram-se no conceito de Norberto Bobbio, que assim define sistema: "Diz-se que um ordenamento jurídico constitui um sistema porque não podem coexistir nele *normas incompatíveis*. Aqui, "sistema" equivale à validade do princípio que exclui a incompatibilidade das normas. Se num ordenamento vêm a existir normas incompatíveis, uma das duas ou ambas devem ser eliminadas. Se isso é verdade, quer dizer que as normas de um ordenamento têm um certo relacionamento entre si, e esse relacionamento é o relacionamento de compatibilidade, que implica a exclusão da incompatibilidade." BOBBIO, Norberto. **Teoria do ordenamento jurídico**. São Paulo: Polis, 1989. p. 80.

239 Em 14 de abril de 2016 foi aprovado o Regulamento nº 679/2016, conhecido como Regulamento Geral de Proteção de Dados ou *General Data Protection Regulation (GDPR),* que substitui a Diretiva nº 95/46. Tal regulamento, por uma questão de adaptação do mercado, só entra em vigor em 25 de maio de 2018.

antes não abrangidas pelo sistema. O Regulamento nº 45/2001[240], por exemplo, é a norma autoaplicável que vincula as instituições e órgãos da União Europeia a um sistema baseado na Diretiva 95/46/CE para a proteção de dados, ainda que de modo mais detalhado decorrente da necessidade de aplicação direta da norma.

Já a Diretiva 2002/58/CE[241], do Parlamento Europeu e do Conselho, rege o tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas. A diretiva aborda questões específicas e sensíveis como a conservação de dados de conexão para fins de faturamento dos serviços de conexão prestados, o envio de mensagens eletrônicas não solicitadas (spam), a utilização de dados pessoais em listagens públicas (como listas telefônicas), e a utilização dos chamados "testemunhos de conexão" ou cookies.

A Diretiva 2006/24/CE[242] complementa o quadro estabelecido, dispondo especificamente sobre a obrigação dos provedores de serviços de comunicação de reter dados de conexão relativos a comunicações levadas a cabo por meio de redes públicas, com especial menção à Internet. Em abril de 2014, no entanto, a Corte de Justiça da União Europeia declarou essa diretiva inválida[243] ao considerar que, enquanto a obrigação de retenção de certos dados de conexão não viola, per se, direitos fundamentais da Carta de Direitos, o modo como é determinada a retenção é desproporcional.

Um degrau abaixo das diretivas e regulamentos, é possível encontrar algumas decisões da Comissão Europeia que ajudam a complementar o quadro regu-

---

240 UNIÃO EUROPEIA. Regulamento (CE) nº 45/2001 do Parlamento Europeu e do Conselho de 18 de dezembro de 2000 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. **Jornal Oficial** L. 008, 12 de janeiro de 2001.

241 Posteriormente complementada e atualizada pelas Diretivas 2006/24/CE e 2009/136/CE. UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. **Jornal Oficial** L. 201, 31 de julho de 2002.

242 UNIÃO EUROPEIA. Directiva 2006/24/CE do Parlamento Europeu e do Conselho de 15 de março de 2006 relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE. **Jornal Oficial** L. 105, 13 de abril de 2006.

243 UNIÃO EUROPEIA. Corte de Justiça da União Europeia, Casos conjuntos C-293/12 e C-594/12. **Digital Rights Ireland Ltd. v. Ireland**, julgados em 8 de abril de 2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=PT&cid=513860>. Acesso em: 09.10.14.

latório. Essas decisões, não sendo produto de deliberações generalizadas[244] – como no caso dos regulamentos e diretivas sobre o assunto, que precisam ser aprovadas pelo Parlamento Europeu –, são mais facilmente revistas e atualizadas, característica que permite um detalhamento ainda maior em suas provisões.

Uma das mais famosas decisões foi a Decisão da Comissão 2000/520/CE, datada de 26 de julho de 2000, que dizia respeito a um programa de "porto seguro" (ou "Safe Harbour"), criado em conjunto com o Departamento de Comércio dos Estados Unidos da América[245] para facilitar as transferências de dados pessoais entre as duas partes por meio do estabelecimento de padrões mínimos de segurança e sigilo. Entre as razões para sua concretização, estava o fato de que a União Europeia via com grande preocupação o cenário legislativo norte-americano no que tocava a proteção de dados pessoais, uma vez que, sendo os Estados Unidos um polo empresarial e tecnológico com grande expressão no mercado de produtos e serviços *online,* havia a legítima preocupação sobre o destino dos dados de cidadãos europeus eventualmente transferidos a empresas localizadas naquele país.

O programa "Safe Harbor" foi encerrado em outubro de 2015, quando a Corte de Justiça da União Europeia, diante das denúncias feitas pelo ex-agente da Agência de Segurança Nacional norte-americana (NSA), Edward Snowden[246], sobre violações generalizadas de privacidade pelo governo estadunidense, julgou inválida a Decisão 2000/520/CE.

Na sequência dessa decisão, entabularam-se novas discussões entre Estados Unidos e União Europeia, a fim de criar um novo programa para garantir o intercâmbio de informações. O resultado desses esforços foi a Decisão de Execução

244 Segundo o artigo 16, 2 do TFUE, o Parlamento Europeu e o Conselho da União Europeia devem adotar o processo legislativo ordinário para dispor sobre a proteção dos cidadãos quanto ao tratamento de seus dados pessoais. Por tal procedimento, de acordo com os artigos 289 e 294 do mesmo tratado, a proposta de normativa (regulamento, diretiva ou decisão) é introduzida pela Comissão Europeia e encaminhada para análise do Parlamento e do Conselho, que proferem ao fim uma decisão conjunta. Em alguns casos, no entanto, a Comissão pode emitir decisões únicas, quando assim autorizado por norma não obstada pelo Parlamento ou pelo Conselho, conforme o artigo 290 do TFUE. No caso, a própria Diretiva 95/46/CE delega à Comissão a regulamentação de alguns pontos específicos através de decisões únicas, como é o caso do artigo 24, item 6, e do artigo 25, item 4.

245 COMISSÃO EUROPEIA. Decisão 2000/520/CE. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípio de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. **Jornal Oficial L** 215, 25 de agosto de 2000.

246 GREENWALD, G.; MACASKILL, E. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian Online**, June 7, 2013. Disponível em: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 30.11.16.

2016/1250/CE[247], que estabeleceu o agora conhecido programa "Privacy Shield", que aprimorou o anterior[248]. O programa, no geral, exige que as empresas afiliadas garantam certos direitos aos indivíduos cujos dados são transferidos, como informações básicas, acesso a mecanismos simples e gratuitos de resolução de disputas, além de exigir o cumprimento de alguns princípios básicos de proteção de dados, sigilo e segurança dos dados e a transparência no tratamento dos mesmos.

É também de grande interesse a Decisão da Comissão 2001/497/CE, datada de 15 de junho de 2001[249], que fornece aos interessados em transferir dados pessoais para destinos externos à União Europeia cláusulas-tipo que apresentam garantias suficientes, nos termos da Diretiva 95/46/CE, para a preservação dos direitos concedidos por aquela diretiva aos titulares dos dados a serem transferidos.

A comprovar a flexibilidade desse tipo de normativa, apenas 3 anos após a publicação da Decisão 2001/497/CE, a Comissão emitiu nova decisão sobre o assunto, publicada em 27 de dezembro de 2004[250], alterando alguns poucos dispositivos da decisão anterior e introduzindo um novo conjunto de cláusulas típicas, que poderiam ser combinadas ou utilizadas em substituição ao conjunto consignado na primeira decisão.

Este sistema bem conhecido e consolidado de normas sofreu grande alteração em 2016, quando foi aprovada uma grande reforma gestada desde 2010[251]. A reforma se deu, sobretudo, pela introdução do Regulamento nº 679/2016 do Parlamento e do Conselho, que substitui a Diretiva nº 95/46/CE e unifica a

---

247 UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. **Jornal Oficial** L. 207/1, 01 de agosto de 2016.

248 A adesão ao programa Privacy Shield é voluntária, apesar de ser requisito para transferências de dados que envolvam a União Europeia. Uma vez feita a adesão ao programa, no entanto, o atendimento a seus requisitos é obrigatório e exigível pela lei local norte-americana. Para mais informações, confira-se: https://www.privacyshield.gov/.

249 COMISSÃO EUROPEIA. Decisão 2001/497/CE. Decisão da Comissão de 15 de junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Directiva 95/46/CE. **Jornal Oficial L** 181, 4 de julho de 2001.

250 COMISSÃO EUROPEIA. Decisão 2004/915/CE. Decisão da Comissão de 27 de dezembro de 2004 que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros. **Jornal Oficial L** 385, 29 de dezembro de 2004.

251 COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões. Uma abordagem global da protecção de dados pessoais na União Europeia. Bruxelas, 4 nov. 2010. COM(2010) 609 final. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pt.pdf>. Acesso em: 24.03.17.

disciplina da proteção dos dados pessoais, uma vez que é diretamente aplicável como se norma interna fosse. A substituição de uma diretiva por um regulamento vem também atender a uma necessidade de unificação do sistema, já que não é mais necessária a incorporação do texto supranacional por uma lei interna. Tal regulamento ficou conhecido como o Regulamento Geral de Proteção de Dados[252], o *General Data Protection Regulation,* ou, simplesmente, GDPR[253].

Entre as principais alterações trazidas pelo GDPR, pode-se apontar algumas que são mais relevantes e que podem ser divididas por sua finalidade: alterações para reforçar os direitos dos usuários, alterações para reforçar as competências das Autoridades de Proteção de Dados, e alterações para *induzir* e *incentivar* certos comportamentos por parte dos responsáveis pelo tratamento.

Em primeiro lugar, em relação aos direitos individuais, a forma de expressão do consentimento e a relevância do adjetivo "informado" foram reforçados, exigindo-se que o titular dos dados tenha acesso facilitado às informações sobre o tratamento, expressas de modo simplificado (ao invés da linguagem geralmente hermética dos contratos), e que seu consentimento seja expressado de modo destacado – com igual facilidade para sua revogação. Ainda para reforçar direitos dos titulares, os direitos de acesso e de eliminação de dados (na forma do "direito ao esquecimento") são reelaborados e expandidos, dando maior segurança ao titular e ao mercado.

No que toca o reforço das Autoridades de Proteção de Dados, podemos citar a especificação de sanções que podem ser impostas aos responsáveis por tratamentos de dados que não respeitem as regras do GDPR, a responsabilização também do agente processador dos dados e a nova obrigação de notificação de violações de segurança de dados. Assim, empresas que sofrerem ataques para roubo de dados ou que tiverem dados pessoais de seus clientes vazados, por exemplo, deverão agora notificar os titulares dos dados e a Autoridade de Proteção de dados sobre tal fato.

---

252 UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial L**. 119/1008, 04 de maio de 2016.

253 Juntamente ao GDPR foi também aprovada a Diretiva nº 2016/680/CE, que regula o tratamento de dados pessoais no contexto da investigação, repressão e persecução criminais pelas autoridades competentes, mas que não nos interessa diretamente no presente estudo. Confira-se: UNIÃO EUROPEIA. Diretiva (UE) nº 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial** L. 119/89, 04 de maio de 2016.

Ainda nessa esteira, o novo Regulamento cria diversas regras sobre procedimentos de avaliação de impacto em privacidade, os chamados *Privacy Impact Assessments*, ou simplesmente PIAs. Apesar de não haver uma obrigação de registro de tratamentos de dados, em certos casos é exigido do controlador ou responsável que elabore tal estudo, de modo a reduzir os riscos à privacidade dos titulares dos dados, podendo submetê-lo à aprovação da Autoridade de controle.

Por fim, o Regulamento traz também algumas práticas que servem como incentivo ao responsável pelo tratamento dos dados pessoais para que este zele pelo cumprimento do regulamento e pela garantia da privacidade dos titulares dos dados.

A primeira mudança vem pela consolidação dos conceitos de *privacy by default* e *privacy by design* como obrigações do responsável pelo tratamento. Nesse sentido, o responsável deve sempre construir seus produtos, serviços e processos tendo em mente a preservação da privacidade e os princípios gerais da matéria, além de utilizar como padrão de operação a escolha pela preservação da privacidade em detrimento da publicidade na ausência de um posicionamento expresso do titular dos dados.

A segunda mudança, de igual importância, vem na reafirmação dos programas de incentivo ao cumprimento do Regulamento pela criação de selos e sistemas de certificação relacionados ao grau de zelo da empresa com a privacidade de seus usuários.

Tutela em camadas, indução de comportamentos e fiscalização multinível

O que se nota pelo panorama traçado é um sistema de proteção construído em camadas: parte-se de garantias fundamentais de grande amplitude, passando a normas ainda bastante gerais que especificam tais princípios e preveem tanto exceções quanto possíveis conflitos com outros princípios, e em seguida ainda a novas normas ainda mais específicas que abordam questões setoriais, por fim chegando a decisões e normativas de ainda maior especificidade, mas que contam com grande flexibilidade em sua criação e atualização.

Nessa estrutura piramidal, os valores essenciais estão contidos no topo, em normas gerais de pouca aplicabilidade prática e direta, crescendo os instrumentos legais em número, especificidade e flexibilidade, conforme se avança para a base da estrutura.

Essa configuração é de imensa importância diante das dificuldades inerentes à regulação de um setor tão influenciado pelo desenvolvimento tecnológico,

como é o caso dos dados pessoais[254]. O importante, a essa altura, é perceber que essa estrutura hierarquizada de valores, princípios e regras é essencial por um fator crucial: a sincronia entre a lei e a realidade. Em um campo fático de rápida evolução, é importante que a lei mantenha um patamar mínimo de aplicabilidade e sejam, no mais, envidados esforços para a atualização constante das normas, de modo que essas possam acompanhar – ainda que a certa distância – o desenvolvimento tecnológico.

Estruturadas como se encontram, as normas comunitárias básicas sobre a proteção de dados fornecem uma estrutura na qual (i) os valores fundantes – cuja atualização não precisa seguir o ritmo da tecnologia – estão bem fixados em normas gerais, que costumam apresentar maiores dificuldades para sua alteração; (ii) os princípios e subprincípios em que se traduzem tais valores são bem desenhados e fixados em normas ainda de caráter geral, mas tecnologicamente neutras, o que garante que possam ser aplicadas ainda que com mudanças razoáveis no campo tecnológico; e (iii) regras específicas criadas pelo sopesamento e fixação legal desses princípios são erigidas em normas de caráter específico e sujeitas a um procedimento simplificado de produção e atualização, permitindo que, ainda que não absolutamente tecnologicamente neutras, sigam a curta distância o desenvolvimento tecnológico.

Do ponto de vista regulatório, a garantia de certos direitos e a condução dos atores envolvidos a um "comportamento ideal" é buscada por vias diferentes, que se complementam. Por um lado, existem princípios gerais e normas de conduta que impõem deveres. Por outro, temos também o recurso a práticas de mercado, como a autorregulação e a criação de sistemas que premiam o cumprimento da lei, mais que simplesmente punir sua violação. Ainda, há no modelo europeu a importante figura das Autoridades de Proteção de Dados, cujas atribuições extrapolam o de uma simples agência reguladora, mas caracterizam um órgão que agrega funções fiscalizatórias, normativas e jurisdicionais, ainda que em uma instância administrativa. Esse último ponto permite que os titulares de dados possam acompanhar de perto o que é feito com seus dados e tenham um canal efetivo e especializado para a resolução de controvérsias que possam surgir, incentivando assim uma fiscalização de direitos por parte do próprio usuário.

254 MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with technology as a regulatory target. **Law, Innovation and Technology**, n. 5, v. 1, 2013.

O Modelo Norte-americano

O segundo modelo regulatório a ser examinado é o vigente nos Estados Unidos. O modelo norte-americano é o segundo mais influente do mundo, sendo que a maioria dos estudiosos estimam que a maioria das leis postas e dos projetos de leis de proteção de dados pessoais atualmente em gestação ao redor do mundo tem grande chance de adotar um dos dois sistemas, ou neles se inspirar[255].

Estrutura normativa e de tutela

Os Estados Unidos não possuem uma lei geral de proteção de dados pessoais no âmbito federal. Em lugar de tratar a disciplina da coleta e do uso dos dados pessoais de uma maneira uniforme, optou-se por dar um tratamento setorial à matéria. Desse modo, o país possui leis federais que disciplinam a proteção e o uso de dados pessoais de crianças e adolescentes, os dados médicos ou de saúde, os dados financeiros, os dados pessoais inseridos no contexto das comunicações eletrônicas, entre outros setores específicos, mas não há uma lei central que defina princípios e regras comuns, ou que estabeleça direitos unificados aos cidadãos. Alguns estados também possuem legislação específica sobre privacidade e proteção de dados, devendo-se destacar o exemplo da Califórnia, que é uma das referências naquele país no tema[256].

Uma das leis mais interessantes no âmbito federal é o *Electronic Communications Privacy Act* de 1986[257], constituído do *Wiretap Act*, o *Stored Communications Act* e o *Pen Register Act*. O *Wiretap Act* proíbe a interceptação, uso ou revelação de qualquer tipo de comunicação telefônica, oral ou eletrônica, aplicando-se tanto ao setor privado quanto ao público (salvo as exceções em caso de investigação criminal, por exemplo). Note-se que a referência aqui é a comunicação *em fluxo*,

---

255 "The United States, which long supported market-based solutions, rejected the legitimacy of the EU's legislation, stoking the first trade conflict of the information age.(...) Against U.S. objections, European rules became the *de facto* international standard with more than thirty countries following the European approach." NEWMAN, Abraham L. Building transnational civil liberties: transgovernmental entrepreneurs and the European data privacy directive. **International Organization**, n. 62, n. 1, p. 104, Jan. 2008. Confira-se também: CASTETS-RENARD, Céline. **Droit de l'internet: droit français et européen**. 2.ed. Paris: Montchrestien, 2012. p. 26.

256 SOTTO, L.J.; SIMPSON, A.P. United States In: **Data Protection & Privacy 2015**, Londres: Law Business Research, 2015, pp. 208-209.

257 ESTADOS UNIDOS DA AMÉRICA. Electronic Communications Privacy Act, 18 U.S.C. §2510 e ss., **Public Law**, Washinton D.C., 21 out. 1986.

o que se extrai do próprio termo *interceptação*. Os dados referentes a comunicações armazenadas, que já foram recebidas ou enviadas e não se encontram mais em fluxo, são protegidos, por sua vez, pelo *Stored Communications Act*, que diz respeito aos dados de comunicação e de cadastro (como nome, endereço, etc) armazenados por provedores de serviço. O *Pen Register Act* regula a utilização pelo governo (e a proibição ao público em geral) dos *pen registers* e outros dispositivos de rastreamento de chamadas. Esses dispositivos servem para identificar os terminais em uma determinada comunicação (geralmente telefônica), mas não tem capacidade para interceptar ou acessar o conteúdo da comunicação em si.

Ainda no âmbito federal, há o COPPA, acrônimo para *Children's Online Privacy Protection Act*[258], lei de 1998 que cria salvaguardas para a interação de crianças com menos de 13 (treze) anos com a Internet em geral e no que diz respeito a sua privacidade. A Lei traz um mecanismo interessante de *safe harbor,* diferente do projeto internacional entre Estados Unidos e União Europeia. Por tal mecanismo, associações setoriais de empresas podem submeter à *Federal Trade Comission* (FTC) códigos de auto regulação que serão então avaliados e eventualmente homologados, tornando-se vinculantes para as empresas associadas. O diferencial aqui diz respeito ao fato de que tais códigos geralmente preveem mecanismos de resolução de disputas entre as empresas associadas e seus consumidores e/ou mecanismos internos de disciplina das empresas envolvidas em possíveis violações de privacidade. Com tais provisões, uma vez aprovado o código, empresas em violação do COPPA estariam primeiro sujeitas aos procedimentos disciplinares setoriais, e só depois, em certos casos, poderia ser submetidas à investigação da FTC.

No setor da saúde, vige o *Health Insurance Portability and Accountability Act* de 1996, mais conhecido por *HIPAA*, que contém regras federais setoriais de privacidade e proteção de dados médicos[259]. Tal lei traz disposições a respeito de padrões de segurança, física e técnica de dados relacionados à saúde em formato eletrônicos; a obrigação de notificar os titulares dos dados, e muitas vezes a Secretaria de Saúde[260] e a mídia local[261] no caso de vazamento ou violações de dados pessoais; as condições básicas para o tratamento justo e legal dos dados

258 ESTADOS UNIDOS DA AMÉRICA. Children's Online Privacy Protection Act, 15 U.S.C. §6501-6506., **Public Law**, Washington D.C., 21 out. 1998.

259 ESTADOS UNIDOS DA AMÉRICA. Health Insurance Portability and Accountability Act, 110 Stat. 1936, **Public Law**, Washington D.C., 21 ago. 1996.

260 U.S. Department of Health and Human Services.

261 Quando o número de indivíduos afetados superar 500 (quinhentos) em um mesmo estado.

pessoais e as situações em que o consentimento do titular é ou não necessário; direitos básicos de acesso aos dados e informação sobre o tratamento e as cabíveis medidas de segurança e sigilo; além de diretrizes específicas sobre a responsabilidade da "entidade abrangida" pela lei por seus funcionários, incluindo-se aí treinamentos, questões de política interna de privacidade e disciplina.

O *Privacy Act* de 1974[262] é a lei federal vigente que estabelece os princípios e regras para a coleta, armazenamento, uso e comunicação de dados pessoais no seio das atividades estatais conduzidas pelas agências federais. A lei aborda regras sobre a revelação de dados pessoais a outras agências ou terceiros, geralmente mediante o consentimento do titular ou diante de alguma circunstância de interesse público - no exercício da administração pública ou em atividades particulares com fins estatísticos, históricos, negocial, entre outros; garante direitos de acesso; limitações quanto à finalidade, quantidade e qualidade dos dados tratados; diretrizes para garantir a segurança, sigilo e a transparência dos tratamentos; diretrizes sobre as políticas internas de segurança e tratamento de dados; a obrigatoriedade de registro dos bancos de dados federais submetidos ao *Privacy Act,* entre tantos outros assuntos menores.

O sistema estadunidense não possui uma Autoridade de Proteção de Dados nos moldes europeus, um órgão técnico, independente e dedicado unicamente à matéria da privacidade e da proteção de dados pessoais. Em seu lugar, certos órgãos já existentes e não exclusivos do governo atuam como agências reguladoras, sendo responsáveis pelo *enforcement* das leis vigentes. Esses são separados por setores econômicos de modo que sua atuação não é necessariamente homogênea, como também não o são necessariamente suas posições em relação às controvérsias que possam surgir sobre este ou aquele conceito. Assim, a *Federal Trade Commission* é responsável, por exemplo, por fiscalizar a aplicação do COPPA e das regras relativas à proteção do consumidor, segundo seu próprio estatuto[263], que podem incluir abusos na coleta e utilização de dados dos consumidores. Já o *Department of Health and Human Services* é responsável pela supervisão do cumprimento do HIPAA. No setor financeiro, temos o *Consumer Financial Protection Bureau*.

Tais agências geralmente têm competências fiscalizatórias, sancionatórias e normativas, podendo complementar as regras setoriais de que cuidam, mas o Poder Judiciário ainda exerce um importante papel no sistema de tutela. Mesmo tais agências e escritórios precisam recorrer ao Judiciário para executar suas

262 ESTADOS UNIDOS DA AMÉRICA. Privacy Act, 88 Stat. 1896, **Public Law**, Washington D.C., 31 dez. 1974.

263 ESTADOS UNIDOS DA AMÉRICA. Federal Trade Comission Act, 15 U.S.C. §41-58., **Public Law**, Washington D.C., 1914.

decisões ou buscar o cumprimento de certas obrigações, o que demonstra a posição central do processo judicial no sistema. Não bastasse tal, na ausência de leis mais amplas de proteção de dados, os princípios e regras gerais necessários para um modelo mais completo de tutela geralmente têm que ser deduzidos de precedentes judiciais, reafirmando sua importância.

Descentralização, contratualismo e judicialização

O modelo regulatório dos Estados Unidos é único na medida que apresenta uma abordagem bastante heterodoxa no que toca às limitações à proteção de dados. Há de fato o reconhecimento de que os dados pessoais têm alguma ligação com a privacidade do indivíduo e com o controle que esse exerce sobre sua vida particular[264], mas a extensão dessa proteção é no geral incerta. Tem-se um "direito à tutela": o titular tem direito a ter considerado o peso de sua privacidade na avaliação do caso concreto, mas o alcance real da privacidade depende desse sopesamento feito pelos tribunais. Tal "direito à tutela", por consequência, dificilmente é autoaplicável ou diretamente exigível pelo titular dos dados daquele que os coleta e os trata.

A norma de direito mais próxima do indivíduo é, pois, o contrato que rege sua relação com a empresa que coleta e utiliza seus dados pessoais. Talvez por conta da alta estima em que tem a liberdade, o legislador parece deixar às partes estabelecer o que é razoável e possível. O instituto central do modelo norte-americano pode ser apontado, pois, como o *consentimento*. As condições e características desse consentimento variam de acordo com o setor de mercado e com a corte competente, mas é bastante claro que o consentimento possui, no contexto norte-americano, valor muito maior que aquele atribuído a ele nos demais modelos regulatórios. Isso porque não se trata aqui de um *consentimento informado*, livre ou expresso, *resultado da consideração do indivíduo sobre o que se pretende com seus dados* e o sopesamento entre benefícios e malefícios. O consentimento, na tradição norte-americana, parece ter maior ligação com a *venda* de informações do que com o estabelecimento de uma relação entre o usuário e o responsável pelo tratamento, dando-se ao contrato o tom de uma transação comercial, ao invés de uma cessão temporária de direitos sobre os dados em questão[265].

---

264 WESTIN, Alan. Privacy and Freedom, New York: Atheneum, 1970 *apud* PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 1. ed. 6. imp, Curitiba: Juruá, 2011, p. 128.

265 "In contrast to other areas of the world such as the United States, where personal information is widely traded like a conventional good, European rules limited the commodification of individual data." NEWMAN, Abraham L. op. cit., p. 104.

O contrato, no entanto, não serve sempre como substituto à garantia de certos direitos abrangentes, principalmente em situações em que uma das partes é uma grande empresa e a outra um indivíduo que deseja usufruir de um serviço seu – ao qual não terá acesso caso não aceite o contrato padrão provedor do serviço. Em muitos momentos, o usuário é forçado a aceitar termos impostos pelo provedor, não importa quão injustos. Esse desequilíbrio contratual, resultado da disparidade de força das partes, gera situações abusivas que não são tuteladas pela lei e, pela massificação dos negócios digitais[266], por sua vez acarretam ações judiciais, individuais ou coletivas, como única solução.

A judicialização de conflitos, ampliada pela ausência de uma norma geral ou mesmo de um órgão regulador específico, tem diversas consequências, tanto para a efetividade dos direitos garantidos quanto para a condução dos negócios em si.

Por um lado, temos que determinada situação considerada lesiva aos interesses de uma das partes é colocada sob exame de uma autoridade judicial que, ainda que não seja especialista no assunto em tela, tem por delegação o poder estatal para dar solução definitiva ao litígio, garantindo a observância da lei tanto no curso do procedimento quanto na execução do provimento. Por outro, consigna-se a solução de um litígio técnico, e que exige rápida resposta, a uma entidade que não possui o conhecimento técnico muitas vezes necessário e cujo prazo mínimo para atingir um primeiro provimento definitivo é grande demais, a ponto de ser totalmente ineficaz do ponto de vista fático.

Afirmamos isso pois a maioria dos dados pessoais em circulação advém e tem como seu contexto a Internet e outros sistemas informatizados, geralmente conectados em rede, e o tempo entre as transações, ações de tratamento, comunicação de dados, é infinitamente menor ao usual, dentro do qual uma solução judicial seria viável.

Em um segundo aspecto, tem-se, no foco da análise, uma consequência mais ampla relacionada ao comportamento das partes desde a concepção de um modelo de negócio até seu efetivo fornecimento. Relegar ao judiciário a garantia de direitos, sem criar outros mecanismos que os garantam ou busquem incentivar a adoção de certas práticas de bom tom no tratamento da privacidade dos indivíduos, instila no empreendedor e nas empresas em geral a ideia de que a garantia da privacidade de seus clientes ou futuros clientes é apenas um fator na análise de rentabilidade e viabilidade de um modelo de negócios, e não um valor que deve ser preservado.

---

266 Confira-se, por exemplo: BARRETT, Brian. Spotify clears up its controversial Privacy Policy. **Wired Online**, 21 ago. 2015. Disponível em: <https://www.wired.com/2015/08/spotify-clears-up-its-privacy-policy/>. Acesso em 19.01.17. PAUL, Ian. Instagram updates Privacy Policy, inspiring backlash. **PC World.** 18 dez. 2012. Disponível em: <http://www.pcworld.com/article/2021285/instagram-updates-privacy-policy-inspiring-backlash.html>. Acesso em 19.01.17.

Do ponto de vista geral, essa abordagem privilegia a livre iniciativa e a inovação, permitindo que usos novos e não regulados da informação sejam descobertos e utilizados para gerar valor aos consumidores. Sob a ótica da proteção de dados pessoais, no entanto, trata-se de um modelo ineficaz de regulação, que recorre apenas a um viés regulatório jurídico, ao invés de avaliar a conduta regulada em termos econômicos, sociais e de "arquitetura", como queria Lessig.[267] Vale, nesse ponto, questionar se a via adotada pelos juristas estadunidenses é a única e mais efetiva alternativa para realizar os dois propósitos aparentemente contraditórios: privacidade e livre iniciativa[268].

O Modelo Uruguaio

O modelo regulatório uruguaio é de especial interesse para nós pois a preocupação com a privacidade de dados dos cidadãos naquele país teve origem semelhante à brasileira na medida em que ambas foram resultado de uma tradição sul-americana de reafirmação e expansão de direitos fundamentais após regimes ditatoriais que tiveram na compilação de dados sobre seus cidadãos, principalmente aqueles de ideais incompatíveis com tais regimes, uma importante arma na repressão de movimentos democráticos[269].

---

267 LESSIG, Lawrence. **Code version 2.0**. [S.l.]: Lawrence Lessig C.C., Kindle Edition, 2011. pos. 1536-1545. ASIN: B004NNVWEI.

268 De uma parte: "A ideia de consentimento do afetado, cujo estágio temporal é necessariamente após a noção de *informação* anteriormente tratada, é tão central ao modelo europeu de proteção de dados, que um dos maiores e mais antigos estudiosos espanhóis sobre o tema afirmou em uma de suas obras que esse 'es la piedra angular a partir del cual se construye el sistema de protección de datos personales'" SILVA, Carlos Bruno Ferreira da. **Proteção de Dados e Cooperação Transnacional,** Belo Horizonte: Arraes, 2014, p. 187. De outra parte, confira-se: "De una parte, argumentamos que, en cuanto expediente legitimador y forma de protección del titular de los datos, el consentimiento es un mecanismo inadecuado: la concepción "individualista" que subyace a este enfoque protector no sirve en un mundo de computación ubicua donde las prácticas de obtención y análisis masivo de datos son inevitables y banalizan la idea del tratamiento "consentido". De otra parte, sostenemos que el discurso oficial del control individual de la información personal ligado a esa idea – al que parece aferrarse aún la futura normativa europea – ha acabado convertido en una suerte de letanía que a duras penas se refleja en la práctica y que predica de la legislación de protección de datos un poder para conformar la realidad social que no tiene." OLIVER-LALANA, A.D.; SORO, J. F. M. El mito del consentimiento y el fracaso del modelo individualista de protección de datos, *In:* TORRIJOS, J. V. (org). **La Protección de los Datos Personales en Internet ante la Innovación Tecnológica**, Navarra: Aranzadi, 2013, pp. 153-196. A respeito dessa discussão, confira-se também: BENNETT, Colin J. **Regulating Privacy: Data Protection and Public Policy in Europe and the United States**, Ithaca: Cornell University Press, 1992, pp. 193-219.

269 "Sinteticamente, apontamos o fato de que um instituto do gênero tenha uma especial razão de ser em sociedades recém-saídas de regimes ditatoriais, como era o panorama em muitos países latino-

Estrutura normativa e de tutela

A principal lei uruguaia no tema é a Lei nº 18.331 de 2008 que trata da "Proteção de dados pessoais e da ação de 'Habeas Data'"[270], representando o ponto central do sistema de tutela daquele país. A referida lei traz as disposições gerais aplicáveis a todos os contextos onde dados pessoais possam ser coletados, tratados e utilizados. Especificamente, a lei traz disposições sobre princípios gerais da proteção de dados; os direitos de informação, acesso, retificação, supressão a dados, proteções especiais para categorias de dados consideradas sensíveis; algumas disposições específicas sobre a utilização de dados pessoais em setores como publicidade, bancos de dados de consumo e telecomunicações; regras para transferências internacionais de dados; registro obrigatório de bancos de dados; a criação do Órgão de Controle, chamado "Unidad Reguladora y de Control de Datos Personales", que consiste, basicamente, em uma Autoridade de Proteção de Dados; e disposições específicas sobre a ação de "Habeas Data", um dos elementos centrais do modelo regulatório.

A Lei nº 18.331 de 2008 foi regulamentada pelo Decreto nº 414 de 2009[271], que trata com maior minúcia alguns temas da Lei de Proteção de Dados. Entre esses temas, podemos citar especificações sobre a comunicação do consentimento para tratamento de dados; medidas técnicas e administrativas de segurança; e detalhes sobre o exercício dos direitos de acesso, retificação e eliminação ou supressão de dados. O decreto não elabora a atribuição normativa do Órgão de Controle, deixando em aberto os temas a serem objeto de tais orientações ou mesmo o peso jurídico de tais documentos.

Algumas outras normativas tratam da coleta e tratamento de dados pessoais em certos setores, como o Decreto nº 396 de 2003, que trata dos dados pessoais referentes à saúde do indivíduo, e o Decreto nº 249 de 2007 que regula a identifica-

americanos na década de 1980 em diante, em cuja sociedade civil persistia o trauma pelo uso autoritário da informação. Em um momento posterior ao fim destes regimes, um instrumento para a requisição das informações pessoais em mãos do poder público, em particular pelos órgãos diretamente encarregados pela repressão à atividades insurrecionais, era tanto desejado quanto necessário, seja para a tutela dos direitos fundamentais envolvidos como também pelo seu importante papel na formação de uma cultura democrática. Com tal escopo foi concebido o *habeas data* - para proporcionar, portanto, ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua própria pessoa armazenadas em bancos de dados [de caráter público]." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 327-328.

270 URUGUAI. Lei nº 18.331 de 2008 sobre a Proteção de dados pessoais e a ação de 'Habeas Data'. **Diario Oficial,** Montevideo, 18 ago. 2008.

271 URUGUAI. Decreto nº 414 de 2009. **Diario Oficial,** Montevideo, 31 ago. 2009.

ção de pessoas por meios informáticos. Por fim, a própria Unidad Reguladora y de Control de Datos Personales emite normativas de caráter particular, interpretando e integrando as regras contidas na legislação vigente sobre Proteção de Dados.

Centralização, registro obrigatório e o remédio do Habeas Data

O modelo uruguaio de regulação e proteção de dados pessoais guarda semelhanças com o modelo europeu, mesmo considerando que sua lei geral de proteção tomou como inspiração a Diretiva 95/46/CE da União Europeia, modelo hoje praticamente ultrapassado, tanto pelo desenvolvimento do sistema uruguaio quando do próprio sistema europeu, com sua recente reforma. Não obstante,, tanto na adoção inicial quanto nos caminhos adotados em um e noutro contexto, algumas diferenças são fundamentais.

À semelhança do modelo europeu de proteção de dados, o Uruguai conta com um arcabouço normativo diversificado e estratificado, ainda que não chegue ao nível de complexidade das normas que têm como referência. Há uma lei geral, cujos pontos mais importantes são desenvolvidos com mais detalhes em decretos regulamentadores. Encontra-se também normativas emitidas pela Autoridade de Proteção de Dados criada naquela lei geral, a "Unidad Reguladora y de Control de Datos Personales" que regulam assuntos específicos e muitas vezes técnicos, como cláusulas contratuais para transferência internacional de dados pessoais[272] e monitoramento de ambientes por vídeo[273]. Ainda, paralelamente, tem-se o incentivo para a adoção de códigos de conduta, que complementam a legislação estatal com a auto regulação dentro dos princípios gerais já estabelecidos.

O tom das normas em vigor, no entanto, não deixa dúvida de que a legislação uruguaia tem forte tendência à centralização de competências. As normativas baseiam-se, antes de tudo, em direitos de acesso, retificação e eliminação de dados, garantidos de modo abrangente, combinado com o registro obrigatório de bases de dados.

Essa configuração permite à Autoridade de Proteção de Dados que realize um controle prévio do tratamento, por meio da análise de informações como os procedimentos de coleta e tratamento de dados, medidas de segurança e descrição técnica da base de dados, destino dos dados em caso de comunicação, entre outras.

272 Confira-se Dictamen nº 003/2009 da Unidad Reguladora y de Control de Datos Personales.

273 Confira-se Dictamen nº 014/2011 da Unidad Reguladora y de Control de Datos Personales.

A Autoridade pode também, seja através de denúncias, inspeções ou solicitação de informações, fiscalizar o cumprimento da lei, podendo aplicar as sanções administrativas permitidas, quais sejam, advertência, multa ou suspensão de bases de dados.

Uma última característica da Autoridade de Proteção de Dados uruguaia é de grande relevância para o presente mapeamento: a inexistência de competência jurisdicional ou de resolução de conflitos. Ao contrário de modelos como o europeu, a Autoridade uruguaia não tem poder decisório para determinar certa conduta a um ente, público ou privado, que entre em conflito com um cidadão. Ao invés disso, quando um cidadão lhe procure com uma querela, a Autoridade deve informá-lo sobre os meios judiciais a sua disposição, para que ele possa buscar a tutela adequada de seus direitos[274]. Não há, pois, uma instância administrativa dedicada às questões de proteção de dados, sendo tais casos direcionados ao Poder Judiciário em geral, que pode ser acionado exclusivamente pelo titular dos dados.

Por fim, é necessário notar que o modelo regulatório uruguaio promove a judicialização de conflitos sobre dados pessoais, contando o sistema com um remédio específico, o Habeas Data. Essa ação visa especificamente permitir ao cidadão "tomar conhecimento de dados referentes a sua pessoa, e sua finalidade e usos, que constem em bancos de dados público ou privados" podendo exigir, segundo o caso, sua retificação, inclusão ou supressão. Na ausência de meios administrativos de solução de controvérsias, salvo a negociação direta com o responsável pelo tratamento ou pela pressão exercida por sanções administrativas da Autoridade de Proteção de Dados em casos coletivos, resta ao cidadão buscar o Poder Judiciário.

Conclusão

Os três modelos regulatórios estudados permitem estabelecer alguns pontos em comum e diferenças fundamentais entre diferentes estratégias regulatórias. Os três locais estudados não foram escolhidos ao acaso, mas sim por representarem modelos de razoável sucesso na garantia de direitos e, principalmente, por se pautarem em diferentes combinações entre soluções normativas, mercadológicas, sociais e técnicas para atingir seus objetivos. Não se pretende

274 É verdade que a Unidad Reguladora y de Control de Datos Personales pode, com base em uma denúncia de violação de um direito garantido em lei, realizar uma inspeção e sancionar a empresa em falta. No entanto, seu provimento será sempre limitado à aplicação de uma das três sanções descritas na lei, não podendo a Autoridade determinar, por exemplo, que a empresa adote determinado comportamento ou tome as providências para garantir determinado direito. A Autoridade de Proteção pode simplesmente autuar as violações da lei, cabendo ao Poder Judiciário qualquer provimento positivo para obrigar a empresa violadora a garantir certo direito.

aqui comparar os modelos de modo a apontar o mais adequado. Além de não ser objeto do presente artigo, em razão da extensão de tal tarefa, a indicação de um modelo regulatório como "ideal" contradiz em sua essência qualquer estudo comparativo de ciências sociais aplicadas.

Após a avaliação dos pontos comuns e das diferenças essenciais, pode-se então arriscar buscar os contornos de cada uma das três estratégias regulatórias, explicitando seus traços fundamentais.

Semelhanças

Os pontos comuns, relevantes para a estratégia regulatória, aos três modelos regulatórios são quatro: (i) a relevância do consentimento; (ii) a obrigação de transparência; (iii) os direitos de acesso, retificação e eliminação de dados; e (iv) as obrigações de segurança e sigilo dos dados pessoais.

Nos três modelos, o consentimento é tido em alta conta, sendo utilizado como condição para a coleta e para o tratamento de dados. Sem exceção, vê-se o consentimento como fator legitimante da utilização dos dados pessoais, talvez como consequência da ideia de que, seja por uma ótica de direitos da personalidade seja por uma ótica econômica, a vontade do indivíduo é necessária para tornar sua disposição um ato justificado.

Pela ótica econômica, o consentimento é a via pela qual, geralmente, o titular dos dados cede seus dados a fim de obter um benefício (como é o caso de plataformas como Google e Facebook) e aprova os termos pelos quais seus dados serão tratados, com clara remissão à liberdade contratual. Pela ótica dos direitos da personalidade, o interesse do indivíduo em um determinado benefício que lhe permita desenvolver sua própria personalidade é o fator legitimante da disposição de um direito que, normalmente, seria indisponível[275].

275 Há alguma discussão na literatura sobre a (in)disponibilidade da privacidade, principalmente quando enquadrada como direito da personalidade. No Brasil, especificamente, esse seria um direito indisponível, segundo o texto frio da lei. Obviamente, a interpretação evoluiu para acomodar a grande disparidade entre o que parece ser uma proibição absoluta e a prática comum. Confira-se: "Em uma série de situações não previstas em lei, mas socialmente admitidas, as pessoas desejam e aceitam limitar, pontualmente, o exercício de algum atributo da própria personalidade. O escritor que concede uma entrevista, revelando ao público detalhes da sua vida particular, deixa de exercer, naquela situação específica, seu direito à privacidade. Tal limitação, derivada da vontade do titular, não deve a toda evidência ser reprimida pela ordem jurídica, porque a vontade individual aí não se opõe, mas se dirige à realização da dignidade humana daquele indivíduo." SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. São Paulo: Atlas, 2013, p. 27.

O segundo ponto em comum diz respeito à obrigação de transparência dos responsáveis pelo tratamento de dados pessoais ou a um direito reflexo a obter informações sobre o tratamento. Apesar de haver ligeiras diferenças nos três modelos, todos preveem a necessidade de se fornecer ao titular dos dados algumas informações básicas antes do início do tratamento de dados. Mesmo nos Estados Unidos, onde não há uma norma específica para proteção de dados, a maioria das normas setoriais e também as normas de proteção ao consumidor[276] trazem obrigações sobre as informações que serão repassadas ao titular dos dados, logo no primeiro contato, as chamadas *privacy notices*.

Em terceiro, todos os modelos avaliados garantem alguns direitos básicos ao titular dos dados, entre eles o de acesso aos dados em tratamento e o de retificação ou eliminação, a depender do ato cabível. Com especial menção ao modelo europeu, o direito de acesso é de suma importância para sua estratégia regulatória, uma vez que parte significativa da tutela reside na fiscalização pelo próprio titular dos dados. O direito de acesso consiste, talvez, no instrumento mais relevante de tais sistemas, pois permite o exercício dos demais direitos como de retificação, oposição, eliminação e contestação de decisões automatizadas – um assunto que adquire cada vez mais importância com os avanços em contratos eletrônicos e inteligência artificial.

O último ponto comum digno de nota diz respeito à segurança e ao sigilo dos dados pessoais. Os três países estudados exigem tanto medidas técnicas quanto físicas e administrativas ou organizativas para resguardar os dados pessoais.

Apesar de isso parecer indicar simplesmente que há um reconhecimento geral à proteção dos dados pessoais, nem essa afirmação é verdade nem esse é o real significado desse fato. Os Estados Unidos, por exemplo, reconhecem um direito geral à privacidade com base em estatutos diversos, sendo os mais comuns o direito de propriedade e a responsabilidade civil: ora se protege o dado como um bem alienado ou cedido, ora com base na responsabilidade daquele que causa dano ao titular dos dados, seja por tratar indevidamente seus dados, seja por descuidar da segurança dos mesmos[277].

---

276 Como *Gramm-Leach-Bliley Act* (1999), *Fair Credit Reporting Act* (1970), e *Fair and Accurate Credit Transactions Act* (2003).

277 "Consumers often bring class action lawsuits against organisations as a result of alleged privacy violations, such as statutory violations or other wrongful acts that affect them, such as information security breaches. In security breach cases, consumers often allege that the organisation was negligent in securing the consumers' personal information, and that such negligence led to the security breach." SOTTO, L.J.; SIMPSON, A.P. United States In: **Data Protection & Privacy 2015**, Londres: Law Business Research, 2015, pp. 213..

O que esse ponto comum vem indicar é que, se o titular dos dados opta por fornecer certos dados pessoais por meio de um contrato, é responsabilidade de quem os recebe cuidar para que a expectativa do contratante – do consumidor, na maioria dos casos – seja cumprida, qual seja, de que apenas aquelas pessoas autorizadas, e para os fins autorizados, possam acessar e utilizar tais dados. Nos modelos uruguaio e europeu, tal conexão é mais simples, pois se baseia antes no direito geral à proteção de dados, mas não deixa de ser também um argumento para exigir que os dados estejam seguros e sejam mantidos em sigilo.

Contrastes fundamentais

Buscar diferenças nos modelos mencionados, de uma maneira simples, é uma tarefa fácil, ainda que exija muito trabalho. No entanto, não buscamos aqui as pequenas diferenças, mas sim aqueles contrastes fundamentais em como cada modelo busca tornar efetivos os direitos e obrigações postos. Para melhor entender os contrastes entre os três modelos, buscamos enquadrá-los em três facetas da estratégia regulatória: o papel do Estado, o papel do mercado e o papel da tecnologia.

No quesito papel do Estado, incluímos não só seu papel normativo, mas também fiscalizatório com a atuação das Autoridades de Proteção de Dados e órgãos semelhantes, e jurisdicional, com a atuação do Poder Judiciário. Os três modelos utilizam-se, de alguma forma, desses poderes para tutelar a proteção de dados, mas o fazem de modo diferente.

O modelo norte-americano utiliza-se de normas setoriais para criar princípios e regras sobre proteção de dados em determinados contextos, mas não possui uma normativa forte e centralizadora, genérica, para garantir um direito geral à proteção de dados. Há alguma atuação das autoridades fiscalizatórias, em geral também setoriais, mas têm ênfase em seu papel fiscalizador/sancionatório e normativo. De modo geral, o papel do Estado no modelo estadunidense é reduzido, e mesmo a legislação existente sobre o tema remete muitos assuntos à auto regulação. O Poder Judiciário aparece como recurso final para a resolução dos conflitos eventualmente surgidos durante a relação entre titular de dados e responsáveis pelo tratamento, mas tem grande importância para o modelo dada a ausência de alternativas mais especializadas para a resolução de controvérsias.

O modelo uruguaio tem uma abordagem diferente na medida em que possui normas centrais, abrangentes e generalistas sobre proteção de dados, reunindo os princípios básicos que devem informar as demais regras do sistema, qualquer que seja sua natureza. Mesmo os códigos de auto regulação são

homologados com sua inserção no campo legislativo estatal por normativa da respectiva Autoridade de Proteção de Dados.

Talvez o ponto de maior interesse aqui seja o modelo fiscalizatório, baseado sobretudo no cadastramento prévio de bancos de dados, a cargo da Autoridade de Proteção, um caso singular na análise. Na ausência de competência específica para solucionar contendas entre titulares e responsáveis pelo tratamento de dados[278], resta ao Judiciário solucionar casos relativos à proteção de dados pessoais. Um aspecto interessante do modelo é o remédio de Habeas Data, que foi adaptado e expandido, de modo a servir como ferramenta universal para execução específica de certas obrigações.

O modelo europeu, por seu lado, apesar de ter um grande número de normas centrais sobre proteção de dados pessoais, delega grande parte da competência legislativa – no que toca os aspectos técnicos e outros assuntos de grande especificidade – à Autoridade de Proteção de Dados. A recente reforma legislativa concedeu à Autoridade de Proteção ainda mais poderes fiscalizatórios e sancionatórios, permitindo a ela maior espaço de manobra. É de imenso interesse o papel central das Autoridades de Proteção no modelo europeu pois, além de suas competências normais, atuam também na resolução de conflitos diretamente entre as partes, em uma esfera administrativa, evitando-se assim a judicialização de inúmeros conflitos.

No que toca o papel do mercado, o modelo estadunidense talvez seja o que mais nele se fia, uma vez que sua regulação esparsa exige que grande parte da prática comum e aceitável seja definida pelos próprios agentes econômicos, seja por meio da prática contratual (sujeita a eventual inspeção judicial), seja pela autorregulação. Em um modelo onde a liberdade contratual é um dos fundamentos básicos da matéria, é de se esperar que a garantia de direitos venha por meio de incentivos econômicos para isso. Assim, ainda que não sempre no interesse do consumidor ou do titular dos dados, há abertura para que a privacidade do consumidor seja definida pelo retorno esperado. Como dissemos ao início do texto, com a crescente conscientização, exige-se cada vez mais dos provedores de serviço, que devem se adequar para não perder relevância competitiva.

O modelo uruguaio é, dentre os modelos analisados, o que menos recorre ao mercado para tentar moldar comportamentos. O modelo de tutela impositivo, como descrito anteriormente, ignora parcialmente o valor dos mecanismos

278 Lembrando que a APD uruguaia pode, diante da denúncia do descumprimento de um direito de acesso, por exemplo, aplicar uma sanção (advertência, multa ou suspensão do banco de dados), mas não tem meios específicos para exigir o cumprimento da obrigação para com o titular dos dados.

econômicos e seu impacto regulatório, fazendo mera referência a códigos de conduta, sem outros pontos de contato interessantes entre Direito e Economia.

O modelo europeu, apesar de não trazer a definição exata da coleta e do tratamento de dados na lei, apresenta-nos uma abordagem interessante para o papel do mercado em um modelo regulatório. Em suma, a União Europeia utiliza mecanismos de mercado para incentivar a adesão a padrões de tutela já definidos nas normas sobre proteção de dados. Tais mecanismos geralmente funcionam em uma base de troca, sendo que os agentes que optarem por aderir a tais regras podem receber benefícios competitivos por isso. O exemplo mais óbvio dessa política é justamente o sistema de certificação criado pelo GDPR, que permite às empresas utilizarem certos certificados e selos de qualidade quando seja constatado o cumprimento substancial das normas em vigor. No contexto atual, em que a privacidade ganha importância para o cidadão comum, a vantagem competitiva oferecida acaba por criar interesses convergentes das duas pontas da transação: proteger a privacidade do usuário deixará de ser um custo para se tornar um diferencial competitivo e uma fonte de receitas.

Por fim, a tecnologia em si tem um papel nos modelos regulatórios. Enquanto todos recomendam certas medidas de segurança e sigilo (como a adoção da criptografia e do processo de anonimização), o modelo europeu possui um diferencial de nota na matéria. Com especial reforço na recente reforma legislativa, os conceitos de *privacy by design and by defaut* e *privacy enhancing technologies*, ganham espaço e incentivam alterações na "arquitetura normal" - o modo e o que a tecnologia permite em razão do modo como é construída - para fazer com que o próprio valor da privacidade tenha lugar na concepção inicial de qualquer serviço ou produto. Essa característica, no entanto, é arriscada na medida em que, incorporada na GDPR, diminui a neutralidade tecnológica do texto e arrisca torná-lo obsoleto mais cedo do que seria esperado.

Modelos regulatórios

Com base nas observações anteriores, ousamos propor o conceito de três estratégias ou modelos regulatórios para a proteção de dados pessoais: o modelo normativo-estatal, o modelo liberal e o modelo eclético.

O modelo normativo-estatal tem como exemplo, neste trabalho, o Uruguai. Suas principais características seriam um sistema normativo centralizador, mantendo a maior parte das competências regulatórias e fiscalizatórias no

próprio Estado, através da forte atuação do Poder Judiciário, onde um procedimento processual específico é utilizado para possibilitar o exercício de direitos.

O modelo liberal, inspira-se no dos Estados Unidos, onde há grande recurso à autorregulação e onde o Estado busca interferir ao criar normas apenas em áreas consideradas sensíveis, como saúde, finanças e menores de idade. Nesse modelo, apesar de haver alguma tendência à judicialização, o principal foco é a liberdade de contratação e a possibilidade de o mercado definir, em sua interação com os consumidores, os comportamentos aceitáveis.

O último modelo tem como exemplo a União Europeia e sua abordagem à proteção dos dados pessoais. O modelo eclético é assim nomeado pois resulta de um grande ajuntamento de estratégias, incluindo o recurso a normas estatais e mercadológicas, mecanismos alternativos de resolução de controvérsias, soluções tecnológicas e o engajamento ativo, tanto do titular dos dados quanto do responsável pelo tratamento de dados, no cumprimento e fiscalização da lei. Esse último ponto talvez seja o mais interessante por trabalhar não pela repressão de condutas (onde cumprir a lei é um modo de não perder dinheiro), mas pela indução, na qual o respeito à privacidade é interessante para todos os envolvidos pelos benefícios daí advindos.

Promovendo a privacidade e a proteção de dados pela tecnologia: Privacy By Design e Privacy Enhancing-Technologies

Jonas Valente[279]

Introdução

O presente artigo visa discutir as possibilidades de proteção de dados por meio de dispositivos e aplicativos. Esse tipo de prática recebeu na literatura especializada o nome de "*Privacy By Design*" (PBD). As tecnologias adotadas com essa finalidade foram denominadas "*Privacy-Enhancing Technologies*" (PETs). Muitas vezes, os conceitos se confundem, mas no presente texto serão trabalhados de forma separada, sendo o primeiro relacionado à prática global de orientação de todo o processo de desenvolvimento e fabricação com o objetivo de assegurar a privacidade e a proteção de dados do usuário e de coletividades e o segundo a denominação de toda sorte de solução tecnológica que tem esta orientação em seu design.

O texto se propõe a um panorama geral preliminar sobre o assunto. Embora o início da reflexão date da metade dos anos 1990 e haja uma considerável literatura internacional sobre essa problemática, a linha introdutória adotada se justifica pela insuficiência do tratamento desse objeto em língua portuguesa. Uma pesquisa na Biblioteca Digital da Sociedade Brasileira de Computação (SBC)[280] com qualquer um dos termos (PBD ou PET) resulta em apenas oito artigos, sendo que nenhum deles trata diretamente do tema[281]. Esse quadro é ainda mais preocupante quando se considera que, no momento de fechamento do presente texto (segundo semestre de 2017), o Brasil realizava discussão sobre a sua legislação específica para a proteção de dados pessoais com a proposição pelo Executivo

279 Doutorando no Programa de Pós-Graduação do Departamento de Sociologia da Universidade de Brasília. E-mail: jonasvalente@gmail.com

280 A biblioteca pode ser acessada pelo endereço: <http://www.lbd.dcc.ufmg.br/bdbcomp/>. Pesquisa realizada em 10 de janeiro de 2017.

281 O levantamento não incluiu possíveis traduções do termo nem o tema da privacidade em geral, o que implica um escopo muito mais amplo do que sua relação com o design.

Federal do Projeto de Lei nº 5.276 de 2016. Nos debates sobre o projeto, a garantia da privacidade por soluções tecnológicas não se colocou como preocupação relevante. São essas inquietações que movem esse esforço reflexivo.

Para dar conta dos objetivos a que se propõe, o texto é divido em três partes. Na primeira, será feita uma contextualização sobre cada um dos "pólos da relação": tecnologia e privacidade. A primeira é discutida dentro da sua crescente importância na sociedade contemporânea e no tocante à sua compreensão como objeto próprio de análise dentro dos estudos sociológicos, com destaque para as abordagens da Teoria Crítica da Tecnologia e da Construção Social da Tecnologia. A segunda é inserida no panorama da ascensão das práticas de coleta e processamento de dados, naquilo que ficou conhecido como "Big Data", e tem sua relevância examinada nesse ambiente.

Em seguida, será apresentado um diálogo entre os dois polos avançando para a discussão sobre a construção social da tecnologia, tendo a privacidade como princípio e critério orientador. São discutidos os conceitos de *Privacy By Design* (Privacidade pelo design) e *Privacy-Enhancing Technologies* (Tecnologias promotoras de privacidade) e será proposto um quadro em que serão sistematizados os mecanismos que devem estar presentes na fabricação e implantação desses componentes. Por fim, o texto apresenta algumas reflexões sobre o tema e analisa sua manifestação no Brasil tomando como referência o debate sobre a regulação da proteção de dados pessoais em curso no Congresso Nacional.

Tecnologia e privacidade

A tecnologia é algo que acompanha a própria história da humanidade e contribuiu para mudanças importantes em diversos períodos. Contudo, a transição para o século XXI evidenciou uma acentuação dessa presença, em especial das Tecnologias da Informação e da Comunicação (TICs). Por meio de redes de telecomunicações, as plantas produtivas e o fluxo de capital foram globalizados, alcançando um patamar distinto superior às relações econômicas entre nações ou impérios coloniais que marcaram o século XX.

Este papel central levou diversos autores a identificar na tecnologia o elemento caracterizador da atual etapa da nossa sociedade. Uma profusão de denominações emergiu, como Sociedade Pós-Industrial[282], Vida Digital[283] , Ci-

282 BELL, Daniel. **O advento da sociedade pós-industrial**. São Paulo: Cultrix, 1973.

283 NEGROPONTE, Nicholas. **A Vida Digital**, Rio de Janeiro: Companhia das Letras, 1995.

bercultura, virtualidade e tecnologias da inteligência[284], Sociedade em Rede[285], Sociedade do Conhecimento[286] e Sociedade da Informação[287] [288].

A Internet é o ápice, até o presente momento, deste fenômeno. Essa rede de redes impactou parte importante da vida social. Na economia, uma parcela representativa das transações econômicas passou a ser feita por diferentes plataformas. O comércio eletrônico ascendeu com a força de lojas de departamentos a pequenos negócios, chegando a movimentar mais de US$ 1,5 trilhão no mundo em 2015[289]. Na cultura, o consumo de produtos audiovisuais na *web* é uma realidade que vem alterando sobremaneira os setores. Em 2017, a expectativa é que 2,15 bilhões de pessoas assistam a vídeos online[290], o que representa 30% da população mundial. Apenas uma plataforma, o Facebook, ultrapassou o país mais populoso do mundo, a China, com 1,71 bilhão de usuários únicos[291]. A Internet espraiou-se para os artefatos (sensores, aparelhos, eletrodomésticos etc.) com a chamada "Internet das Coisas" (*Internet of Things*).

Contudo, é arriscado, e desaconselhável, transformar essa assunção em uma visão laudatória dos sistemas técnicos, naquilo que ficou conhecido na literatura como "determinismo tecnológico". Um elemento de tamanha impor-

---

284 LEVY, Pierre. **As tecnologias da inteligência**. São Paulo: Ed. 34, 1997.

285 CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

286 STEHR, Nico. Modern societies as knowledge societies. In: RITZER, George. SMART, Barry. **Handbook of Social Theory**. London: Sage, 2001.

287 INTERNATIONAL TELECOMMUNICATIONS UNION [traduzido por Marcelo Amorim Guimarães]. **Documentos da Cúpula Mundial sobre a Sociedade da Informação** [livro eletrônico]: Genebra 2003 e Túnis 2005 / São Paulo : Comitê Gestor da Internet no Brasil, 2014.

288 Uma revisão crítica profunda, rigorosa e qualificada dessas denominações e do papel das tecnologias da informação e da comunicação pode ser encontrada em Fuchs & Sandoval (2014) e em Bolaño et al. (2010). Embora reconheçamos a importância deste avanço e a necessidade de discutir a tecnologia como objeto específico, nos filiamos a essas correntes que não a localizam como o elemento diretor das transformações sociais, mas como uma esfera de atividade (HARVEY, 2010) que estabelece uma relação dialética com as demais, molda as dinâmicas sociais e é forjada por elas.

289 E-Commerce Is the Next Frontier in Global Expansion. The 2015 Global Retail E-Commerce Index. **ATKearney**. Disponível em: <https://www.atkearney.com/consumer-products-retail/e-commerce-index/full-report/-/asset_publisher/87xbENNHPZ3D/content/global-retail-e-commerce-keeps-on-clicking/10192>. Acesso em: 23.03.17.

290 Worldwide Digital Video Viewers: eMarketer's Estimates for 2016–2020. **Emarketer Report**. Publicado em: 11.01.17. Disponível em: <https://www.emarketer.com/Report/Worldwide-Digital-Video-Viewers-eMarketers-Estimates-20162020/2001983>. Acesso em: 23.03.17.

291 Informação relativa a setembro de 2016. Disponível em: <http://newsroom.fb.com/company-info/>. Acesso em: 15.01.17.

tância merece escrutínio atento, que examine sua essência e presença na sociedade. Sem o tempo necessário para uma digressão mais profunda, indica-se que a opção do texto é a de se aproximar da perspectiva que percebe os artefatos como resultados de decisões políticas e demandas sociais. Dentro desse campo, o referencial adotado inclui duas abordagens: a da teoria crítica da tecnologia[292] e a da construção social da tecnologia[293].

Um artefato não é o resultado da mente de um engenheiro, que busca os melhores caminhos para cumprir determinada tarefa. Ao contrário, ele é criado a partir de demandas que se expressam por meio de relações sociais de produção e envolvem diferentes visões e disputas de poder. Estão em jogo aí os objetivos, as instâncias de formulação, as correlações entre as diversas forças que incidem na fabricação, o embate entre diferentes modelos, a concorrência de soluções alternativas e as dinâmicas de mercado para a consolidação ou não do produto. De acordo com Feenberg, "The choice between alternatives ultimately depends neither on technical nor economic efficiency, but on the ´fit´ between devices and the interests and beliefs of the various social groups that influence the design process."[294] . Ao estudar a história social da televisão, Williams[295] reforça essa percepção: "*Any particular technology is then as it were a by-product of a social process that is otherwise determined. It only acquires effective status when it is used for purposes which are already contained in this known social process*."[296].

Feenberg[297] sugere que as disputas de poder não estão apenas nas demandas ou nos usos da tecnologia, mas terminam por ser inscritas no seu próprio conteúdo ou "*design*". Os componentes desse tipo de sistema trazem inscritos nele as determinações dos agentes sociais que tiveram o controle do processo.

---

292 Entre os autores dessa abordagem destaca-se: Marcuse (1973), Feenberg (1996; 2002; 2005), Noble (1995, 2011) e Winner (1986). Ela dialoga com a Construção Social da Tecnologia, cujo trabalho fundador é o de Bijker & Pinch (1993).

293 Essa abordagem tem como grandes expoentes Bijker & Pinch (1993).

294 FEENBERG, A. Marcuse ou Habermas: duas críticas da tecnologia**. Inquiry: An Interdisciplinary Journal of Philosophy,** v. 39, 1996, p.79. Disponível em: <http://www.sfu.ca/~andrewf/marhabportu.htm>. Acesso em: 05.01.17.

295 WILLIAMS, R. **Television: technology and cultural form**. Londres: Routledge, 2003.

296 Com o intuito de evitar qualquer ruído no conteúdo, as citações em inglês foram mantidas no idioma, sem tradução própria. WILLIAMS, R. **Television: technology and cultural form**. Londres: Routledge, 2003, p. 6.

297 FEENBERG, A. Marcuse ou Habermas: duas críticas da tecnologia. **Inquiry: An Interdisciplinary Journal of Philosophy,** v. 39, 1996, p.79. Disponível em: <http://www.sfu.ca/~andrewf/marhabportu.htm>. Acesso em: 05.01.17.

Noble[298] coloca a fabricação de um aparato como uma viagem de muitos caminhos possíveis. É a definição do que é relevante socialmente e o poder dos atores que estabelecem esses enunciados e hegemonizam os processos e instâncias que vão determinar o caminho tomado e a solução tecnológica resultante.

Essa disputa se manifesta nas Tecnologias da Informação e da Comunicação (em especial na Internet) e no tratamento dos dados pessoais, chamados de "o novo petróleo"[299]. Reguladores, agentes empresariais e uma vasta literatura apontam a economia do futuro apoiada no processamento dessas informações em larga escala, processo denominado *Big Data*[300]. Entretanto, esse cenário traz novas preocupações acerca de velhos problemas. Entre as diversas ponderações sobre os riscos associados à Internet, uma delas merece destaque e será o objeto de debate no presente artigo: a garantia da privacidade, visto que o "novo petróleo" não é um recurso natural em águas profundas aguardando para ser descoberto, mas é o registro de quem somos e do que fazemos de forma cada vez mais detalhada.

Neste momento do percurso, é válido realizar uma parada para retomar o que se quer dizer com privacidade, a sua importância e os esforços para a sua garantia nas mais diversas esferas. Westin[301] a define como "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Ela envolve a capacidade de o indivíduo poder se isolar ou se retirar do convívio com os outros. Outra possibilidade de exercício da privacidade é a manutenção do convívio, mas sem uma identificação, de forma anônima.

Altman define privacidade[302] como "selective control of access to the self". Isso implica dotar o indivíduo de formas e controle da sua presença, manifestação ou participação nos espaços públicos ou mesmo privados que reúnam um grupo considerável. O autor elenca quatro elementos relativos ao conceito: (1) o controle das fronteiras das relações pessoais; (2) o conflito entre privacidade pretendida e privacidade real, com a variação para além ou para aquém do

298 NOBLE, David. **Progress Without People: New Technology, Unemployment, and the Message of Resistance**. Toronto: Between the Lines Press, 1995, p.324.

299 TOONDERS, J. Data Is the New Oil of the Digital Economy. **WIRED**. Disponível em: <https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/>. Acesso em: 23 mar. 2017.

300 Mayer-Schonberger & Cukier (2013, p. 12) afirmam que o *Big Data* envolve "applying math to huge quantities of data in order to infer probabilities". Eles apontam três características-chave: volume, velocidade e variedade.

301 WESTIN, A. **Privacy and freedom**. New York: Athenaeum, 1967, p.7.

302 ALTMAN, I. **The environment and social behavior**. Monterey, CA: Brooks/Cole. 1975, p.24.

desejado, não correspondendo ao nível ótimo necessariamente; e (3) a manifestação em diversos níveis, do individual ao coletivo. Burkert[303] problematiza a percepção da privacidade como algo individual e argumenta que o conceito de privacidade deve estar inserido em uma perspectiva mais ampliada, em uma dimensão "política", estando imerso em um conjunto de direitos relacionados à comunicação e à participação democrática. O ocultamento intrínseco à privacidade deve ser uma opção do sujeito juntamente ao inverso, a sua exposição como ator político que assume posições e se mobiliza.

Kwecka[304] et al. vão no mesmo sentido ao alegar que o conceito deveria ser tomado como um bem público relacionado à garantia da democracia e ao exercício de outros direitos, como a livre associação e a participação pública. Afirmam que: "*Privacy enables individuals to criticize and resist measures or acts of government that are of an undemocratic or even totalitarian nature*". A privacidade não seria a cortina que permite ao indivíduo permanecer no isolamento, mas o elemento que assegura sua inserção livremente na vida em sociedade e no debate público. Os autores ponderam que um dos desafios para avançar neste sentido é a transformação da privacidade em algo renunciável e cambiável por serviços e por benefícios, seja junto ao Estado (como o exemplo da segurança pública) seja junto a uma empresa (como no caso do uso de sites de redes sociais).

A relevância dessa possibilidade de "proteção" do mundo público e de controle da manifestação é reconhecida como direito em diversas legislações. O artigo XII da Declaração Universal dos Direitos Humanos enuncia: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques"[305] .

A Convenção Europeia de Direitos Humanos assegura em seu artigo 8º o "*right to respect for private and family life*", que inclui o respeito à vida privada, ao lar e à correspondência[306] e a não interferência por autoridade estatal no exercício do direito, à exceção de previsões legais no tocante a questões de segurança na-

303 BURKERT, H. Privacy-Enhancing Technologies: Typology, Critique, Vision. In: AGRE, Philip. E. ROTENBERG, Marc (eds.). **Technology and Privacy: the new landscape**. MIT Press, Londres, 1997, p.136.

304 KWECKA, Zbigniew. BUCHANAN, William. SCHAFER, Burkhard. RAUHOFER, Judith. "I am Spartacus": privacy enhancing technologies, collaborative obfuscation and privacy as a public good. **Artificial Intelligence and Law**, volume 22, Issue 2, June 2014, p116.

305 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em:< http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf.>. Acesso em: 03.08.16.

306 COUNCIL OF EUROPE. **European Convention of Human Rights**. 1950, p.10. Disponível em: <http://www.echr.coe.int/Documents/Convention_ENG.pdf>. Acesso em: 18.01.17.

cional, segurança pública, prevenção de crimes e proteção de direitos de outros. A Constituição Federal do Brasil assevera em seu Artigo 5º, inciso X, que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", direito estendido também ao lar e às correspondências do cidadão.

Mas esse direito, enunciado como princípio na Constituição, demanda regulamentação detalhando o que esta garantia compreende e de que forma ela será respeitada e promovida, bem como qual é a responsabilidade dos atores sociais e do Estado nisso. Na Europa, por exemplo, a proteção de dados foi positivada com a diretiva 95/46/EC[307] , atualizada pela Regulação Geral de Proteção de Dados[308]. Na América Latina, em países como, por exemplo, Argentina, Chile, Colômbia, Costa Rica, México, Nicarágua, Peru e Uruguai, já há legislações próprias para a proteção de dados[309] . O caso brasileiro será detalhado mais adiante.

A tecnologia a serviço da privacidade

Após a discussão sobre a importância da privacidade e sua afirmação em legislações de diversos países, o próximo passo é colocar uma pergunta: estas conseguem ser efetivas em um cenário de coleta de dados em tempo real por bilhões de sensores espalhados nos mais variados espaços de vivência das coletividades? Para um conjunto de autores, entre os quais nos incluímos, infelizmente não. Não se trata aqui de invalidar esses arcabouços normativos em uma visão resignada quanto à "vitória do *Big Data* sobre a privacidade", mas de reconhecer a complexidade da fiscalização na realidade concreta do respeito a este direito tão importante em um ambiente baseado em dados.

A solução passaria pela consideração dessa preocupação como uma diretriz orientadora da elaboração de soluções tecnológicas, perspectiva que ganhou a denominação de *Privacy By Design* para autores em diversos campos, da ciência da computação ao direito. O conceito consiste na compreensão da necessi-

307 COUNCIL OF EUROPE. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. **On the protection of individuals with regard to the processing of personal data and on the free movement of such data**. November, 23, 1995.

308 EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament** and of the Council of 27 April 2016.

309 ANGARITA, N.. **Latin America and Protection of Personal Data: Facts and Figures (1985-2014)**. University of Los Andes Working Paper. 2014. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412091>. Acesso em 10.07.17.

dade de "information systems be designed in such a way that privacy and data protection rules are automatically enforced and that default settings restrict data processing to a necessary minimum"[310] . Para D'acquisto et al.[311] [312] , "it is a process involving various technological and organizational components, which implement privacy and data protection principles". Hornung[313] define o conceito como "*data protection through technology*". Ele vê essa abordagem como um complemento necessário às regulações como forma de enfrentar os desafios de assegurar a privacidade um cenário de qualificação do processamento de dados e da computação invasiva.

Essa leitura foi impulsionada por autoridades regulatórias como as da Holanda e do Canadá. Cavoukian[314] defende a inclusão da privacidade no *design* dos sistemas informatizados "*by default*".[315] Ou seja, não como uma opção, mas como naqueles parâmetros originais e regulares dos dispositivos. Ela elenca sete princípios fundantes desta abordagem, quais sejam:

1. medidas proativas e preventivas, e não reativas ou para remediar situações;
2. privacidade como "***default***";
3. privacidade constitutiva do artefato, e não um anexo, adaptação ou elemento externo;
4. funcionalidade completa de modo que a privacidade seja compatível com outros objetivos, tais como segurança;
5. alcance, garantindo que as medidas se estendem por todo o ciclo de vida do dado e não somente em alguns momentos;
6. visibilidade e transparência; e
7. respeito à privacidade do usuário.

---

310 KOOPS, B-J. HOEPMAN, J-H. LEENES, R. Open-source intelligence and privacy by design. In: **Computer Law & Security Review**, No 29. 2013. p. 678.

311 D´ACQUISTO, G. DOMINGO-FERRER, J. KIKIRAS, P. TORRA, V. DE MONTOJYE, I-A. BOURKA, A. **Privacy by design in Big Data**: **An overview of privacy enhancing technologies in the era of Big Data analytics**. ENISA (European Union Agency for Network and Information Security), 2015, p.21.

312 Equipe responsável por importante relatório da Agência Europeia para a Informação e Segurança de Dados (Enisa).

313 HORNUNG, G. Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework. **Innovation: The European Journal of Social Science Research**, Vol. 26, Nos. 1 2, 2013, p.182.

314 Foi comissária para Informação e Privacidade do estado de Ontário, no Canadá.

315 CAVOUKIAN, A. **Information & Privacy: 7 foundational principles**. Internet Architecture Board. 2011. Disponível em: . Acesso em 18 de outubro de 2016.

D´Acquisto[316] identifica um conjunto de estratégias relacionadas ao *Privacy By Design*:

1. Minimizar – os dados coletados devem ser reduzidos ao mínimo possível;
2. Esconder – os dados e sua interrelação não devem ser publicizados;
3. Separar – o processamento dos dados deve se dar em compartimentos separados sempre que possível;
4. Agregar – os dados devem ser processados com alto nível de agregação e com o mínimo de detalhes;
5. Informar (transparência) – os sujeitos dos dados devem ser sempre informados dos processamentos de suas informações;
6. Controlar – os sujeitos dos dados devem ter controle sobre a coleta e o processamento de seus dados;
7. Fiscalizar e aplicar as leis – as políticas de privacidade devem estar em conexão com as exigências legais e devem poder ser fiscalizadas; e
8. Demonstrar – controladores de dados devem poder demonstrar o respeito às políticas de privacidade e aos requisitos legais.

Associado a este conceito está o de *Privacy-Enhancing Technologies* (PETs). Hes e Borking[317] [318] usam o termo "to refer to a variety of technologies that safeguard personal privacy by minimizing or eliminating the collection of identifiable data". Para Heurix et al.[319] essas tecnologias envolvem a Segundo os autores, o objetivo é proteger os usuários assegurando anonimato, pseudoanonimato, desvinculação e obstáculos à observação de suas atividades. Burkert[320] afirma que o termo "refers

316 D´ACQUISTO, G. DOMINGO-FERRER, J. KIKIRAS, P. TORRA, V. DE MONTOJYE, I-A. BOURKA, A. **Privacy by design in Big Data**: **An overview of privacy enhancing technologies in the era of Big Data analytics**. ENISA (European Union Agency for Network and Information Security), 2015, p.22.

317 HES, R. BORKING, J. **Privacy-Enhancing Technologies: a path to anonymity**. Registratiekamer, The Hague, August 2000, p.7.

318 Em um documento de referência do campo elaborado pelas autoridades regulatórias de proteção de dados da Holanda e do Canadá.

319 HEURIX, J. ZIMMERMANN, P. NEUBAUER, T. FENZ, S. A taxonomy for privacy enhancing technologies. In: **Computer & Security**, 53. 2015, p.1.

320 BURKERT, H. Privacy-Enhancing Technologies: Typology, Critique, Vision. In: AGRE, Philip. E. ROTENBERG, Marc (eds.). **Technology and Privacy: the new landscape**. MIT Press, Londres, 1997, p.135.

to technical and organizational concepts that aim at protecting personal identity". Entre os objetivos estariam buscar reduzir ao máximo os dados coletados, mitigar ou eliminar o processamento destes de forma conjunta e dar ao sujeito da informação e controle sobre o que é feito com ela.

Para o autor, o conceito tem que ser separado das tecnologias de segurança de dados. Um dos pontos positivos das PETs seria exatamente este, o de se dissociar deste campo e de fixar os limites dele para a garantia da privacidade. Isso porque a segurança de dados está preocupada, como o nome frisa, com a integridade das informações processadas, muitas vezes independentemente da legitimidade desta ação. Tal abordagem não abarca de forma abrangente a preocupação com os dados dos indivíduos, organizações e coletividades como na discussão da privacidade e proteção de dados. Van Blakron et al.[321] , em obra referência sobre o tema, compreendem esses aparatos tecnológicos como "a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system".

Na literatura sobre o assunto, autores elencam um conjunto de atributos das PETs. Eles ganham diferentes nomes, alguns chamados de princípios, outros de funções e outros de elementos centrais. Com base nessas contribuições, propõe-se a seguir uma sistematização para aquilo que será chamado de "mecanismos"[322]. O termo visa designar tanto estratégias das PETs quanto atributos específicos e dimensões que elas devem preservar para cumprir seu objetivo de garantir a privacidade do usuário.

---

321 VAN BLAKRON, G. W. BORKING, J. J. VERHAAR, P. PET. In: VAN BLAKRON, G. W. BORKING, J. J. OLK, J. G. E. (org.). **Handbook of privacy and privacy-enhancing technologies: the case of intelligent software agents**. PISA Consortium. 2003, p.33.

322 Sabemos que cada um dos aspectos listados a seguir enseja intensos debates e são objeto de uma literatura específica considerável, como os processos de anonimização, a criptografia, as interfaces de controle do usuário, os instrumentos de regulação, a transparência, entre outros. No entanto, nos limites do presente artigo não será possível entrar em cada uma dessas problemáticas. O texto se propõe apenas a uma apresentação mais preliminar e esquemática do debate.

Mecanismo	Descrição
Limitação da coleta de dados	Os dados coletados devem ser os necessários para aquele sistema ou atividade realizado, não devendo ir além disso ou conter qualquer outra forma de excesso. Exemplo: um aplicativo de localização deve registrar o local do usuário apenas quando este acionar a funcionalidade para a operação solicitada (identificar a distância ou tempo entre um ponto e outro ou guiar o usuário pelo caminho escolhido), não devendo ir além disso (continuar registrando o deslocamento do usuário após o trajeto solicitado ao aplicativo).
Propósito específico	Para além da quantidade de dados coletados deve ser o mínimo possível, o objetivo do seu uso tem que ser específico e estar claramente informado para o usuário. O controlador não pode, após a autorização da coleta de informações, mudar a finalidade da coleta de dados ou aplicar outra que não tenha sido informada. Exemplo: Uma televisão que possui ação de comando por voz não poderia, por exemplo, gravar as conversas das pessoas no ambiente onde ela está. Tal proibição é válida tanto para o desvio de finalidade clandestino quanto para uma eventual nova finalidade que o aparelho possa vir a ter (como, em uma situação hipotética, a indicação de grades de programação personalizadas utilizando palavras-chave a partir das conversas gravadas).
Autenticação e autorização	Os dados processados devem ser aqueles que precisam ser conhecidos. Os dados não podem estar disponíveis para todos, mas para aquele ente ou pessoa responsável por aquele processamento. Isso se dá por meio da definição de autorização e autenticação para acesso a esses dados. Exemplo: Em um hospital, um médico de uma especialidade não poderia ter acesso a toda a ficha de um paciente, mas apenas às informações relevantes para o tratamento que desenvolve. Assim como, nesse mesmo exemplo, o funcionário do setor financeiro que encaminha os pagamentos das consultas não poderia acessar o prontuário do paciente.
Anonimização[1]	É a modificação de qualquer dado que identifique o indivíduo para que este não possa ser identificados novamente durante o processamento de suas informações[2]. Uma modalidade menos efetiva é a "desidentificação" por meio da qual há apenas a retirada de dados que permitem a descoberta do indivíduo, como nome, documento de identidade etc. Há dois princípios: "*data masking*" e "*data synthesis*". No primeiro, é criada uma "versão" de um dado diferente do original, podendo ela ser alterada ou apenas resumida a partir da exclusão de detalhes. No segundo, é produzida uma síntese do dado original mantendo determinados atributos. Outra estratégia é impedir que os diversos dados isolados possam, de forma combinada, re-identificar uma pessoa. Exemplo: A *K-anonymity* é uma família de modelos de anonimização que combina um conjunto de atributos "quase-identificáveis" (aqueles concernentes ao indivíduo, mas que não permitem uma identificação direta, como idade, bairro etc.) impedindo o rastreamento do registro original.

Pseudo-identidade	A criação de referências para o dado do usuário de modo que ele não possa ser identificado. Um dos caminhos é incluir no sistema de dados um "*identity protector*"[3], que substitui a identidade do usuário por uma outra referência. Isso pode ocorrer com uma alteração no próprio sistema, com um outro dispositivo controlado pelo usuário ou por um sistema controlado por um terceiro (órgão público ou banco de dados privado, por exemplo). Exemplo: Uma tecnologia pode criar um primeiro código (as iniciais do nome mais o ano de nascimento, por exemplo). Em um outro sistema, é gerado um *username* para o código criado. Este *username* é usado como referência de um determinado dado (a faixa salarial do usuário para uma análise de aumento da renda do trabalho, por exemplo). Desta forma, o processador do dado não poderia identificar de quem se trata.
Criptografia	Criptografia é uma medida notória para garantir segurança e confidencialidade. A informação é codificada por meio de uma chave. Apenas o receptor da informação possui a chave que permite recompor a mensagem original. Esse conjunto de técnicas pode contribuir nas etapas de armazenamento, transferência e acesso. Exemplo: A técnica de *Blind Signatures,* usada em sistemas de votação eletrônica em alguns países. Ela permite que alguém possa autenticar uma mensagem ("assiná-la") sem ter acesso ao conteúdo dela. No caso de uma votação, os responsáveis pela urna ou mesmo pelo sistema como um todo, como os tribunais eleitorais, podem validar os votos, assinando-os, mas sem ler seus conteúdos.
Biometria	Uma medida mais segura, mas com riscos. A biometria impede o acesso não autorizado a senhas e a informações que não são suas. É mais fácil um *password* ser descoberto ou uma informação de cartão de crédito ser coletada, para citar dois exemplos, do que o uso de uma impressão digital. Contudo, o controle dos dados biométricos torna-se algo perigoso tanto do ponto de vista de governos como de empresas. Alguns modelos de computadores, por exemplo, já solicitam identificação de retinas.
Possibilidade de auditagem	Os dados devem poder ser auditados por um terceiro. Este pode ser uma autoridade regulatória ou mesmo um ente privado. A legislação europeia prevê a existência de uma autoridade de proteção de dados que pode acessar informações em servidores para desempenhar seus deveres de supervisão. Exemplo: Um caso inverso ao mecanismo proposto é o de sites de redes sociais como o Facebook. A plataforma não disponibiliza seus dados para auditagem tanto por entes específicos quanto por autoridades estatais. Até mesmo a solicitação de informações por via judicial encontra dificuldades de retorno por parte da empresa.

Desagregação	As instâncias de coleta e processamento devem ser descentralizadas ao máximo, devendo ser responsabilidade de entes diferenciados ou, no caso de serem os mesmos atores, em sistemas distintos. Esse mecanismo dificulta a identificação do usuário e o abuso no uso dos dados pessoais ao criar "catracas" para que um determinado ente ou interessado possa acessar a informação sobre aquele indivíduo. Exemplo: no âmbito do Estado Brasileiro, por exemplo, a centralização dos diversos sistemas (Receita Federal, Sistema Único de Saúde, Justiça Eleitoral, Sistema Nacional de Informações de Segurança Pública, entre outros) permite um controle preocupante sobre os cidadãos e cria a chance de abusos por agentes governamentais.
Controle pelo usuário	O usuário deve poder ter o controle das informações que deseja disponibilizar, do processamento feito com elas. Deve poder, também, ter os canais para desautorizar alguma informação, algum uso específico ou mesmo para apagar informações disponíveis em determinado sistema informatizado. Este controle deve ocorrer com interfaces amigáveis e com informações claras e atualizadas. Exemplo: Kolter et al.[4] criaram uma arquitetura de privacidade centrada no usuário. A intenção dos autores era que ela incentivasse a criação de uma comunidade de privacidade operando de forma colaborativa. A solução dos autores funcionava por meio de um *plugin* no *browser* do usuário composto por três componentes. O primeiro, "gerenciador de preferências", auxiliava o usuário a definir que informações desejava compartilhar. O segundo fornecia ao usuário o registro do fluxo real de dados pessoais e o terceiro permitia o acesso ao histórico dos fluxos de dados.

Elaboração própria a partir de Van Blakron et al.[323] , Hornung[324] e Hes e Borking[325].

A despeito das diversas possibilidades de mecanismos e alternativas, a adoção do *Privacy By Design* como diretriz orientadora e das *Privacy-Enhancing Technologies* como soluções técnicas ainda enfrentam obstáculos. Entre eles está a falta de visibilidade e publicidade destas soluções, a má usabilidade, os preços inacessíveis e as dificuldades criadas por atores de mercado. Rubinstein[326] também identifica um cenário de disseminação ainda incipiente. Ele aponta uma

323 VAN BLAKRON, G. W. BORKING, J. J. VERHAAR, P. PET. In: VAN BLAKRON, G. W. BORKING, J. J. OLK, J. G. E. (org.). **Handbook of privacy and privacy-enhancing technologies: the case of intelligent software agents**. PISA Consortium. 2003, p.37.

324 HORNUNG, G. Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework. Innovation: The European Journal of Social Science Research, Vol. 26, Nos. 1 2, 2013, p.185.

325 HES, R. BORKING, J. **Privacy-Enhancing Technologies: a path to anonymity**. Registratiekamer, The Hague, August 2000, p.7.

326 RUBINSTEIN, I. S. Regulating Privacy By Design. **Berkley Technology Law Journal**. Vol. 26, 2011, p.1412.

falta de clareza entre o princípio e sua aplicação prática nas diversas soluções. As empresas não teriam claro como materializar o PBD. Outro problema está no lado da demanda. As PETs ainda não se tornaram populares entre os internautas e a demanda por este tipo de medida tem sido baixa. "Reasons include consumers' lack of knowledge concerning the privacy risks associated with web surfing, search, social networks, e-commerce, and other daily internet activities and their limited understanding of how PETs or privacy by design might help reduce these risks"[327]. Do lado da oferta, o ímpeto de coleta de dados das empresas, tanto as "dadointensivas" quanto as que utilizam essa matéria-prima como insumo (em especial como organizador da publicidade online e da oferta de serviços personalizados), deriva em pouco ou nenhum interesse em promover o PBD a menos que haja uma exigência regulatória ou forte pressão das pessoas.

D'Acquisto et al.[328] elencam alguns desafios do PBD e das PETs que são potencializados pelo movimento dos agentes econômicos e pela pressão pela ampliação do Big Data em larga escala nas relações de produção:

1. Como minimizar a obtenção das informações pessoais em um cenário em que o volume e a variedade caracterizam as práticas de coleta de dados?
2. Como buscar a compartimentalização das diversas etapas da cadeia (coleta, armazenamento, processamento) quando a lógica do *Big Data* é a centralização e a integração?
3. Como buscar a "anonimização" e o processamento "escondido" se o re-uso e a re-identificação de dados e usuários são características das estratégias de *Big Data*?
4. Como garantir o controle dos usos dos dados pelos seus donos em um ambiente de reprocessamentos e novos processamentos após os consentimentos dados?
5. Como trabalhar com a informação ao usuário e seu controle em um cenário de coleta em fluxo e não estática, como no caso de sensores?

---

327 RUBINSTEIN, I. S. Regulating Privacy By Design. **Berkeley Technology Law Journal**. Vol. 26, 2011, p.1412.

328 D´ACQUISTO, G. DOMINGO-FERRER, J. KIKIRAS, P. TORRA, V. DE MONTOJYE, I-A. BOURKA, A. **Privacy by design in Big Data: An overview of privacy enhancing technologies in the era of Big Data analytics**. ENISA (European Union Agency for Network and Information Security), 2015, p.22.

Cartrysse e Van der Lubbe[329] alertam para outro aspecto mais básico, mas não menos importante: a capacidade dos dispositivos de não permitirem qualquer tipo de invasões e acessos indesejados por terceiros. As PETs se assentam no princípio de que as operações ocorrem em artefatos seguros, quando há uma sorte de riscos em relação a isso. Eles citam alguns recursos que podem ser utilizados para atestar a integridade dos dispositivos, como a "*watermarking*" (implantação de "marcas d'água") em programas. Essas marcas permitem identificar se o programa foi alterado ou não. Os autores listam outros tipos de ameaças:

1. Alteração das funcionalidades do programa;
2. Cópia e duplicação do programa;
3. Danificar o programa;
4. Adoção de identidade alheia para uso do programa ou roubo de seus dados;
5. Armazenamento inseguro de dados;
6. Não separação de dados públicos e privados;
7. Vulnerabilidade do programa para invasões por terceiros; e
8. Ação do programa contra o usuário provocada por vírus ou conteúdos maliciosos.[330]

Conclusões e estudos futuros: a legislação brasileira e a agenda necessária

Os desafios para a implantação do PBD e a sua concretização na fabricação das PETs são complexos. Assim como no debate acerca da governança da Internet em si, os instrumentos regulatórios nacionais e as frágeis diretrizes normativas construídas internacionalmente contrastam com um avassalador espraiamento de grandes plataformas pelo planeta. Com um mercado cada vez mais verticalizado (que reúne conglomerados ou alianças interempresariais) e globalizado, o PBD é ao mesmo tempo uma estratégia fundamental e que exige

329 CARTRYSSE, K. VAN DER LUBBE, J. C. A. Providing privacy to agents in an untrustworthy environment. In: VAN BLAKRON, G. W. BORKING, J. J. OLK, J. G. E. (org.). **Handbook of privacy and privacy-enhancing technologies: the case of intelligent software agents**. PISA Consortium. 2003, p.81.

330 CARTRYSSE, K. VAN DER LUBBE, J. C. A. Providing privacy to agents in an untrustworthy environment. In: VAN BLAKRON, G. W. BORKING, J. J. OLK, J. G. E. (org.). **Handbook of privacy and privacy-enhancing technologies: the case of intelligent software agents**. PISA Consortium. 2003, p.83.

suporte na sua legitimação nas esferas regulatórias e implantação efetiva junto ao mercado de dispositivos e aplicações.

A afirmação dessa agenda significa enfrentamento às resistências de um amplo segmento de agentes econômicos, desde os principais conglomerados atuantes na Internet (Apple, Google e Facebook) até outros agentes que têm voltado suas estratégias concorrenciais cada vez mais para uma produção baseada em dados. A oposição também reside nos governos, seja pelo aspecto da violação de privacidade para fins de inteligência (prática antiga e elevada a novo patamar no mundo conectado, como as denúncias de Edward Snowden revelaram) seja para a gestão das ações e políticas públicas, por meio da integração de bancos de dados, criação de cadastros únicos e outras iniciativas neste sentido.

Esta agenda implica uma série de medidas normativas e organizacionais de fixação de parâmetros (*standards*) de fabricação que envolvem o conjunto das plataformas garantindo, ao mesmo tempo, uma flexibilidade para que elas possam se adaptar aos países onde as legislações de proteção de dados são mais rígidas. A referência neste sentido é a Regulação Geral de Proteção de Dados aprovada pela União Europeia em 2016, que entrará em vigor em 2018[331] , que prevê de forma específica e explícita em seu Artigo 25 o *Privacy By Design* como diretriz, obrigando os controladores de dados[332] a adotar medidas técnicas e organizacionais voltadas à implementação dos princípios de proteção de dados.

---

331 EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament** and of the Council of 27 April 2016.

332 **Article 25** Data protection by design and by default 1.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 organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, 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. 2. The controller shall implement appropriate technical and organizational 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. 3. 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. **Reform of EU data protection rules**. European Commission. Disponível em: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>. Acesso em: 23 mar. 2017.

O Brasil ainda não possui uma legislação específica, apenas o princípio constitucional de proteção à vida privada e reserva do lar e das comunicações. Entretanto, encontra-se em debate, no momento de fechamento deste artigo (segundo semestre de 2017), uma regulação de proteção de dados pessoais, vários projeto de Lei em debate no Congresso, sendo o mais importante o PL 5.276 de 2016. De autoria do Poder Executivo, ele foi objeto de intenso debate por todos os segmentos durante a sua elaboração[333], que contou com consulta pública e embates no interior do governo federal no período anterior à derrubada da presidenta Dilma Rousseff por um processo de *impeachment*.

O PL objetiva "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Art. 1º); dispõe sobre o tratamento de dados de qualquer por indivíduo ou pessoa jurídica independentemente do local desde que a coleta ou o processamento ocorram no país ou o seu objeto seja destinado a cidadão ou entidade brasileira (Art. 3º); abarca todo "dado relacionado à pessoa natural identificada ou identificável", diferenciando como sensíveis as informações sobre origem racial ou étnica, convicções religiosas ou políticas, filiação a associações e dados relacionados à saúde ou vida sexual (Art. 5º); fixa princípios para o tratamento como a definição de finalidade específica, a adequação e a necessidade relacionadas ao propósito informado no momento da coleta, o livre acesso do usuário, a transparência e a não discriminação (Art. 6º); exige o consentimento e permite o tratamento em hipóteses específicas (Art. 7º), estabelece exigências de transparência e disponibilização de informações ao usuário (Art. 8º), entre outras disposições.

O projeto não trata de forma explícita e específica de medidas técnicas de garantias da privacidade. Ele apenas tangencia possibilidades. O Artigo 12 indica uma alternativa neste sentido: "Art. 12. O órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento, ou solicitar a apresentação de relatório de impacto à privacidade". O Artigo 13 prevê a fixação a posteriori de parâmetros e a fiscalização: o parágrafo 2º estabelece que o órgão competente "poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança". Em relação a ações de fiscalização, o parágrafo 3º define que o compartilhamento e o uso de dados anonimizados deve "ser objeto de publicidade e de transparência, sem prejuízo do órgão competente poder solicitar ao

333 ZANATTA, R A. F. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito e Internet III: Marco Civil da Internet**. São Paulo: Quartier Latin, 2015.

responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento".

O Art. 39 cria a figura de um relatório de privacidade que poderá ser exigido do operador do tratamento de dados: "O órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento". Aqui coloca-se um problema importante: o frágil arranjo regulatório proposto pelo projeto depende de um "órgão competente" que o próprio projeto menciona não cria efetivamente, deixando para um cenário de insegurança jurídica total quanto a quem absorverá as prerrogativas institucionais no âmbito do Executivo e se haverá condições para fazê-lo. Na discussão no Congresso, entidades da sociedade civil organizadas em torno da Coalizão Direitos na Rede têm levantado o debate sobre a necessidade de uma autoridade de proteção de dados como há em diversos países da Europa ou no Canadá.

O Capítulo VII do projeto dispõe de forma mais clara sobre a segurança de dados, ao obrigar os operadores a adotar medidas de segurança técnicas "aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (Art. 45). No entanto, conforme argumentado por Burkert[334] , o *Privacy By Design* vai além da segurança de dados, tendo esta uma condição, não a sua finalidade.

Com os desafios expostos para a implementação das regulações, uma nova lei não pode prescindir do *Privacy By Design* e da fixação de obrigações e parâmetros com vistas a criar exigências para plataformas, prestadores de serviço e operadores de tratamento de dados. O Projeto de Lei 5.276/2016 avança em diversos aspectos, mas ainda é insuficiente, devendo trazer obrigações mais efetivas com vistas a proteção de dados de indivíduos, entidades e coletividades. A experiência europeia pode ser uma referência importante, mas a prática do PBD e as PETs fornecem um instrumental rico para a formulação dessas diretrizes numa peça legal que pretende ser o marco normativo para o tema no país.

334 BURKERT, H. Privacy-Enhancing Technologies: Typology, Critique, Vision. In: AGRE, Philip. E. ROTENBERG, M (eds.). **Technology and Privacy: the new landscape**. MIT Press, Londres, 1997.

Ethical Considerations About Privacy and other Challenges in the Digital Era

Katia A. Lima[335]

Introduction

As contemporary societies keep developing around new technologies that promote multiple and faster ways for us to communicate in a more global scale, one can observe, however, that safeguards and regulations for digital media (with the popularization of the Internet) are still at a considerable immature stage. The spreading of these new tools raises indeed a variety of tricky issues as we try to understand their impact in our lives, not only individually, but also as social and professional groups and communities. On the one hand, the Internet can work to counter silence and powerlessness, by allowing people to engage via new spaces through which they can bridge geographical barriers not possible before, and to interact and express themselves more easily; on the other, at the same time, these tools now strongly influence our habits and the nature of our social interactions, including our perception of ourselves, of others, and of our enlarged world thereby.

With the increased number of digitally mediated encounters nowadays, sometimes bringing together quite diverse people, bigger challenges may arise about the access, documentation, and transferring of information (be it through messages, posts, blogs, searches, etc.). Such encounters and the information we share with others can now be not only archived for future reference, but can also become promptly available pretty much everywhere. These may at times lead to undesired broadcasts and abuses, consequently raising damages, complaints, and litigation.

Such possibility can have a big impact on people's lives, depending on the different hierarchical levels of their social and professional relations, that is: from employers with regards to their employees (in terms of power and influence), from governments with regards to its citizens (in terms of censorship

335 Ph.D. candidate and researcher on Applied Ethics at University of Sherbrooke (Longueuil, Canada). Research collaborator for ITS-Rio and for Inter@ctiva/Communalis (partnership of University of Montreal and UFRJ).

and mass surveillance), from more powerful to weaker nations (in terms of exercising pressure and benefiting in business and diplomatic practices), etc. Not to mention, of course, foreigners and underprivileged people who were already prone to suffer a significant amount of discrimination and exclusion, due to their immigration status, cultural background and/or religion.

As we are now also caught in the wave of Big Data, our activities and personal information are thus being constantly tracked, collected, archived, copied, manipulated, transferred, cross-referenced, and exposed — be it with or without the person's acknowledgement and consent. For example, different technologies can now track users' visit history (including links to previous and subsequent websites), what information they access and retrieve, how much time they spend on a given article, what they buy (and where and when they buy it), what ads they view and for how long, what personal data (including financial data) they enter into web forms, what software they are using, what emails they receive, open (including when and where it's accessed) and to whom it's forwarded. Online newspapers, e.g., can now quite easily obtain records of the political or other interests of their readers, and online bookstores may get records of what books their customers have viewed or purchased (on any topic, including health, finance, etc). [336]

With its accompanying increased potential for abuses, the boundaries between 'public' and 'private' have thus, considerably changed, and further issues are raised about confrontation *vs.* collaboration, both within and among different cultures.[337] After all, all this has blurred the lines between mass and interpersonal communication, which may sometimes turn out to be rather perturbing in both ways, up and down the power ladders within and among societies. [338]

Now, one of the best promises of digital media is its democratic potential, not only to enable more information gathering, but also to promote wider direct ('personal') communication by engaging people and allowing them to participate more easily in the building of healthier democracies. We can indeed allow for an increase of both inclusion and substantial institutional transparency, through easier ways of giving access to individuals, within and among groups and institutions,

---

336 See also an interesting article from **The Economist** regarding the issue of language analysis, reproduction and translation, entitled "Finding a voice" (Technology Quarterly, Jan. 7th 2017). Available at: <http://www.economist.com/technology-quarterly/2017-05-01/language>. Accessed on: 22 mar. 2017.

337 KATZ, James E. and RICE, Ronald E. **Social Consequences of Internet Use: Access, Involvement, and Interaction.** MIT Press, 2002.

338 BAYM, Nancy K. **Personal Connections in the Digital Age**: **Digital Media and Society Series**. Polity, 2010.

some of which that used to be much more segregated and elitist (including in politics). But as the old saying goes, with rights also come responsibilities.

Delicate and controversial questions are consequently brought up involving grey zones about such issues, for example: What may be considered *private* vs. *public* information in the Internet? What degree of *transparency* should governments, legislators, and companies demonstrate to their constituents and clients, with respect and in contrast to the guarantees for protecting the information they gather and handle about regular citizens? Should basic access and protection of personal data be guaranteed for everyone, indistinctively?

The communication revolution

I do not want to live in a world where everything I do and say is recorded. That is not something I am willing to support or live under.

Edward Snowden

The Internet is not such a new technology. It was originally conceived to serve as a decentralized military communications system, commissioned in 1969 by the U.S. Department of Defense as the Advanced Research Projects Agency Network (ARPANET), which could continue working even if parts of it suffered a military attack. It was then diffused in a large scale only 20 years later, especially after the World Wide Web server and browser were made available to the general public in the 1990s.

More technically, therefore, it was conceived as a decentralized worldwide system networked to allow for the exchange of data among computers spread apart, through what was called 'packet switching' and through standardized protocols that enable this exchange. Through packet switching, messages (in the form of e-mails, audio, video, or other file formats) are broken down into small blocks of digital information. Each block contains specific addresses (IPs) and reassembly instructions, to be sent via the most efficient routes to their final destination, where they are eventually reassembled.

In other words, by breaking messages down into smaller packets that can travel independently, the so-called 'packet switching technology' takes optimal advantage of bandwidth and enables data exchange among millions of networked computers with unprecedented speed, reach, and interactivity. Because of these characteristics, the Internet is fast and reliable, thus having

become in many places the primary means by which individuals, organizations, governmental offices and businesses now communicate in a daily basis.

Between the early 1990s, during which the Internet first became available for public and commercial use, and the year of 2006, it grew to encompass almost 1 billion users. These users took advantage of a multitude of communication technologies, among which we have the World Wide Web, electronic mail and instant messaging systems, and social media groups, that engage people in a wide range of activities, both at personal and professional levels.[339]

Such developments also prompted a rapidly growing social demand for the 'network of everything', both from the side of the business world and the public's desire to build its own communication networks more 'privately'[340]. Regarding the scope of the processes of communication, more particularly, one can easily observe that, before the popularization of the Internet, we were typically able to distinguish 'interpersonal' communication from broader 'mass' communication in a much more explicit way, that is: the former being more private and interactive (with feedback loops), involving sender(s) and receiver(s) as individualized subjects; while the latter being public, traditionally one-directional (from one to many), and only subsequently being farther diffused to groups and society at large.[341]

As Baron indicates, digital communication offers much more 'volume control' towards limiting our social environment by managing, scrutinizing, and documenting our interactions.[342] Such new tools and business models, supported by the policies of regulatory agencies, have allowed for both an organizational and a technological convergence between the two systems.[343] It began to take place more pointedly in the first decade of the 21st century, leading to the gradual formation of the new multimedia system now in vogue.

---

339 STAPLES, William G. **The Encyclopedia of Privacy**. Greenwood Press, 2007, p. 298. According to further available statistical data, about 40% of the world population now has some access to the Internet (that number keeps growing each day), with the **first billion** having been reached in 2005, the **second billion** in 2010, and the **third billion** in 2014. Available at: <http://www.internetlivestats.com/internet-users/>. Accessed on: 27.03.17. Not to mention, of course, the use of some sort of telephone connectivity and e-banking transactions.

340 CASTELLS, M. **The Internet Galaxy**: **Reflections on the Internet, Business, and Society**. Oxford, 2003.

341 SCHILLER, J. **Mobile Communications.** Pearson/Addison-Wesley Publisher, 2007.

342 BARON, N. S. **Always On: Language in an Online and Mobile World.** Oxford, 2008.

343 JENKINS, H. **Convergence Culture: Where Old and New Media Collide.** New York: New York University Press, 2006.

Information and Communication Sciences have, consequently, become an interdisciplinary field mainly devoted to find solutions for effective information exchange models, including the safe management of its registries and data analysis. This happens within broader social contexts (i.e., involving interacting individuals at some point or another), whether such communications are institutional or personal in scope, and according to their specific ranges and necessities. The evolution on this field is inexorably linked to the developments and transformations of the ICT industry, given that the fast changes and capabilities of its tools have culminated on our becoming what is now called a 'global information society'. Such context encompasses interacting agents worldwide, including people from very different backgrounds, values, and interests. The effects and consequences of such tools end up reverberating throughout a variety of social dimensions and aspects, reaching far beyond the mere frontiers and requirements of its specifications and anticipated domains.

In a nutshell, the Internet and the worldwide diffusion of digital media (with all its powerful tools and protocols) are altering our communication dynamics to a huge extent forever. This is also due to a new revolutionary form of interaction that Manuel Castells (2009)[344] calls 'mass-self-communication', which has become not only possible with the Internet but also much more feasible. Castells has defined it in the following way:

> a new form of communication characterized by the capacity of sending messages from many to many, in real time or particular chosen time, and with the possibility of using not only point-to-point communication, but also narrowcasting, broadcasting, streaming, all depending on the purpose and characteristics of the intended communication practice exercised by interlocutors.[345]

He also observes that, to some extent, a significant amount of this practice may be getting closer to 'electronic autism' than indeed to 'actual communication' more broadly. On the other hand, anything posted on the Internet, despite the initial intention of its author, becomes susceptible of being reprocessed in unexpected ways, within a wider (even globalized) communication community[346]. Social-networking sites such as MySpace, WhatsApp, Facebook, YouTube, and other user-generated

344 CASTELLS, Manuel. **Review on Communication Power**. Oxford University Press, 2009. (also appearing in **Communications, The European Journal of Communication**, 2010, p. 571, ISBN 978-0-19-956-701-1).

345 CASTELLS, Manuel. **Review on Communication Power**. Oxford University Press, 2009. p.55

346 Recall, e.g., the case of the anti-Islam video, available at: <https://m.youtube.com/watch?v=7TLtWBsWSlY>, accessed on: 27 mar. 2017, that spread very quickly all over the world through YouTube, as well as the charges published by the magazine Charlie Hebdo, which arose violent retaliations throughout the world.

content web sites now also constitute means of 'mass communication', much more dynamic and interactive than the way traditional media typically handled mass consumption. Let us not forget that the ways in which such interests are negotiated in the current digital context may bring significant implications for a person's self-determination, integrity, safety (especially for victims of crimes, e.g., of domestic violence), medical and financial reputation, opportunities for free political deliberation, dissent, activism, access to employment opportunities, identity protection from fraud, among other forms of abuse and manipulation.[347]

Digitized products and wireless communication, including games, music, images and news shared online, as well as instant messaging and social media tools, now cover a large range of human (inter)activities, from personal support networks to professional tasks and political mobilization. And one of the key features of wireless communication is not just mobility, but also the possibility of 'perpetual connectivity' (i.e., being always online), which raises yet a whole new set of ethical questions and challenges, given its proneness to abuses.[348] One is even entitled to say that the grid of electronic communication and digitized information now encompasses a good amount of what people do, wherever and whenever they do it, in a daily basis, hence its increasing importance and wide range of concerns.[349]

Among other things, such issues touch at the very intersection of State, private sector, and civil society action, especially regarding some democratic rights of citizens. This is due to the fact that our interactions are increasingly mediated through networks and platforms created, maintained, and operated by ICT companies as well as monitored by governmental agencies. The activities of the private sector now have an outsized impact on the freedom of expression and privacy of millions of users, given their role as gatekeepers of the global exchange of information and ideas[350].

About the requirement of 'consent' with the terms of use for services and applications in the Internet, we can find for example: "Consent is related to the concept of informational self-determination. The autonomy of the data subject is both a precondition and a consequence of consent: it gives the data subject

---

347 CASTELLS, M. **Review on Communication Power**. Oxford University Press, 2009 (also appearing in **Communications, The European Journal of Communication**, 2010, p. 571, ISBN 978-0-19-956-701-1).

348 CASTELLS, *Op.Cit*.

349 Please also refer to notes 6 and 7 above.

350 The European Union has thus recently issued a new directive evoking that : "Accordingly, the Directive has not kept pace with technological developments, resulting in a void of protection of communications conveyed through new services". Available at: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>. Accessed on 22.03.17.

influence over the processing of data. However, as explored in the next chapter, this principle has limits, and there are cases where the data subject is not in a position to take a real decision. The data controller may want to use the data subject's consent as a means of transferring his liability to the individual." [351]

Thus, while the rapid growth in size and power of the ICT industry has led to unprecedented opportunities for larger and faster access to information and communication, it has also triggered new forms of control and abuses that may threaten the very existence of a free and open Internet. This includes, of course, the possibility of State control and censorship towards a 'surveillance society', as the revelations by Mr. Snowden have shown us quite explicitly.[352] Also, as Jenkins has pointed out (citing Sola Pool's pioneering work: 1983), the so-called 'convergence of modes' is blurring even further the lines between regular dual connection (such as 'p2p' communication) and broader communication (such as 'one-to-all' connectivity), thus redesigning the whole communication landscape given that: "a single physical means – be it wires, cables or airways – may carry services that in the past were provided in separate ways."[353] Conversely, a service before provided by any one particular medium – be it broadcasting, the press, or telephony – can now be provided in much more interactive ways. The unilateral relationship that used to exist between the medium and its users is increasingly eroding. These are structural transformations that have brought a wide range of consequences to the way people handle information now and in the future.[354] Thus, telecommunication, broadcasting, and computer networks

351 Available at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Accessed on: 22.03.17. On the other hand, the following is also reasonably argued: "Typically, individuals cannot use a service unless they agree to the terms of use, which, in addition to being complex or legalistic, frequently present a 'take it or leave it' approach. Under such an approach the user must agree to provide personal data for all of the purposes the organization represents – even if some are not directly related to the service – in order to access the service. This substantially limits the ability of the individual to protect their personal data by giving meaningful consent. Generally, the emphasis on consent based on overly complex privacy policies that provide few real options and few limitations on collection and use diminish the effectiveness of privacy protections that are intended to support the individual's role in controlling his or her own personal data." Extracted from OECD Privacy Framework 2013. Available at: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Accessed on 22.03.17.

352 MACASKILL, Ewen. Edward Snowden, NSA files source: 'If they want to get you, in time they will'. **THE GUARDIAN**. Available at: <https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why>. Accessed on 22.03.17. "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State" (by Glenn Greenwald, 2015).

353 JENKINS, *Op. Cit.,* p.10.

354 COWHEY, Peter and ARONSON, Jonathan. **Transforming Global Information and Communication Markets—The Political Economy of Innovation.** Cambridge: MIT Press, 2009.

have converged on the basis of digital networking, with its new data transmission and storage technologies, developing at a frenetic speed, particularly optic fiber, satellite communication and, more recently, the clouds.[355]

A new "world ecology"

Like it or not, we are all increasingly cosmopolitans, citizens of the world, not simply citizens of a given nation.

Charles Ess

The above remarks seem to suggest indeed the need for a more holistic approach to digital media, as it's well prompted by Luciano Floridi. [356] Floridi suggests, among other things, that we overcome once and for all the outdated distinction between 'virtual' and 'real', as the former is increasingly becoming part of (thus, as real as) a good amount of our daily interactions and transactions (both personal and professional)[357], into a much more complex and dynamic whole which he termed 'infosphere'.

He also offers an interesting overall view of the many senses that information came to assume, ranging from 'raw-data' (be it mathematical, physical, economic, statistical, biological, etc.), to more elaborate (cross-referential) systems for management, interpretation, and text analysis. Accordingly, we find ourselves now at an unprecedented condition as 'inforgs' (i.e., informational organisms), whose identity and integrity are also shaped by the very information made available and handled in such enlarged world ecology.[358] This includes our interactions and dependence on smart machines, working with and for us through ever more complex and powerful algorithms.

---

355 See, e.g.: LEADERS: *Cloud Computing. The sky's limit.* **THE ECONOMIST**. Published on 17.10.15. Available at:

<http://www.economist.com/news/leaders/21674714-shifting-computer-power-cloud-brings-many-benefitsbut-dont-ignore-risks-skys-limit?cid1=cust/ednew/n/n/n/20151015n/owned/n/n/nwl/n/n/NA/email>. Accessed on 22.03.17.

356 FLORIDI, Luciano. **The Cambridge Handbook of Information and Computer Ethics**. Cambridge, 2010.

357 Recent advances on the so-called Internet of Things (IoT) and artificial reality (including the new game fever of 'PokemonGo') have been increasingly contributing to make such a line even finer.

358 FLORIDI, Luciano. **Information**. Oxford. 2011. Floridi coined the terms 'infosphere' and 'inforgs', both inspired by Alan Turing's groundbreaking ideas on computation.

All this results from the addition of further semantic layers of meanings being allowed, for example, by 'big-data' and the use of 'cloud' systems.[359]

Charles Ess also indicates some important implications resulting from such a multi-informational medium, which is being pretty fast re-engineered.[360] He alerts us to be careful not to continue just perpetuating exclusion, now at an incredible pace, thus preparing further ground for enormous 'digital slums'. Unless we manage not only to spread such powerful tools and resources in a more inclusive way (allowing people everywhere to have access to the Internet and mobile devices), but also to better educate users on handling these tools more carefully. This also includes passing relevant requirements to better regulate such media resources and the companies and institutions that provide and administer their services.

Both Ess[361] and Floridi[362], as well as other concerned researchers (Castells 2009, Baker 2005, Lever 2012), have thus been calling our attention about the complex cultural processes resulting from such 'multilayered transformation of communication'.[363] A communication revolution that now finds itself at the very intersection between sometimes contradictory (though not necessarily incompatible) main trends, namely: the development of a 'global plural culture' (or multiple identity cultures), on the one hand; and, on the other, the simultaneous rise of 'individualism' vs. 'communalism' as two opposing, yet equally powerful, cultural patterns that may characterize democratic societies.[364]

---

359 See also Floridi's most recent presentation, entitled: "Ethics in the Age of Information" for the Oxford Internet Institute. Available at: <https://youtu.be/lLH70qkROWQ>. Accessed on 27.03.17.

360 ESS, C. **Digital Media Ethics**. Polity, 2009.

361 *Ibid.*

362 FLORIDI, L. *Op.Cit.* (2010, 2011)

363 CASTELLS, M. **Review on Communication Power**. Oxford University Press, 2009 (also appearing in **Communications, The European Journal of Communication**, 2010, p. 571, ISBN 978-0-19-956-701-1); BAKER, L.C. **Free Internet Access, Digital Divide, and Health Information**. Jstor Publisher, 2005; LEVER, A. **On Privacy.** Routledge, 2012.

364 Recall, as well, some interesting aspects already highlighted at "Du papyrus à l'hypertexte" (La Découverte, 1999), concerning narrow-streaming and the concentration of people into micro-communities. In talking about micro-communities, another point worth mentioning is the current plan by Google think tank (former Google Ideas, now Jigsaw) to offer a counter movement for stopping aspiring ISIS recruits. See e.g.: GREENBERG, Andy. Google's clever plan to stop arising ISIS recruits. **WIRED**. Published on 09 jul. 2016. Available at: <https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/>. Accessed on 22.03.2017.

At the core of this situation is the formation of 'globalized' media businesses, whose networks have been made possible mainly by public policies and institutional changes put in place, characterized by liberalization, privatization, and regulated 'deregulation', both at national and international levels. In such a context, Castells compiles the main transformations that have been taking place in the last decades in the following way:[365]

- *widespread commercialization of media resources all over the world;*
- *globalization and concentration of media business through conglomerations and networking merges;*
- *the segmentation, customization, and diversification of media markets, with an emphasis on the cultural identification of the audience;*
- *the formation of multimedia business groups that reach out to the Internet and all forms of digital communication;*
- *and increasing business convergence between telecommunication, software and hardware companies.*[366]

Such transformations have been happening in the many dimensions of the communication process. Together they form what has been referred to as a 'communication revolution' in this century. It can be characterized as the 'inflection point' identified by the emergence of new media through the increasingly broader interaction of technological and communication changes. This is all based on the digitization of information, computer networking, advanced software, diffusion of enhanced broadband transmission capacity (local/global via wireless) and increasing Internet access to as many people as possible. [367]

Various dimensions of the transformations, with the popularization of digital media, have thus converged into a system where no single transformation can be understood without the others. Each component of such landscape, underlying the evolution of this 'multimodal communication system', can be said to represent an interactive net of social relationships that ultimately are also expressions of 'power relations'. This becomes most apparent in the persisting

365 CASTELLS, *Op. Cit.*, p. 56.

366 Without being necessarily implied any order of causality by this sequence of presentation in his list.

367 CASTELLS, M. **Networks of Outrage and Hope. Social Movements in the Internet Age.** Cambridge: Polity Press, 2012. Let us also observe that about 97% of the global available information has been digitized, which moves an e-market of about U$1,5 trillion in developed countries alone (source: *E-marketer*, 2012 - 2014).

'digital divides' between and within countries, depending on their consumer power and their level of communication infrastructures.

As users appropriate themselves of these new ways and tools to communicate, they are now able to build their own systems of 'mass-self-communication' via SMS, blogs, podcasts, wikis, etc., through which file-sharing and p2p networks make the circulation, encryption, and reformatting of any digitized content possible much more reliably.[368] If we consider just the 'blogosphere', with about 60 million blogs updated per day,[369] the Web can already be said to constitute a multilingual and international communication space with no historical precedents.[370] However, all around the world, most blogs are usually personal in nature, with about 52% of bloggers declaring that they blog 'mostly for themselves' and with only 11% being about politics (Lenhart & Fox 2006: Pew Internet Project survey).

Now, some of us may still recall the preoccupations with the turning of the millennium for computer systems and operations, due to the change of the year 1999 to 2000 (a problem that was referred to as the 'Y2K bug'). [371] This seemed to present a huge problem, given that many (if not most) algorithms had been written without accounting for such change in the first two digits of the year. This problem had been postponed for decades by developers and managers due to mere commodity or more immediate financial concerns. The typical rationale was that programmers or managers were no longer so sure about what their programs contained or how they were structured (sometimes in billions of lines of accumulated programming), and the cost of documenting or redoing it all from scratch would be enormous.

The Y2K problem thus serves to highlight its main cause, that is: the so-called Myth of Amoral Computing and Information Technology (MACIT). It can come up in many ways, but it basically consists of disclaiming responsibility (or postponing it as much as possible) with respect to Information Technology and Systems. Therefore, it is no longer clear at what point we can begin to hold people responsible for what is in such programs and for the products they sell

368 CASTELLS, *Op.Cit.*, 2009.

369 Documented by Baker, back in 2008, being certainly much higher now.

370 A fact that also brings us the power to find interesting ways for fighting against hunger and diseases where it's needed, see e.g.: EVANS, Bryce. Using Big Data to Achieve Food Security. *In:* BUNNIK, Anno; CAWLEY, Anthony; MULQUEEN, Michael; ZWITTER, Andrej. **Big Data Challenges: Society, Security, Innovation and Ethics**. Palgrave Macmillan, 2016.

371 For more details about the Y2K Bug and the AMCIT, please refer to: DE GEORGE, Richard. **The Ethics of Information Technology and Business in the series Foundations of Business Ethics**. Blackwell Publishing, 2003.

or use involving them. The MACIT mainly springs from the fact that moral responsibility requires not only causal responsibility (i.e., causal connection with a sequence of events in question), but also involves knowledge of what one does and the consent for doing it.

If any of those conditions are not met, there is then a tendency to mitigate responsibility to a greater or lesser extent, according to 'excusing conditions' offered for not meeting such requirements. Most often the favored disclaimer is ignorance or lack of transparency (i.e. the opacity of programs). But, of course, past century programmers knew the year 2000 was coming one day, and many foresaw the problem, but it was considerably and persistently ignored anyway. As it turned out, we did not have any major disasters caused by the Y2K bug, after all, but not because it did not present a real threat.

Actually, its avoidance was possible thanks to the stepping up of accountable administrators and technical managers who came together and finally took the necessary steps to prevent major crashes with the arrival of the new century. As Richard De George well summarizes it: [372]

> The delayed response to the Y2K problem indicated that management for the most part still tends to think of Information Technology and Systems as something that remains a service function for their corporations, off in a back set of rooms, instead of being prominently in the center of it, The disconnection between corporate leaders and their technical divisions is the clearest indication that firms have not moved consciously into the Information Age. They are backing into it or being pulled by a technology they do not completely understand, even as they become more and more dependent on it. Yet if we are truly in a developing Information Age, then Information Technology and Systems need to be at the center of things, and management has to both understand it and take responsibility for it.

The point can accordingly be generalized beyond the Y2K problem, as those who produce or incorporate programs into products are responsible for those products and programs, just as they are responsible for other products or goods they sell. Yet, as already noted with respect to the AMCIT, there is a tendency for companies to disown responsibility for computer malfunctions or breakdowns, and for commercial software producers to issue disclaimers with their products, claiming for example that by downloading or opening the product, the user relieves the company of all responsibility. That this is

372 DE GEORGE, Richard. **The Ethics of Information Technology and Business**. Blackwell Publishing, 2003, p.13.

usually accepted without much complaint by the public is, at least, puzzling and probably a symptom of our increasing dependence upon them.

Hence, further concerns arise from this new 'world ecology' (*infosphere*), on what regards not only data protection (given the Big Data wave), but also about 'net neutrality', which became another important controversial issue at the moment. Net neutrality basically refers to the indiscriminate ('isonomic') treatment of content packages by service providers; such treatment is important, for example, to avoid that some users be allowed unequal bandwidth in proportion of their deemed 'importance' as clients, based on the package they can afford.[373]

The way governments and companies handle users' communications over the Internet (and digital media governance in general) became increasingly relevant also to protect other important democratic rights, such as freedom of expression and privacy. As Sérgio Branco well puts it: "In short, we could say that if "all humans are equal before the law," the correspondent parallel for the Internet would be, "all data is equal before the Web." [374] A higher alert and awareness about such rights finally came after Edward Snowden's staggering revelations (2013) concerning the surveillance practices of the American National Security Agency (NSA).[375]

Troubling concerns following Mr. Snowden's revelations have been raised about the very access and control by governments over citizens' personal information (mainly with respect to the FIVE EYES group: United Kingdom, United States, Australia, New Zealand, and Canada). Consequently, the landscape about privacy has become so intricate that some people may be led to conclude that is now hardly

---

373 Tim Wu (who coined the term) defines it as: "[T]he principle that Internet service providers and governments regulating the Internet should treat all data on the Internet the same, not discriminating or charging differentially by user, content, website, platform, application, type of attached equipment, or mode of communication." Extracted from a recent article about net neutrality by Prof. Sérgio Branco (ITS Rio): BRANCO, Sérgio. Net Neutrality: You love it, even if you don't really know what it is. **DROITDU.NET**. Available at: <http://droitdu.net/2016/11/net-neutrality-you-love-it-if-you-dont-really-know-what-is-is/>. Accessed on: 27.03.17.

374 *Ibid.*

375 For some organizations concerned with such issues, see e.g. <http://performance.cira.ca>, <https://openmedia.org/en/ca>, <https://www.eff.org>, <http://www.onlinecompliancepanel.com>, <https://cjfe.org>, accessed on 27.03.17. Also, in Brazil, the Institute for Technology and Society of Rio de Janeiro (ITS-Rio) was created, available at: <http://itsrio.org/en>. Accessed on 27.03.17. It is composed by the main collaborators to the text for Brazil's Internet Civil Code ('Marco Civil da Internet') as a result of the engagement among general citizens, legal and IT experts, and politicians, under the supervision by the Brazilian Ministry of Communications. (See also: <http://www.ebc.com.br/tecnologia/2014/03/veja-o-texto-aprovado-na-camara-sobre-marco-civil-da-internet> Accessed on: 23.03.17. And: <http://jornalggn.com.br/noticia/brasil-tem-6º-orcamento-mais-transparente-do-mundo-diz-organizacao>. Accessed on: 23.03.17.

possible to continue expecting a considerable amount of privacy at all.[376] On the other hand, though agreeing that the Internet might indeed become the ultimate mass surveillance technology, others may argue that technology *per se* does not necessarily imply such extrapolations, which can still be prevented, provided that we regulate the Internet more strictly.[377] About the limits of privacy, more generally, Annabelle Lever sensibly puts the matter this way:[378]

> If the purposes of privacy protection are to support our agency, bodily integrity and security, then the limits of privacy would seem to be set by those things which threaten or actually violate our agency, bodily integrity and security. So understood, the reasons of controversy about privacy become quite clear… In modern constitutional democracies, unlike feudal regimes, we do not generally need privacy in order to avoid the worst forms of violence, but to ensure that we are able to pursue our own ideas of what makes life worth living in the face of different opinions, beliefs and tastes of other people.

With that said, the current state of affairs on the issue shows, however, that we still do not have much of a consensus on exactly what the 'right to privacy' is, on what it is supposed to protect or prohibit, nor on what its justification is for supplying a principled basis to legislation or social policies. This is probably due to the fact that the notion of privacy seems to be very relative to each particular culture. Claims to privacy are interpreted and applied in different societies depending on their cultural expectations, history, and accepted practices. Or, yet, as De George well puts it: "Different societies have different views about what constitutes privacy, about how important it is, and about how much it needs or deserves protection."[379] That philosophers, legislators, and judges still largely disagree on the specifics about the right to privacy also reflects to a considerable extent what we find in popular views and the media.

---

376 MORGAN, Jacob. Privacy Is Completely and Utterly Dead, and We Killed It. **FORBES**. Available at: <http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#46c9c18fdfbd>. Accessed on: 23.03.17.

377 The European Union through its Parliament has leaned towards such an approach, especially after Mr. Snowden's revelations, having more recently adopted a new framework called "Privacy Shield" for dealing with American companies. On this subject, see e.g. **European Commission – Press Release**. Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions. Available at: <http://europa.eu/rapid/press-release_IP-17-16_en.htm>. Accessed on: 23.03.17.

378 LEVER, A. **On Privacy**. Routledge. 2012, p.53.

379 DE GEORGE, Richard. **The Ethics of Information Technology and Business**. Blackwell Publishing, 2003, p.40.

This owes to the fact that the notion of privacy is to a certain degree relative to one's own culture, given that what is right or wrong, good or bad, with respect to privacy is in part culturally determined. That is to say that how privacy claims are interpreted and applied in different societies also depends on cultural expectations, history, accepted practices, existing laws, among other factors, whence derives its high complexity and wide space for controversy. In other words, as De George emphasizes: "Different societies have different views about what constitutes privacy, about how important it is, and about how much it needs or deserves protection."[380] Thus, to determine more consistently which practices do or do not violate privacy, so as to provide a reasonable basis for businesses and for possible legislation and social policy on this issue, it is of crucial importance first to get some clearer notion of the concept of privacy, of why it is important to protect, as well as a determination about the current status of any claimed 'right to privacy'. A reasonable place to begin with might be the existing legislations about it.

We may start, for example, by noting that the Universal Declaration of Human Rights in its Article 12 states the following: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection by the law against such interferences or attacks[381]." As De George sensibly claims, this may well be taken as an affirmation also of the human 'right to privacy', among other rights, which could serve as an international stand for it, no matter what medium of interaction one is using. Yet, given existing disagreements and differences of approach about both the 'concept of privacy' and its reaches and protection rights, especially now with the popularization of the Internet, we find that legislations many times provide rather unclear characterizations of privacy (not to mention of the right to have it protected), leaving wide room for ambiguous interpretations and abuses.

Thus, the creator of the World Wide Web (Sir. Tim Berners-Lee) also reasonably defends the need of a separate 'Universal Declaration' (or Magna Carta) concerning human rights such as 'the right to privacy', now more specifically directed to Internet issues. It would have to state, e.g., more precise

380 *Ibid.*

381 BROWNLIE, I. **Basic Documents on Human Rights**. 2. ed. Oxford: Clarendon Press. 1981, p. 253.

recommendations and requirements for the treatment of users' personal data by companies and governments who have access to them.[382]

Now, no matter which approach one may choose about it, that is: whether favoring broader access to personal information and free exploration of Big Data (in the name of business expansion and innovation), or rather defending stronger restrictions (in the name of data protection); it is important to keep in mind that governance for the Internet is ultimately supposed to reflect and manage the continuing power struggles among competing interests of different stakeholders in societies. And this is so that, hopefully, we come to find a middle ground (through legislation and diplomatic treaties and agreements) for conciliating as many of those sides and concerns as possible; and this, without compromising hard conquered universal human rights either. [383]

When it comes to democratic environments, it may be easier to handle, as long as authorities and the general public can fast overcome the misrepresentation that privacy protection is unimportant and/or that the digital realm is not 'really' affecting their lives that much. As Mr. Snowden has relentlessly warned us alongside his revelations concerning the threat of mass surveillance through digital media: "Arguing that you don't care about the right to privacy because you have nothing to hide, is no different than saying you don't care about free speech because you have nothing to say." [384]

382 On this respect, one finds that the American and European approaches differ considerably, and would need to be reconciled to a big extent. See, e.g.: Get off my cloud. **THE ECONOMIST**. Available at: <http://www.economist.com/news/international/21671982-european-court-ruling-presages-transatlantic-battle-over-data-protection-and>. Accessed on: 22.03.17.

383 Consider, e.g, this point:"Big Data and mass surveillance are difficult to reconcile with the mandate of the European Union under Article 16 TFEU in the area of privacy and data protection". HIJMANS, H. **The European Union as Guardian of Internet Privacy**. Springer International Publishing, 2016. For more interesting points with respect to the Big Data wave and the problems posed for data protection, one may also refer to the informative chapter on the subject at the present book, written (in Portuguese) by Rodrigo Dias de Pinho Gomes: "Desafios à privacidade: big data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais."

384 Extracted from an informative discussion about privacy (animated by Nuala Nualo O'Connor) among Edward Snowden, Glenn Greenwald and Noam Chomsky. Available at: <https://www.youtube.com/watch?v=IOksJKfapVM>. Accessed on 27.03.17. Also, refer to Mr. Snowden's TedTalk presentation available at: <https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet>. Accessed on: 27.03.17.

Conclusive remarks

As we have seen by the above, ranging from culturally diverse television networks to the World Wide Web, digital media now encompasses the handling and incredible reach of packages of communication protocols. These can help us work towards bridging cultural and inequality gaps and/or refrain from doing so. It all depends on how we, citizens of democratic societies, choose to manage our tricky situation as 'inforgs' in this enlarged *infosphere* now surrounding us[385]. If the path chosen is to nourish further fragmentation of people into 'cultural islands', by creating digital divides (people, communities, and countries with vs. without access), then we may be inevitably bringing undesirable trenches of resistance to the very 'web democratization' envisioned by its creator, Sir. Tim Berners-Lee[386].

The growing interest of corporate media in E-business and digital communication is just one symptom of how significant its influence has increasingly become for society in general. Castells points out that Internet-based forms of communication constitute 'mass' communication because they reach a potentially enlarged audience (through p2p and social networks); on the other hand , it is multimodal and self-generated in content, self-directed in emission, and self-selected in reception by 'many-to-many' as well.[387]

This is not only a new communication realm but also, ultimately, "a new communication medium whose backbone is made of computer networks, whose language is digital, and whose senders are more globally distributed and interactive." [388] A medium that has at least the potential capabilities to allow for unlimited diversity, autonomous production, and greater collaboration, resulting from a more dynamic and direct communication flow towards enlarged meaning construction in the public minds. This new setting, seen from such a perspective, also sounds ideal for democratic institutions and education to flourish in more distributive and participative ways.

---

385 As mentioned above, both of these terms were coined by Floridi (FLORIDI, Luciano. **The Cambridge Handbook of Information and Computer Ethics**. Cambridge, 2010) inspired by Alan Turing's seminal work on computation.

386 Let us recall, e.g., that in so-called developed countries people now buy packages from communication service providers that already include Internet access, not just phone line or cable TV, as before. In Canada, e.g., packages should now include a basic acceptable limit for content and speed access, thanks to concerns about 'net neutrality' that recently made it to be guaranteed by law to all Canadians: Available at: <http://www.crtc.gc.ca/eng/internet/performance.htm>. Accessed on 23.03.17.

387 CASTELLS, *Op. Cit.*, 2009.

388 *Ibid.*, p. 70.

This communication revolution, with its highly promising autonomous character and technological innovations, could only take place by being shaped and promoted by governments that are now "largely influenced by business strategies for profit-making and market expansion." [389] This amounts, of course, to a whole range of ethical concerns about the legitimacy of such 'global' communication expansion vs. exploitation and, consequently, of appropriate contexts for genuine (ethical, free, open) discussion and collaboration, given the potential for corruption and for manipulation of the access to information.

It may, after all, become just another powerful form of control just to favor a few 'beneficiaries', instead of allowing for a broader and democratic access to most or, ideally, all citizens (at least, within democratic environments). In other words, as we are reminded by the SAS Analytics public campaign (2015): "technology is only as good as the people who drive it." But, if well managed, a broader access to such media can certainly empower social actors and individual citizens to further advance their projects, defend their interests, and assert their values, while they also become increasingly aware of the crucial role that these media can play in their culture, education, and politics within contemporary societies.

The Myth of Amoral Computing and Information Technology (MACIT) points particularly to the tendency of equating whatever is expected of anyone, in any field, also to be applied for computing or information systems as required by law. If it is legal, it is permissible, and the reverse. But this view is yet too simplistic and fails to capture the reality of the relation between law and ethics, especially when dealing with complex issues arising by the fast spreading and reach of digital media. In the case of computer related and mediated activities, part of the task, before even passing legislation, is coming to prior conclusion (as broad a consensus as possible) about the ethicality of new practices as they arise. After all, good legal practice in democratic environments is one that allows people freedom of activity to the broadest extent possible, compatible with a 'freedom for all'. It only criminalizes activities when it becomes harmful to people's integrity in some way and, thus, unethical. The extent to which it is unethical and harmful is not decided by looking at the law, but the other way around. Law looks at ethics, because there is generally a lag of law behind ethical judgments and decisions, that is: we can and do consider actions or practices unethical before they are made illegal (cases to mention are slavery, sexual harassment, religious and racial discrimination, just to name a few).

389 *Ibid.*, p. 71.

Now, if we are indeed to have any reasonable aspiration for constructing a responsible 'global electronic metropolis' (as it is suggested by ongoing fast developments and power at the Silicon Valley empire), it's urgently pressing upon us the adoption of a globally accepted Magna Carta for the Internet, as Sir. Tim Berners-Lee has been insisting upon.[390] One that could serve at least as referential guidelines for discussion and further analysis to the different societies and governments, as they each attempt to best apply them to their particular contexts and concerns.

The European Union as well as the continental Republic of Brazil, where social media has spread at an incredible pace and extension, have both been pioneers on this struggle. The European Parliament has recently released its new directives about privacy and data protection,[391] and Brazil has adopted its first Bill of Rights for the Internet (Marco Civil da Internet) in 2014.[392] The text for the Brazilian law was openly discussed among specialists, academics, and the public, through a platform particularly conceived for that end.[393] No wonder, it took about eight years for the text to be finally ready and sanctioned by Brazil's former president Dilma Rousseff. Nonetheless, polemic questions about data protection and net neutrality continue to make the news in the country, as some guarantees are still lacking, not-followed, or perhaps intended to be overcome by the new interim government following Ms. Rousseff's controversial impeachment in 2016: à surveiller! [394]

---

390 BERNERS-LEE, Tim. The Wider World Web. **THE ECONOMIST**. Available at: <http://www.theworldin.com/article/10648/wider-world-web>. Accessed on: 23.03.17.

391 Refer to: European Commission – Press Release. Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions. Available at: < http://europa.eu/rapid/press-release_IP-17-16_en.htm>. Accessed on: 27.03.17.

392 PL 12.965 / 2014 – Marco Civil da Internet. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Accessed on: 27.03.17.

393 Refer to: Ascom do MCTI. Governo lança plataformas públicas para regulamentação do Marco Civil da Internet. Published on 28.01.15. Available at: <http://www.mcti.gov.br/visualizar/-/asset_publisher/jIPU0I5RgRmq/content/governo-lanca-plataformas-publicas-para-regulamentacao-do-marco-civil-da-internet>. Accessed on: 23.03.17.

394 See, e.g.: "Marco Civil da Internet: entidades pedem que Michel Temer não altere decreto." **CANALTECH**. Published on: 07.06.16. Available at: **<**https://canaltech.com.br/noticia/internet/marco-civil-da-internet-entidades-pedem-que-michel-temer-nao-altere-decreto-68881/>. Accessed on 23.03.17; Available at: RODRIGUES, Fernando. "Banda larga fixa terá limite de dados até o fim de 2017, diz ministro." **PODER 360**. Published on 12.01.17. Available at: <http://www.poder360.com.br/governo/banda-larga-fixa-tera-limite-de-dados-ate-o-fim-de-2017-diz-ministro/>. Accessed on: 23.03.17.

Direito ao Esquecimento na Internet: Entre a Censura Digital e a Busca pela Verdade na Sociedade Conectada

Lívia Helayel[395]

Introdução

Na chamada Era do Conhecimento e Informação, a corrida pelo desenvolvimento tecnológico nos fez mudar drasticamente a maneira como buscamos e armazenamos dados e informações em geral. A grande consequência disso é que acontecimentos privados se tornam públicos em poucos *clicks*. Assim, surge como conceito o chamado direito ao esquecimento como mecanismo de defesa do indivíduo contra a memória permanente da internet.

O debate sobre esse tema foi ampliado quando o Tribunal de Justiça da União Europeia obrigou a empresa Google, no ano de 2014, a excluir de seus resultados – desindexar – referências a *websites* que trouxessem notícias ou informações "inexatas", "inadequadas", "irrelevantes" ou "excessivas", de parte interessada, mediante requerimento. Essa decisão se tornou o *leading case* envolvendo o direito ao esquecimento na internet, sendo discutido e utilizado no mundo inteiro.

Como não poderia deixar de ser, a referida decisão europeia foi, e ainda é, amplamente discutida no Brasil, mesmo que o Superior Tribunal de Justiça (STJ), no Recurso Especial nº 1.593.873, tenha firmado entendimento de que seus preceitos não se acomodam no ordenamento jurídico nacional, uma vez que se assim fosse, o Google exerceria papel de "censor digital". Esse termo foi usado pela Relatora do caso em questão, Ministra Nancy Andrighi, para argumentar que se o direito ao esquecimento na internet alcançasse os provedores de aplicação de

395 Pós-graduada em Propriedade Intelectual pela PUC-Rio, Lívia Helayel atua em escritório tradicional e de referência nessa área, tendo ainda integrado o Grupo de Pesquisa do ITS-Rio em Privacidade na Internet, durante o ano de 2016. Dedica sua atividade profissional a assuntos envolvendo Marcas, Concorrência Desleal, Direito Autoral e Direito de Personalidade, tendo como clientes grandes empresas estrangeiras do setor tecnológico/digital e do entretenimento, o que motiva seu constante aprimoramento nesses assuntos.

busca - que são meros mecanismos de pesquisa de conteúdo que existe na rede -, a eles se estaria conferindo atribuição de censor em meio digital.

Apesar da efetiva aplicação de um "direito a ser esquecido" ter sempre permeado diversos institutos e princípios jurídicos, tal fundamento reaparece com novas nuances em uma sociedade altamente conectada e preocupada com o fluxo de informações e dados pessoais dispostos na internet que, aparentemente, nada esquece[396] - e em consequência, nós também não. Dessa forma, necessário se faz distinguir o direito ao esquecimento, como garantia de não ser punido novamente por fatos já ultrapassados, do direito ao esquecimento na internet, ou direito de desindexação, apagamento ou remoção de conteúdo *online*.

Tratar-se-á, portanto, exclusivamente do direito ao esquecimento em ambiente virtual, indagando se esse conceito se presta à proteção da privacidade na internet ou a exercer censura *sui generis*. Adicionalmente, intentou-se defender que, observando a forma como a sociedade busca informação em tempos de Modernidade Líquida na qual, conforme explica Zygmunt Bauman, "livrar-se das coisas tem prioridade sobre adquiri-las", a melhor defesa contra a informação que se pretende "esquecer" é a disponibilização de mais informação.

Ainda sobre Google Spain *vs.* Costeja

O direito a ser esquecido na internet foi reconhecido em 2014, pela União Europeia, em um caso ainda muito debatido até hoje: Google Spain vs. Costeja. Mario Costeja González, descontente que uma pesquisa de seu nome no provedor de busca da Google resultava em links de notícias antigas sobre dívidas que não mais tinha, denunciou o ocorrido à Agência de Proteção de Dados Espanhola, alegando que a indicação a esses links violava o seu direito à privacidade. O caso chegou ao Tribunal de Justiça da União Europeia, que decidiu em favor do indivíduo.

Conforme mencionado anteriormente, o Tribunal de Justiça da União Europeia decidiu em favor de Costeja em seu pedido contra a Google, esboçando o que se tornou o *leading case*, referência mundial, envolvendo direito ao esquecimento na internet, que para fins de clareza de entendimento também é chamado de direito à desindexação de resultados em provedor de aplicação de busca.

396 MAYER-SCHONBERGER, Viktor. **Delete: the virtue of forgetting in the digital era**. Princeton: Princeton University Press, 2009. p. 2. "Today, with the help of widespread technology, forgetting has become the exception, and remembering the default".

A partir dessa decisão da Corte Europeia, doutrinadores e pesquisadores do mundo inteiro imediatamente se preocuparam com a possível afronta à liberdade de expressão e comunicação. Esse receio tornou-se ainda maior quando as autoridades francesas de proteção de dados ordenaram que a Google removesse globalmente[397] qualquer referência a sites que pudessem ser acessados na União Europeia, que contrariassem suas diretrizes, ainda que isso pudessem resultar em censura. Não se pretende discutir jurisdição da internet ou a expansão do controle de reguladores estrangeiros sobre o que pode ou não pode constar na internet, mas, de fato, a censura de conteúdo digital em todo o mundo é consequência aparente das regras impostas pela União Europeia.

A decisão no caso concreto se expandiu a todos os usuários e cidadãos europeus, os quais hoje fazem pedidos para a Google de remoção de conteúdos "inexatos" "inadequados", "irrelevantes" ou "excessivos" relacionados a si[398]. Assim, em cumprimento à decisão, a Google oferece a possibilidade do usuário preencher um formulário, requerendo o apagamento da indexação de conteúdo - que nada mais é do que o resultado da pesquisa feita no buscador pelo nome do indivíduo. Posteriormente, a Google, exercendo papel de julgador[399], avalia o caso e decide se na situação de fato caberia a desindexação dos conteúdos resultantes da busca, recebendo um papel secundário de "censor digital"[400].

Há que se constatar que as soluções apresentadas consoantes ao direito ao esquecimento *online* europeu são falhas e podem vir a prejudicar a criação de alternativas conciliatórias, destinadas a resolução ponderada de situações que envolvam o conflito entre direito à privacidade e liberdade de expressão/acesso à in-

397 Google contesta decisão da França sobre "direito global ao esquecimento". **ESTADÃO**. Link. Publicado em: 19 mai. 2016. Disponível em: <http://link.estadao.com.br/noticias/cultura-digital,google-contesta-decisao-da-franca-sobre-direito-global-ao-esquecimento,10000052269>. Acesso em: 11 set. 2016.

398 RODRIGUES, Otávio Luiz Junior. Direito de apagar dados e a decisão do tribunal europeu no caso Google. **CONSULTOR JURÍDICO**. "O Tribunal de Justiça da União Europeia definiu que o direito de oposição será exercitável quando os dados (i) foram inexatos; (ii) inadequados; (iii) impertinentes ou (iv) excessivos. Essa qualificação deverá considerar os seguintes fatores: (a) atualização do tratamento de dados ou (b) conservação dos dados por tempo superior ao necessário, "a menos que a sua conservação se imponha para finalidades históricas, estatísticas ou científicas". Publicado em: 28 mai. 2014. Disponível em: <http://www.conjur.com.br/2014-mai-28/direito-comparado-direito-apagar-dados-decisao-tribunal-europeu-google-espanha>. Acesso em: 10 set. 2016.

399 BRANCO, Sérgio. Nine questions regarding the right to be forgotten, "who should decide in which cases a right to be forgotten is applicable? Private entities, such as Google, or only Courts?" **DROITDU.NET**. Publicado em: 17 nov. 2016. Disponível em: <http://droitdu.net/2016/11/nine-questions-regarding-the-right-to-be-forgotten>. Acesso em: 15 mar. 2017.

400 Termo usado pela Ministra Nancy Andrighi em sede do Recurso Especial (REsp 1.316.921) que se verá adiante.

formação. Afinal, não se verificam critérios objetivos para delimitar o que seriam conteúdos "inexatos" "inadequados", "irrelevantes" ou "excessivos". No Brasil, por exemplo, os direitos à privacidade e à liberdade de expressão são princípios fundamentais, constitucionalmente garantidos. Assim sendo, podemos nos socorrer da ponderação desses princípios, no caso a caso, para decidirmos acerca do direito ao esquecimento[401]. Ao que tudo indica, o STJ tem esse mesmo entendimento.

A leitura do STJ sobre a desindexação de conteúdo

Contrariando a tendência estabelecida pela Corte Europeia no caso Costeja e, em certa medida, contrariando decisões dos Tribunais nacionais sobre o tema[402], a 3ª turma do STJ proveu recurso da Google em caso em que se pediu o direito ao esquecimento direcionado ao provedor de aplicação, em 10 de novembro de 2016, por decisão unânime[403].

O STJ decidiu que a Google não pode ser obrigada a eliminar de seu sistema os resultados derivados da busca de determinado termo ou expressão, pois, assim, exerceria controle prévio de conteúdo publicado na web. Essa decisão assenta o entendimento dado, em momento anterior ao Marco Civil da Internet (Lei 12.965/14), no caso Xuxa *vs* Google em 2012, em que a apresentadora solicitou, dentre outros pedidos, a remoção de links de notícias e imagens que aparecessem ao se buscar o termo "Xuxa pedófila"[404].

Em síntese, o Recurso Especial 1.593.873/SP foi interposto contra Acórdão do Tribunal de São Paulo em favor de S. M. S.[405], que requeria o apagamento de pesquisas realizadas por meio de seu nome, uma vez que poderiam levar a páginas que reproduzissem imagens suas de nudez. A sentença anterior havia extinguido o feito sem análise do mérito, porque considerou a ilegitimidade

401 "Ocorrendo conflito entre direitos fundamentais, o intérprete deve se valer do sobreprincípio da proporcionalidade, realizando a ponderação de valores a fim de eleger o que deve prevalecer no caso concreto". (TJSE. Processo nº 201513600288)

402 AMENDOLA, Gilberto. TJs acatam 1/3 dos recursos por direito ao esquecimento. **ESTADÃO**. Publicado em: 24 jul. 2016. Disponível em: <http://politica.estadao.com.br/noticias/geral,tjs-acatam-13-dos-recursos-por-direito-ao-esquecimento,10000064593>. Acesso em: 10 out. 2016

403 Pedido de direito ao esquecimento não pode ser direcionado ao Google. **MIGALHAS**. Publicado em: 10 nov. 2016. Disponível em: <http://www.migalhas.com.br/Quentes/17,MI248798,51045-Pedido+de+direito+ao+esquecimento+nao+pode+ser+direcionado+ao+Google>. Acesso em: 20 nov. 2016.

404 STJ, REsp 1.316.921 - RJ. Relatora Min. Nancy Andrighi. Consulta realizada em: 15 jan. 2017.

405 A autora da ação originária não foi revelada uma vez que o caso está em segredo de justiça.

passiva da Google, mas o Acórdão do Tribunal de São Paulo deu provimento à apelação interposta por S. M. S., estabelecendo que o conteúdo não seria de interesse público, sendo, portanto, aplicável o direito ao esquecimento em afirmação do preceito constitucional da dignidade da pessoa humana[406].

Em sede do Recurso Especial em questão, a Google sustentou pela impossibilidade do bloqueio das palavras-chaves apontadas que pudessem levar às imagens de nudez de S. M. S., tendo em vista que o Marco Civil da Internet exigiria a indicação do conteúdo infringente por meio de URLs, que permitam a localização clara do material pelo provedor de busca.

Ao examinar o caso, a Ministra Relatora Nancy Andrighi reafirmou os conceitos estabelecidos por ela mesma e confirmados pela Corte Superior no caso Xuxa *vs* Google, de 2012, fazendo ainda as devidas ressalvas acerca do efetivo reconhecimento de um direito ao esquecimento[407] - que não se aplicaria quando se tratasse de provedores de aplicação de busca[408]. Assim, a decisão pelo acolhimento do Agravo Interno do Recurso Especial foi unânime, restabelecendo a decisão do juízo de primeiro grau, que extinguiu o feito sem resolução do mérito por ausência de legitimidade do Google.

Sobre a influência do Marco Civil da Internet na referida decisão, a relatora limitou-se a mencionar que tal lei preencheria parcialmente a ausência legislativa sobre o tema direito ao esquecimento na internet[409]. Indica, por conseguinte, que o artigo 7º, inciso X, do MCI, permite a exclusão de dados pessoais que tiver a própria pessoa fornecido a determinada aplicação de internet. Assim, não tendo

406 STJ, AgInt no REsp 1.593.873 - SP. Relatora Min. Nancy Andrighi. Consulta realizada em: 17 nov. 2016

407 STJ, AgInt no REsp 1.593.873. Relatório e Voto, p. 4-5 : " (...) definiu-se o direito ao esquecimento como 'direito de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores, de natureza criminal, nos quais se envolveu, mas que, posteriormente, fora inocentado'. "Também se assentou que o direito ao esquecimento vigeria no ordenamento pátrio não apenas com fundamento nos princípios gerais do direito, mas também em regras da legislação ordinária.".

408 STJ, AgInt no REsp 1.593.873. Relatório e Voto, p. 11-12 : "O papel dos provedores de pesquisa se restringe à identificação de páginas na Internet onde determinado dado ou informação, ainda que ilícito, estão sendo livremente veiculados. Como afirmado acima, a recorrente não armazena as informações e imagens indicadas pela recorrida, de modo que não há como lhe imputar responsabilidade por elas.". "*(...) [E]*ste Superior Tribunal de Justiça entendeu que os provedores de pesquisa: (i) não respondem pelo conteúdo do resultado das buscas realizadas por seus usuários; (ii) não podem ser obrigados a exercer um controle prévio do conteúdo dos resultados das buscas feitas por cada usuário; e (iii) não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão".

409 STJ, AgInt no REsp 1.593.873. Relatório e Voto, p. 15.

sido a própria autora que forneceu as informações que pretende desindexar, não alcançaria os buscadores (provedores de aplicação de busca) o pedido em questão.

Com relação a esse ponto, é importante destacar que considerar o postulado do artigo 7º, inciso X, do MCI como uma vertente do direito ao esquecimento não é aceito por parte da doutrina. Carlos Affonso Pereira de Souza entende, por exemplo, que esse artigo versa sobre a exclusão de dados posteriormente ao encerramento da relação contratual entre o titular dos dados e a empresa. Por outro lado, Lucca Belli tem entendimento no mesmo sentido da decisão em comento, qual seja, de que o inciso X do artigo 7º do MCI trataria de direito ao esquecimento parcial[410].

Os argumentos utilizados pelo STJ pela não aplicabilidade do direito ao esquecimento aos provedores de aplicação de busca parecem respeitar a posição preferencial[411] [412] da liberdade de expressão, ao contrário da determinação da Corte Europeia no caso Costeja. Ainda que a decisão do Tribunal de Justiça Europeu tenha imposto à Google a aplicação do direito ao esquecimento na internet, observando a "natureza da informação em questão, sua sensibilidade para a vida privada da pessoa em causa e o interesse do público em dispor dessa informação"[413], o mero atributo de poder conferido pelo status de "censor" seria contrário aos preceitos do ordenamento jurídico brasileiro[414].

Mantém-se, portanto, o previamente estabelecido pelo STJ, consoante ao caso Xuxa *vs.* Google, que dispôs: "essa provedoria de pesquisa é uma espécie do gênero provedor de conteúdo, pois não inclui, hospeda, organiza ou de qualquer outra forma gerencia as páginas virtuais indicadas nos resultados disponibilizados, se limitando a indicar links onde podem ser encontrados os termos ou expressões de busca fornecidos pelo próprio usuário"[415].

---

410 Programa Conexão Futura. **CANAL FUTURA**. Exibido em: 7 out. 2016.

411 Tal critério é adotado no controle de constitucionalidade de restrições impostas à liberdade de expressão pelo Estado em nome do interesse público. SCHREIBER, Simone. Conteúdo e justificativa teórica da liberdade de expressão. **Revista Jus Navigandi**, Teresina, ano 10, n. 781, 23 ago. 2005. Disponível em: <https://jus.com.br/artigos/7184>. Acesso em: 14 jan. 2017.

412 SARMENTO, Daniel. Parecer em ARE 833248. "(...) o sistema constitucional brasileiro (...) atribuiu uma posição preferencial às liberdades de expressão e de imprensa no confronto com direitos da personalidade, como vem reconhecendo o STF e a doutrina". Acesso em: 15 mar. 2017

413 Google Spain SL vs. Mario Costeja. C-131/12. Publicado em: 13 mai. 2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5650361efaad440a996d4f09dc436711b.e34KaxiLc3qMb40Rch0SaxyKbN90?text=&docid=152065&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=644413>. Acesso em: 10 out. 2016.

414 STJ. AgInt no REsp 1.593.873 - SP. Rel. Min. Nancy Andrighi. Consulta realizada em: 17 nov. 2016.

415 STJ, REsp 1.316.921 - RJ, Rel. Min. Nancy Andrighi, p. 6. Consulta realizada em: 15 jan. 2017.

A Ministra Nancy Andrighi ainda firma entendimento acerca da comparação entre a decisão europeia e a brasileira, explicando o porquê da impossibilidade de se adequar àquela aos preceitos normativos pátrios. Nesse sentido, diz que "concordar com tal solução no contexto normativo brasileiro, equivale a atribuir a um determinado provedor de aplicação de internet – no caso, o buscador Google – a função de um verdadeiro censor digital, que vigiará o que pode ou não ser facilmente acessado pelo público em geral, na ausência de qualquer fundamento legal"[416].

Censura digital e a exigência do que é verdade

Filie-se aos preceitos do *leading case* europeu ou à interpretação dada pelo STJ, fato é que o direito ao esquecimento na internet deve ser tratado como exceção e não regra, visto que é da rede que grande parte da população mundial retira informação [417] [418] [419]. Logo, restringir o acesso a conteúdos obstaculiza, per se, a obtenção da melhor informação.

Ao observarmos nossos hábitos em ambiente virtual e, principalmente, a forma como a internet vem se construindo ao longo dos anos, temos uma verdadeira sensação de memória permanente[420]. De fato, tal "memória permanente" pode gerar transtornos aos indivíduos, como no caso da Professora da Pensilvânia que postou uma foto sua fantasiada de pirata com o título "Pirata Bêbada" (ou "*Drunken Pirate*",

416 STJ, REsp 1.316.921 - RJ, Rel. Min. Nancy Andrighi, p. 16.

417 Internet é a primeira fonte de informação para 47% dos brasileiros, aponta estudo. **IBOPE**. Publicado em: 17 abr. 2014. Disponível em: <http://www.ibope.com.br/pt-br/noticias/Paginas/Internet-e-a-primeira-fonte-de-informacoes-para-47-dos-brasileiros-aponta-estudo.aspx>. Acesso em: 17 nov. 2016.

418 JUNIOR, Paulo Roberto. Cerca de 70% dos brasileiros ativos no Facebook se informam pela rede social. **OBSERVATÓRIO DA IMPRENSA**. Publicado em: 21 abr. 2015. Disponível em: <http://observatoriodaimprensa.com.br/e-noticias/cerca-de-70-dos-brasileiros-se-informam-pelo-facebook/>. Acesso em: 17 nov. 2016.

419 BI Intelligence. Here's how people are consuming their news today. **BUSINESS INSIDER**. Publicado em: 10 out. 2016. Disponível em: <http://www.businessinsider.com/heres-how-people-are-consuming-their-news-today-2016-10>. Acesso em: 17 nov. 2016.

420 ROSEN, Jeffrey. The Web Means the End of Forgetting. **THE NEW YORK TIMES**. "(…) we are only beginning to understand the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent — and public — digital files". Publicado em: 21 jul. 2010. Disponível em: <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=2&pagewanted=all&>. Acesso em: 17 out. 2016.

no original) e perdeu seu diploma de magistério[421]. Ainda, outro exemplo, é o de um Psicoterapeuta Canadense que tentou visitar os Estados Unidos, mas fora impedido na fronteira: o motivo seria um artigo científico que haveria publicado sobre suas experiências com a droga LSD há mais de trinta anos atrás[422].

Em certa medida, portanto, almejar o reconhecimento do "direito a ser esquecido na internet" auxiliaria na tentativa de impedir a taxação do próprio indivíduo, no presente, por atos e opiniões passadas, tergiversando a temida "memória permanente". Destarte, é certo que casos como o de Mario Costeja, S. M. S. e Xuxa tornam-se mais comuns no mundo conectado.

No entanto, considerando que vivemos no mundo das aparências, das redes sociais e da sociedade líquida[423] – termo cunhado por Zygmunt Bauman – na qual, a todo o momento, é oferecida a nós a oportunidade de nos reinventar, a informação pode ser vista como uma ameaça. Consequentemente, fazer cumprir o direito ao esquecimento na internet tangencia a censura de informações. Cria-se, dessa forma, o paralelo da vida líquida[424] com a censura digital, apropriando-se do conceito de Bauman para classificar o direito ao esquecimento na internet como uma censura líquida[425]. Afinal, "esquecer" na rede é o mais almejado para aquele que deseja a reinvenção através dos olhos dos outros.

---

421 ROSEN, Jeffrey. The Web Means the End of Forgetting. **THE NEW YORK TIMES**. "(…) we are only beginning to understand the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent — and public — digital files". Publicado em: 21 jul. 2010. Disponível em: <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=2&pagewanted=all&>. Acesso em: 17 out. 2016.

422 Op cit.

423 PALLARES-BURKE, Maria Lúcia. A Sociedade Líquida. Entrevista de Zygmunt Bauman a Folha de São Paulo. **FOLHA DE SÃO PAULO**. "Tudo está agora sempre a ser permanentemente desmontado, mas sem perspectiva de nenhuma permanência. Tudo é temporário. É por isso que sugeri a metáfora da "liquidez" para caracterizar o estado da sociedade moderna, que, como os líquidos, se caracteriza por uma incapacidade de manter a forma. Nossas instituições, quadros de referência, estilos de vida, crenças e convicções mudam antes que tenham tempo de se solidificar em costumes, hábitos e verdades 'auto-evidentes'". Disponível em: <http://www1.folha.uol.com.br/fsp/mais/fs1910200305.htm>. Acesso em: 18 nov. 2016.

424 BAUMAN, Zygmunt. **Vida líquida**. Ed. Zahar, 2016, p. 8. "Entre as artes da vida-líquido moderna e as habilidades necessárias para praticá-las, livrar-se das coisas tem prioridade sobre adquiri-las".

425 Para Zygmunt Bauman, o conceito de liquidez seria a incapacidade de manter a forma; inconstância e incerteza gerada pela falta de pontos de referência previamente estabelecidos. Da mesma forma se desenha o direito ao esquecimento na internet. BAUMAN, Zygmunt, **Modernidade Líquida**, pg. 14, Ed. Zahar: "São esses padrões, códigos e regras a que podíamos nos conformar, que podíamos selecionar como pontos estáveis de orientação e pelos quais podíamos nos deixar depois guiar, que estão cada vez mais em falta".

Para países latino-americanos com democracia recente e frágil e histórico de violentas ditaduras nas quais imperou a repressão, é temerário imaginar a possibilidade de um mecanismo facilitador da censura[426] de quaisquer matizes. Nos últimos anos, as tentativas de se legislar sobre o direito ao esquecimento e o uso indiscriminado desse conceito pelos Tribunais brasileiros comprovou o porquê desse temor[427] [428].

Não se pretende negar que, em tempos de pós-verdade[429], em que opiniões pessoais são mais relevantes do que fatos, a verdade absoluta seja utópica. Entretanto, o apagamento, ou o esquecimento na internet, vai de encontro às liberdades de expressão e informação, na medida em que impede a procura pela verdade mínima dos fatos. Acerca da busca pela verdade, ou "exigência do verdadeiro", Marilena Chauí tem relevante ensinamento, ao dispor que "a verdade é, ao mesmo tempo, frágil e poderosa. Frágil porque os poderes estabelecidos podem destruí-la, assim como mudanças teóricas podem substituí-la por outra. Poderosa, porque a exigência do verdadeiro é o que dá sentido à existência humana"[430].

Por essa razão, é fácil concluir que, não só a manutenção, como também a constante atualização da informação que se deseja apagar, permite tanto aos atores do fato a possibilidade de esclarecimento acerca do que realmente aconteceu, quanto ao público, o acesso à discussão, confronto de versões e análise dos elementos que estão ali permeados. Resta dizer que somente através do livre acesso à informação, aperfeiçoaremos nosso processo democrático e evitaremos a censura - em todos os matizes - e o apagamento de nossa história.

---

426 SÁ, Nelson. Direito ao esquecimento ‹não existe› e é usado para censura, afirma advogada. **FOLHA DE SÃO PAULO**. Publicado em: 07 ago. 2016. Disponível em: <http://www1.folha.uol.com.br/cotidiano/2016/08/1799831-direito-ao-esquecimento-nao-existe-e-e-usado-para-censura-afirma-advogada.shtml>. Acesso em: 11 set. 2016.

427 Direito à memória. **ESTADÃO.** Disponível em: <http://opiniao.estadao.com.br/noticias/geral,direito-a-memoria,10000064979>. Acesso em: 11 set. 2016.

428 LEMOS, Ronaldo. O fim da Era Cunha na Internet. **FOLHA DE SÃO PAULO**. Publicado em: 18 jul. 2016. Disponível em: <http://www1.folha.uol.com.br/colunas/ronaldolemos/2016/07/1792652-o-fim-da-era-cunha-na-internet.shtml>. Acesso em: 11 set. 2016.

429 CASTILHO, Carlos. Apertem os cintos: estamos entrando na era da pós-verdade. **OBSERVATÓRIO DA IMPRENSA**. Publicado em: 28 set. 2016. Disponível em: <http://observatoriodaimprensa.com.br/imprensa-em-questao/apertem-os-cintos-estamos-entrando-na-era-da-pos-verdade/>. Acesso em: 10 out. 2016.

430 CHAUÍ, Marilena. **Convite à Filosofia**. São Paulo: Ática, 2000. p. 134.

Considerações Finais

Partindo da premissa de que vivemos na Era da Informação e do Conhecimento e que nossa informação é adquirida em grande parte, e de forma crescente, por meio da internet, tudo está amplamente sujeito ao debate público na rede. Dessa forma, a aplicação do direito ao esquecimento na internet, ou desindexação de conteúdo por buscadores, dificultaria nossa procura e também a própria percepção da informação, que seria comprometida pela falta de certeza se algum fato foi suprimido.

Adotar, pois, o direito ao esquecimento na internet sem cotejar o interesse público e as liberdades de expressão e informação, é atribuir qualidade de censor digital para indivíduos, julgadores e legisladores que efetivem a remoção de determinado conteúdo. Ao seguir por esse caminho, teríamos ainda o desafio de evoluir como sociedade, já que estaríamos sendo privados de informações que, em certa medida, macula riam nosso processo de busca pela verdade.

Ética e Privacidade: Múltiplos Olhares e Partir do Campo da Comunicação

Luiz Peres-Neto[431]

Introdução

Em 1999, o seriado televisivo "The West Wing", cujo enredo girava em torno do dia a dia do fictício presidente dos Estados Unidos da América (EUA), Josiah Bartlet, pressagiou, em um de seus episódios, que a privacidade seria o tema político de principal envergadura nas duas primeiras décadas século XXI. Em um momento no qual a penetração da internet na vida doméstica ainda era muito mais um mercado em potencial - e uma utopia comunicacional - do que uma realidade, o seriado vislumbrou muitos dos desdobramentos trazidos pela irrupção das novas tecnologias da informação e da comunicação (TICs) na vida de milhões de pessoas. A sagaz análise deu-se em um episódio no qual era discutida a indicação de um magistrado para a Suprema Corte, processo político extremamente trabalhoso e de grande envergadura no contexto político norte-americano. Após avaliar um dos postulantes, que marcava certas posições sobre o aborto como meio para pensar as liberdades individuais, um dos assessores diz ao presidente Bartlet que a discussão não deveria girar em torno da questão do aborto e sim sobre a privacidade, que esta última deveria ser entendida como eixo central para pensar as liberdades nas duas primeiras décadas do século XXI.

> "Não é sobre o aborto! É sobre os próximos 20 anos. Nos anos 20 e 30 foi o papel do Estado. Nos anos 60 foram os direitos civis. Nos próximos 20 anos, o debate vai ser sobre a privacidade. Falo da Internet. Dos telefones celulares. Das estatísticas sanitárias. De quem é gay e quem não é. Moral? Em um país nascido para ser livre, o que pode ser mais fundamental do que isso?" (Sam Seaborn, personagem interpretado por Rob Lowe em "The West Wing", Episódio 9, 1ª Temporada,1999)

431 Pós-doutor pela Annenberg School for Communication, da University of Pennsylvania (EUA), onde foi CAPES/ Fulbright Post-doctoral Researcher Fellow. É doutor e mestre em Ciências da Comunicação pela Universidad Autónoma de Barcelona (Espanha). Desde 2012 é professor titular do Programa de Pós-Graduação em Comunicação e Práticas de Consumo (PPGCOM) da ESPM-SP (Brasil).

A coincidência ou presságio ficcional ficou mais claro após alguns acontecimentos que marcaram a cena política nas primeiras duas décadas do século XXI. Em especial a partir de 2009, tais como as revelações de documentos secretos e de cabos diplomáticos pelo portal WikiLeaks[432], as inúmeras revelações sobre as manipulações realizadas por sites como Facebook e Google com os dados pessoais de seus usuários sem o consentimento dos mesmos[433] ou ainda as revelações do ex-agente da National Security Agency (NSA), Edward Snowden, de que, entre outras práticas, o governo dos Estados Unidos (EUA) incrementou a coleta, o armazenamento e o processamento de dados sobre a quase totalidade de informações que trafegam na internet, seja dentro da sua jurisdição ou não, consolidando práticas de espionagem que incluíam, até mesmo, chefes de Estado e uma longa lista de atores políticos, consolidando uma política interna e externa de vigilância contumaz, ampla e irrestrita.

A presença da privacidade como um grande eixo de discussão política global nas duas primeiras décadas do século XXI nos permite problematizá-la por meio de inúmeras perspectivas. Tomando a privacidade como um elemento político, a proposta desenvolvida neste artigo passa por examinar as dimensões éticas da mesma. A filosofia moral e política servirá de guia para iluminar algumas das questões éticas que norteiam o debate político sobre a privacidade. Tal debate se dá em uma arena eminentemente comunicacional, o que pautará as reflexões apresentadas.

De tal sorte, será analisado, em um primeiro momento, como uma moralidade negativa, arrojada pelos gregos à vida privada, estendeu-se da Antiguidade clássica até o devir da modernidade. Evidentemente, não serão esmiuçadas todas as propostas filosóficas contidas no período em torno da ética da priva-

---

432 Ao longo do ano de 2010, a organização não governamental WikiLeaks publicou uma série de documentos confidenciais do Departamento de Estado do governo dos Estados Unidos da América (EUA) relativos a atuação norte-americana nos conflitos armados do Iraque e do Afeganistão, a abusos e torturas sistemáticas na prisão militar de Guantánamo, além de uma série de cabos diplomáticos. O conjunto dessas informações mostrava constantes violações aos direitos fundamentais e à privacidade, como explica GREENBERG, Andy. **This machine Kills Secrets**. Julian Assange, the cypherpunks, and their fight to empower whistleblowers. Nova Iorque: Plume, 2013.

433 Pelo menos dois exemplos podem ser citados para ilustrar esta afirmação: em 2010, o The Wall Street Journal publicou que Google e Facebook manipularam ao longo de 2009 dados pessoais de seus usuários sem o consentimento dos mesmos, o que levou a ambas empresas não só terem que pedir desculpas publicamente como, ademais, se verem forçadas a alterarem as suas políticas de privacidade. Em NISSEMBAUM, Helen. A contextual approach to privacy on-line. **Journal of the American Academy of Arts & Sciences**, vol.140, nº 4, 2011, p.32-48; por sua vez, em 2014, o Facebook manipulou a "timeline" de mais de 700 mil internautas para controlar as emoções às quais eram expostos, em uma pesquisa realizada sem o consentimento dos usuários, o que levou a empresa a novamente ter que se desculpar publicamente, além de ter que responder a um processo na Inglaterra.

cidade, o que seria uma tarefa incompatível com o escopo deste trabalho. No entanto, como bem relata McStay[434], observa-se que foi prestada pouca atenção à privacidade ao longo de todo esse amplíssimo período.

Da Antiguidade até a modernidade, ainda segundo McStay[435], atribuiu-se à vida pública (a vida na *polis*) um valor ético virtuoso enquanto à privacidade ou à vida privada recaia uma moralidade negativa. Isso perdurou, hegemonicamente, nas reflexões éticas sobre privacidade até a o final do século XIX quando a irrupção de novas tecnologias da comunicação e da informação - então limitadas ao surgimento da fotografia e do jornalismo - exigiram novos parâmetros morais para separar os valores e a moralidade das esferas públicas e privadas.

Tais parâmetros gestaram-se em torno à discussão sobre a liberdade de expressão. Sendo assim, em um segundo momento, será discutido, neste trabalho, como o direito à privacidade se frágua a partir de uma ética liberal burguesa umbilicalmente conectada à problematização da liberdade de expressão e à consolidação das culturas do consumo. Esta proximidade se agudiza com a complexificação do cenário comunicacional, com a proliferação dos meios de comunicação de massa e, hodiernamente, o advento das novas mídias e redes de comunicação apoiadas na web 3.0.

A ressemantização moral da privacidade impulsada pela modernidade - que se estende até os dias atuais - se dá pela via do consumo e pela consolidação de uma ética utilitarista como valor hegemônico, o que permitirá refletir como a privacidade se converteu em um bem jurídico de titularidade individual e, assim mesmo, em um bem de consumo capaz de, nos dias atuais, mediar o acesso a quase todos os produtos e serviços digitais que são consumidos a partir da noção de consentimento.

Afinal, o não consentimento às políticas de privacidade daqueles que nos oferecem tais bens ou serviços pressupõe um veto no acesso aos mesmos, reduzindo a ética das políticas de privacidade a uma ética em rede do tudo ou nada.

As moralidades da privacidade

Muitos dos autores que, contemporaneamente, debatem temas atinentes à privacidade situam problemas ou levantam questões éticas sobre as suas reconfigurações, em especial, no tocante às imbricações da mesma com as mídias digitais e as

434 McSTAY, Andrew. **Privacy and philosophy**. Nova Iorque: Peter Lang, 2014.

435 McSTAY, Andrew. **Privacy and philosophy**. Nova Iorque: Peter Lang, 2014.

tecnologias da comunicação e da informação (TICs) sem nem sempre precisarem o que entendem por ética. A omissão ou o não desenvolvimento dos desdobramentos de tais postulados éticos não necessariamente constitui uma falha ou um problema insolúvel. Aponta, contudo, para a dificuldade manifesta que se tem para refletir e construir análises a partir da ética na discussão sobre a privacidade por mais que, paradoxalmente, tenha-se uma grande facilidade para identificar problemas que afligem ou atentem contra aquilo que, intuitivamente, entende-se por ética.

Com grande sensibilidade, o filósofo espanhol Fernando Savater[436] explica que, se indagados, nós saberíamos identificar problemas éticos com grande facilidade, ainda que dificilmente consigamos definir o entendemos por ética(o). Nesse sentido, muitas das considerações éticas sobre os problemas e desdobramentos da privacidade caem no fosso do senso comum ao omitirem o que entendem por ética.

O campo da ética nem sempre oferece um caminho suave para a discussão de qualquer temática. Dentre as muitas razões para esta situação, é possível arrolar ao menos três explicações. Em primeiro lugar, faz-se necessário situar epistemologicamente o que se entende por ética, conforme mencionado anteriormente. Expor uma definição do que se entende por ética é sempre um trabalho complicado. Trata-se, ademais, de um termo que, por vezes, confunde-se com a ideia de moral. Com efeito, para Cortina e Martinez[437] , os dois podem ser tratados como sinônimos na medida em que designam termos próximos, como caráter (*ethos*, de origem grega) e costume (*mores*, de origem latina), respectivamente. Segundo os mencionados autores, moral poderia, contudo, ser entendida como a atribuição livre de um valor a uma ação enquanto a ética se ocuparia de uma reflexão sobre a moral em prol do bem comum ou, caso se queira seguir a proposta aristotélica, da vida boa.

Ainda que se possa diferenciar ética de moral, Cortina[438] assegura que esta separação responde muito mais a um anseio didático do que a uma necessidade analítica. Isto não exime, evidentemente, a necessidade de situar um ponto de partida para enfeixar uma análise, por exemplo, sobre a privacidade a partir do campo da moralidade. A ética, portanto, se atém à discussão sobre o fenômeno da moral, entendido esse como a capacidade individual de ajuizar e imputar valores às ações humanas em arras de um bem comum. Neste trabalho, será adotada tal definição.

436 SAVATER, Fernando. **Ética para meu filho**. São Paulo: Martins Fontes, 1996.

437 CORTINA, Adela; MARTÍNEZ, Emilio. **Ética**. 3ª ed. São Paulo: Loyola, 2012.

438 CORTINA, Adela. **Ética sem moral**. São Paulo: Martins Fontes, 2010.

Uma segunda dificuldade que se faz presente, ao adotar a ética como um eixo norteador de uma discussão, é a frequente confusão da mesma com postulados religiosos, místicos ou moralistas. O moralismo ocorre precisamente quando empregamos um conjunto de valores individuais para atribuir uma virtude ou vício à ação de um terceiro, tomando os nossos valores individuais como verdades absolutas. Por sua vez, não é difícil aduzir que os valores religiosos ou crenças individuais partem de reflexões próximas à esfera da moral. No entanto, por mais que possamos falar em uma ética cristã, judaica, protestante, etc., tais valores não devem ser impostos ou tidos como verdadeiros uma vez que tomam como pressuposto o universo da fé e, portanto, um espaço comum relativo aos que comungam de uma mesma crença, não sendo, obviamente, absoluto. A simples diversidade de opções religiosas já indica uma multiplicidade de visões sobre crenças e modos de ver a vida; ademais, tais éticas respondem a valores (costumes) circunscritos a comunidades em particular, por mais estendidas que estas sejam. Tal parcialidade não é uma prerrogativa do universo religioso. Deve ser estendida a todas as propostas ou paradigmas morais dada a intrínseca relatividade do fenômeno moral.

Com efeito, é preciso ter cautela ao assumir certos valores ou moralidades como "verdades absolutas". Não há um sistema ético perfeito capaz de reparar as angústias morais que nos afligem. A ética, como produto de nossa criação, revela a busca do ser humano por respostas que confortem ou reduzam a incerteza das nossas ações ante situações conflitivas ou nas quais mais de um "dever ser" se imponha[439] . A ética é um espaço importante da nossa dimensão humana, daquilo que nos constitui. Ante as ambiguidades e claudicações inerentes à conduta humana, o campo da ética representa uma tentativa desesperada de reduzi-las. Precisamente por isso, não devemos falar de verdades no campo da moralidade. Como bem lembra Quintana[440], "não há verdade ou falsidade no mundo da moral, há apenas opiniões subjetivas, e isso diante de teorias e autores que defendem o contrário".

Tal afirmação desemboca em uma terceira e última dificuldade para abordar qualquer questão a partir da ética. De qual(is) ética(s) falamos? Ao longo da história da filosofia moral, distintos paradigmas foram gestados na tentativa de responder as questões que fundamentam a reflexão moral. Falamos de ética dos meios, ética dos fins, ética universal, relativa, ética das consequências, pragmática, ética da responsabilidade, etc, e poderíamos citar muitas outras

439 MORIN, Edgar. Ética. O método 6. 2.ed. Porto Alegre: Sulina, 2005.

440 QUINTANA, Fernando. Ética e política. São Paulo: Atlas, 2014, p.4.

propostas que tentam responder à pergunta de o que devo fazer para gozar da vida boa ou como a mesma está relacionada com o bem comum e a justiça. Por vezes, certos autores esperam que um destes paradigmas seja o certo, o verdadeiro, e esquecem que a subjetividade é a matéria-prima da moral. Que não há nenhuma ética sem um sujeito. Consequentemente, é preciso ter claro que não há imparcialidade no terreno da moral. Como recorda Cortina:

> o pecado da unilateralidade, cometido por todo aquele que adota uma única perspectiva, começa a ser percebido como tal em contato com a unilateralidade contrária, de modo que os adversários, com o tempo, acabam indo procurar um terceiro, que os supere, conservando-os[441].

Este último tópico ou dificuldade é extremamente emblemático quando revisamos a literatura sobre as políticas de privacidade atreladas às TICs. Com inaudita frequência, adota-se um paradigma moral para responder a uma questão ou situação concreta, universalizando-o como verdadeiro e capaz de dar cabida a todo e qualquer problema moral que surja em torno à miríade de situações subjacentes à discussão sobre a privacidade.

A busca por respostas jurídicas urgentes em torno dos problemas derivados da privacidade digital - necessárias, cabe dizer - muitas vezes acaba por eclipsar os conflitos éticos subjacentes. Ao assumir, por exemplo, o consentimento do usuário como um bálsamo moral capaz de autorizar instituições públicas ou organizações privadas a dispor dos dados pessoais de terceiros - com independência do ajustamento legal de tal conduta, centrando-se unicamente na questão ética - assume-se a ética do consentimento como uma espécie de ética total para as políticas de privacidade digital. Não é preciso ser filósofo nem especialista em tecnologia para saber da incompletude ou das falhas subjacentes a esta opção para tomá-la como moralidade universal para a dissolução dos conflitos éticos fraguados em torno à privacidade. Neste ponto, fica claro que é bastante comum a priorização de um elemento jurídico que dê fiança às partes implicadas em uma relação virtual subordinando ou até mesmo dando por dissolvida qualquer contradição ou problema ético.

Não há, no entanto, uma "bala de prata" moral capaz de dissolver os conflitos éticos que florescem - e a cada dia são maiores e mais complexos - no bojo da discussão da privacidade ante a multiplicidade de situações que as TICs oferecem. O conhecimento das respostas dadas pela ética à questão da privacidade, contudo, pode nos auxiliar a entender melhor não só a dimensão deste

441 CORTINA, Adela. Ética sem moral. São Paulo: Martins Fontes, 2010, p.41.

problema como também possíveis caminhos para compreendê-lo desde uma perspectiva mais holística, mais humanista.

Na história das ideias, dificilmente encontra-se um tema que não tenha sido objeto de reflexão dos pensadores gregos chamados de clássicos. Consequentemente, dificilmente não haveria uma reflexão seminal sobre as relações entre privacidade e a filosofia moral e política. Na obra "A República", Platão situa a privacidade como a esfera da vida restrita ao *oikós* (do grego, casa), àquilo que é circunscrito aos *idees* ou *idio*, origem etimológica da palavra idiota, empregada inicialmente para designar pessoas que não possuíam direitos políticos ou a capacidade para participar ou exercer funções na *polis*, na vida pública. Encontra-se, nas reflexões platônicas, pelo menos duas questões fundamentais.

Em primeiro lugar há uma manifesta vontade de contrapor à noção de privacidade o conceito de vida pública, limitando a primeira ao âmbito da vida doméstica. Mais do que situar uma fronteira, a vida privada e a vida íntima não teriam nenhum interesse para a vida da (e na) *polis*, razão pela qual todo aquele que não fosse cidadão seria um "idiota", alguém que deveria ficar circunscrito à vida doméstica e, portanto, despido da capacidade política. A vida privada não representava uma esfera que requeresse qualquer tipo de atenção e, consequentemente, de reflexão.

Indiretamente, Platão constrói uma moralidade negativa à privacidade. Essa erige-se ao despir de interesse público e político tudo aquilo que for privado. O mundo da privacidade seria, portanto, uma dimensão menor da vida humana. Para Platão, apenas na "cidade justa", no espaço público, podem ser desenvolvidas as boas artes do governo e do conhecimento.

Por seu turno, e a raiz do anteriormente exposto, as reflexões platônicas sobre a privacidade não buscam edificar uma separação dialética entre público e privado já que esta última esfera não é de interesse. A virtude - e, portanto, a vida justa, capaz de construir o bem comum - se dá unicamente na *polis*. De tal sorte não há uma ética da/ para a privacidade.

A despeito das enormes diferenças que marcam a filosofia platônica (idealista) da proposta aristotélica (realista) tampouco há na visão do filósofo estagirita uma proposta ética para a privacidade. Isto porque tampouco Aristóteles considera a esfera privada como um espaço relevante para a reflexão moral.

Como é sabido, Aristóteles defende em sua "Ética a Nicômaco" a tese de que a ética é um saber prático, uma teoria da ação humana centrada na busca do bem para o homem; bem este que seria, por extensão, o bem da *polis*. A finalidade da ética é, portanto, encontrar o caminho para a vida boa e, consequentemente, lográ-la para a vida na *polis*. Como ser social, o homem necessita desenvolver-

-se na *polis*. Destarte, Aristóteles dá à política um amplo destaque e a relaciona diretamente com a ética (procede daí a célebre ideia "*Zoon politikón*", do homem como um animal político, da *polis*). Nesse sentido, a ação moral é a base para a ação política não havendo cabida para uma ética privada já que a mesma se dá na vida na *polis*. A vida boa não se encontra na vida privada e sim na vida pública.

Ainda que tampouco Aristóteles tenha declinado um olhar para a privacidade, sua proposta ética - assim como a platônica que a precede - aproxima definitivamente os campos da filosofia moral da política. Em síntese, desembocamos na formulação de perguntas em torno às questões da vida boa ou do justo, costuradas por reflexões acerca das virtudes na vida pública, duas tradições teóricas que ao longo da história da filosofia moral e política engendraram grande parte dos debates nesta área.

É extremamente interessante vislumbrar tanto em Platão como em Aristóteles a subjacente ideia de que o que é virtuoso é, necessariamente, público e que a privacidade carece de tal moralidade. Como aponta McStay[442] , nasce a partir das reflexões de Platão e Aristóteles a visão de que só se requer da privacidade quando há algo a ser escondido do público. Dito de outro modo, a privacidade apenas é necessária para quem tem algo a ser ocultado. Ambos ignoram a possibilidade de que parte da consciência moral se dá precisamente na microfísica da intimidade, na solidão privada do eu.

É difícil arriscar uma proposição tão arrojada, mas, em certa medida, pode-se assumir que parte da moralidade negativa que permeia a noção de privacidade forjada a partir da potência das obras de Platão e Aristóteles reforça equívocos do senso comum de que só se precisa de privacidade para "esconder algo do público". É frequente deparar-se, no ciberespaço, com críticas à privacidade digital nas quais atribui-se a quem precisa da mesma a necessidade de esconder ou ocultar algo, como se a privacidade se resumisse a isso ou como se todos nós fossemos transparentes aos olhos do público. Com fina ironia, ao criticar tal argumento, Byung-Chul Han[443] lembra que, psicanaliticamente, não somos muitas vezes transparentes nem com a nossa própria consciência, nem com nós mesmos.

Apenas são encontradas as bases de uma reflexão moral que contradiga esta moralidade negativa em torno da privacidade a partir do devir da modernidade e o surgimento do pensamento liberal. As revoluções burguesas transformaram radicalmente não apenas o modo de produção mas, como defende Peter Gay[444], significaram uma avassaladora transformação no modo de viver a vida,

442 McSTAY, Andrew. **Privacy and philosophy**. Nova Iorque: Peter Lang, 2014.

443 HAN, Byung-Chul. **La sociedad del cansancio**. Barcelona: Herder Editorial, 2013.

444 GAY, Peter. **A educação dos sentidos**. São Paulo: Companhia das Letras, 1989.

nos costumes, na cultura, na ética. Autores como Stuart Mill[445], John Locke[446], entre outros, invertem a ideia de que a esfera da privacidade representaria a defesa de um lugar ou espaço para "esconder algo" do conhecimento do público e lançam as bases para a defesa de um território pessoal que deve ser protegido.

Guardadas as diferenças temporais, tanto Mill como Locke vão lutar contra a tese de que o governo e a política podem dominar a vida das pessoas, quer seja no âmbito público quer seja no âmbito privado. Emergem, a partir do pensamento liberal dos mencionados autores, o esboço moral fundamental para a defesa do controle das informações sobre si, daquilo que se quer (ou não) dividir com o público, a necessidade de se ter controle sobre si em termos de autonomia e dignidade da pessoa. A modernidade, em suma, frágua a noção ética da liberdade como fundamento moral expressado na autonomia individual.

Um elemento central para esta discussão é, com efeito, a noção de liberdade. Mill[447] defende que deve haver um limite ao poder que a sociedade pode exercer sobre os indivíduos, ou seja, defende tanto a separação entre a esfera pública da privada como, ademais, postula a necessidade de dar ao indivíduo a garantia de que este possa atuar segundo as suas vontades em certos âmbitos da sua vida, com independência dos postulados legislados pela sociedade. No entender de Mill, os indivíduos devem ter total liberdade para agir segundo as suas vontades sempre e quando as mesmas não atentem contra a liberdade de terceiros ou causem algum tipo de dano à integridade dos próprios sujeitos.

Irrompe com força a tese da necessária autonomia do sujeito[448]. Ademais, é a partir do pensamento liberal de autores como John S. Mill que também ganha corpo a noção de consentimento, base moral - e jurídica - para as políticas de privacidade contemporâneas. A autonomia da pessoa humana permitiria, segundo a tese liberal, que os sujeitos tomassem decisões livres do excesso de controle e pressão da sociedade. Outro ponto chave na equação liberal se dá na valorização da liberdade de expressão que passa a ser um elemento fiador da privacidade, o que será trabalhado com mais vagar a continuação.

---

445 MILL, John Stuart. **Sobre la libertad.** Barcelona: Folio, 2007.

446 LOCKE, John. **Segundo tratado sobre o governo civil**. São Paulo: Edipro, 2013.

447 MILL, John Stuart. **Sobre la libertad.** Barcelona: Folio, 2007, p.19.

448 É impossível não mencionar a Immanuel Kant (1724 -1804) ao tratarmos o tema a autonomia moral. No entanto, a complexidade da proposta kantiana nos forçaria a um debate que escapa ao âmago da discussão proposta neste artigo. Os pensadores liberais como Mill aprofundam a ideia de autonomia a partir de um conceito de liberdade. por ser esta última mais útil ao debate acerca da privacidade, não entraremos nos meandros dessa discussão, ainda que cometamos o pecado da superficialidade.

Privacidade, Liberdade de Expressão e as Culturas do Consumo

Conforme defendem Briggs e Burke[449], a "tecnologia não poderia nunca ser separada da economia e o conceito de uma revolução industrial de ser precedida por uma revolução comunicacional - longa, contínua e inacabada". A revolução tecnológica impulsada por Gutenberg permitiu muito mais do que a criação de novos espaços comunicacionais que, entre outras mudanças sociais e culturais, auxiliaram, decisivamente, no impulso à primeira e segunda revoluções industriais. Para os supracitados autores, a ideia de liberdade de expressão, que já vinha sendo conquistada, paulatinamente, com a derrocada do Antigo regime, alcançou um novo patamar com a tecnologia da prensa; e, consequentemente, a defesa de novos direitos políticos tais como as liberdades de imprensa, de informação, reunião, associação, entre outros, ante as novas sociabilidades gestadas a partir das relações entre tecnologia, comunicação e economia.

Não sem controvérsias Habermas[450] defende que, entre os séculos XVIII e XIX, a partir de um conjunto de fatores econômicos e socioculturais, consolidou-se uma esfera pública mediadora das relações entre Estado e sociedade, a partir da qual as manifestações das opiniões individuais, livres e racionais, pautadas pelo ideal cívico e a partir do acesso a informações, permitiam a construção de um debate público que daria forma e conteúdo à chamada opinião pública. Essa última, por sua vez, seria o motor da democracia burguesa liberal representativa. Gestada sob os auspícios do pensamento liberal, este processo permitiu, na visão de Habermas , a construção de uma esfera pública livre do poder ou interesse político do Estado e dos interesses privados (particulares). Mais do que uma mudança política, para o citado autor, esta transformação tem o signo de uma mudança cultural estrutural.

A esfera pública descrita por Habermas é um espaço eminentemente comunicacional, no qual o discurso, o debate racional e a argumentação entre iguais constituem princípios que balizam a ação humana. De tal sorte, não haveria uma esfera pública sem os direitos de expressão. Ainda que a esfera pública burguesa habermasiana centre todo o seu esforço na discussão sobre a dimensão de um debate público, a mesma permite vislumbrar uma esfera privada não mais circuns-

449 BRIGGS, A. BURKE, P. **Social History of the Media**: From Gutenberg to the Internet. Nova Iorque: Polity, 2006, p.86.

450 HABERMAS, Jürgen. **Historia y crítica de la opinión pública**. La transformación estructural de la vida pública. Barcelona: Gustavo Gili, 2002.

crita a uma moralidade negativa. Isso porque essa última deixa de ser um espaço segregado da esfera pública como propunham os pensadores gregos; a esfera privada passa a ser entendida como complementar e interdependente à esfera pública.

Com efeito, a esfera privada - constituída na modernidade a partir das mudanças estruturais da esfera pública - passa a ser entendida como o impenetrável domínio da vida no qual tem-se o domínio de si com um maior grau de autonomia. Se, por um lado, um menu de direitos e garantias sociais oferecidos pelo Estado passam a governar uma parte da vida das pessoas (por exemplo, a partir da universalização da educação), por outro lado, a vida íntima ganha um novo revestimento cultural na medida em que enfraquece os laços sociais comunitários, permitindo que a privacidade represente um espaço impenetrável aos olhos do público. A ética da privacidade moderna é aquela que permite a separação de valores próprios da vida pública daqueles circunscritos à vida privada.

Quando Warren e Brandeis[451] teorizaram a clássica definição de privacidade como "o direito de ser deixado só", respondiam, em parte, as angústias e anseios fraguados pela vida moderna nas metrópoles. A ideia de um "direito a estar só" responde aos temores inseridos pelo jornalismo e pela fotografia que, na virada do século XIX para o XX, transformaram a vida privada daqueles personagens cuja atuação pública recaía um interesse público em objeto de vigilância e perseguição.

Como explica Solove[452] , prévio à conceitualização de Warren e Brandeis , não era comum o uso de expressões como "privacidade", "intimidade" ou "esfera privada". De tal sorte, assume-se que a enunciação do ideal da "privacidade" provém do campo da seminal proposta dos supracitados autores. Tal definição remete, em primeiro lugar, à constatação dos pressupostos morais da mesma forjados no liberalismo e numa ética utilitária. A noção de que o direito à privacidade seria aquele que permitiria aos indivíduos ficarem sós recupera claramente os fundamentos políticos e morais da ética utilitarista de autores como John Stuart Mill e, em particular, de John Locke, para quem a liberdade está relacionada não só com a dimensão ontológica que fundamenta que somos nós como também à gestão dos bens e propriedades pertencentes a nós mesmos. Ser livre é poder dispor daquilo que se tem/ possui.

A proposta ética utilitarista, também conhecida como "ética das consequências", parte da ideia de que todos os indivíduo são livres e racionais sendo,

---

451 WARREN, S. D. BRANDEIS, L. D. "The right to privacy". **Harvard Law Review**, nº 4, vol. 5, 1890, p.193–220. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>. Acesso em: 01.02.15.

452 SOLOVE, Daniel. **Understanding Privacy**. Cambridge (MA): Harvard University Press, 2008.

portanto, capazes de arbitrar moralmente uma conduta a partir de um cálculo feito sobre as suas consequências. Ao decidir apertar (ou não) o botão da bomba atômica, prezaríamos pelas consequências dessa ação, deliberando em função das mesmas, tendo como régua o bem causado ao maior número de pessoas.

Ao permitir o casamento da ética com um cálculo moral, o utilitarismo favoreceu o florescimento de uma ética aplicada e a aparente dissolução de situações éticas extremas. A ética utilitária oferece um cardápio de soluções ou um guia de como proceder ("dever ser"). Contudo, para Bilbeny[453], uma das principais críticas a esse paradigma é ênfase depositada na dimensão racional. Autores críticos à "ética das consequências" costumam argumentar que nem sempre um sujeito age pautado pela razão, nem sempre se tem todas as informações e variáveis que permitam a realização de um cálculo moral racional; igualmente, o simples fato de se dispor de toda sorte de informação não assegura por si só uma decisão racional. Não se pode ignorar no âmbito das ações morais os afetos e as emoções.

Em que pesem tais críticas, a partir da proposta de Warren e Brandeis, a ética utilitária passou a revestir e fundamentar quase a totalidade das políticas de privacidade uma vez que apresenta uma aparente solução aos conflitos morais subjacentes à própria ideia de privacidade. Warren e Brandeis conjuminam os limites para o exercício da liberdade de expressão com a tese que que a privacidade é um bem que pode ser gerido pelo seu titular.

Faz-se, contudo, igualmente necessário situar o contexto histórico no qual Warren e Brandeis gestaram o conceito de privacidade e como os valores morais circunscritos no mesmo se veem refletidos nessa teorização. A transição entre os séculos XIX e XX, nos Estados Unidos, assistiu ao surgimento de uma "classe ociosa", uma parte expressiva da burguesia capitalista que se consolidava e abraçava a comunicação do consumo como um instrumento de marcação da sua condição e classe social. Nesse contexto, ver e ser visto a partir do consumo de determinados bens ou serviços funcionava como um importantíssimo marcador social.

Tal processo de marcação social gerou, conforme explica Veblen[454], um contexto de disputa pela disposição pública de certos signos do consumo material. Mais do que uma simples disputa, se constituiu um tipo de emulação que requeria um contínuo processo de vigilância e observação do outro. De olho nesse fenômeno, muitos dos jornais de circulação diária dos EUA começaram a publicar "colunas de costumes", o que hoje conhecemos como colunas sociais.

---

453 BILBENY, Norbert. Ética. Barcelona: Ariel, 2012.

454 VEBLEN, Thortein. **Teoría de la clase ociosa**. Madrid: Alianza, 2004.

Rapidamente, essas passaram a comercializar a intimidade de certos personagens cuja vida privada tinha (ou não) certo interesse público.

Se a comercialização da intimidade alheia serviu para alavancar a venda de jornais, como explica Mott[455], a mesma também serviu para que Joseph Pulitzer, então editor do "New York World" propusesse a separar o conceito de informação e interesse público daquilo que passaria a ser denominado como jornalismo marrom. Esse fenômeno apenas reforça os pressupostos e esforços que permeiam a proposta de Warren e Brandeis.

Ainda que de maneira marginal, cabe acrescentar que Warren tinha razões pessoais para buscar elementos jurídicos que assegurassem a separação entre vida pública e vida privada. Casado com a filha de um importante senador, há registros fiáveis, conforme explica DeCew[456], de que a vida privada de Warren era não muito condizente com os valores próprios de uma ética puritana, tendo sido esse flagrado por fotógrafos de algumas colunas sociais na porta de algumas casas de moralidade alternativa.

Ainda que não seja isenta de conflitos e contradições, a consolidação da noção sobre a privacidade como um bem individual foi essencial para o desenvolvimento da indústria cultural de massa e o estabelecimento de possíveis fronteiras entre a esfera pública e a privada. Segundo Solove[457], a partir da ideia de que a privacidade seria uma espécie de direito à solidão, podemos observar que alguns limites passaram a ser respeitados, quer seja no tocante às garantias para o exercício da liberdade de expressão, quer seja para a observação do direito à privacidade.

Sem vetar o exercício da liberdade de expressão, Warren e Brandeis (1890) permitiram que a esfera da vida privada, em plena transformação no bojo da consolidação da sociedade de consumo, fosse revestida de uma proteção. Conseguiram, assim, arregimentar as bases tanto para um voo maior do capitalismo, no tocante à industrialização da cultura de massas, quanto, ademais, construir uma fronteira clara que separasse o mundo público do privado, retirando desse último a até então moralidade negativa.

A racionalidade imposta pela ética utilitarista no seio do conceito moderno de privacidade fez, contudo, que os principais pressupostos implicados no debate sobre a privacidade passassem a ser a conjugação do binômio controle

455 MOTT, Frank. **American journalism**: a history of newspapers in the United States through 250 years, 1690-1940. Londres: Routledge/Thoemmes, 2000.

456 DeCEW, Judith W. **In pursuit of privacy. Law, Ethics, and the rise of technology**. Ithaca: Cornell University Press, 1997.

457 SOLOVE, Daniel. **Understanding Privacy**. Cambridge (MA): Harvard University Press, 2008.

(das informações sobre si) e liberdade, contrapondo um mundo privado a um outro, exercido na esfera pública. Inaugura-se, destarte, em torno à privacidade a noção da existência de uma esfera íntima (direito a ser deixado só) cujo contraposto público estaria em mãos dos sujeitos-consumidores, posto que estes teriam, racional e livremente, o controle das informações sobre si mesmo e publicizariam apenas aquilo que consentissem. A transgressão deste direito estaria apenas justificada quando invocada uma questão de interesse público.

No entanto, a visão moderna de que existiria um mundo privado rodeado de um outro público, separados por uma clara fronteira controlada por cada um de nós talvez tenha sido apenas um "sonho de uma noite de verão" ilustrado. A tessitura de uma sociedade em rede, nos moldes propostos por Castells[458], indica que há uma complexidade muito maior do que uma fronteira clara entre uma esfera pública e outra privada.

Desse modo, uma ética para a privacidade fundada na racionalidade, plasmada no binômio informação-consentimento não é capaz de dar conta da infinidade de problemas que se deriva do novo contexto de vida em rede. Paradoxalmente, praticamente todas as políticas de privacidade contemporâneas ainda estão fundamentadas na noção moderna de consentimento. Nissenbaum[459] defende que não se pode mais assumir o binômio informação-controle como capaz de garantir o direito à privacidade posto que não somos mais capazes de controlar as informações (dados ou metadados) sobre nós, ainda que qualquer um possa exercer, parcialmente, certa liberdade ou veto no uso dos mesmos.

Em um contexto no qual o mais mínimo objeto, dado ou ação tem o potencial de excitar um amplo circuito comunicacional orientado para o consumo, a proposta utilitária passa a ser um claro limite para o entendimento de uma ética da privacidade, despejando essa última num fosso de constatações pessimistas ou de propostas estritamente jurídicas, obviando as desiguais relações de poder que sustentam as interações cotidianas na sociedade em rede.

Pressupor que um usuário-consumidor, quer seja de um PC, aplicativo ou site, ao aceitar os termos propostos por uma das partes (a parte mais poderosa da relação, diga-se de passagem) e cujos pontos não são negociáveis, leu e consentiu racionalmente com tudo o que estava proposto é de uma ingenuidade moral ímpar ou de uma canalhice ética sem-fim.

---

458 CASTELLS, Manuel. **Communication power**. Oxford: Oxford University Press, 2009.

459 NISSEMBAUM, Helen. "A contextual approach to privacy online". **Journal of the American Academy of Arts & Sciences**, vol.140, nº 4, 2011, p.32-48.

Não aceitar, hoje em dia, uma determinada política de privacidade é assumir um veto à participação à cultura do consumo. Enquanto organizações e instituições não aceitarem que precisarão ceder no tocante ao modelo de privacidade que contemporaneamente utilizam, do ponto de vista da ética apenas teremos um sinistro caminho pela frente, modificável apenas a partir de escândalos (cada vez mais frequentes) ou pequenas ações net-ativistas.

Business Models and Big Data: How Google uses your Personal Information

Marcela Mattiuzzo[460]

Introduction

In March 2016, the German competition authority (Bundeskartellamt) released a statement revealing it had initiated proceedings against Facebook under suspicion that the company was infringing data protection regulation to abuse its dominant position in social networks. The president of the German authority, Andreas Mundt, claimed that "[f]or advertising-financed internet services such as Facebook, user data are hugely important. For this reason it is essential to also examine under the aspect of abuse of market power whether the consumers are sufficiently informed about the type and extent of data collected[461]."

Digital businesses have been under scrutiny for some time, and antitrust authorities are not the only ones concerned with their handling of users' privacy. The field of data protection gained such prominence that an agreement between the United States and the European Union was crafted solely to address transatlantic data transfer. The Safe Harbor Framework[462], as it was known,

460 Visiting Researcher at Yale Law School (2016-2017) and Master of Laws Candidate at the University of São Paulo. Partner at VMCA Advogados. Former Chief of Staff and Advisor for the President at the Brazilian Administrative Council for Economic Defense (2015-2016).

461 Bundeskartellamt Press Release - Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules. Available at: <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html> Accessed on: 19 September 2016.

462 The Safe Harbor Framework between the United States and the European Union was a mechanism by which organizations could transfer data across the Atlantic. It was established for the EU, concerned with US handling of personal information, wished to better protect its citizens' data. The Framework operated owing to seven principles: notice, choice, onward transfer, access, security, data integrity, and enforcement. On October 6, 2015, the European Court of Justice issued a judgment declaring the framework inadequate.

was later struck down by the European Court of Justice (ECJ)[463], creating a "data crisis" that led to the approval of the new Privacy Shield agreement[464].

Simultaneously, several jurisdictions have created agencies and authorities whose goal is to deal with privacy regulation. The most noteworthy example, but by no means the only one, is the European Union. Since 1995, the European Commission (EC) established the region-wide Directive 95/46/EC, which puts forward parameters for the processing and circulation of personal data[465]. The Directive also created the Working Party on the Protection of Individuals with regards to the Processing of Personal Data, known as the Article 29 Working Party. In 2012, the EC proposed a comprehensive review of personal data regulation by means of Regulation 2016/679 (the General Data Protection Regulation – GDPR), reinforcing the role of data protection[466].

Owing to this body of legislation, several Member States have developed national authorities to enforce European-wide rules[467]. The GDPR, which shall come into force in 2018, will establish a new framework for cooperation between such national bodies[468].

---

463 PADOVA, Yann. The Safe Harbour is invalid: what tools remain for data transfers and what comes next? **International Data Privacy Law**, vol. 6, n. 2, p. 139-161.

464 Prompted by revelations of mass surveillance by the American government, the new framework aims to protect "the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers." It was drafted owing to the requirements set forth by the ECJ in its October 2015 ruling. Available at: <http://europa.eu/rapid/press-release_IP-16-2461_en.htm>. Accessed on: 3 November 2016.

465 The Directive is not immediately binding on companies, but rather on Member States, who had to instate legislation and authorities to oversee the flow and handling of personal data. The three principles of the Directive are transparency, legitimate purpose, and proportionality.

466 The European Union allows for issuance of both directives and regulations, and these instruments serve different purposes. While a directive has to be transposed into national law by means of other legal instruments – and the Member State is thus free to establish any framework within the general principles of the directive to enforce it – a regulation is immediately enforceable in all of the EU. That is why the vacatio for regulations is usually longer, since several national authorities must simultaneously adapt to the new rules. The GDPR is no exception to this tendency; approved in 2016, it will come into force in 2018.

467 The most prominent of which is the Irish Data Protection Agency. The growth of Irish regulation over privacy is a natural consequence of the geographical distribution of many Silicon Valley companies within the European Union. When expanding across the Atlantic, many of them chose Ireland as their principal non-US headquarters (mostly due to tax exemptions).

468 In the United States, the Federal Trade Commission is one of the agency's responsible for privacy regulation. It should be noted, however, that American regulation on the topic is not centralized. The protection extended varies according to the type of transaction, which is why some authors

Concern over privacy regulation in the online world is therefore not a novelty, nor have governments ignored its growing impact in the past decades. But because technologies evolve at a pace with which legislation cannot keep up, there has been much debate on whether the current frameworks adequately protect users' privacy and whether changes are necessary – even if those changes would come at the expense of economic efficiency.

Such concerns also gained prominence due to the process of economic concentration and consolidation in the online environment. Today, a small number of large companies control much of the world's personal information, and the bulk of information grows at an exponential rate. The size and relevance of such companies shifted their role from objects of regulation to architects of some markets, in a movement some authors refer to as "code is law"[469]. The algorithms that shape these online platforms have effectively become the norm for much of the web.

Personal data has been an asset for business for many years. It arguably has been so ever since the concept of advertising was invented, as businessmen have long concluded they have higher success-rates when they target ads according to their audience[470]. The very definition of personal data helps clarify this point. The Irish Data Protection Commissioner[471], whose Data Protection Act dates back to 1988 – a time before commercial internet existed – defines personal data as "data relating to a living individual who is or can be identified either

usually refer to the American regulation of privacy as "limited". For more on the regulatory models put forward by the European Union and the United States, see Guilherme Guidi's article.

469 LESSIG, Lawrence. **Code:Version 2.0**. Chapter 1 - Code is Law. Basic Books, New York, 2006.

470 CRAIG, Terence; LUDLOFF, Mary E. Privacy and Big Data. Chapter 1 - The Perfect Storm. O'Reilly Media, Inc., Sebastopol, 2011, p. 5: "In the pre-digital days, there were companies that specialized in analyzing buying behavior, like AC Nielsen, and companies that "rented" out their customer list, segmented by income level, sex, marital status, buying behavior, etc. Chances are your mailbox, like ours, was stuffed with all kinds of offers and you seemed to get phone calls about buying or selling something every hour. Most likely, those offers were the result of information you gave to your bank, credit card company, grocery store, or as a magazine subscription holder. But the information was, to some extent, blind. Your name and address were rented, usually as part of a group, but the renter (the business or organization that bought the advertising) did not have that information until, and unless, you responded. If you did, you then became a part of that company's mailing list and they would begin to build their own profile about you. So, even then, there were multiple profiles of you in multiple lead or customer databases based on your behavior with a specific company or organization."

471 Irish personal data regulation has become particularly relevant over the past years as many Silicon Valley companies established their European subsidiaries in the country – the original reason was mostly related to tax benefits, but it inadvertently rendered Ireland a center of personal data discussions and its law particularly important within the European context.

from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller"[472].

Why then would this topic be particularly relevant for online markets? The answer lies in the fact that the expansion of the internet catapulted data to a much more significant position, creating what is now referred to as Big Data. Big Data is a concept originally coined by Doug Laney[473] to describe the new ways by which data is collected, profiled and utilized by businesses in the internet age. He claimed there are three dimensions to that concept, which were later expanded to the "Four Vs" of Big Data: volume, variety, veracity, and velocity[474].

Data is considered to be "big" because it is produced and collected in impressive **volume**. IBM estimates that the world generates around 2.5 quintillion bytes a day, and commentators point out that most of the current volume of data was created in the last two years[475]. Also, data is of an unforeseen **variety**. Businesses have access to basic information about a person such as name, age, and gender, but also to detailed characteristics, running from health condition to daily and hourly location available via GPS.

The **veracity** of data refers to the trustworthiness of the information gathered. That is not to say data is necessarily false, it simply means to convey it can be misleading, either because it is outdated, or because it implies biases. Lastly, data is big when it can be gathered and processed in a speedy fashion. The **velocity** of data analysis is growing, which is essential in enabling its use for business purposes.

This conceptualization of big data is popular, but not uncontroversial. Commentators have argued that there is no real threshold with which to measure data in order to verify when it is "big"[476]. True as it may be, the

---

472 As per the Data Protection Act of 1988, revised in 2016.

473 Available at: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf> Accessed on: 2 nov 2016.

474 Some authors talk of five Vs instead of four, including variability (or sometimes value) among the characteristics. I will only consider four Vs as the relevant aspects raised by variability and value are, in my view, already encompassed in this definition.

475 STUCKE, Maurice E.; GRUNES, Allen P. **Big Data and Competition Policy**. Oxford University Press, 2016.

476 "It is not a precise scientific concept, but a highly contested idea that means different things depending on who is talking about it. There is, and will never be, any consensus on what "big data" means, nor on how its processing differs from the data analytical techniques of the past. There is no clear threshold at which point "data" becomes "big data." It is a highly fashionable, and therefore inherently suspect, idea that encompasses a complex array of technologies, practices and interests. "Big data"

idea of Big Data has gained ground. One of the factors that stimulated its popularization and growth was the massification of smartphones. There were around 7.4 billion mobile subscriptions in the first quarter of 2016, 63 million of which were new subscriptions, and the numbers are expected to reach 9 billion by 2021[477]. Smartphones are devices that carry people's lives around with them. They store an astounding amount of data, including the pictures one took, the contacts that person shares, the places she visited, her emails, SMS messages, the videos she looked up, the apps she downloaded. That information, which was complex and time-consuming to gather, is now available at the reach of one's hand in smartphones – and for businesses to use in the cloud[478].

With such an array of data available, it is to be expected that within the realm of Big Data, the variety of business is considerable. This article will concentrate in one specific type of online business that can be referred to as online advertising platforms (OAPs). By that expression I mean every company that carries its business online and relies on advertising to earn the biggest bulk of its profits[479].The advertising promoted by OAPs is of a particular nature because it makes use of personal data in an effective and intensive way.

The amount of data available to OAPs due to development of Big Data is tremendously vaster than the amount usually available to other businesses, even those that identified their strategy as "targeted advertising" long before the internet was economically viable[480]. OAPs monetize personal data as their main source of revenue, profiling users and selling targeted advertising as a result.

It comes as no surprise that after reaching such extraordinary levels, the usage of personal data, although profitable and often efficiency-enhancing, has

---

in and of itself means nothing, and signifies nothing, in the absence of a wider understanding of the organizations that are conducting the analysis, and an assessment of those organizations wider interests and motives." Colin Bennett, **Privacy Protection in the Era of "Big Data"**: Response to Office of Privacy Commissioner's Discussion Paper on "Consent and Privacy", p. 2.

477 Ericsson Mobility Report. Available at: <https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf> Accessed: 5 November 2016.

478 STUCKE, Maurice E.; GRUNES, Allen P. **Big Data and Competition Policy**. Oxford University Press, 2016.p. 29 – Smartphones as an example of how big data and privacy intersect.

479 Therefore, companies such as Uber and Amazon, which are usually associated with the expansion of Big Data, are excluded from this definition.

480 One example is the broadcast television market. Esther Gal-Or, Mordechai Gal-Or, Jerrold H. May, William E. Spangler, (2006) Targeted Advertising Strategies on Television. Management Science 52(5):713-725. It should be noted that some offline businesses do have access to immense amount of data, the primary example being the credit-card industry, but usually the data collected by such companies is protected by contractual clauses that to some extent prevent it from being used for advertising.

raised privacy concerns. Today's targeted advertising depends on zettabytes of data collected by OAPs, including everything from a user's friend list and the place where she lives, to her social security number and most liked books. If accessing such wide array of information allows for terrifically accurate search results, it also brings about some concerns.

Much like in Franz Kafka's "The Trial", the handling of personal data by private-owned enterprises is to a great extent nothing short of a black box. It is carried out by a largely inaccessible and somewhat non-accountable authority, which handles information in a rather obscure way, claimed to be beneficial to users, but never revealed to the public. Its gatekeepers are Silicon Valley billionaires and their team of experts.

Even if we assume these people to have the best of intentions, and trust their ability to forego financial interests for "the greater good" – considering they already have enough money for generations of Gates and Zuckerbergs – there still is strong disagreement about what that greater good should be. How much information should companies be allowed to have, or differently put, how much should users be allowed to give away? Should we protect users' privacy even when those users would gladly give their data away in exchange for free services? Are users even aware of precisely what they are giving away, and to what will be the commercial use of such data? Should we somewhat limit the way data is transferred among companies?

These and many other questions remain unanswered. It is not the goal of this article to present final answers for any of them, but it is my goal to provide some insight into how precisely one OAP has made use of personal data to monetize its business, and with that hopefully shed some light on how privacy considerations are to be inserted into future policy undertakings that aim to regulate the online advertising industry.

The Google Case

Back when Larry Page and Sergey Brin were Ph.D. students at Stanford University, they designed Google to be a revolutionary search engine. In Page's own words, their goal was, and still is, "to organize the world's information and to make it universally accessible and useful". Search remains the most famous of Google's interfaces (a proof of that is the mere fact that the word "google" is now a synonym for search, officially included in the Oxford English Dictionary as such). But the company grew tremendously and expanded to new areas, which

prompted its creators to reorganize it in the form of a holding in the year 2015. This holding is called Alphabet and its business include everything from email servers to mapping the Earth. Nevertheless, the bulk of Alphabet's revenue still comes from advertising. Out of the more than 90 billion dollars the company generated in 2016, approximately 87% came from the platform's ad services[481].

The jump from being a search engine to becoming an advertising platform was neither automatic nor uncontroversial. Page and Brin developed Google in order to offer a good product, but they had no predetermined business model that would allow the company to generate income. At one point, venture capitalists realized the company's potential and funded its initial undertakings, but investors soon started to wonder how the two former Stanford Ph.D.s would be able to turn a profit. Ideas on how to make money ran from licensing the algorithm and selling it to other internet businesses to going down the road already traveled by Yahoo! and placing advertising on Google's page, just as any other website would do. The problem for Google was the lack of stickiness of search – back then, online advertising was sold based on a webpage's ability to retain a given user for a long period of time, since ads where in display format and aimed at calling users' attention. Search, and particularly Google's search, was the exact opposite of that, the company offered users a fast result for a query and directed them to other webpages, which seemed to dismantle the advertising endeavor from the get-go.

It was largely the founders' obsession with the cleanliness of Google's search results, and also their distaste for annoying ads, that lead the company to a different path: the creation of AdWords. One of the key minds responsible for coming up with the functioning of AdWords was Eric Veach. Salar Kamangar, Google employee #9, was also a key participant in the process. Kamangar focused more heavily on the business model, while Veach was the mathematician behind the project[482]. The distinctive feature of AdWords is its ability to generate revenue while also allowing for results connected to the search query – and later to the page's content. It moves away from the display ad model towards a textual approach, and it has been laying Google's golden eggs for over a decade.

---

481 Data for 2015 is available at: <http://www.investopedia.com/articles/investing/020515/business-google.asp> Accessed on: 8 September 2016. Alphabet's Fiscal Annual Result for 2016 show that advertising is the primary source of revenue for the company: <https://abc.xyz/investor/pdf/20161231_alphabet_10K.pdf > Accessed on: 5 March 2017.

482 A brief overview of the story is available at: <http://www.bloomberg.com/news/articles/2006-03-05/the-secret-to-googles-success> Accessed on: 14 October 2016.

AdWord

AdWords is Google's platform for advertisers. It is responsible for offering ad space in exchange for payments and it functions as a fairly elaborated auction.

It should never be underemphasized that the specific type of auction developed by Google for AdWords has been so immensely successful that commentators have gone so far as to name the underlying process the "Googlenomics"[483]. The development of this auction process has taken years to perfect and involved dozens of people[484]. It goes way beyond the scope of my analysis to fully scrutinize its functioning. Nonetheless, my goal is to give a fairly comprehensive outline of AdWords, focusing on how it depends on users' personal data in order to properly function[485].

What advertisers pay for at AdWords is ad space. Such space is distributed so that ads may be placed: (i) in a search results page (which is what happens when a user types a search query into Google Search), (ii) in a page pertaining to Google's search partner network, a network of websites that incorporates Google Search onto their webpages, or (iii) in any random website which chooses to be a part of the Display Network, a system that pays the website for showing AdWords results[486].

Since the system functions as an auction, there is competition among advertisers to determine how the ads will be selected. Such choice will take place owing to several factors, but it is largely related to the keywords typed by the user – in case of searches – and to the content of the webpage – in case of the Display Network (and of several Google-owned websites such as Gmail and YouTube), as well as to the specific kind of user those advertisers aim at.

---

483 LEVY, S. The Secret of Googlenomics: Data-Fueled Recipe Brews Profitability. **The Wired**. September 22, 2009.

484 A complete account of the building and functioning of AdWords is provided by Stephen Levy in his book "**In the Plex: How Google Thinks, Works, and Shapes Our Lives**" (2011).

485 It should also be said I will build my analysis based primarily on materials provided by Google itself, to avoid second-hand reading as much as possible. Google has a platform where it provides users (and specially advertisers) information on AdWords: <www.support.google.com/adwords> Accessed on: 5 March 2017. Whenever I use quotation marks and do not specify where they came from, the source is this platform.

486 That is called AdSense. The functioning of AdSense will be described in a separate section.

AdWords was not always as it is today. It started out as a two-tiered system, composed of the Premium and Select versions. As Steven Levy puts it:

> Google's ads were always plain blocks of text relevant to the search query. But at first, there were two kinds. Ads at the top of the page were sold the old-fashioned way, by a crew of human beings headquartered largely in New York City. Salespeople wooed big customers over dinner, explaining what keywords meant and what the prices were. Advertisers were then billed by the number of user views, or impressions, regardless of whether anyone clicked on the ad. Down the right side were other ads that smaller businesses could buy directly online. The first of these, for live mail-order lobsters, was sold in 2000, just minutes after Google deployed a link reading see your ad here[487].

With time, Google shifted strategy and decided to expand the auction system to encompass AdWords Select. The auction was initially only available for search results. The reason is straightforward: search results are an "easy" way to effectively select your audience and they do not require much from the platform. The user types keywords, the platform sells ad space based on those keywords, and that is the end of the story[488]. Google's job is to capture that information already provided by the users and monetize it. The idea sounds terribly simple, but the ability to effectively match users and keywords is one of the reasons why Google was the undisputed leader in online advertising for quite some time.

In its efforts to gain more ground, Google introduced the Display Network (DN) as a part of AdWords. In the company's own words

> [t]he Adwords Search Network reaches people when they're already searching for specific goods or services. The Display Network helps you capture someone's attention earlier in the buying cycle. For example, if you run an art supply store, you can catch a mom's eye when she's reading reviews about the best brands of washable paints, but before she puts her toddler in the car seat and heads out to buy.[489]

---

487 LEVY, S. The Secret of Googlenomics: Data-Fueled Recipe Brews Profitability. **The Wired.** September 22, 2009.

488 Google was not the first to figure this out. GoTo, later renamed Overture, had done so before, by introducing pay per click and auction advertisement. But GoTo's CEO, Bill Gross, never patented any of those inventions. Moreover, the company's business model relied on ranking ads without taking quality into consideration, mixing organic search results and advertisement, and requiring bidders to pay the price they submitted in the auction, incentivizing bid shading. See footnote 21 for more on optimal bidding strategies.

489 Available at: https://support.google.com/partners/answer/2404190?hl=en-AU

Leaving aside the claim that people in the search network are already searching for goods and services, with which I disagree for reasons exposed elsewhere[490], it is worth turning to why Google decided to expand its business in such a way. The expansion was only possible because Google dramatically increased the amount of data collected from users and the places within the internet where it collects such data from.

The DN does not offer traditional brand advertising[491], it goes much further than that. It matches users' online behavior to advertising opportunities outside of the typical search result page. For that reason, the DN functions rather differently than the traditional Search Network and they will be described separately.

The Search Network

Advertisers on the Search Network buy ad space from Google choosing among keywords they believe to have some relevance for the substance of their ad. For example, a shoe store will probably select keywords such as "tennis shoes" and "sneakers" for its ad, whereas a beer retailer might prefer words such as "bbq drinks" and "cheap beer".

Among the advertisers that select the same keywords, Google determines who gets to be ranked higher and more prominently in its pages using Ad Rank. According to Google, "Your Ad Rank is a score that's based on your bid, auction-time measurements of expected CTR, ad relevance, landing page experience, and the expected impact of extensions and other ad formats." Let me break down each of these variables.

---

490 MATTIUZZO, M. **Propaganda Online e Privacidade – o varejo de dados pessoais na perspectiva antitruste**. SEAE 2014. See also GOLDFARB, A.; TUCKER, C. **Substitution Between Offline and Online Advertising Markets**, 2011.

491 Traditional brand advertising involves raising brand awareness. It entails bombarding potential consumers with information about the brand, in several different situations, not necessarily connected to a specific selling opportunity. A brand that heavily and consistently invests on brand advertising is Coca-Cola. Coca's strategy of placing billboards in highways, full-page ads in the newspaper, etc., is not intended to make the potential customer immediately stop what she is doing in order to purchase the product, but to make the consumer aware of the product, so that when she is faced with the decision of buying a beverage, she chooses a Coca-Cola instead of something else. Brand advertising can focus on several strategies by associating a brand with a number of different scenarios or moods. For my purposes here, what should be noted is that it is different from what Google offers to most of its advertisers.

is the maximum price an advertiser is willing to pay for the ad. Google offers two different bid strategies for the Search Network: CPC and CPA[492]. The Cost-Per-Click (CPC) strategy is the one by which advertisers pay only when their ads are effectively clicked on by the users. Under this strategy, each advertiser determines a "max CPC" (or maximum Cost-Per-Click), which is the maximum price it is willing to spend on an ad. The max CPC is not necessarily the amount the advertiser will effectively pay, since the final value will depend on other potential buyers' bids. The model is a variation of the second-price sealed-bid auction, also known as Vickery auction: the price paid is not the winner's bid price, but however much is necessary for him to maintain his position as the winner. If the only consideration to be taken into account were the bid price, then Google would charge the winner the second-best price. (If User P bids $10, User L bids $6, and User M bids $2, User P will win and pay $6.)[493] This is however *not* the real price paid by the advertiser, as the final price is calculated depending on the final Ad Rank, which will be further explained below.

The Cost-Per-Acquisition (CPA) is a strategy focused on conversions. A conversion is an action other than a click made by a user after viewing an ad. It can be anything from the subscription to a mailing list to a purchase. Unlike in CPC, Google does not charge users for each conversion, it rather finds what the AdWords algorithm believes to be an optimal CPC bid whenever the ad is eligible to appear. The advertiser chooses the "target CPA" and Google's job will be to get as many conversions as possible with that given amount. To do so, Google needs two things: first, historical information about the ad. Second, a way to track conversions.

---

492 Google also allows for Cost-Per-Thousand Viable Impressions, which will be covered in the next section.

493 Google certainly designed this strategy based on auction theory. The company soon realized it makes more money by adopting a Vickery-type auction than by charging the max CPC from the winner (which would represent a first-price sealed auction). The strategy seems senseless at first glance, as the company would make more money if it simply charged User P in my example the $10 it is willing to pay. But by charging the second-best price the company prevents advertisers from bidding too low (or bid shading) and bringing overall prices down. Essentially, the Vickery model creates an equilibrium in which the optimal strategy is to "tell the truth" and provide each bidder's real valuation for the good being auctioned. An overview of auction theory that explains these equilibria in detail is KLEMPERER, Auction Theory – A Guide to the Literature. A study focused on Google's practices is provided by VARIAN, Position Auction.

It should be noted, however, that some scholars have raised questions as to precisely how adherent to Vickery auctions Google's practices truly are. Edelman, Ostrovsky and Schwarz argue that the Search Network runs a "generalized second-price auction", in which equilibrium is not reached by bidding true valuation. Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords.

CPA is significant for my purposes because in order to track conversions an advertiser needs a "tag" on her website. It is "[t]his tag [that] will place a **cookie** on a user's computer or mobile phone when he or she clicks your ad. If the user reaches one of your conversion pages, AdWords looks for the cookie and records a successful conversion for you." In other words, Google is no longer relying on data that a user directly entered into the search tool, it is rather following the user around the web to see how she behaves after exposure to an ad. That way it can provide a more useful and complete targeting strategy for advertisers[494].

is the bundle of measurements used by Google to determine the relevance of an ad to the user. It encompasses:

1. Expected clickthrough rate	The likelihood that an ad will be clicked
2. Ad relevance	How closely the ad matches the intent behind a user's search
3. Landing page experience	How relevant, transparent and easy-to-navigate the page is for users

The Click-Through Rate (CTR) "measures how likely it is that your ads will get clicked when shown for that keyword, irrespective of your ad's position, extensions, and other ad formats that may affect the visibility of your ads". In other words, if users click more on Ad A than on Ad B, Ad A will have a higher CTR.

The relevance of an ad to users is a tricky concept, as there is much debate about the usefulness of ads, and also considering the subjectivity of usefulness. But in Google's own words "[t]his status describes how well your keyword matches the message in your ads. For example, if someone searches for your keyword and your ad shows up, would your ad seem directly relevant to their search?".

Relevance, other than being measured in absolute terms, can also be tailored to specific audiences or individuals. That is to say that Google built into the algorithm a feature that allows ads to have more relevance when they are believed to be particularly suited to a person, given this person's profile. Google's privacy policy explains that the platform may show a user who is searching for "vacation" and earlier searched for "bike" ads related to biking while on vacation, which will probably not happen to those who search for "vacation"

494 I will refrain from any judgement on the practices carried out by Google, and I urge readers to do the same. My goal now is solely to explain, as best as I can, what the platform does in order to make a profit. A reader should not understand this statement, or any other in this part of the text, as revealing of my approval/disapproval of the company's strategy.

and had earlier looked for "movie theaters"[495]. This is but one example of how data can be used to personalize the ad experience, but there are many others. Google can pull data not only from Search, but also from YouTube, Gmail, and partner sites to personalize ad experience. Since changes in the use of personal data for advertising have recently been introduced by the company, they will be explored in more detail in item "My Activity" below.

The landing page is the page where the user is directed to once she clicks the ad. When measuring this variable Google is interested in the experience the page provides to users and in its relevance given the search terms provided. Google's Chief Economist Hal Varian states that a good landing page is relevant, provides original content, is easy to navigate and transparent.

refers to additional information placed in an ad, such as phone numbers, e-mail, address, etc., which can somewhat reveal more about the business and as such increase the final score in the auction.

The higher a given ad ranks according to these variables, the better it will be positioned in a search result page. Google does not disclose the specific weight of these variables and uses a blind system to determine final positioning – it does not reveal advertisers how much others are bidding, nor other advertisers' quality scores or extensions/formats. However, it does disclose the advertiser's Ad Rank – the weighing of bid price, quality, and ad extensions/formats. As mentioned, the final price paid by the advertiser will be however much is necessary for her to maintain her position as the first in line. See Table 1 below for an example provided by Google[496]:

Table 1

Bidder	*Bid*	*Quality*	*Format Impact*	***Ad Rank***
Blue	$4	Low	N/A	**5**
Green	$3	High	Low	**15**
Yellow	$2	High	High	**20**
Red	$1	Medium	Medium	**8**

495 Available at: <https://privacy.google.com/how-ads-work.html?modal_active=how-ads-work-proof-overlay&article_id=c4-p-search-ads-1> Accessed on: 27 October 2016.

496 Insights on the AdWords Auction. Available at: <https://www.youtube.com/watch?v=PjOHTFRaBWA> Accessed on: 24 October 2016.

What determines the order in which ads will appear is the result in the last column, Ad Rank. This means that, in this example, Yellow will be placed first, followed by Green and Red – assuming there are three positions available. Blue, despite having the highest bid, will not be displayed. Moreover, Yellow will not necessarily pay $3 – which is the second-highest bid, it will pay however much it needs in order to maintain its Ad Rank above 15. The same holds true for Green, which needs only to keep its Ad Rank above 8, and for Red, which should maintain Ad Rank above 5.

There is no way of knowing exactly how much these bids will be. Experience has shown that Yellow will likely pay less than its bid price, but only the algorithm can tell the exact numbers. Despite the lack of full transparency, it is undisputable that Google tries to rank its ads owing to relevance, not simply based on how much advertisers are willing to pay for it. That indicates the company is effectively interested in showing users more useful ads – which is not only a symptom of benevolence, rather a consequence of the payment model, as Google's profit to some extent depends on whether the ads are clicked on by users. Nevertheless, this indicates strong concern with how annoyed users become with the ads shown by the platform. In the words of Anastasia Holdren when describing AdWords and its functioning:

> AdWords works because it doesn't seem like advertising. To Google's credit, the displayed advertising results are extremely relevant to the searcher's query. Ads are displayed at the moment someone is looking for something and presented as potential solutions to their search. This relevancy is the key to the effectiveness of the system for both searchers and advertisers[497].

As mentioned, the concept of relevance in advertising is contestable, but the statement by Holdren is revealing. She stresses how AdWords is a revolution of sorts because it turns ads into "solutions" to problems or requests by users[498]. This understanding of "ads as solutions" is entirely dependent on the OAP's reliance on personal data, and its ability to match users and advertisers.

What should be added is that Google's organic search results – the results that are not determined by the bid process, rather by a different Google

497 HOLDREN, A. Google AdWords. **O'Reilly Media**, Inc. 2011. Introduction to Google AdWords.

498 She is not alone in that statement, see JACOBSON, H. Google AdWords for Dummies. Wiley, 2009. How to Think Like a Prospect. "In the Magic Yellow Pages, you don't have to flip through hundreds of pages. In fact, the book doesn't *have* any pages — just a blank cover. You write down what you're looking for on the cover, and then — Poof! — the listings appear. The most relevant listings, according to the Magic Yellow Pages, appear on the cover. Subsequent pages contain more listings, in order of decreasing relevance."

algorithm intended to provide the best result for the search query – cannot be bought by advertisers. The algorithm, and the algorithm alone, determines the ranks of pages, and though some companies heavily invest on moving their pages up on the organic search, they do so without paying Google off[499].

Display Network and AdSense

The Display Network and AdSense are essentially two sides of the same coin. The DN is the advertiser platform, whereas AdSense is the website-owner interface – or as Google prefers to call it, the publisher. Both are brought together – and combined with DoubleClick Ad Exchange – to create a market for online advertising[500]. Any website that offers advertising space can be a part of AdSense free of charge. On the other hand, to be able to place ads at the DN advertisers use a platform similar to the AdWords Search Network and must pay for Google's services.

The two main differences between the Search Network and the Display Network regard the format in which ads are presented and the way those ads are selected by the advertiser and by the platform. Display allows for ad formats other than text, including images, videos, and rich text, whereas Search only accepts text. More importantly, ads for the DN are selected based not only on keywords, but also on topics, audiences, and placement.

Google offers three methods for targeting ads in the DN: (i) contextual targeting – focused on the traditional keywords and on topics (which are the themes a given webpage is related to, such as sports, fashion, electronic equipment, etc.); (ii) audiences – focused on the users she intends to reach, the advertiser may select according to interest categories, remarketing and demographics (meaning the advertiser can either choose an user specifically

499 There are antitrust investigations in several jurisdictions that try to prove this is not entirely accurate and that Google may have altered the algorithm to privilege some websites in organic search. The allegations, however, focus on Google's alleged attempt to leverage the dominant position in search onto other markets. There is no allegation that Google somehow accepts money for better positioning.

500 To be perfectly accurate, DN is wider than AdSense. It also covers DoubleClick Ad Exchange and the Google websites. Ad Exchange is a different platform, also owned by Alphabet, that has a separate bidding process and different functionalities. The reason why I will not get into details about Ad Exchange is simple: any advertiser who chooses the DN to display its ads automatically has access to all Ad Exchange websites that comply with AdWords's guidelines. Moreover, Google controls the auction process so that the comparison between Ad Exchange bids and AdWords bids is normalized. To understand more about Ad Exchange and how it differs from AdSense: <https://support.google.com/adxseller/answer/4599464?hl=en>. Accessed on: 5 March 2017.

interested in the content of her ad, an user who has already visited her website before, or a user part of a gender or age group); and (iii) placement – which allows the advertiser to either exclude or target specific websites and apps.

Other than being selected by the advertiser owing to different criteria, the platform selects ads to be shown at the DN in a different way. The overall parameters are the same, meaning an ad will appear depending on the calculation of the Ad Rank, but the way in which bids can be cast differs, and so does the effective price advertisers pay for the placement.

First, regarding . Other than the traditional CPC and CPA, advertisers may also choose the Cost-Per-Thousand-Viewable-Impressions (vCPM). vCPM is a strategy focused on impressions, as the name suggests. From the options provided by Google, this is the one that most closely resembles brand awareness. The advertiser will not pay for the ad when a user clicks on it, rather when the user sees it in a webpage[501, 502].

Second, with reference to , Google introduces some variations that aim at making the results fairer, since payment on the DN depends heavily on incremental clicks[503].

To understand incremental clicks, one must remember Google will not always face a dilemma of either showing the ad or not showing it. The platform has several placements available and it can decide to show both ads, but also to place them so that the winner is more visible.

Because different placements can render different amounts of clicks, Google does not charge the same price for both advertisers when it shows both ads, it charges the winner more based on the incremental clicks it will enjoy from being better positioned in a page.

Imagine two ads, ß and μ. Both ads rank high enough so that the platform decides to show them both. ß bids $10 and μ bids $5, both are of equal quality, making ß the overall winner who will enjoy better positioning. How should Google charge ß?

501 Google has a way of measuring views, called the Active View. The definition of a "viewable" ad is the following: "An ad is counted as "viewable" when 50 percent of your ad shows on screen for one second or longer for display ads, and two seconds or longer for video ads."

502 The competition between CPC and vCPM bids is corrected by Google to avoid comparing apples and oranges. The platform does so by calculating an expected click-rate for every 1,000 impressions, instead of the usual clickthrough rate.

503 It can also depend on service fees for audience targeting, if that is the chosen method.

What the company does is divide payment according to the so-called incremental clicks. Because of the more favorable positioning, ß is clicked on ten times for every eight clicks for μ, meaning there are two incremental clicks for ß that should reflect the price paid by the advertiser. Assuming the result rested solely on bid prices[504], ß would pay $5 for those two clicks and the same price as μ for the remaining eight. Imagining the third place on the auction went to Ω, who bid $4 and was not selected to be shown, ß would pay $4 for the remainder of the clicks.

In this example, considering a total of ten clicks, ß would pay ($5 x 2) + ($4 x 8) = $42.

To highlight the difference between the DN and the Search Network, one can imagine what the final price for ß would be if the ad was placed in search. If there were two available placements and the bids followed the exact same pattern, ß would win and pay $5 for each click. μ would also be shown, though in the less visible position, and pay $4 per click. There would however be no comparison between incremental clicks for ß and μ, meaning the price would remain constant and depend solely on clicks or conversions. ß would then pay $5 x 10 = $50 for every ten clicks/conversions [505].

As mentioned, the DN relies not only on Google's own platforms, such as YouTube and Gmail, it also includes third-party websites. Those websites are part of AdSense, a vast network reportedly encompassing 90% of the Internet[506] and governed by a set of policies put forward by the platform[507,508]. From those policies, the one that is particularly relevant for my purposes regards advertising cookies.

---

504 Again, it does not. The final Ad Rank encompasses ad quality and extensions/formats. Nevertheless, simplifying the analysis in this regard is effective and sufficient to clarify the workings of the platform.

505 The problem earlier identified by Edelman, Ostrovsky, and Schwarz apparently does not exist here. Because the Display Network internalizes incremental clicks in its charging mechanism, advertisers' best strategy truly is to bid true valuation.

506 Signing up to AdSense is free of charge. The way Google makes money by use of this tool relies on sharing the revenue from the ads placed on a publisher's webpage. The platforms gets 32% and the publisher retains the remaining 68%.

507 The DN also includes DoubleClick Ad Exchange. Ad Exchange is a different platform, also owned by Alphabet, that has a separate bidding process and different functionalities. The reason why I will not get into details about Ad Exchange is simple: any advertiser who chooses the DN to display its ads automatically has access to all Ad Exchange websites that comply with AdWords's guidelines. Moreover, Google controls the auction process so that the comparison between Ad Exchange bids and AdWords bids is fair.

508 AdSense program policies include everything from limitations on clicks and impressions – the third-party websites, which Google refers to as publishers, may not click their own ads to inflate impressions or clicks – to copyright law – more specifically, Google reserves the right to pull the page from AdSense if it receives notice that the publisher is in violation of the Digital Millennium Copyright Act.

If Google lets advertisers target specific audiences, it must be able to properly profile such audiences, creating well specified groups to attract the advertisers who will extract value from tailored eyeballs. That is why to be part of AdSense a website must abide by a privacy policy that "discloses that third parties may be placing and reading cookies on your users' browsers, or using web beacons to collect information as a result of ad serving on your website[509]."

Cookies and beacons are both mechanisms that allow for some form of user identification or tracking. A beacon is an image, usually transparent, placed in a website to track the way such website is navigated. Unlike cookies, beacons do not store any identifiably personal information about a user. A cookie, on the other hand, is a text file placed in a user's browser by a webpage, aimed at tracking traffic through that page[510]. It is assigned to that individual user, meaning the website can "remember" her whenever she comes back, which significantly increases the user experience, helps to improve the site, and is also naturally useful for advertising purposes.

Cookies can be first-party or third-party. First-party cookies are placed on the browser by the website the user is visiting, whereas third-party cookies are placed by other websites – a common use for third-party cookies is precisely advertisement[511]. Having a wide set of third-party cookies placed in a range of different websites is what allows Google to create user profiles.

In short, Google requires access to users' behavior on a publisher's website to give access to AdSense. It is worth noting, however, that ever since this system has been in place – and especially after DoubleClick's acquisition in 2007, which significantly broadened the scope of third-party cookies under Google's control – the company has kept the first-party and third-party cookies database apart. In other words, though Google had access to a lot of personal information about its users, it never sold advertisement customized to specific individuals, just to specific "groups of data".

509 As per the AdSense program policies, available at: <https://support.google.com/adsense/answer/48182?hl=en>. Accessed on: 5 December 2016.

510 For more on cookies, see: <https://www.google.com/policies/technologies/cookies/> Accessed on: 5 December 2016.

511 As Hoofnagle, Behavioral Advertising: The Offer You Cannot Refuse (2012) point out, "The privacy problem from cookies comes from the aggregation of this tracking across different websites into profiles and through attempts at linking this profile to the user's identity. By tracking these identifiers across websites that users visit, advertisers can infer users' interests, perhaps sensitive ones, such as medical conditions, political opinions, or even sexual fetishes."

While Google requires from advertisers that they the transmit users' data, it also requests its partners to do so under some conditions. The information provided cannot be accompanied by usernames, passwords, email addresses, and any other personal identifiable information. Failing to comply with this rule is cause for exclusion from AdSense. Google always claimed it intends to sell relevant ads for a user, but it does not need to know who that person really is. The goal is to reach the 25-year-old runner, who lives in the countryside of Brazil and likes to jog in the morning, by providing her with ads for sneakers, but there is no need for Google to know that person's name, address, or social security number[512].

This paradox is the reason why Google had such a hard time explaining how it uses Gmail to target advertising. There is no individual in California who reads the messages and decides which user likes (or could potentially enjoy) specific products, the company uses robots and scans the messages for keywords that will enable targeted ads – but it should come as no surprise that users had a hard time coming to terms with the idea[513].

On June 2016, the panorama described above changed. When MyActivity was introduced, Google modified its privacy policy and establish a new way to sell advertising, by mixing data collected in its own platforms (Gmail, YouTube, Maps, etc.) and information acquired via third-party cookies.

MyActivity and the Rise of Personalized Web Targeting

As the Ad Rank clearly determines, personal data plays a decisive role in monetizing the Search and Display Networks. In Search, personal data used to target ads is primarily the information the user types into the platform. In the DN, that information is also the users' online behavior and demographics. But the information Google collects on users' is much vaster than that, though the company has long kept much of it out of reach from advertisers.

Because of the services Google provides, such as Gmail and Maps, and the array of websites that provide third-party cookies information to the DN, the company has a database that arguably encompasses sufficient information about a person to identify her name, address, work, political views, friends,

512 Arguably, it is also a feature Google implemented in order to protect itself from requests by national security and police authorities.

513 Google's Privacy Policy states: "Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection."

hobbies (including the ones she would not care to share with others), where her friends live, at what time she regularly goes to bed, which road she most frequently takes to get to work, and even her health condition.

Google highlights that it does not sell personal data, it only uses that data to target ads. What it does sell is ad space, commercialized owing to personal information. The company also emphasizes that the auction process is entirely automatized and no human being actually reads emails, checks demographic data, or verify users' search history in order to place ads. The algorithms are responsible for running robots through each users' information and coming up with Ad Ranks.

In August 2016, however, the rules for targeting changed. The company had long resisted the trend, set primarily by Facebook, of combining personal information and advertising. But now, according to the new privacy policy, the "[i]nformation we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account"[514].

Users connected and logged into one of Google's services will have their information collected and used for advertising, unless they opt-out by changing their preferences in MyActivity.[515] The concern, from a fundamental rights standpoint, is most users have the tracking mechanisms activated without understanding what changed and what the consequences for their privacy would be. In June, Google launched MyActivity, but no comprehensive explanation about the modifications and their potential risks was detailed. The move prompted two consumer groups to file complaints with the United States Federal Trade Commission (FTC), claiming it to be "deceptive"[516].

MyActivity is a central that gathers and controls all activity by a user who is logged into Google's services. The categories of data collected by Google are: (i) Web & App Activity – includes searches and browsing activity, ranging from search history to recent apps[517]; (ii) Location History – a map of everywhere you

514 Available at: <https://www.google.com/policies/privacy/#infocollect>. Accessed on: 5 December 2016.

515 The use of tools such as VPN or Tor will also affect data collection. Since these mechanisms are not the norm and their use, though relevant, is still very limited when compared to the bulk of people who access one of Google's services every day, I will ignore their effect.

516 Available at: <https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking> Accessed on: 29 December 2016.

517 According to Google, the information saved as Web & App Activity includes: "Searches and other things you do on Google products and services, like Maps; Your location, language, IP address, and whether you use a browser or an app; Ads you click, or things you buy on an advertiser's site; Information on your device like recent apps or contact names you searched for; Websites and apps you use; Your activity on websites and in apps that use Google services; Your Chrome browsing

go with any of your devices[518]; (iii) Device Information – contacts, calendars, music, as well as information about the device itself[519]; (iv) Voice and Audio Activity – commands you give your device, as well the frequency with which you tap the microphone icon[520]; (v) YouTube Search History; and (vi) YouTube Watch History.

MyActivity also allows users to decide to keep these categories of data collection activated or paused. A user who pauses collection can make use of services and not have her data stored. A user who does not pause collection allows Google to use that information to make the services more accurate and possibly more useful, and also to sell advertising.

Final Remarks – The Impact of Business Models on Personal Data Regulation

Personal data is an asset for many companies, and particularly for those which, like Google, center their business model on online advertising. The tension between users' privacy and companies' interests has led to regulatory efforts in many jurisdictions, aimed at preventing abuses and controlling the ways and ranges by which personal information is collected and how it is processed and used for commercial purposes[521].

---

history." Accessed on: 15 January 2017. Available at: <https://support.google.com/websearch/answer/54068?p=web_app_activity&hl=en&authuser=0&visit_id=1-636200982761610875-3253655500&rd=1> Accessed on: 5 December 2016.

518 Google mentions five categories of information included in Location History: "Quality and length of your connections to cell networks, GPS, Wi-Fi networks, or Bluetooth; State of your location settings; Reboot occurrences and crash reports; Apps used for turning Location History on or off; Battery levels".

Available at: <https://support.google.com/accounts/answer/3118687?visit_id=1-636200986127793708-3253655500&p=location_history&hl=en&rd=1> Accessed on: 15 January 2017.

519 The information about a device can include the activity on your screen (whether or not it is on), the battery level, the quality of Wi-Fi or Bluetooth connection, touchscreen and sensor readings, and crash reports. Available at: <https://support.google.com/accounts/answer/6135999?p=account_device_info&hl=en&authuser=0&visit_id=1-636200987855038708-3253655500&rd=1>. Accessed on: 15 January 2017.

520 As Google states, audio may be saved even when you are offline. Available at: <https://support.google.com/websearch/answer/6030020?p=account_voice_audio&hl=en&authuser=0&visit_id=1-636200991416533018-3253655500&rd=1>. Accessed on: 15 January 2017.

521 The rise of regulation cannot be solely attributed to the private sector's use of personal information, but that certainly was a factor in the passing of legislation. Other relevant circumstances include the collection of data by the government itself and the complexification of the digital environment.

The new model put forward by Google through MyActivity gives users control over what type of personal information is to be stored and used by the company. It is a solution clearly based on a self-regulatory model, in which users are free to do with personal data as they see fit – under these assumptions, data is to some extent understood as property. Whether or not this method is the best solution for the problem is a discussion for a different article, but what cannot be denied is that tools such as MyActivity require a considerable degree of digital education and engagement from the part of the user, as they assume the individual to have knowledge not only about herself and the data she produces, but also about the platform and how it processes her information.

Another debate regards the fit of this model to personal data regulation around the world. It is true that from the outset a surprising degree of convergence was observed in personal data regulation in many countries, which adopted similar principles in regulating the matter[522]. However, significant differences do exist, especially in terms of implementation. Google apparently has adopted a method that, as mentioned, is well-suited for a self-regulatory approach such as the one put forward by the United States. But not all jurisdictions have followed this trend. Countries with regulation more closely associated with the European model have a different take on privacy matters and particularly on the implementation of personal data protection[523]. It remains to be seen how they will deal with Google's new privacy policy.

The businesses that rely on Big Data are growing in relevance and expanding their services. Hence, personal data issues are bound to increase. Due to the fluidity of this market and the fast-pace of technology, one should question not only if the current regulation is equipped to deal with today's problems, but also if it is sufficiently flexible to address the challenges that will arise from the development of technology and from new business models.

¿SU DINERO O SUS DATOS?

522 BENNETT, C. J. **Regulating Privacy: Data Protection and Public Policy in Europe and the United States**. Cornell University Press, 1992. p. 95-115.

523 NEWMAN, A. L. **Protectors of Privacy: Regulating Personal Data in the Global Economy**. Cornell University Press, 2008. p. 23-41.

La Ecología Criminal y la Desorganización Social

Márcio Ricardo Ferreira[524]

Introducción

La constante y vertiginosa evolución de las nuevas tecnologías de la información y de la comunicación nos ha introducido en un mundo novedoso, diferente y mucho más complejo de lo esperado. Parece evidente que la nueva configuración social y la difusión de la información tiene una repercusión directa sobre los nuevos comportamientos delictivos. Así que, en primer lugar, desde una perspectiva puramente ontológica, se han de tratar las características de la nueva sociedad surgida posteriormente a las revoluciones modernas. Pero principalmente, analizar de que manera este proceso de desarrollo ha culminado en riesgos capaces de comprometer las condiciones básicas de vida a través del proceso de modernización tecnológico.

Por otro lado, cabe señalar los delitos usuales y las nuevas oportunidades delictivas, para entonces observar si el Clásico Derecho Penal basado en mecanismos tradicionales y obsoletos está (o no) preparado para enfrentar el nuevo paradigma de la Macrocriminalidad Inmaterial en el Ciberespacio. Igualmente, serán analizadas las exigencias de lidiar con la complejidad de cuestiones globales de los problemas presentados por las Nuevas Tecnologías de la Información y la Comunicación a los órganos de control. Todas estas observaciones, sirven para intentar explicar de que manera el crecimiento descontrolado de las nuevas tecnologías influyeron en las estructuras sociales. Hecha estas consideraciones, el estudio parte para la cuestión central del tema, la extorsión mediante secuestro virtual de datos personales. En particular, intentar descubrir porque el *RANSOMWARE* se ha convertido en uno de los virus más rentables de la historia, con potencial para

524 Doctorando en Derecho Penal por la Universidad de Salamanca – (España). Maestría en Ciencias Jurídico-criminales por FDUC - Facultad de Derecho de la Universidad de Coimbra (Portugal); Postgrado en Derecho Penal y Procesal Penal por la UBA - Universidad de Buenos Aires – (Argentina). E-mail: f.marcior@usal.es

generar disturbios masivos entre la población civil y provocar daños irreparables en los sistemas integrados de datos a través de la extorsión y el chantaje.

Por fin, delante de todos esos factores, en orden de desarrollar la reflexión sobre la vertiente ética de esta nueva revolución, se planteará como justificativa para el crecimiento de la delincuencia informática, la problemática de la desorganización social en internet vivida por la sociedad actual. Sobretodo, ofrecer una respuesta para el comportamiento de las personas en red, haciendo frente a las consecuencias que generan estos tipos comportamentales en el índice de criminalidad.

La globalización y los cambios sufridos por la sociedad desde las revoluciones modernas

El objetivo final de Internet es el de apoyar y mejorar

nuestra existencia en red en el mundo.

Tim Berners-Lee

Una nueva configuración social ya fue iniciada, tal vez la más grande de todas las revoluciones. La Globalización, fue responsable por la gran difusión de los conocimientos científicos e innovaciones tecnológicas en los últimos tiempos, asintiendo adelantos en la salud, la educación y el trabajo. "Hay un flujo antes inimaginable de informaciones, de ideas, de conocimientos tecnológicos y científicos, bien como de capitales al alrededor del planeta"[525].

La información ha constituido un recurso absolutamente básico para el desarrollo mundial, este fenómeno ha traído un cambio radical en las condiciones básicas de vida, gracias a las posibilidades de acceso, manipulación y control de la información. Pero mucho más que un aumento en la expectativa de vida, la globalización ha facultado al hombre acceder a la información de forma veloz, permitiendo que los países desarrollasen un sistema de intercambio global, no solo de bienes, sino también, de servicios y tecnología.

Estas transformaciones son resultado del conocimiento técnico-científico experimentado sobre todo, desde la Guerra Fría, sintetizada en la revolución tecnoló-

525 SARCEDO, Leandro. **Política Criminal e Crimes Econômicos – uma crítica constitucional.** São Paulo: Alameda, 2012, p.74.

gica. De acuerdo con Baumer[526], ese cambio, todavía tímido en el siglo XVII, efectivamente se aceleró en los siglos XIX y XX, considerando especialmente las grandes revoluciones de los tiempos modernos, como la Revolución Francesa, la Revolución Industrial y la Revolución Tecnológica. En otras palabras, hubo un fuerte cambio en la estructura social, acelerando el ritmo de vida con nuevos e innumerables estímulos. De hecho, la estructura actual del mundo globalizado ha traído innegables avances a los medios de comunicación, de transporte, de servicios y de información. Sin embargo, si por un lado el desarrollo de conocimientos técnicos y de la ciencia permitió al hombre controlar y protegerse de los fenómenos de la naturaleza, por la otra, el proceso de socialización y los desarrollos recientes en el campo de tecnologías acabó resultando en otros tipos de amenazas[527].

Dicho de otra manera, eso proceso de modernización gradualmente dio lugar a riesgos capaces de comprometer las condiciones básicas de vida a través del desarrollo, creando una especie de auto-destrucción, que llevó la sociedad actual a consecuencias negativas generadas por el propio proceso de modernización tecnológica.

Estos son algunos de los aspectos que lleva a reflexionar la Política Criminal actual y la utilización de las TIC´s[528], teniendo en cuenta que la tecnología es una de las bases para el progreso (o no) social. Un buen ejemplo, es la fusión de la robótica, que tuvo un efecto devastador en el mercado laboral mundial, que resaltó las diferencias entre ricos y pobres. A lo largo del siglo XX, las máquinas han sustituido a los hombres no sólo en tareas mecánicas, sino también en trabajos cognitivos. Las máquinas están suplantando poco a poco los trabajadores humanos en un espectro de oficios hasta poco inimaginable. Desde la conducción de coches hasta las tareas domésticas, los robots se ocuparon de muchos puestos de trabajo. El impacto que la *Inteligencia Artificial* tuvo en la sociedad y el mercado laboral en los últimos años fue descomunal. "Todo lo que pueda ser automatizado, se automatizará". Las habilidades humanas que las máquinas pueden reproducir a bajo coste se van a multiplicar por el efecto de la

526 BAUMER, Franklin. **O Pensamento Europeu Moderno.** Volume I, séculos XVII e XVIII. Lisboa: Edições 70, 1990, p.37.

527 En este sentido, cuanto más avanza la modernización, más aún las sociedades se quedan hundidas, consumidas, modificadas y amenazadas en sus bases, que puede muy bien ocurrir sin reflexión, superando el conocimiento y la conciencia. Ver: SILVA, Rosane Leal da. **As tecnologias da informação e comunicação e a proteção de dados pessoais**. Anais do XIX Encontro Nacional do CONPEDI. Fortaleza, 2010, p.89.

528 Por su parte, las TIC's pueden definirse como el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Se trata de un concepto amplio en el que caben los ordenadores, teléfonos móviles, cámaras y un sinfín de aparatos tecnológicos que utilizamos a diario. Disponible en: <http://www.serviciostic.com/las-tic/definicion-de-tic.html>. Fecha de consulta: 28.11.16.

automatización desmedida[529]. Lo dicho hasta aquí, supone que la sociedad está enferma, el mundo vive una epidemia – **la dependencia tecnológica**. No es por menos que las personas siéntanse incomodadas cuando pasan mucho tiempo lejos de sus *smartphones* y ordenadores, o sea, están dominados por la tecnología. De manera que, si las máquinas cambian para protagonistas, el hombre corre el riesgo de vivir en función de ellas. Está bien el tema de la usabilidad, pero hasta cierto punto, ya que si pasa de la facilidad, la tecnología se puede transformar en un arma contra el proprio ser humano.

Culturalmente, hemos aprendido que la tecnología está directamente asociada con el progreso y la civilización, que nos lleva a la adopción de nuevos padrones sociales. "Como en anteriores revoluciones industriales, han impuesto su modelo económico, apoyándose en una concreta ideología. La ideología de la Globalización se asiente sobre el pensamiento neoliberal de la eficacia tecnocrática y del beneficio"[530]. A eso, mucho se debe a los padrones sociales y las ideas positivistas de progreso tecnológico y desarrollo social. Los positivistas afirmaban que la ciencia y tecnología iba a servir a todos, y que además de eso, el progreso tecnológico ayudaría en el desarrollo social, incluso, ante la ignorancia, puesto que iba a imprimir mayor racionalidad a las acciones humanas.

El moderno sueño era la suposición de que todo podría ser resuelto a través de la ciencia y la razón, que todavía culminó en la dependencia tecnológica actual. La estrategia capitalista de desarrollo tecnológico, también fue un instrumento para imponer control y dominación sobre la sociedad. Básicamente, el sistema capitalista cuño la idea de que el desarrollo tecnológico representaría un camino de bien estar social[531]. La afirmativa puede ser traducida en la idea de

529 Tal como evidenciado por Lemos e Lévy: "Después de la modernidad que controló, manipuló y organizó el espacio físico, nos vemos ante a un proceso de desmaterialización, post-moderno del mundo. El ciberespacio hace parte de un proceso de desmaterialización del espacio y de instantaneidad temporal contemporáneo, tras dos siglos de industrialización moderna que insistía en la dominación física de la energía y de las materias, y en la compartimentación del tiempo. Si en la modernidad el tiempo era una forma de esculpir el espacio, con la cibercultura contemporánea observamos un proceso en el cual el tiempo real irá poco a poco exterminando el espacio". Ver: LEMOS, André; LÉVY, Pierre. **O futuro da Internet**: em direção a uma ciberdemocracia planetária**.** São Paulo: Paulus, 2010, p.20.

530 BORJA JIMÉNEZ, Emiliano. **Globalización y Concepciones del Derecho Penal.** Estudios Penales y Criminológicos XXIX, ISSN 1137-7550, Universidad de Santiago de Compostela, 2009, p.141.

531 "La tecnología es el instrumento más apropiado para imponer una dominación y control sobre la naturaleza y la sociedad" y que el progreso tecnológico, en cierto modo, constituye una estrategia de desarrollo capitalista, no necesariamente ligados a las necesidades básicas de la gente; se ha convertido en un "factor ideológico debido al hecho de que irradian la idea de que él representa la ruta del bienestar social de todos los segmentos sociales". Ver: ZARTH, Paulo Afonso et. al. **Os caminhos da exclusão social**. Ijuí: Editora UNIJUÍ, 1998, p.35-36.

que no existe más Estado o sociedad sin plan tecnológico. De forma qué, queda la siguiente pregunta para reflexión: ¿La sociedad está preparada para cambios tan rápidos? ¿El Derecho Penal tradicional está preparado para los nuevos retos?

Todo lo dicho hasta aquí deja claro la magnitud de los cambios sociales que, al mismo tiempo, ha cambiado las estructuras delictivas contemporáneas.

El Nuevo Paradigma de la MacroCriminalidad Inmaterial en el Ciberespacio

El crimen creciente es un fruto del progreso

Arnaldo Jabor

En los últimos años, el derecho penal ha experimentado profundas transformaciones, resultado no sólo de un conjunto de mudanzas en la sociedad, sino también para el desarrollo de las tecnologías y descubrimientos científicos que exigen nuevas respuestas. Todo indica un nuevo paradigma criminológico, innovaciones descritas de manera emblemática con la expresión "*Sociedad del Riesgo*". Además, el concepto de Sociedad del Riesgo se cruza directamente con la globalización – riesgos que no respetan fronteras de ningún tipo. De manera puntual, se refiere aquí a la estructura de las *Revoluciones Científicas* como nuevo paradigma de la criminalidad, la *Macrocriminalidad Inmaterial Transnacional* en el *Ciberespacio*[532].

Este nuevo paradigma de la criminalidad puede ser visto de manera aún más clara, con las realizaciones científicas que generaron modelos que, por periodo más o menos longo, orientaran el desarrollo posterior de la ciencia Político Criminal exclusivamente en busca de una solución para los problemas por ellas suscitados. "Las TIC´s, unido a internet han potenciado los efectos de la delincuencia tradicional[533]. "La instantaneidad de los procesos comunicativos y el carácter eminentemente di-

532 Siguiendo a Miró Llinares, podemos definir el ciberespacio como el lugar de intercomunicación social transnacional, universal, popularizado y en permanente evolución derivado del uso de las TIC`s. Ver LLINARES, Fernando Miró. **EL CIBERCRIMEN - Fenomenología y Criminología de la delincuencia en el ciberespacio.** Marcial Pons: Madrid, 2012, p.74.

533 BARRANCO, María Concepción Gorjón. Ciberespacio y delito: la transposición de los instrumentos internacionales. **Política Criminal ante el reto de la delincuencia transnacional** (Dir. Ana Isabel Pérez Cepeda). Tirant lo Blanch, Valencia: 2016, p.679.

námico de las interacciones materializadas en la llamada *sociedad de la información* constituyen transformaciones que no pueden ser ignoradas por la ciencia jurídica"[534]

La nueva criminalidad tecnológica es global y viene acompañada a menudo por una mayor complejidad de los demás tipos de delictivos, pues no sólo se basa en factores técnicos o económicos, sino también en estructuras especiales, con mayor número de víctimas y gran cobertura geográfica en la ejecución de los crímenes. Los crímenes perpetrados en la red mundial de ordenadores puede lograr un conjunto indeterminable de personas. En este escenario, militan problemas específicos de esta nueva rama del conocimiento que, gradualmente, surgen conflictos derivados de la relación derecho/informática con marcada complejidad[535]. Volviendo el trinomio virtual-actual-real, es fácil comprender las dificultades enfrentadas por los órganos oficiales de control en el ciberespacio. La gran dificultad de establecer reglas para el control en el ciberespacio es que no se limita a sus fronteras. El tratamiento de la delincuencia en la *Web* se convirtió en un desafío para las naciones acostumbrados a lidiar con un delito menos sofisticado[536]. Por lo tanto, al partir de un análisis de la relación establecida entre los medios electrónicos y el hombre, se hace evidente la amplitud de los mecanismos de fuga disponibles para que el ciberdelincuente pueda salir inmune a los castigos físicos.

Segundo la filosofía libertaria criptoanarquista de uno de los fundadores de la *Electronic Frontier Foundation,* el americano John Perry Barlow: "La visión es la de que las leyes del mundo real no tendrían validad en el ciberespacio, pues ese sería, un mundo aparte, un mundo este ajeno al derecho tradicional[537]. El

534 GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações Eletrônicas e Dados no Processo Penal**, Dissertação de Mestrado da Faculdade de Direito da Universidade de São Paulo, 2012, p.12.

535 "[...]El uso de las tecnologías de la información y la comunicación revelan nuevos conflictos, entrecruzada por cuestiones técnicas ajenas al universo jurídico que, además de no tener respuestas listas en su aparato normativo, todavía encuentra dificultades para reglamentar cuestiones tan dinámicas, como la protección de los datos personales introducidos en la red mundial de computadoras. Ese cuadro hace con que en los primeros años de utilización de internet proliferasen los códigos deontológicos o de buena conducta y las políticas de privacidad y seguridad puestas en las páginas web de empresas que actúan en el sector." Ver: SILVA, Rosane Leal da. **As tecnologias da informação e comunicação e a proteção de dados pessoais**. Anais do XIX Encontro Nacional do CONPEDI. Fortaleza, 2010, p.390.

536 "La criminalidad que ocurre en este universo presenta numerosas dificultades para la acción del Estado, no sólo por la exigencia de mejores aparatos y conocimientos técnicos por parte de los organismos oficiales, a fin de identificar el acto y el autor, pero también debido a las características del espacio virtual, que permite la comunicación entre personas y la propagación de las imágenes más allá de los límites geográficos del Estado." Ver: SILVA, Rosane Leal da. **As tecnologias da informação e comunicação e a proteção de dados pessoais**. Anais do XIX Encontro Nacional do CONPEDI. Fortaleza, 2010, p.01.

537 NETO, Arnaldo Sobrinho de Morais. **Cibercrime e Cooperação Penal Internacional.** 2009, p.44. Disponible en: <http://www.egov.ufsc.br/portal/sites/default/files/arnaldo-sobrinho-cibercrime-e-

activista americano, escribió la llamada *Declaración de Independencia del Ciberespacio* creada en 1996 como respuesta al *Telecommunications Act*[538]:

> Gobiernos en el mundo industrial, vosotros cansados gigantes de carne y acero, vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquélla con la que la libertad siempre habla. Declaro el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente (…).

A partir de este punto de vista, se puede concluir que el mundo virtual no presenta cuerpos físicos, la diferencia del mundo real, es que no hay coacción física, ya que la identidad de los ciberdelincuentes pueden distribuirse en muchas jurisdicciones. Por lo tanto, el ciberespacio subvierte radicalmente las reglas de los Estados que creen en su soberanía, basados en fronteras y espacios físicos. Eso imposibilita el establecimiento de límites territoriales en una especie de auto-regulación del ciberespacio, en un mundo totalmente ajeno del mundo real.

El *cibercrimen* o *ComputerKriminalität* es una delincuencia amplia, variada y cambiante que no se puede asociarse a determinada tecnología o a un grupo específico[539]. En medio a estos problemas, es útil recordar la época en que los organismos de control enfrentaban a los delitos comunes, o tradicionales. En aquel tiempo, había un criminal, la pólvora, la sangre, las huellas dactilares y el arma del crimen, pero principalmente, lo que el territorio en el que se ejecutaban los delitos era tangible. Fue así que la criminalidad en el ciberespacio rom-

cooperacao-penal-internacional.pdf>. Fecha de consulta 07.01.17.

538 La Ley de Telecomunicaciones de 1996, cambió la ley de telecomunicaciones Estadounidense de 1934. Firmada por el presidente Bill Clinton, representó una gran mudanza en la ley de telecomunicaciones americana, una vez que su principal objetivo fue la desreglamentación de los mercados convergentes de radiodifusión y de telecomunicaciones.

539 En esta dirección, Carolina Morales Deganut indica que si bien es cierto que el origen de este tipo de ataques es muy antiguo, es posible que la preocupación de la comunidad internacional se haya incrementado últimamente por ser una práctica que no reconoce fronteras y que ha progresado significativamente al calor de las facilidades que brinda la nueva tecnología y la utilización de herramientas propias de un mundo globalizado, ya sea en el plano de las comunicaciones o en el marco financiero, lo que lleva a la necesidad de ampliar la operatividad del principio de universalidad en la preparación, ejecución y resultado se producen en un mismo territorio. Ver: RIQUERT, Marcelo A. **Crisis Penal - Política Criminal, Globalización y Derecho Penal.** Buenos Aires: Ediar, 2007.

pió con los padrones defensivos, desarrollando una realidad compleja y mutable. Una realidad en la que, entre muchos hallazgos, pone en manifiesto el incremento de la diversidad de las relaciones sociales, inaugurando nuevos espacios de interés jurídico, pero no siempre tan fácilmente accesible por los mecanismos hasta entonces creados por la ciencia del derecho penal[540]. Dicho de otra forma, la ciencia jurídico-penal sufre con los rápidos cambios vividos en la sociedad en los últimos siglos, eso ha provocado transformaciones a muchos conceptos que llevaron años para afincarse[541]. Mudanzas que indican una nueva configuración social que está estableciendo una mutación en el pensamiento jurídico penal tradicional ante la necesidad de adaptarse a las nuevas realidades.

RANSOMWARE – la extorsión mediante secuestro de datos personales

Cada un posee en su naturaleza alguna cosa que,

si lo manifestase en público, suscitaría reprobación.

Goethe

Piratas informáticos raptan ordenadores y exigen rescate. *RANSONWARE* es una de las nuevas tendencias de la cibercriminalidad mundial[542]. La creatividad de los ciberdelincuentes ha creado una de las prácticas delictivas más audaces en el ciberespacio, la extorsión mediante secuestro virtual de datos personales. Considerado uno de los crímenes informáticos más intrigantes y creativos en los cuales se involucran la privacidad en internet. No solamente las personas pueden

---

540 Desde la enorme difusión de la obra de Ulrich Beck, es un lugar común caracterizar el modelo social postindustrial en que vivimos como "sociedad del riesgo" o "sociedad de riesgos" (*Risikogesellschaft*) - Ver: SILVA SANCHÉZ, Jesús-María. **La Expansión del Derecho Penal – los aspectos de la política criminal en las sociedades postindustriales.** Segunda edición revisada y ampliada. Madrid: CIVITAS, 2001, p. 26-27.

541 Desde finales de los años 80 del pasado siglo, el desembarco de las altas tecnologías de la información y comunicación (en adelante TIC) ha dado lugar a episodios de esta naturaleza. Su uso pervertido ha potenciado los efectos negativos de la delincuencia transnacional, que ha encontrado en el ciberespacio un lugar ideal donde desarrollar sus actividades y expandir sus beneficios. Ver: SIEBER, U. **El control de la complejidad en el ciberespacio global: la armonización de los delitos informáticos**, en los caminos de la armonización penal. Tirand Lo Blanch, Valencia, 2009, p.157.

542 Disponible en: <http://www.dn.pt/sociedade/interior/piratas-informaticos-raptam-computadores-e-exigem-resgate-5592314.html>. Fecha de consulta: 07.01.17.

ser secuestradas. A millones de quilómetros de su casa, cualquier grupo de piratas informáticos puede hacer lo mismo a su ordenador. Primero aprisiónale con un *software* de encriptación, después pídele un rescate para libertarlo[543]. "Con la expansión global en la red, en el nuevo milenio, formas de delitos tradicionales adoptaran nuevas modalidades mediante el uso de las tecnologías emergentes"[544].

Conocido por *RANSOMWARE (**RANSOM** – RESCATE y **WARE** – SOFTWARE),* se utiliza de un *modus operandi* muy sofisticado que consiste básicamente en un software malicioso que se camufla dentro de otro archivo o programa apetecible para el usuario, son archivos adjuntos en correos electrónicos, vídeos de páginas de dudoso origen o incluso en actualizaciones de sistemas y programas en principio fiables. Los ciberdelincuentes atacan ordenadores de empresas de recursos humanos, por ejemplo, responsables por la contratación y selección de personas, que, sin saberlo, diseminan e-mails de empleos con el software malicioso. Millones de base de datos fueron tomadas como rehenes en los últimos años por hackers. La actuación de estos criminales es variada y creativa, invade la privacidad de las víctimas al bloquear completamente el ordenador o teléfono móvil, lo que impide el acceso a las imágenes, contactos importantes, conversaciones profesionales y archivos personales. En el caso de las empresas el problema es aún peor, pues los archivos son de mayor valor[545].

Según los datos de un periódico llamado "El Confidencial":

> Las empresas españolas pierden, de media cada una, más de 1,3 millones de euros (1.4 millones de dólares al cambio actual) anuales como consecuencia de ciberataques o incidentes de seguridad, menos que la media global que son 2.16 millones de euros (2.3 millones de dólares). Los principales incidentes que causan estas pérdidas son el robo de información, como los

543 Disponible en: <http://www.dn.pt/sociedade/interior/piratas-informaticos-raptam-computadores-e-exigem-resgate-5592314.html>. Fecha de consulta: 07.01.17.

544 SAIN, Gustavo Raúl. **Delito y Nuevas Tecnologías: fraude, narcotráfico y lavado de dinero en internet.** 1ª. Edición. Ciudad Autónoma de Buenos Aires: Del Puerto, 2012, p.7.

545 Para reflexión: ¿De qué manera la fuga de informaciones podría perjudicar una persona si cayese en las manos de hackers mal-intencionados? ¿Como seria si las siguientes informaciones fueran diseminadas? Por ejemplo: charlas privadas con amigos en el aplicativo *WhatsApp*; cuenta de *e-mail* con mensajes con el abogado o familiares; fotos íntimas salvas en el teléfono móvil; perfil en el *Tinder* con *matches* y cambio de mensajes; datos o tarjeta de crédito salvos en la *AppStore*; cuenta en el *CandyCrush* nivel 456 y centenas de horas investidas; planillas de gastos e archivos personales salvos en *GoogleDrive?*

> planes estratégicos, documentos relacionados con fusiones o adquisiciones y los de carácter financiero, seguidos por la captura de e-mails[546].

"En los próximos años, vamos asistir a un aumento de ataques informáticos, sean de sencillos utilizadores o de grupos que se dedican al robo de informaciones institucional o empresarial, dice por su vez, Rui Ribeiro, profesor de la área de las tecnologías de la Universidad Lusófona, para quien el *Ransomware* es un método de crecimiento, porque los ordenadores quedan completamente bloqueados y solamente consiguen ser libertados a través de una clave de desencriptación muy compleja"[547].

Ese pesimismo es justificable, pues una vez que ha invadido el ordenador, el malware se activa y provoca el bloqueo de todo el sistema operativo y lanza el mensaje de advertencia con la amenaza y el importe del "rescate" por los tres primeros días que se ha de pagar para recuperar toda la información, de lo contrario aumenta el cobro. Más aún, los secuestradores bloquean el ordenador de la víctima y piden dinero - o *Bitcoin*[548] - a cambio una clave que promete desbloquear el dispositivo. Aunque en algunos de los casos los delincuentes devuelvan los archivos tomados, dejan instalado un virus en el servidor a fin de facilitar futuras invasiones.

¡**Su dinero o sus datos!** Así de simple, después de secuestrar los datos empiezan un chantaje emocional a las víctimas. En general, los ciberdelincuentes suelen atrapar a ancianos y personas con poco conocimiento en tecnología. Pues la vergüenza, la necesidad de recuperar los datos y la presión ante un mensaje alarmante, son algunos de los factores que provocan que algunos de los afectados por este tipo de virus terminen pagando el rescate por sus datos**.** Para potenciar la incertidumbre y el miedo de la víctima, en algunas ocasiones incluyen en la amenaza la dirección IP, la compañía proveedora de internet y hasta una fotografía captada desde la webcam de la víctima.

Un tipo de *RANSOMWARE* muy conocido, es el ***Virus de la Policía***, que tras bloquear el ordenador infectado lanza un mensaje simulando ser la Policía y advirtiendo que desde aquel equipo se ha detectado actividad ilegal relacionada

546 Disponible en: <http://www.elconfidencial.com/tecnologia/2016-11-23/una-empresa-espanola-pierde-de-media-1-4-millones-al-ano-por-ciberataques_1293123/>. Fecha de consulta 28.11.16.

547 Disponible en: <http://www.dn.pt/sociedade/interior/piratas-informaticos-raptam-computadores-e-exigem-resgate-5592314.html>. Fecha de consulta: 07.01.17.

548 El *Bitcoin* o dinero virtual es una moneda electrónica descentralizada concebida en 2009, y que al contrario de la mayoría de las monedas no está respaldado por ningún gobierno, ni depende de la confianza de ningún emisor central.

con la pederastia o la pornografía infantil. Así, para volver a acceder la información, el malware pide a la víctima el pago de un rescate en concepto de multa.

Pero lo peor, aún está por venir, unos de los principales retos de los criminosos, además de los ordenadores, es colonizar otros dispositivos relacionados con las TIC´s, como por ejemplo, los teléfonos móviles[549]. En realidad, todos los dispositivos conectados a internet son un potencial ejército de *zombies* cargados de virus esperando a que un ciberdelincuente los despierte[550]. La interconectividad de los aparatos electrónicos en nuestras vidas – ***La Internet de las Cosas*** – videocámaras, impresoras, *Routers*, televisores, e incluso neveras, también pueden ser puertas de entradas para los ciberdelincuentes, creando una red vulnerabilidad para la captura y secuestro de datos personales.

Todavía, más que hacer comprar comida en el supermercado o encender el aspirador utilizando técnicas de Ransomware, los cibercriminales podrían, por ejemplo, tomar el control del coche y programarlo para que el motor acelere a fondo o para que el sistema de frenos deje de funcionar. Los coches suelen estar equipados con tecnologías especiales que aprovechan el acceso a internet y brindan beneficios adicionales al conductor[551]. "De ahí viene la gran cantidad de datos que la gente

549 En los últimos años, el uso de Smartphones y tablets ha crecido exponencialmente, por este motivo, los ataques a dispositivos móviles con malware seguirá en aumento. *Check Point* vaticina que el 20% de los empleados de una empresa será responsable por alguna brecha de seguridad poniendo en riesgo los datos corporativos. Esto lo harán sin saberlo, ya que será a través de malware en el proprio dispositivo móvil o porque se han conectado a un *Rogue AP* y un cibercriminal ha conseguido sus credenciales mediante ataques MITM. Disponible en: <http://www.redeszone.net/2016/11/01/los-dispositivos-moviles-iot-cloud-seran-los-principales-objetivos-los-cibercriminales-2017/>. Fecha de consulta: 28.11.16.

550 Si eres un fan de 'Regreso al Futuro II' sabrás que la mitad de las predicciones futuras realizadas en los años ochenta ya forman parte de nuestro día a día. Sin embargo, los guionistas no predijeron que cualquier aparato de casa pudiera conectarse a Internet, con el peligro de poder ser 'hackeado' y controlados mediante "*Ransomware*" sin que nosotros podamos hacer nada. Disponible en: <http://www.europapress.es/portaltic/software/noticia-son-ataques-ransomware-enfrenta-casa-conectada-20161107155247.html>. Fecha de consulta: 28.11.16.

551 Los coches modernos contienen, típicamente, más de 100 millones de líneas de código y son cada vez más inteligentes, automatizados y, más que todo, conectados a internet. Más los fabricantes no saben exactamente que software esta integrado en sus coches porque provienen de proveedores y deberá contener, probablemente, componentes de "*open-source*" con vulnerabilidades de seguridad, eso es, un ambiente interesante para ataques. Los "Hackers" van, segundo las empresas *Sysmatec* o la *Black Duck*, llevar a cabo un ataque de ancha escala a coches que podrá incluir o secuestro de coches por "*ransonware*", o la localización de choches auto-conducidos con fines obscuros o aún la vigilancia no autorizada y la recogida de datos sobre los coches. Esta situación podrá conducir también a una batalla legal entre fabricantes de software y de coches para apurar responsabilidades. Disponible en: <http://www.computerworld.com.pt/2016/12/27/desafios-de-ciberseguranca-previstos-para-2017/>. Fecha de consulta 07.01.17.

disponen diariamente, pues cuanto mayor sea el número de datos personales, mayor será la información obtenida y por consiguiente más valioso"[552]. El problema es que estas nuevas máquinas recompilaran informaciones, hábitos y tendencias de manejo de los conductores, así, estas informaciones podrían ser secuestradas y verse afectados los datos personales de los conductores. Por eso, el gran reto de los fabricantes de automóviles es fortalecer sus medidas de seguridad para evitar los ciberataques.

Las ciberamenazas serán más inteligentes, autónomas y complejas de detectar que nunca. Se espera que se produzcan más ataques dirigidos contra perfiles de alto nivel, como celebridades, políticos o grandes empresas[553]. El problema esta en la investigación, los ciberdelincuentes actúan de servidores de cualquier parte del mundo, pues hay software y redes que propician el anonimato. Este rasgo precisamente abre la puerta para que los criminales detrás del *RANSOMWARE* clásico, se enfoquen más en víctimas empresariales, instituciones y otras entidades ya que por lo general, estas no tienen otra alternativa que pagar y recuperar la información secuestrada. "Se calcula que las infecciones por *RANSOMWARE* se han doblado en las empresas, pasando de casi 25.000 ordenadores infectados en 2014 al doble en 2015"[554]. En 2010, un virus complejo infectó e invadió usinas iranís de uranio, creando no solamente prejuicios financieros descomunales, sino también, el riesgo para la vida de millones de personas inocentes. El *RANSOMWARE* se ha vuelto el virus más rentable de la historia, pero los nuevos tipos tendrán la capacidad de cambiar aún más rápidamente para maximizar su eficiencia.

Delante de la gravedad de los ataques - "Los gigantes de la seguridad informática Intel y Kaspersky, junto a Europol y la policía holandesa han desarrollado un portal llamado ***No More Ransom*** para ayudar a los usuarios a combatir la creciente amenaza de este tipo de malware y que puedan recuperar sus archivos de forma gratuita, con el fin de ir acabando poco a poco con la tendencia de pagar el rescate para lograr el descifrado de los datos"[555]. Debido a esa complejidad

552 STAIR, Ralph M. **Princípios de Sistemas de Informação: uma abordagem gerencial**. Trad. Maria Lúcia Iecker Vieira e Dalton Conde de Alencar. 2.ed. Rio de Janeiro: LTC Editora, 1998, p.4.

553 De acuerdo con el portugués Carlos Cabreiro – actualmente, la Policía Judiciaria portuguesa ya investiga ataques informáticos a empresas cuyo objetivo, segundo los datos indiciarios, es la recogida de información. Ahora es preciso percibir la motivación: si fue un hurto sencillo, si fue para la divulgación pública o si existe una motivación concurrencial, de acceso a datos de un concurrente. Lea más en: <http://www.dn.pt/sociedade/interior/piratas-informaticos-raptam-computadores-e-exigem-resgate-5592314.html>. Fecha de consulta 07.01.17.

554 Derecho en la Red, disponible en: <https://derechodelared.com/2015/12/17/historia-del-ransomware-infografia/comment-page-1/>. Fecha de consulta: 28.11.16.

555 Una arma importante contra el *Ransomware* – <www.nomoreransom.org>. Fecha de consulta 07.01.17.

en su catalogación, la instrumentalización jurídica para integrar el *RANSOMWARE* en el contexto punitivo ha sido variada. De manera que es necesario identificar y controlar cualquier evento que pueda afectar negativamente los datos personales de los usuarios de la red, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias. Si acaso eso no ocurra muy pronto, la economía mundial digital estará amenazada.

La ecología criminal y la desorganización social en red

Una de las primeras teorías sociológicas del crimen, la Escuela de Chicago, ofrece un ejemplo expresivo de ese proceso de desarrollo social. Lo que hace con que la experiencia urbana de Chicago y su interpretación teórica asuman un buen comparativo en relación al *Ciberespacio y la Sociedad de la Información*.

La Ecología Criminal, que, aplicada a los problemas humanos y sociales, plantea la perspectiva del equilibrio de una comunidad humana con su ambiente. Los principales autores son Shaw y McKay (1942). Lo que sorprendió a estos es que una mayoría de los delincuentes surge de las mismas áreas, los mismos barrios; por ello pensaron que debían fijarse en la organización social, en el ambiente, en la ecología del lugar donde crecen los delincuentes[556]. La teoría de la Desorganización Social se refiere no solo a los indicadores de pobreza, sino también a la transitoriedad de las relaciones sociales, el estado de descomposición, abandono, crisis o transición de una sociedad.

De acuerdo con Costa Andrade y Figueiredo Dias:

> La Escuela de Chicago y la teoría ecológica del crimen dejó claro las implicaciones del crecimiento vertiginoso del espacio urbano provocado por el proceso de industrialización. Ellos pusieron la ciudad y sus modelos de convivencia y interacción el centro de las preocupaciones de los teóricos y moralistas de los fines del siglo XIX y principios de siglo XX. Por sus dimensiones sin precedentes, por su heterogeneidad étnica y cultural, por el anonimato y atomismo de su interacción, la ciudad moderna caracterizase por la ruptura de los mecanismos tradicionales de control (familia, vecindario, religión, escuela) y por la pluralidad, prácticamente sin límites, de las alternativas de conducta. ***"traducción nuestra"*** [557].

556 LARRAURI, Elena P. **Introducción a la Criminología y al Sistema Penal.** Editorial Totta S.A., 2015, p.67.

557 COSTA ANDRADE, Manuel da; FIGUEIREDO DIAS, Jorge de. **Criminologia – o Homem Delinquente e a Sociedade Criminógena.** 2ª. Reimpressão. Coimbra: Editora Coimbra, 1997, p.269.

Es precisamente ese tipo de análisis que este punto del trabajo pretende demostrar, especialmente los cambios que los individuos enfrentan en la modernidad y su consonancia con el enfoque contemporáneo del tema. Puesto que uno de los principales culpables por el crecimiento de la delincuencia en internet es, sin lugar a dudas, la desorganización de sus usuarios. Que no tiene conciencia de la importancia de los mecanismos de seguridad en internet. El uso cada vez más intenso de datos personales en la *Sociedad de la Información* ha creado un desequilibrio entre los usuarios, precisamente por la cantidad de información que las nuevas tecnologías son capaces de agregar. Los usuarios de internet se convirtieron en una gran red de informantes acerca de los demás y de nosotros mismos. La sociedad conectada ya se conformó con la extinción de la privacidad.

Existen muchas herramientas y medidas que las personas pueden tomar para evitar la vigilancia del gobierno y mejorar la seguridad en internet contra los ciberdelincuentes, como por ejemplo, usar criptografía y claves seguras de protección. El problema es que la sociedad actual no está preparada para los rápidos cambios fruto del proceso de modernización, de forma que, la sociedad no sabe cómo lidiar con eso, y no sabe cómo portarse en el ciberespacio con seguridad, de modo que, se exponen y se ponen en peligro. Hay una desorganización general en red, y eso es el mayor culpado por el aumento de la criminalidad *online*.

Para aquellos refutan esa idea, deben contestar antes las siguientes preguntas: ¿Usted hace *check-in* en la empresa? (el último día de trabajo antes de las vacaciones) ¿Hace *selfies* en casa con su animal de estimación? ¿Hace *selfies* en el coche nuevo? ¿Otro *check-in* con sus hijos? Bueno, seguramente hay mucha gente desconocida que ya sabe dónde estas personas trabajan, cuántos hijos tienes, que coche, el nombre de toda su familia y incluso dónde estudian sus hijos. ¿Tenéis algún dispositivo de seguridad y privacidad en su correo electrónico, en el perfil de las redes sociales? ¿En algún momento habéis visitado la página web del banco utilizando una red *wifi* pública?

Bueno, parece no haber dudas cuanto a la desorganización en red, lo que ocasiona casi siempre en un aumento de la delincuencia. Es común la gente crear claves secretas utilizando nombre de parejas, fecha de cumpleaños o número del móvil, eso trae más oportunidad para los criminosos acostumbrados con estos tipos de facilidad. Los usuarios de internet se ponen en estado de vulnerabilidad cuando informan dónde estarán en las prójimas horas o el lugar dónde frecuentan regularmente. Esto es, utilizan programas pirateados bajados de la *web*, pues el uso parece ventajoso en virtud de su gratuidad, todavía presentan excesivos peligros de contaminación. Dicho de otra manera, protegerse en el ciberespacio, puede hasta ser un poco fastidioso, pero es importante tener

una postura defensiva a fin de evitar, o mismo, minimizar los problemas. En otras palabras, la mayoría de las trampas *online* podrían ser evitadas si las personas tuviesen los mínimos cuidados en la red. Los cibercriminosos están siempre atentos a nuevas oportunidades, ahora con las redes sociales está mucho más fácil. Es decir, los criminosos no necesitan más monitorear el hogar de sus víctimas personalmente, ahora solamente necesitan hacer una pesquisa en Google o en Facebook lograr su acción delictiva.

Hubo un aumento significativo en el número de delitos informáticos, sobretodo, en los países en que la inclusión digital ha venido de forma tardía, rápida y desorganizada, sin investimentos en educación técnica. Todo eso parece confirmar que el mal comportamiento y la falta de sentido común en red, es el principal responsable por el aumento de la criminalidad informática. Así que, no resultará curioso, entonces, que las nuevas oportunidades delictivas aparezcan como resultado de la desorganización en red vivida actualmente en la sociedad. Por consiguiente, el (mal) uso de las comunicaciones personales entre particulares a través de las redes telemáticas y la mala utilización de los contenidos introducidos en ellas han creado nuevas oportunidades delictivas. De cara al futuro, la necesidad de protegerse a múltiples niveles es una cuestión urgente y real que afecta a gobiernos y usuarios por igual. Si no toman medidas inmediatas, hay un gran riesgo de acabar por interrumpir el progreso de la economía digital global. La "***Ciberguerra Fría***" es una corrida al armamiento para descubrir y guardar las vulnerabilidades de software, algunas de las cuales presentes en software que utilizamos diariamente[558].

El gran problema, es que con las ganas de alcanzar el progreso tecnológico, el hombre no llevó en cuenta sus implicaciones sociales relacionadas con los límites morales, políticos e individuales. La busca desmedida por la modernización llevó al hombre hacia la paranoia de seguridad, busca por más rentabilidad y desarrollo tecnológico.

Conclusión

Las justificativas encontradas para el aumento de la criminalidad informática es inequívoca. En primer plano se puede afirmar que las transformaciones generadas por la Revolución Tecnológica tuvieron consecuencias trágicas para la sociedad, que no está preparada para cambios tan rápidos. Las nuevas tecnologías

558 Leer más en: <http://www.computerworld.com.pt/2016/12/27/desafios-de-ciberseguranca-previstos-para-2017/> Fecha de consulta 07.01.17.

crecieron en una rapidez increíble, a cada día surge un nuevo y más moderno aparato tecnológico. Sin embargo, las leyes no acompañan, eso es, el Derecho Penal no cambia con la misma velocidad. Por lo tanto, está claro que este fenómeno de modernización corresponde a una nueva etapa de riesgo, surgido durante el proceso de desarrollo social. En eso sentido, cuanto más avanza el progreso, más aún las sociedades quedan amenazadas en sus bases, haciendo del mundo globalizado un mecanismo facilitador de la expansión de la criminalidad.

Otro elemento con gran parcela de responsabilidad por el aumento de las oportunidades delictivas y la vulnerabilidad de los datos personales, es "*la negligencia de los usuarios en red*", que ha originado muchas discrepancias entre las diversas infraestructuras. La llamada *Desorganización Social en el Ciberespacio* es otro gran responsable por las nuevas formas delictivas empleadas hacia los datos personales. La *cultura de descuido y desidia por la seguridad en las TIC´s* facilita la obstaculización ilegítima y el secuestro de datos personales de particulares y empresas. La exposición exasperada de las personas en las redes sociales, abre las puertas para que archivos mal intencionados detrás del *RANSOMWARE* tengan más éxito. Vulnerables, los internautas están expuestos a los nuevos ataques de *RANSOMWARE,* que esparcirán más rápidamente y tendrán más capacidad de autoreplicarse dentro de las organizaciones antes de iniciar los pedidos de rescate. Los secuestros de datos personales serán más inteligentes y complejos de detectar que nunca.

Finalmente, las estrategias y planes para prevenir los secuestros de datos incluyen programas de formación de usuarios, con mayor incremento en los investimentos de educación técnica en las empresas., del contrario, el comercio electrónico estará en riesgo.

Anonimato, Proteção de Dados e Devido Processo Legal: Por que e como Conter uma das Maiores Ameaças ao Direito à Privacidade no Brasil

Mariana Cunha e Melo[559]

Introdução

O objetivo deste artigo é analisar os aspectos procedimentais da defesa do anonimato na internet. A discussão sobre o anonimato hoje não envolve apenas a existência de assinatura em textos escritos, mas também tem implicações na proteção de dados pessoais. Não se trata, portanto, apenas da liberdade para se manifestar com uma máscara ou sem assinatura, mas de impor limites à possibilidade de monitoramento de qualquer atividade online. Nesse sentido, fala-se muito, além do direito de escrever anonimamente, no direito de ler anonimamente[560].

---

559 Bacharel em direito pela UERJ, mestre em direito pela Nova York University (NYU) e doutoranda em direito no UniCEUB, sob orientação do Professor Luís Roberto Barroso. Autora do livro "The 'Marco Civil da Internet' and its unresolved issues: free speech and due process of law", publicado pela Editora CTV em 2016. Pesquisadora no Centro Brasileiro de Estudos Constitucionais, vinculado ao UniCEUB, comentarista do Observatório do Marco Civil, ex-integrante do conselho consultor da ONG Index on Censorship (mandato janeiro-julho de 2016) e advogada no escritório Barroso Fontelles, Barcellos, Mendonça, em Brasília.

560 ELECTRONIC FRONTIER FOUNDATION, Anonymity and Encryption, fev. 2015, p. 7. Disponível em: <https://www.eff.org/document/eff-comments-submitted-united-nations-special-rapporteur-promotion-and-protection-right> Acesso em: 23.03.17: "The ability to read and access information anonymously is also crucial for the exercise of free expression. Article 19 of the Universal Declaration of Human Rights, which enshrines the right to freedom of opinion and expression, includes the right to seek, receive, and impart information and ideas through any media. … In other words, the right to seek and receive information is chilled when the government or others have unchecked access to records that document the viewing or reading habits of individuals". Ver também: COHEN, Julie E. A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace. **28 Conn. L. Rev**. 981-1039 (1996). Disponível em: <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1815&context=facpub> Acesso em: 23.03.17: "Anonymous advocacy has always been controversial. Anonymous reading, in contrast, is something that is taken for granted".

Qualquer discussão sobre anonimato costuma atrair dois pólos para o debate. Por um lado, há um receio razoável de que o anonimato seja utilizado para cometer toda espécie de abuso *online*. *Cyberbullying*, ataques a grupos minoritários e calúnias em geral – tudo assume um alcance virtualmente impossível de ser previsto ou restringido[561]. A internet reduz os custos envolvidos em cometer uma variedade de crimes relacionados ao discurso. A gravidade da situação é tal que Danielle Citron, uma das mais proeminentes especialistas em crimes de internet, compara o padrão de comportamento dos que cometem crimes de ódio na internet a grupos mascarados como a Ku Klux Klan[562].

Nesses casos, o anonimato dificulta a identificação dos responsáveis pelos abusos e provoca, ele mesmo, um efeito inibidor no discurso. Imagine-se a situação em que uma ativista pelos direitos dos animais defenda a alteração da legislação federal em um blog. E, como resultado, sofra toda espécie de ataque à sua intimidade e privacidade por um grupo de opositores. Seria plenamente possível que essa militante se sentisse insegura para defender suas posições publicamente. Consequentemente, o debate público seria retraído ao invés de se expandir pelo uso do anonimato.

Engana-se, contudo, quem imagina uma solução radical para o problema da nossa ativista. O anonimato é frequentemente utilizado pelos mais diversos grupos de pessoas para emitir opiniões ou disseminar informações no debate público sem risco de represálias no mundo eletrônico ou físico. Imagine-se que a ativista tenha criado um blog, por meio de um pseudônimo, para fazer campanha contra um político local, acusado de corrupção. O político, em contrapartida, busca obter a identidade da ativista com o objetivo de prejudicá-la em seu emprego ou ameaçá-la de outra forma. Se o parâmetro para a obtenção de sua identidade não levar em conta a ilicitude do que houver sido dito e a relevância de se divulgar esses dados pessoais, o político não terá dificuldades de prejudicar a ativista, ainda que essa não tenha cometido qualquer ilícito.

Em apertada síntese, é possível identificar três motivos para reconhecer alguma relevância no anonimato na internet[563]. ***Em primeiro lugar***, o direito

561 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320 (2008).

562 CITRON, Danielle Keats, Cyber Civil Rights, **89 Boston University Law Review**, 81, 2009.

563 Para mais informações sobre essa discussão, v.: CUNHA E MELO, Mariana. **The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law**. Curitiba, CRV, 2016. ORGANIZAÇÃO DAS NAÇÕES UNIDAS, Report on encryption, anonymity, and the human rights framework. Disponível em: <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> Acesso em: 23.03.17; ELECTRONIC FRONTIER FOUNDATION, Anonymity and Encryption. Feb.

de evitar a vigilância – ou até a possibilidade de vigilância – é de extrema valia em um mundo que está progressivamente mais afeito a iniciativas de vigilância absoluta. E aqui vale lembrar que, ainda que não haja efetiva vigilância sobre todas as pessoas a todo o tempo, a *possibilidade* de vigilância provoca efeitos no comportamento das pessoas e na percepção sobre sua própria liberdade. É a ideia da sociedade no Panóptico.

Em segundo lugar, o anonimato na internet também tem um viés libertador, de empoderamento, que é permitir o controle do fluxo de informações sobre si. Trata-se de dar aos usuários o poder de proteger seus próprios dados da vigilância privada ou do Poder Público – essa é uma das funções mais poderosas do anonimato na internet[564].

Por fim, ***em terceiro lugar***, a internet é considerada o grande mercado de ideias hoje, um fórum público. Muitas ideias e opiniões, contudo, são objeto de represálias de todas as formas – inclusive pela violência física. Nesse sentido, vale registrar o trabalho de ONGs como a Association for Progressive Communications (APC), que combate violência contra mulheres na internet, da Derechos Digitales, que promove campanhas para o uso seguro da internet para fins de propagação de ideias[565], da Electronic Frontier Foundation[566] e da Access Now[567], duas das maiores organizações mundiais de defesa dos direitos civis na internet. Em muitos casos, esconder a identidade dos ativistas é a primeira fronteira de defesa contra violência na internet.

Há, portanto, um interesse na defesa do anonimato na internet – ao menos em alguma medida e em certas circunstâncias.

Também do ponto de vista normativo, a discussão sobre o anonimato na internet atrai posições em aparente conflito. Por um lado, a Constituição Federal veda textualmente o anonimato no âmbito da manifestação do pensamento (art. 5º, IV). Por outro, a mesma Carta garante a inviolabilidade do sigilo de dados que, uma vez divulgados, permitem a identificação do usuário, e a proteção da intimidade dos cidadãos (art. 5º, X e XII). No mundo de hoje, não há como compatibilizar uma interpretação literal do primeiro dispositivo com o sentido

2015. Disponível em <https://www.eff.org/document/eff-comments-submitted-united-nations-special-rapporteur-promotion-and-protection-right> Acesso em: 23.03.17.

564 Confira-se em: <https://www.apc.org/en/node/15007/>. Acesso em: 23.03.17

565 Confira-se em: <https://www.derechosdigitales.org/notemasainternet/>. Acesso em: 23.03.17

566 Confira-se em: <https://www.eff.org/wp/blog-safely>. Acesso em: 23.03.17

567 Confira-se em: <https://www.accessnow.org/issue/freedom-of-expression/> Acesso em: 23.03.17

mais essencial dos dois últimos[568]. Afinal, fosse a vedação ao anonimato levada às últimas consequências, como uma autorização genérica à quebra do sigilo de dados em qualquer caso, a proteção constitucional ao sigilo de nada valeria.

O que existe hoje, no entanto, é que de fato os pedidos de fornecimento de dados sobre a identidade das pessoas são deferidos de forma quase automática. Não se exige sequer um fundamento relevante para que o pedido seja deferido. E pior: o maior interessado sequer é chamado ao processo.

No entanto, assumindo que há ao menos um interesse mínimo no anonimato, conforme sustentado acima, essa restrição automática do direito ao sigilo de dados à revelia de seu titular causa um gravíssimo problema de devido processo legal. Como se sabe, o devido processo legal compreende o direito de participar do procedimento capaz de resultar em restrição de sua liberdade ou de seus bens. Envolve, ainda, o direito à ampla defesa e ao contraditório – isto é: o direito de que se tenha a oportunidade de ser ouvido no processo. A restrição de um direito fundamental sem a oitiva de seu titular, portanto, fere de morte o devido processo legal.

Em matéria de anonimato e sigilo de dados, no entanto, a garantia da participação no processo enfrenta uma dificuldade prática muito clara. Afinal, se o direito que está em jogo é o direito ao sigilo da identidade, como o seu titular poderia se apresentar nos autos para se defender formalmente sem revelar seus dados – renunciando, assim, ao próprio direito que ele pretendia defender?

Para enfrentar esse problema de devido processo legal, deve-se investigar meios que permitam a defesa do sigilo: (i) antes do cumprimento da ordem de fornecimento de dados; e (ii) sem que o titular desse direito seja forçado a se identificar no processo. É esse o objeto de investigação do presente artigo.

Em primeiro lugar, será apresentado um panorama geral da legislação brasileira sobre anonimato e quebra de sigilo de dados sobre comunicações. Nesse ponto, serão delineadas justificativas para a interpretação mitigada da vedação ao anonimato. *Em segundo lugar*, serão analisadas as repercussões do procedimento atual de fornecimento de dados para a garantia do devido processo legal. *Em terceiro lugar*, serão expostos os fatores mais relevantes para a criação de um procedimento adequado para requisição de dados em juízo, de modo a respeitar o devido processo legal.

568 Para uma discussão hermenêutica sobre uma interpretação mitigada da vedação do anonimato, v.: CUNHA E MELO, Mariana. **The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law**. Curitiba, CRV, 2016.

Pedidos de identificação de usuários de internet: entre a vedação ao anonimato e a proteção de dados

A jurisprudência brasileira sobre pedidos de identificação de usuários na internet é bastante permissiva. Em muitos casos, o pedido de fornecimento de dados é deferido de forma quase automática, com fundamento exclusivo na proibição constitucional ao anonimato. Em inúmeras oportunidades, as Turmas de Direito Privado do Superior Tribunal de Justiça afirmaram a obrigação dos provedores de serviço de internet de garantirem a possibilidade de identificação de seus usuários para "coibir o anonimato"[569]. Aos poucos, a jurisprudência se desenvolveu para passar a exigir que os provedores armazenassem dados de usuários por ao menos três anos – justamente para viabilizar a identificação antes do fim do prazo prescricional da pretensão de reparação civil[570-571].

---

569 BRASIL, STJ, DJe 02/05/2012, REsp 1306066/MT, Rel. Min. Sidnei Beneti: "RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. PROVEDOR. MENSAGEM DE CONTEÚDO OFENSIVO. RETIRADA. REGISTRO DE NÚMERO DO IP. DANO MORAL. AUSÊNCIA. PROVIMENTO. 1.- No caso de mensagens moralmente ofensivas, inseridas no site de provedor de conteúdo por usuário, não incide a regra de responsabilidade objetiva, prevista no art. 927, parágrafo único, do Cód. Civil/2002, pois não se configura risco inerente à atividade do provedor. Precedentes. 2.- É o provedor de conteúdo obrigado a retirar imediatamente o conteúdo ofensivo, pena de responsabilidade solidária com o autor direto do dano. 3.- O provedor de conteúdo é obrigado a viabilizar a identificação de usuários, coibindo o anonimato; o registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na internet constitui meio de rastreamento de usuários, que ao provedor compete, necessariamente, providenciar".

570 BRASIL, STJ, DJe 18/06/2014, AgRg no REsp 1402104/RJ, Rel. Min. Raul Araújo: "A responsabilidade subjetiva do agravante se configura quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide; II) não mantiver um sistema ou não adotar providências, que estiverem tecnicamente ao seu alcance, de modo a possibilitar a identificação do usuário responsável pela divulgação ou a individuação dele, a fim de coibir o anonimato. O fornecimento do registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na internet constitui meio satisfatório de identificação de usuários". No mesmo sentido, v.: BRASIL, STJ, DJe 23/05/2014, AgRg no REsp 1396963/RS, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 28/05/2014, AgRg no REsp 1285756/MG, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 26/05/2014, AgRg no REsp 1395803/RJ, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 22/05/2014, AgRg no REsp 1395768/RJ, Rel. Min. Raul Araújo.

571 BRASIL, STJ, DJe 10/03/2014, REsp 1417641/RJ, Rel. Min. Nancy Andrighi: "2. Recurso especial que discute os limites da responsabilidade dos provedores de hospedagem de blogs pela manutenção de dados de seus usuários. 3. Ao oferecer um serviço por meio do qual se possibilita que os usuários divulguem livremente suas opiniões, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada imagem uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, do dever de informação e do princípio da transparência, deve este adotar as providências que,

A vedação constitucional e o interesse em viabilizar a responsabilização de autores de ilícitos na internet não são, contudo, os únicos elementos na resolução desse tipo de conflito. Com efeito, em oposição a essa linha jurisprudencial, precedentes que tratam sobre sigilo de dados parecem seguir um caminho diferente. No Brasil, a tutela dos sigilos constitucionais é dividida em duas categorias diferentes: a proteção prevista textualmente no art. 5º, XII da Constituição e aquela extraída de uma garantia geral à intimidade e à vida privada, no art. 5º, X. No primeiro grupo, estão os sigilos sobre o *conteúdo* das comunicações. No segundo, os demais sigilos protegidos, como o bancário, o fiscal e dos *dados sobre comunicações* – **que constituem *informações sobre os atos de comunicação* efetuados pelos indivíduos.** Nessa categoria, se incluem o sigilo telefônico – lista das chamadas recebidas e efetuadas, com as respectivas datas e horários – e os registros eletrônicos relacionados à troca de e-mails – como o número de IP e as respectivas informações de data e horário.

Como se sabe, a proteção específica conferida pelo art. 5º, XII da Constituição é a mais substancial. Primeiramente, somente admite a quebra do sigilo em sede de investigação de crimes graves – nunca em processo cível. Além disso, nos termos da legislação de regência, exigem-se: (i) "indícios razoáveis" do cometimento de um *crime*; (ii) demonstração da inexistência de meios alternativos (necessidade); (iii) o crime investigado deve ser punível por reclusão (crime grave) (Lei nº 9296/1996, art. 2º); e (iv) limitação temporal (art. 5º).

conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por *culpa in omittendo*. Precedentes. 4. Uma vez ciente do ajuizamento da ação e da pretensão nela contida - de obtenção dos dados de um determinado usuário - estando a questão sub judice, o mínimo de bom senso e prudência sugerem a iniciativa do provedor de conteúdo no sentido de evitar que essas informações se percam. Essa providência é condizente com a boa-fé que se espera não apenas dos fornecedores e contratantes em geral, mas também da parte de um processo judicial, nos termos dos arts. 4º, III, do CDC, 422 do CC/02 e 14 do CPC. 5. As informações necessárias à identificação do usuário devem ser armazenadas pelo provedor de conteúdo por um prazo mínimo de 03 anos, a contar do dia em que o usuário cancela o serviço". No mesmo sentido, v.: BRASIL, STJ, DJe 26/11/2013, REsp 1398985/MG, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 25/03/2014, REsp 1403749/GO, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 26/09/2013, REsp 1383354/SP, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 26/06/2012, REsp 1300161/RS, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 02/08/2012, REsp 1192208/MG, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 19/06/2012, REsp 1308830/RS, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 31/08/2011, REsp 1186616/MG, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 08/08/2011, REsp 1193764/SP, Rel. Min. Nancy Andrighi.

A garantia geral à intimidade, ainda que mais branda, impõe também uma série de requisitos de validade à quebra dos demais sigilos[572]. A jurisprudência exige também nesses casos que a decisão de quebra de sigilo receba uma fundamentação específica com a demonstração: (i) de indícios de que uma pessoa específica tenha cometido atos ilícitos[573]; dos *fatos* que se pretende comprovar com a quebra de sigilo[574], (ii) dos *indícios* de que os fatos serão comprovados por

572 BRASIL, STF, DJ 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello (Tribunal Pleno): "Essa diretriz jurisprudencial [de se exigir fundamentação adequada das decisões de quebra de sigilo] (...) reconhece que o direito à intimidade – que representa importante manifestação dos direitos da personalidade – qualifica-se como expressiva prerrogativa de ordem jurídica que consiste em garantir, em favor da pessoa, de qualquer pessoa, na esfera de sua vida privada, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros, notadamente a do Poder Publico. Daí a correta advertência feita por Carlos Alberto Di Franco, para quem 'um dos grandes desafios da sociedade moderna é a preservação do direito à intimidade. Nenhum homem pode ser considerado verdadeiramente livre, se não dispuser de garantia de inviolabilidade da esfera de privacidade que o cerca".

573 TJSP, 13a Cam. Crim., HC 00430001-50.2014.8.26.0000/Franca, rel. Des. Augusto de Siqueira, j. 07/08/2014: "Muito embora os direitos sejam relativos, inclusive os constitucionais, sua flexibilização não pode ser indiscriminada, admitindo obtenção de informações sobre dados de quaisquer assinantes da empresa de telefonia, ao longo de um ano. A autorização deve ser concreta, ou seja, incidir sobre a prática de crimes específicos, cometidos por determinada ou determinadas pessoas e pelo tempo necessário à obtenção da prova. Nesse sentido já se decidiu: '(...) [A] **indicação do indivíduo ou do telefone objeto de investigação, e assim das razões que levam a autoridade a propor a quebra do sigilo legal, têm de ser deduzidas a 'priori'**, sem prejuízo do relatório posterior das diligência' (TJSP - Habeas Corpus n. 993.08.045010-2 Rel. Desembargador Aben-Athar). 'Habeas Corpus Sigilo de dados cadastrais de clientes de concessionárias de serviços telefonia **Não indicação de fato concreto e de pessoas individualizadas Autorização de quebra de sigilo genérica e sem fundamentação específica. Inadmissibilidade** Devassa que afronta as garantias constitucionais da intimidade e da privacidade (art. 5o, X, CF) e o princípio da dignidade da pessoa humana (art. 1o, III,CF) Receio fundado de represália jurídico-penal decorrente do descumprimento da sobredita ordem judicial genérica 'Mandamus' concedido, com extensão' (TJSP - Habeas Corpus n. 990.09.227159-8 Rel. Desembargador Moreira da Silva)".

574 BRASIL, TJSE, Cam. Crim, HC 2010314476, rel. Des. Geni Silveira Schuster, j. 08/02/2011: "A determinação de fornecimento de senha franqueando a agentes policiais o acesso ilimitado a dados cadastrais de clientes afronta o disposto no inciso X, do art. 5o da Constituição Federal, já que qualquer pessoa pode ter devassado os seus dados, uma vez que a ordem judicial não é específica, não se vinculando a um caso concreto".

meio do provimento excepcional[575]; (iii) da necessidade da medida[576]; e (iv) do lapso temporal em que os dados deverão ser captados[577].

---

575 BRASIL, STF, DJ 04 ago. 2006, MS 25668/DF, Rel. Min. Celso de Mello: "A QUEBRA DE SIGILO - QUE SE APÓIA EM FUNDAMENTOS GENÉRICOS E **QUE NÃO INDICA FATOS CONCRETOS E PRECISOS REFERENTES À PESSOA SOB INVESTIGAÇÃO - CONSTITUI ATO EIVADO DE NULIDADE**. - A quebra do sigilo inerente aos **registros bancários, fiscais e telefônicos**, por traduzir medida de caráter excepcional, revela-se incompatível com o ordenamento constitucional, quando fundada em deliberações emanadas de CPI cujo suporte decisório apoia-se em **formulações genéricas, destituídas da necessária e específica indicação de causa provável**, que se qualifica como **pressuposto legitimador da ruptura, por parte do Estado, da esfera de intimidade a todos garantida pela Constituição da República**".

576 BRASIL, STF, DJ 23 fev. 06, MS 25812 MC, Rel. Min. Cezar Peluso.

577 BRASIL, STF, DJ 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello: "A QUEBRA DE SIGILO NÃO PODE SER UTILIZADA COMO INSTRUMENTO DE **DEVASSA INDISCRIMINADA**, SOB PENA DE OFENSA À GARANTIA CONSTITUCIONAL DA INTIMIDADE. - A **quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes**. É que, se assim não fosse, a quebra de sigilo converter-se-ia, ilegitimamente, em **instrumento de busca generalizada e de devassa indiscriminada da esfera de intimidade das pessoas**, o que daria, ao Estado, em desconformidade com os postulados que informam o regime democrático, o **poder absoluto de vasculhar, sem quaisquer limitações, registros sigilosos alheios**. (...) **Para que a medida excepcional da quebra de sigilo bancário não se descaracterize em sua finalidade legítima**, torna-se imprescindível que o ato estatal que a decrete, além de adequadamente fundamentado, também indique, de modo preciso, dentre outros dados essenciais, **os elementos de identificação do correntista (notadamente o número de sua inscrição no CPF)** e o lapso temporal abrangido pela ordem de ruptura dos registros sigilosos mantidos por instituição financeira". STF, DJ 23 fev. 06, MS no 25.812, Rel. Min. Cezar Peluso: "O outro requisito é a **existência de limitação temporal do objeto da medida** (d) [quebra de sigilo bancário], enquanto predeterminação formal do período que, constituindo a referência **do tempo provável** em que teria ocorrido o fato investigado, seja suficiente para lhe esclarecer a ocorrência por via tão excepcional e extrema. E é não menos cristalina a racionalidade desta condição decisiva, pois **nada legitimaria devassa ilimitada da vida bancária, fiscal e comunicativa do cidadão**, debaixo do pretexto de que Comissão Parlamentar de Inquérito precise investigar **fato ou fatos específicos, que são sempre situados no tempo, ainda quando de modo só aproximado**. Ou seja - para que se não invoque nenhuma dúvida ao propósito -, a Constituição da República não tolera devassa ampla de dados da intimidade do cidadão, quando, para atender a necessidade legítima de investigação de ato ou atos ilícitos que lhe seriam imputáveis, basta seja **a quebra de sigilos limitada ao período de tempo em que se teriam passado esses mesmos supostos atos. Que interesse jurídico pode enxergar-se na revelação de dados íntimos de outros períodos?** Só a concorrência de todos esses requisitos autoriza, perante a ordem constitucional, à luz do princípio da proporcionalidade, a prevalência do interesse público, encarnado nas deliberações legítimas de CPI, sobre o resguardo da intimidade, enquanto bem jurídico e valor essencial à plenitude da dignidade da pessoa humana". V. também: STF, *DJ* 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello (Tribunal Pleno): "A QUEBRA DE SIGILO NÃO PODE SER UTILIZADA COMO INSTRUMENTO DE DEVASSA INDISCRIMINADA, SOB PENA DE OFENSA À GARANTIA CONSTITUCIONAL DA INTIMIDADE. - A quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes. É que, se assim não fosse, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada e de devassa indiscriminada da esfera de intimidade das pessoas, o que daria, ao Estado, em desconformidade com os postulados que informam o regime democrático, o poder absoluto de vasculhar, sem quaisquer limitações,

Essas exigências se justificam, mesmo nas situações regidas pelo art. 5º, X da Constituição porque, nas palavras do Ministro Cezar Peluso, "não se pode sacrificar direito fundamental tutelado pela Constituição – o direito à intimidade –, mediante uso da medida drástica e extrema da quebra de sigilos, quando a existência do fato ou fatos sob investigação pode ser lograda com recurso aos meios ordinários de prova"[578]. Em uma única proposição: "[r]estrições absolutas a direito constitucional só se justificam em situações de absoluta excepcionalidade"[579] [580].

De forma específica, quanto à proteção dos *dados sobre comunicações* na internet, o Marco Civil da Internet, como esperado, incorporou os princípios gerais explorados pela jurisprudência constitucional. Em seu artigo 22, dispõe textualmente que ordens de quebra de sigilo dos registros de conexão ou de re-

registros sigilosos alheios"; STF, *DJ* 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello (Tribunal Pleno): "Para que a medida excepcional da quebra de sigilo bancário não se descaracterize em sua finalidade legítima, torna-se imprescindível que o ato estatal que a decrete, além de adequadamente fundamentado, também indique, de modo preciso, dentre outros dados essenciais, os elementos de identificação do correntista (notadamente o número de sua inscrição no CPF) e o lapso temporal abrangido pela ordem de ruptura dos registros sigilosos mantidos por instituição financeira"; STF, *DJ* 04 ago. 2006, MS 25668/DF, Rel. Min. Celso de Mello (Tribunal Pleno): "A QUEBRA DE SIGILO - QUE SE APÓIA EM FUNDAMENTOS GENÉRICOS E QUE NÃO INDICA FATOS CONCRETOS E PRECISOS REFERENTES À PESSOA SOB INVESTIGAÇÃO - CONSTITUI ATO EIVADO DE NULIDADE. - A quebra do sigilo inerente aos registros bancários, fiscais e telefônicos, por traduzir medida de caráter excepcional, revela-se incompatível com o ordenamento constitucional, quando fundada em deliberações emanadas de CPI cujo suporte decisório apóia-se em formulações genéricas, destituídas da necessária e específica indicação de causa provável, que se qualifica como pressuposto legitimador da ruptura, por parte do Estado, da esfera de intimidade a todos garantida pela Constituição da República".

578 BRASIL, STF, DJ 23 fev. 06, MS 25812 MC, Rel. Min. Cezar Peluso.

579 BRASIL, STF, DJ 23 fev. 06, MS 25812 MC, Rel. Min. Cezar Peluso.

580 No mesmo sentido, vale ver a manifestação do Ministro Celso de Mello: BRASIL, STF, DJ 14 fev. 2001, MS 23669, Rel. Min. Celso de Mello: "A GARANTIA CONSTITUCIONAL DA INTIMIDADE, EMBORA NÃO TENHA CARÁTER ABSOLUTO, NÃO PODE SER ARBITRARIAMENTE DESCONSIDERADA PELO PODER PÚBLICO. - O direito à intimidade - que representa importante manifestação dos direitos da personalidade - qualifica-se como expressiva prerrogativa de ordem jurídica que consiste em reconhecer, em favor da pessoa, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros na esfera de sua vida privada. A transposição arbitrária, para o domínio público, de questões meramente pessoais, sem qualquer reflexo no plano dos interesses sociais, tem o significado de grave transgressão ao postulado constitucional que protege o direito à intimidade, pois este, na abrangência de seu alcance, representa o 'direito de excluir, do conhecimento de terceiros, aquilo que diz respeito ao modo de ser da vida privada' (HANNAH ARENDT). O DIREITO AO SIGILO BANCÁRIO - QUE TAMBÉM NÃO TEM CARÁTER ABSOLUTO - CONSTITUI EXPRESSÃO DA GARANTIA DA INTIMIDADE. - O sigilo bancário reflete expressiva projeção da garantia fundamental da intimidade das pessoas, não se expondo, em consequência, enquanto valor constitucional que é, a intervenções de terceiros ou a intrusões do Poder Público desvestidas de causa provável ou destituídas de base jurídica idônea".

gistros de acesso a aplicações de internet devem indicar: (i) "fundados indícios da ocorrência do ilícito"; (ii) "justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória"; e (iii) o "período ao qual se referem os registros".

O que se tem, portanto, é a proibição do anonimato, de um lado, e uma proteção robusta ao sigilo dos dados sobre comunicações, de outro. Longe de se tratar de situação inconciliável, o aparente conflito entre as normas exige apenas uma acomodação hermenêutica dos dois comandos normativos[581].

E note-se: a necessidade de interpretação *temperada* da proibição do anonimato sequer é inédita na história brasileira. No direito penal, a parte final do art. 5º, IV da Constituição é fundamento também para a proibição das denúncias anônimas. A vedação, contudo, foi mitigada para barrar apenas o oferecimento de denúncias fundadas *exclusivamente* em acusações anônimas, mas admitir que essas sejam usadas como um dos elementos da denúncia[582]. A flexibilização

581 Para uma discussão mais profunda sobre a viabilização da flexibilização da interpretação da regra da vedação do anonimato, v.: Mariana Cunha e Melo, **The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law.** Curitiba: CRV, 2016.

582 BRASIL, STJ, DJe 16/05/2013, RMS 38.010/RJ, Rel. Min. Herman Benjamin: "2. O simples fato de o Inquérito Civil ter-se formalizado com base em denúncia anônima não impede que o Ministério Público realize administrativamente as investigações para formar juízo de valor sobre a veracidade da notícia. Ressalte-se que, no caso em espécie, os servidores públicos já estão, por lei, obrigados na posse e depois, anualmente, a disponibilizar informações sobre seus bens e evolução patrimonial. (...) 5. **A vedação ao anonimato, constante no art. 5º, IV, da Constituição Federal, há de ser harmonizada, com base no princípio da concordância prática, com o dever constitucional imposto ao Ministério Público de promover o Inquérito Civil e a Ação Civil Pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos (art. 129, III).** 6. Nos termos do art. 22 da Lei 8.429/1992, o Ministério Público pode, mesmo de ofício, requisitar a instauração de inquérito policial ou procedimento administrativo para apurar qualquer ilícito previsto no aludido diploma legal. 7. Assim, ainda que a notícia da suposta discrepância entre a evolução patrimonial de agentes políticos e seus rendimentos tenha decorrido de denúncia anônima, não se pode impedir que o membro do Parquet tome medidas proporcionais e razoáveis, como no caso dos autos, para investigar a veracidade do juízo apresentado por cidadão que não se tenha identificado. 8. Em matéria penal, o STF já assentou que 'nada impede, contudo, que o Poder Público provocado por delação anônima ('disque-denúncia', p. ex.), adote medidas informais destinadas a apurar, previamente, em averiguação sumária, 'com prudência e discrição', a possível ocorrência de eventual situação de ilicitude penal, desde que o faça com o objetivo de conferir a verossimilhança dos fatos nela denunciados, em ordem a promover, então, em caso positivo, a formal instauração da persecutio criminis, mantendo-se, assim, completa desvinculação desse procedimento estatal em relação às peças apócrifas' (Inq 1.957, Rel. Min. Carlos Velloso, voto do Min. Celso de Mello, julgamento em 11.5.2005, Plenário, DJ de 11.11.2005). 9. Em se tratando de suposto ato de improbidade que só pode ser analisado mediante documentos, descabe absolutamente adotar medidas informais para examinar a verossimilhança, ao contrário do que se passa, por exemplo, em caso de denúncia anônima da ocorrência de homicídio. 10. O STJ reconhece a possibilidade de investigar

da proibição constitucional foi justificada nesses casos para que fosse compatibilizada com o interesse constitucional na persecução criminal. Ainda que essa circunstância não justifique, por si só, a interpretação mais branda da proibição do anonimato, indica que a vedação não merece – e não recebe – a interpretação absoluta defendida por alguns críticos do uso do anonimato na internet.

A questão do devido processo legal

O tópico anterior fez uma análise positiva dos dois pólos da discussão sobre anonimato na internet no Brasil[583]. Sob o viés da proteção do sigilo constitucional (art. 5º, X), foram vistos alguns requisitos para a fundamentação das decisões de quebra. Essas garantias estão no cerne da proteção procedimental da intimidade dos usuários de internet e devem ser feitas valer. Às previsões já aventadas pela jurisprudência e pelo Marco Civil, porém, devem ser acrescidas outras, igualmente importantes, mas frequentemente negligenciadas na prática brasileira.

Com efeito, o conteúdo básico do devido processo legal impõe que não se afaste a proteção constitucional do sigilo de dados sem que ao menos a notificação do interessado para que esse possa, se achar necessário, defender seu direito fundamental. Importantes argumentos de ampla defesa conduzem a essa conclusão. ***Em primeiro lugar***, trata-se da literalidade do art. 5º, LIV da Constituição. Com efeito, o dispositivo determina que "ninguém será privado da liberdade ou de seus bens sem o devido processo legal". O princípio, portanto, pressupõe uma oitiva prévia de quem está por ter sua liberdade restringida. No caso da quebra de sigilo, a hipótese dificilmente poderia ser mais grave. Afinal, a divulgação de dados sigilosos representa a restrição máxima da garantia do sigilo.

Seria possível argumentar que essa circunstância não é inconstitucional nem infrequente no ordenamento brasileiro. E isso porque o sistema processual admite a concessão de decisões liminares sem a prévia oitiva do réu. A existência dessa prática, no entanto, não resolve o problema constitucional. Primeiramente, porque a própria ideia de provimento de tutela satisfativa *inaudita altera pars*

a veracidade de denúncia anônima em Inquérito Civil ou Processo Administrativo, conforme se observa nos seguintes precedentes, entre os quais se destacam a orientação já firmada por esta Segunda Turma e uma recente decisão da Primeira Turma: RMS 37.166/SP, Rel. Ministro Benedito Gonçalves, Primeira Turma, DJe 15.4.2013; RMS 30.510/RJ, Rel. Ministra Eliana Calmon, Segunda Turma, DJe 10.2.2010; MS 13.348/DF, Rel. Ministra Laurita Vaz, Terceira Seção, DJe 16.9.2009".

583 Para uma análise normativa desta autora sobre a matéria, v.: CUNHA E MELO, Mariana. **The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law**. Curitiba, CRV, 2016.

em restrição direta a direitos fundamentais é, em si, questionável. Não por outra razão, os tribunais superiores registram em diversos julgados e o Congresso Nacional explicitou na Lei nº 8.437/92 a impossibilidade de concessão de liminar satisfativa em processo civil[584], penal[585], trabalhista[586] e contra a fazenda pública[587].

Em segundo lugar, a exemplo do que ocorre em conflitos de outros direitos fundamentais[588], quando o autor de um pedido de quebra aciona o provedor de serviço de internet, a discussão sobre a necessidade e pertinência do fornecimento dos dados é substancialmente mitigada[589]. No mínimo, o peso argumentativo de um terceiro defender direito alheio é consideravelmente menor do que o peso da defesa do próprio interessado. Isso porque a demanda perde o enfoque de conflito entre direitos fundamentais e passa a assumir contornos de direito do consumidor – o cidadão que se sentiu ofendido, de um lado, e a empresa provedora de serviço de internet, de outro. Além disso, do ponto de vista do conteúdo da defesa do conteúdo impugnado, quando se retira o foco da discussão da relação autor-ofendido para a relação provedor-ofendido, uma série de questões podem passar despercebidas. O provedor não terá subsídio para deduzir razões específicas da legalidade da conduta do usuário cujo sigilo seria quebrado. Tampouco poderia a empresa defender de forma precisa a relevância da manutenção do sigilo de dados em cada caso.

Não por outra razão, o Código de Processo Civil restringe o alcance subjetivo dos efeitos da sentença. O art. 506 dispõe que a sentença faz coisa julgada para as partes da demanda e que não beneficia nem prejudica terceiros. Além disso, o art. 18 prevê que a nenhuma das partes é dado defender, em nome próprio, direito alheio. Nesse particular, a legislação processual pretende evitar que se criem

584 BRASIL, STJ, DJ 20 jun. 2005, AgRg no REsp 584.527/RN, Rel. Min. Laurita Vaz.

585 BRASIL, STF, DJ 21 mai. 2012, HC 112487/PR, Rel. Min. Celso de Mello.

586 BRASIL, STF, DJ 29 ago. 2003, RE 162309/PE, Rel. Min. Marco Aurélio.

587 BRASIL, Lei nº 8.437/1992, art. 1º, § 3º.

588 V. CUNHA E MELO, Mariana, O significado do Direito ao Esquecimento, **Jota**, nov. 2016. Disponível em: <http://jota.info/artigos/o-significado-direito-ao-esquecimento-22112016> Acesso em: 23.03.17.

589 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 330 (2008). "Finally, although a motion to quash may well be appropriate, without proper notice, John Doe subpoenas can easily become ex parte proceedings. In many jurisdictions, defendants must rely on the business policies of the subpoena's target or the goodwill of the plaintiff to receive notice. Even if the plaintiff does attempt to notify the defendant, he could fail—the defendant is, after all, anonymous. If the subpoena becomes ex parte, one of the defendant's most important defenses—his own vigorous advocacy—is eliminated. This combination of severe consequences meted out after limited trial process, possibly without opposition from the defendant whose identity is at risk, is a dangerous recipe that demands a carefully balanced standard".

substitutos processuais fora das hipóteses legais taxativas. Essa proibição tem o claro objetivo de proteger ao menos três classes de interesse: (i) o da parte em não ter seu direito defendido por terceiros sem seu consentimento; (ii) o do *ex adverso* em litigar com seu real opositor, inclusive como requisito para a obtenção de um provimento válido; e (iii) o do intermediário, que seria prejudicado com o ônus excessivo de proteger, além dos seus próprios interesses, o direito de outrem – e sem condições materiais para fazê-lo de forma plenamente adequada.

Em terceiro lugar, além dos riscos para o usuário titular do direito ameaçado pelo pedido de fornecimento de dados, há também dois graves problemas procedimentais que agridem a esfera jurídica dos provedores de serviço da internet e que merecem destaque. O primeiro é o ônus de ser o único capaz de contraditar ordens abusivas direcionadas a seus usuários. Trata-se de uma situação difícil em que o provedor de serviços ou assume o ônus – financeiro e de imagem – inerente à impugnação reiterada de ordens judiciais ou relega seus usuários ao risco de uma quebra de sigilo sem contraditório nem controle externo.

O segundo, relacionado ao primeiro, é que frequentemente o provedor de serviço é condenado a arcar com os ônus sucumbenciais em caso de deferimento do pedido de fornecimento de dados. Ocorre que a intervenção do Poder Judiciário é indispensável para a legitimidade da quebra de sigilo, por comando legal e constitucional. Ou seja: em princípio, a empresa não "dará causa" ao processo judicial[590] ao resistir a uma pretensão legítima do autor da demanda. Afinal, não poderia legalmente fornecer os dados de identificação de usuários sem uma decisão judicial. Assim, a "causa" do processo, nesses casos, é a exigência constitucional de judicialização do conflito. Nesses casos, não parece coerente com a teoria processual a empresa ser obrigada a arcar com a sucumbência.

Em suma: já vimos que há boas razões jurídicas para que pessoas ofendidas por atos ilícitos na internet tenham meios de identificar os responsáveis pelas ilicitudes. Vimos também, contudo, que a Constituição brasileira protege os sigilos de dados em geral e, em especial, aqueles que dizem respeito às comunicações. Nesse cenário, a quebra de sigilos sem a oitiva do interessado é providência no mínimo pouco usual no panorama processual e constitucional.

590 Na doutrina processual civil brasileira, a parte que dá causa ao processo arca com os custos da ação. Ou seja: o autor, caso esse tenha ajuizado a demanda sem que tivesse o direito material pleiteado ou o réu, caso esse tenha resistido a uma pretensão legítima do autor, obrigando-o a se valer da estrutura judicial para garantir seu direito. V.: DINAMARCO, Cândido Rangel. **Instituições de Direito Processual Civil**, vol II, 6ª ed. São Paulo: Malheiros, 2009.

O próximo tópico irá analisar alternativas para conciliar os dois pólos: (i) o interesse na identificação dos responsáveis pelo cometimento de ilícitos; e (ii) a garantia do sigilo de dados e do devido processo legal.

Modelos de proteção do devido processo legal aplicado à proteção de dados

Nos Estados Unidos, o anonimato é considerado um direito fundamental decorrente da liberdade de expressão[591]. Essa proteção especial do anonimato pode soar estranha no sistema brasileiro que, nesse particular, adotou postura diametralmente oposta. No Brasil, o anonimato é vedado pelo mesmo dispositivo constitucional que garante a livre manifestação do pensamento.

Como já mencionado, no entanto, a parte final do art. 5º, IV da Constituição não encerra todas as discussões sobre a identidade de usuários de internet. Isso porque a proteção dos sigilos constitucionais deve também ser equacionada nesses casos. E, vale notar, essa proteção especial aos sigilos e à privacidade de forma geral não encontra paralelo no direito constitucional norte-americano. Esse enfoque especial na liberdade de expressão nos Estados Unidos e na privacidade no Brasil é marca de uma dicotomia clássica entre as tradições jurídicas norte-americana e europeia, muitas vezes caracterizada como um enfoque maior na liberdade, de um lado, e na dignidade da pessoa humana, de outro[592].

O que é importante notar neste ponto é que, seja qual for o fundamento constitucional e o ponto de vista da proteção material – liberdade de expressão (anonimato) ou privacidade (sigilo de dados) –, é possível concluir que o ato de fornecer dados pessoais capazes de identificar usuários de internet é de considerável gravidade constitucional nos dois países. Por essa razão, não há qualquer incoerência em voltar-se à experiência americana em busca de modelos de proteção ao devido processo legal em matéria de fornecimento de dados de usuários.

E os Estados Unidos possuem vasta experiência na elaboração desses procedimentos, equacionando a proteção do anonimato dos usuários de internet, de um lado, e a possibilidade de responsabilização dos autores de ilícitos, de outro. Apesar das grandes diferenças nos parâmetros aplicados e em alguns detalhes

591 SUPREMA CORTE DOS ESTADOS UNIDOS, **Mclntyre v. Ohio Elections Commission**, 514 U.S. 334, 342 (1995)

592 WHITMAN, James Q., The Two Western Cultures of Privacy: Dignity versus Liberty, **113 The Yale Law Journal**, 1165, Apr., 2004. Disponível em: <http://www.jstor.org/stable/4135723> Acesso em: 23.03.17.

procedimentais, é possível identificar um procedimento geral que se generalizou entre os Estados federados. A característica mais marcante desse procedimento é que ele é sempre ajuizado contra um *John Doe* ou uma *Jane Doe*. O termo se refere a um nome genérico, algo que, no Brasil, chamaríamos de "Fulano de Tal". Em linhas gerais, o processo contra um *John* ou *Jane Doe* é formalizado por um autor definido contra uma pessoa ainda desconhecida. Nesses casos, a primeira fase do procedimento é, naturalmente, desvendar a identidade do réu – o que muitos denominam de "*unmask John Doe*" (desmascarar John Doe)[593].

Existem diversos procedimentos diferentes para processar um John Doe, a depender do Estado da federação americana[594]. A depender das opções específicas locais, o processo pode ser mais favorável aos autores[595] ou aos réus[596]. É possível, contudo, extrair uma ideia geral a partir de uma análise conjunta desses procedimentos. Com efeito, e de forma geral, duas características importantes devem ser destacadas: (i) viabilizam a tutela procedimental do direito fundamental a ser restringido (liberdade de expressão ou privacidade) sem desguarnecer a proteção dos interesses daqueles ofendidos por ilícitos praticados na internet por usuários anônimos[597]; e (ii) permitem uma análise individualizada da justiça e da necessidade de se fornecer os dados dos usuários, o que favorece um rigor maior na apreciação da matéria.

---

593 ELECTRONIC FRONTIER FOUNDATION, **Test for Unmasking Anonymous Speech. Internet Law Treatise**. Disponível em <http://ilt.eff.org/index.php/Speech:_Anonymity#Tests_for_Unmasking_Anonymous_Speakers> Acesso em: 23.03.17.

594 Nathaniel Gleicher identifica ao menos sete modelos: Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999); Mobilisa, Inc. v. Doe 1, 170 P.3d 712 (Ariz. Ct. App. 2007); Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231 (Ct. App. 2008); Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005); Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); *In re* Subpoena Duces Tecum to Am. Online, Inc. (*In re AOL)*, 52 Va. Cir. 26 (Cir. Ct. 2000), *rev'd on other grounds sub nom*. Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001). GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320 (2008).

595 V., por exemplo: ESTADOS UNIDOS DA AMÉRICA, CORTE FEDERAL DE VIRGÍNIA, **In re AOL**, 52 Va. Cir. 26.

596 V., por exemplo: ESTADOS UNIDOS DA AMÉRICA, CORTE SUPERIOR DE NEW JERSEY, **Dendrite**, 775 A.2d 756.

597 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 325 (2008): "Although John Doe subpoenas are procedural tools, the standards governing them define the extent of First Amendment rights online. A standard that is too permissive severely weakens the ability of citizens to speak anonymously, limiting freedom of speech online. Too restrictive a standard leaves the increasing litany of targets of online harassment with no defense. Only a consistent nationwide standard for John Doe subpoenas will ensure balanced protection for both anonymous online speakers and the targets of anonymous online speech".

De forma mais específica, vale destacar o profundo e sistêmico estudo desenvolvido por Nathaniel Gleicher. Em artigo antológico, o especialista em cyber segurança condensou o complexo material jurisprudencial sobre o tema e extraiu seis fatores principais para a formulação de uma moldura legal que regule com justiça e segurança o processo de fornecimento de dados de usuários.

A ***primeira*** é a oportunidade de o interessado participar do procedimento e apresentar defesa sem que precise desvendar sua identidade. Esse é o ponto central da defesa do devido processo legal nesses casos. Sem dúvida, é uma questão que, por si só, provoca muitas dificuldades. Como notificar o usuário objeto da ordem? Qual deve ser o meio adequado? Quem deve ter o ônus da notificação e suportar os custos? Como permitir a representação de uma pessoa nos autos de um processo sem sua adequada qualificação? Qual seria o prazo de resposta do usuário?

Não cabe no propósito deste artigo desenvolver todos esses questionamentos. As três primeiras perguntas demandam uma reflexão mais urgente e merecem uma consideração adicional. Quanto à distribuição do ônus da notificação, dentre as diversas alternativas, existem jurisdições que exigem que o próprio autor empregue um "esforço razoável" para notificar o usuário do ajuizamento da ação e o seu teor[598]. Como o interesse na obtenção da informação é exclusivamente do autor, parece fazer sentido, ao menos em princípio, que ele arque com esse ônus.

Por outro lado, o esforço razoável de alguém se comunicar com um usuário anônimo nem sempre será uma tarefa simples[599]. Assim, outras jurisdições optam por requerer que o próprio destinatário da ordem de fornecimento de dados se comunique com o titular dos dados requeridos – ou seja: o prestador do serviço utilizado pelo usuário anônimo. A empresa, em geral, está em posição privilegiada para contactar seus usuários e, portanto, teria maior probabilidade de sucesso no propósito de notificar o interessado[600].

---

598 SUPREMA CORTE DE DELAWARE, **Doe No. 1 v. Cahill**, 884 A.2d 451, 461 (Del. 2005). V., também: ELECTRONIC FRONTIER FOUNDATION, **Test for Unmasking Anonymous Speech. Internet Law Treatise**, disponível em <http://ilt.eff.org/index.php/Speech:_Anonymity#Tests_for_Unmasking_Anonymous_Speakers>. Acesso em: 23.03.17.; "As best practices, those third parties should: **Make reasonable efforts** to notify the person whose identity is sought; If possible, agree to a timetable for disclosure of the information to the party seeking it that provides a reasonable opportunity for the Internet user to file an objection with a court before disclosure; Forward the exact statements and material provided by the person seeking the identity, including information about the cause of action alleged in the lawsuit and the evidence provided by the identityseeker to the court where provided to the service provider".

599 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** , 320, 346 (2008).

600 É o caso da regulação no Estado da Virginia. Confira-se em DIGITAL MEDIA LAW PROJECT, **Legal Protections for Anonymous Speech in Virginia**, disponível em <http://www.dmlp.org/legal-guide/legal-protections-anonymous-speech-virginia>. Acesso em: 23.03.17.

Quanto ao meio de notificação, Gleicher aventa três possibilidades, em escala decrescente de confiabilidade em sua eficácia: (i) notificação direta – via e-mail ou outro meio privado; (ii) notificação pelo meio de comunicação utilizado para a suposta ofensa; e (iii) notificação via publicação[601]. As opções naturalmente não são excludentes e podem ser combinadas de múltiplas formas. E a notificação direta nem sempre será possível em razão da falta de informação sobre o usuário em questão.

Nos Estados Unidos, organizações de defesas de direitos civis na internet, como a *Electronic Frontier Foundation* atuam na representação de *John Doe*'s em juízo[602].

O direito brasileiro não admite a tramitação de processo contra pessoa indeterminada. De outra forma, não seria possível a autuação do processo (CPC, art. 206), a citação (CPC, art. 238) ou a representação da parte por advogado constituído nos autos (CPC, art. 104). Há, por outro lado, uma figura no processo civil brasileiro, que atua em casos em que a parte, apesar de titular de direitos, não possui capacidade de estar em juízo. Trata-se da figura da curatela especial, que o Código de Processo Civil e a Lei Complementar nº 80 atribuem à Defensoria Pública. A curatela especial se presta a garantir a presença nos autos de quem, de outra forma, não poderia. O art. 72 do Código de Processo Civil prevê a atuação do curador especial para assistir (i) a parte incapaz sem representante legal ou quando os interesses desse e daquele forem conflitantes; e (ii) o réu revel, quando esse estiver preso ou em casos de citação ficta (por edital ou por hora certa), até que seja constituído advogado nos autos.

Do ponto de vista prático, a atividade da Defensoria Pública nos casos previstos no art. 72 do Código de Processo Civil não se distancia muito da atividade das organizações sem fins lucrativos nos Estados Unidos. Os dois se prestam a viabilizar a defesa nos autos em casos em que o próprio titular do direito se vê impossibilitado de fazê-lo por seus próprios meios – seja porque é incapaz para os atos da vida civil e não tem representante legal, conforme previsto no art. 72, I do Código de Processo Civil (impossibilidade jurídica), seja porque não foi localizado, conforme previsto no art. 72, II do Código de Processo Civil (impossibilidade fática), seja porque o comparecimento aos autos faria perecer o próprio direito que se defenderia em juízo, como no caso do anonimato (impossibilidade lógica).

---

601 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 347 (2008)

602 Uma lista dos processos em que o EFF atua pode ser encontrada em: <https://www.eff.org/issues/free-speech>. Acesso em: 23.03.17.

Nesse contexto, seria de se imaginar a possibilidade de se chamar a Defensoria Pública à responsabilidade de defender o sigilo de dados dos usuários, inclusive fazendo esforços razoáveis para tentar contactá-los para fins de alinhamento da estratégia de defesa. Isso, é claro, sem prejuízo de, uma vez comunicado da pendência de processo judicial, o usuário poder optar por constituir seu próprio representante. A providência estaria alinhada com as funções e os objetivos básicos da Defensoria Pública, esculpidos nos arts. 3º e 4º de sua lei orgânica: a "primazia da dignidade da pessoa humana"; a "prevalência e efetividade dos direitos humanos"; a "garantia dos princípios constitucionais da ampla defesa e do contraditório"; e a promoção da "mais ampla defesa dos direitos fundamentais dos necessitados, abrangendo seus direitos individuais, coletivos, sociais, econômicos, culturais e ambientais, sendo admissíveis todas as espécies de ações capazes de propiciar sua adequada e efetiva tutela".

O ***segundo*** fator relevante é que se exija um nível mínimo de plausibilidade da pretensão do autor. A exigência faz muito sentido se considerarmos que, até que seja confirmada a ilicitude da conduta do usuário, deve ser protegido o sigilo de dados, no caso brasileiro, e o anonimato, na tradição norte-americana. Além de se tratar de uma exigência própria do direito material em jogo, o requisito também assume um claro contorno de proteção da presunção de inocência (CF, art. 5º, LVII).

No Brasil, esse tipo de exigência aparece no direito processual civil sob a forma do requisito do *fumus boni juris*. Nos Estados Unidos, por outro lado, há uma grande variedade de níveis de exigências. São eles: (i) boa-fé (*good faith*), um requisito muito brando e que no direito brasileiro aparece como uma exigência geral para todos os litigantes, a todo momento, sob pena de multa[603]; (ii) sobreviver a um pedido de arquivamento (*motion to dismiss*), que exige apenas que a pretensão do autor supere o nível de *especulação*, assumindo que todas as alegações sejam verdadeiras; (iii) sobreviver a um pedido de julgamento sumário (*summary judgement*), que exige a prova de um elemento essencial para a fundamentação da pretensão do autor; e (iv) estabelecer um caso *prima facie* (*a prima facie evidentiary showing*), que exige que nenhuma prova em contrário tenha sido apresentada até o momento[604].

Antes de qualquer consideração quanto ao parâmetro legal de plausibilidade do direito do autor, vale notar que a possibilidade de provimento de tutela satisfativa em restrição direta a direitos fundamentais deve ser considerada com

603 BRASIL, Código de Processo Civil, arts. 5º e 79-81.

604 CORTE DE APELAÇÕES DO TERCEIRO DISTRITO, **Valencia v. Citibank Int'l**, 728 So. 2d 330.

grande cautela[605]. Do ponto de vista material, os já referidos requisitos impostos pela jurisprudência do Supremo Tribunal Federal em matéria de quebra de sigilo de dados sobre comunicações e pelo art. 22 do Marco Civil da Internet já estabelecem sarrafo suficientemente alto para garantia do direito fundamental à privacidade – se observados com rigor pelas Cortes, naturalmente. Trata-se, vale lembrar, da exigência de demonstração da ilegalidade da conduta, na necessidade da providência e do período de tempo compreendido pela ordem.

Quanto ao ***terceiro*** fator, a relevância da obtenção das informações requeridas, seu fundamento central repousa também na circunstância de se estar diante da restrição de um princípio fundamental. E que, por dever de razoabilidade[606], essas restrições devem ser mantidas em um mínimo indispensável para proteger outros princípios de mesma estatura constitucional. Nesse ponto, mesmo as jurisdições com procedimentos mais vantajosos aos autores exigem que a "informação sobre a identidade requerida seja centralmente necessária para viabilizar a pretensão material do autor"[607]. Outros Estados exigem que a "informação seja suficiente para estabelecer ou contradizer que a pretensão ou a defesa seria inviável com o uso de qualquer outro meio"[608]. Apesar da pluralidade de níveis de exigência, a noção é muito próxima da exigência brasileira de interesse de agir nos procedimentos cíveis em geral e, em especial, quando se trate de restrição a direitos fundamentais.

O ***quarto*** fator, ponderação de interesses entre o autor e o réu não representa qualquer novidade ao direito brasileiro. De toda forma, é um fato importante de ser destacado para que não se perca de vista que pedidos de fornecimento de dados são conflitos entre direitos fundamentais. O ***quinto*** aspecto relevante é a exigência de que as provas produzidas sejam específicas, para evitar que o autor afogue a corte e o réu em documentos desnecessários, dificultando a defesa. Por fim, o ***sexto*** fator destacado por Gleicher consiste na demonstração de que o autor esgotou todos os meios extrajudiciais disponíveis para identificar o usuário antes de submeter a matéria à corte.

---

605 Não por outra razão, os tribunais superiores registram em diversos julgados e o Congresso, na Lei nº 8.437/92, a impossibilidade de concessão de liminar satisfativa em processo civil (BRASIL, STJ, *DJ* 20 jun. 2005, AgRg no REsp 584.527/RN, Rel. Min. Laurita Vaz), penal (BRASIL, STF, *DJ* 21 mai. 2012, HC 112487/PR, Rel. Min. Celso de Mello), trabalhista (BRASIL, STF, *DJ* 29 ago. 2003, RE 162309/PE, Rel. Min. Marco Aurélio) e contra a fazenda pública (BRASIL, Lei nº 8.437/1992, art. 1º, § 3º).

606 V.: BARROSO, Luís Roberto; DE BARCELLOS, Ana Paula. O começo da história: o Papel dos Princípios no Direito Brasileiro, p. 65, disponível em <http://www.emerj.tjrj.jus.br/revistaemerj_online /edicoes/revista23/revista23_25.pdf> Acesso em: 23.03.17.

607 ESTADOS UNIDOS DA AMÉRICA, CORTE FEDERAL DE VIRGÍNIA, **In re AOL**, 52 Va. Cir. 26.

608 ESTADOS UNIDOS DA AMÉRICA, CORTE FEDERAL DE WASHINGTON, Doe v. 2theMart.com, 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001)

Conclusão: regras e procedimentos para o fornecimento de dados de usuários

A correta calibragem do procedimento a ser adotado para o fornecimento de dados de usuários é de extrema relevância e complexidade[609]. Sua definição impacta o nível de proteção à privacidade, ao devido processo legal e à presunção de inocência, de um lado, e aos direitos à honra e à intimidade, de outro. Ainda que a sintonia fina do procedimento demande uma análise mais detida dos riscos e benefícios em cada detalhe, espera-se que a presente análise ajude a traçar linhas gerais de uma moldura legal adequada para o fornecimento de dados. E que o presente estudo sirva de propulsor para pesquisas complementares nessa área.

609 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 329 (2008): "John Doe subpoenas can have severe consequences, potentially causing irreparable harm to defendants if granted, and denying plaintiffs the opportunity to seek relief for their harms if denied. A defendant who is exposed could be subject to reprisals or severe social and professional sanctions, making extreme care necessary when exposing potentially innocent defendants. At the same time, a plaintiff who is denied the identity of his defendant is left with no recourse and has his suit effectively denied without a hearing on the merits".

Desafios à Privacidade: Big Data, Consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de Dados Pessoais

Rodrigo Dias de Pinho Gomes[610]

O que é big data?

O termo *big data* surgiu no início do século XXI[611], sendo inicialmente utilizado por astrônomos e geneticistas, em momento no qual a memória dos computadores não se mostrava capaz de armazenar toda a quantidade de informação disponível, obrigando-os a pensar em novas formas e instrumentos para analisar estes grandes bancos de dados.

Trata-se de uma expressão bastante ampla, vaga e imprecisa[612], muitas vezes até criticada[613], que comporta diversas interpretações e variados significados, principalmente por ser utilizada por diversos setores, como especialistas em tecnologia, juristas e autoridades públicas.

Apesar de ser objeto de ampla difusão[614], não se alcançou uma definição uníssona do termo, valendo destacar algumas que servem como orientação ao presente estudo.

---

610 Advogado. Mestre em Direito Civil pela UERJ. Pesquisador na European University Institute - San Domenico di Fiesole, Itália. Especialista em Direito Civil-Patrimonial pela PUC-RIO.

611 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big Data: A Revolution That Will Transform How We Live, Work, and Think**. New York. Houghton Mifflin Harcourt, 2013. p. 6.

612 "Big data is a generalized, imprecise term that refers to the use of large data sets in data science and predictive analytics." Kate Crawford and Jason Schultz, big data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C.L. Rev. 93 (2014). Disponível em: <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>. Acesso em: 29/08/2016.

613 "Big data is, in many ways, a poor term." BOYD, Danah. CRAWFORD, Kate. **Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon**. Information, Communication & Society. Vol. 15, Issue 5. 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. p. 663.

614 Pesquisa pelo termo "*big data*" no google.com revela aproximadamente 263.000.000 resultados. Acesso em: 15/08/2016.

Viktor Mayer-Schonberger, professor da Universidade Oxford, defende que: "Big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more."[615]

O Instituto de Tecnologia & Sociedade do Rio define o termo na seguinte passagem: "O conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores."[616]

O Article 29 Working Party, organização de caráter consultivo e independente, criada pela Diretiva 95/46/EC do Parlamento Europeu, assim estabelece[617]:

> Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organizations, which are then extensively analyzed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals[618].

Em 2001, Doug Laney[619] já previa este cenário, especialmente no campo empresarial, com o aumento crescente da relevância dos bancos de dados, lan-

---

615 Tradução livre: big data refere-se a coisas que se podem fazer em grande escala, que não podem ser feitas em escala menor, de forma a extrair novas ideias ou criar novas formas de valor, de maneira que acabam mudando mercados, organizações, a relação entre os cidadãos e os governos, dentre outros. MAYER-SCHONBERGER, Viktor. op. cit., p. 6.

616 Big data no projeto Sul Global. Relatório sobre estudos de caso. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 09 ago. 2016.

617 "The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently". Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>. Acesso em: 30 out. 2016.

618 Tradução livre: "Big data se refere ao crescimento exponencial tanto na disponibilidade quanto no uso automatizado de informação: refere-se a conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grande porte, que são amplamente analisados (daí o nome: *analytics*) usando algoritmos de computador. Big data pode ser usado para identificar tendências mais gerais e correlações, mas também pode ser processado, de modo a afetar diretamente os indivíduos." Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> Acesso em 12/10/2016>. Acesso em: 30 out. 2016.

619 LANEY, Doug. **Data Management - Controlling Data Volume, Velocity and Variety**. META GROUP. Publicado em: 06 fev. 2001. Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-

çando a pedra fundamental do que foi denominado "3 V" no universo do big data, ao afirmar que as companhias deveriam dar atenção especial ao substancial incremento do volume, velocidade e variedade das informações.

Volume se refere à grande quantidade de dados, velocidade seria aquela com a qual as informações são captadas e transmitidas – muitas vezes em tempo real e ininterruptamente –, e variedade seria a multiplicidade de tipos de dados e fontes para a obtenção desses em larga escala. Em síntese: "The evolving era of big data implies, by its very nature, a lack of control, since the volume of data is unprecedented, diverse in variety and moving with a velocity that is increasingly approaching real time."[620]

Afirma-se ainda que, além dessas três dimensões que compõem o big data, deve-se ainda incluir a veracidade[621]neste conjunto, pois, diante da enorme quantidade de informações contidas nos bancos de dados, certamente haverá dados imprecisos e até equivocados, urgindo por cautela e tecnologia de ponta para identificar e não se deixar enganar por tais imperfeições[622].

Atualmente, não é exagero afirmar que o termo big data se tornou um verdadeiro jargão[623], sendo para alguns a expressão de um fenômeno[624] cultural e tecnológico. Vale frisar que muitos dos benefícios provenientes do big data ocorrem através da análise e utilização secundária[625] do banco de dados, ou seja, distante da finalidade inicial para qual os dados foram coletados. Em outras palavras:

3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em: 09 ago. 2016.

620 HIJMANS, Hielke. **The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU**. Springer International Publishing, 2016. p. 96.

621 "For the purpose of this report one more interesting dimension of big data is also veracity, which describes the incompleteness (inconsistency, inaccuracy) of data". Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016.

622 The Four V's of Big Data. IBM Big Data & Analytics Hub. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 15 ago. 2016.

623 Big data no projeto Sul Global - Relatório sobre estudos de caso. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 09 ago. 2016.

624 BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. "We define big data1 as a cultural, technological, and scholarly phenomenon". **Information, Communication & Society.** Vol. 15, Issue 5. 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. p. 663.

625 "With big data, the value of information no longer resides solely in this primary purpose. As we've argued, it is now in secondary uses". MAYER-SCHONBERGER, Viktor. op. cit. p. 153.

> One of the main targets of big data analytics is to use data, alone or in combination with other data sets, beyond their original point and scope of collection. The scalability of storage allows for potential infinite space, which means that data can be collected continuously until a new value can be created from insights derived out of them[626].

Um exemplo contundente da utilização secundária das informações se verificou através da análise de mais de 350 milhões de *tweets* pela Organização das Nações Unidas na tentativa de auxiliar o Poder Público no combate à fome em locais menos favorecidos[627].

Assim, sem qualquer pretensão de esgotar o tema ou oferecer uma definição jurídica precisa, parece possível entender que big data se refere, necessariamente, à análise de grande quantidade de dados[628], realizada de maneira automatizada por algoritmos, com intuito de extrair resultados e benefícios.

O acúmulo de conhecimento e informação, que um dia significou estudar, conhecer e compreender o passado, está se transformando, significando, com o big data, a habilidade de prever o futuro[629]. Com isso, abre-se a possibilidade concreta de se achar uma agulha no palheiro[630], utilizando-se de algoritmos e mecanismos de inteligência artificial, que alimentados de maneira contínua com tais bancos de dados extraem valores disso, permitindo até a tomada de decisões autônomas e fornecendo novos dados cuja análise humana jamais poderia conceber ou imaginar.

---

626 **Privacy by Design in Big Data**. ENISA. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016.

627 "When correlations between social media conversations on food-related topics and official inflation data started to emerge, Jakarta's Global Pulse analysts were able to flag the likely local impacts of the crisis and deploy resources accordingly. In 2014, Global Pulse implemented over 25 joint data innovation projects worldwide. Implementation involved the analysis of over 350 million tweets". EVANS, Bryce. Using Big Data to Achieve Food Security. In: BUNNIK, Anno; CAWLEY, Anthony; MULQUEEN, Michael; ZWITTER, Andrej. **Big Data Challenges: Society, Security, Innovation and Ethics. Palgrave Macmillan**, 2016. p. 129.

628 Big data is less about data that is big than it is about a capacity to search, aggregate, and cross-reference large data sets. BOYD, Danah; CRAWFORD, Kate. **Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society**. Vol. 15, Issue 5. 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>, p. 663. Acesso em: 21/03/2017.

629 MAYER-SCHONBERGER, Viktor. op. cit. p. 190.

630 "However, big data changes the paradigm. One can collect large amounts of data and draw effect from it. In other words: one can find the needle in the haystack." HIJMANS, Hielke. **The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU.** Springer International Publishing, 2016. p. 100.

Contudo, apesar dos inegáveis benefícios econômicos e sociais, o big data desafia diversos institutos jurídicos, concebidos em conjuntura totalmente diversa da atual, especialmente a privacidade, que se desenvolveu com base no consentimento do titular para tornar lícito o tratamento de seus dados pessoais. Adiante, pretende-se demonstrar como o consentimento tem sofrido questionamentos, inclusive no continente Europeu onde a tutela da privacidade se mostra mais efetiva, revelando ainda, de maneira singela, algumas formas alternativas de legitimar o tratamento de dados pessoais.

Big data e consentimento

Com razão se afirmou que "o consentimento é o pilar regulatório adotado para a proteção de dados pessoais"[631], funcionando desde a década de 1990 na Europa[632] como ponto de partida a legitimar e justificar a licitude da coleta, tratamento e análise de dados pessoais do titular. O regulamento 2016/679 do Parlamento Europeu e do Conselho[633] faz reacender essa chama em diversas passagens, trazendo o instituto do consentimento como a chave mestra do cofre que dá acesso aos dados pessoais, porém contemplando novas formas, além dele, que conferem licitude ao tratamento de dados.

Considerando a efetiva tutela dos dados pessoais naquele continente, através da chamada quarta geração de leis[634] que estabelece limitações e regras rígidas sobre o consentimento, instituindo procedimentos estritos de coleta, tratamento, compartilhamento e armazenamento dos dados pessoais, tem-se a

631 O que está em jogo no debate sobre dados Pessoais no Brasil? INTERNETLAB. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Acesso em: 27 ago. 2016.

632 "At EU level, reliance on consent as a criterion for legitimising personal data processing operations was foreseen from the very beginning of the legislative process that ended with the adoption of Directive 95/46/EC." Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016.

633 Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 15 jan. 2017.

634 Sobre as gerações de leis de tutela dos pessoais: BIONI, Bruno R. **Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet**. 2016. Dissertação (Mestrado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016. p. 145-148.

ideia de que seria árdua a tarefa conciliá-las[635] com o universo trazido pelo big data, tornando o instituto até mesmo obsoleto[636].

No Brasil, o texto da Lei 12.965 / 2014 – Marco Civil da Internet –, notadamente em seu artigo 7º, menciona a privacidade como direito essencial ao acesso à rede mundial de computadores, trazendo ainda vários incisos que tratam da privacidade dos usuários.

Estabelece, dentre outras, a obrigação de prestar "informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet", o "não fornecimento a terceiros de seus dados pessoais", garante a proteção dos dados e veda a sua utilização para outros fins além daqueles expressamente autorizados, determinando ainda a necessidade de "consentimento expresso" na coleta e tratamento dos dados, "que deverá ocorrer de forma destacada das demais cláusulas contratuais"[637].

Inobstante, a legislação mencionada informa que, quando a finalidade inicial for alcançada, deve-se pôr fim ao tratamento de dados pessoais, o que também pode, em tese, obstaculizar muitas práticas típicas do big data. Por exemplo, benefícios e resultados satisfatórios que em determinados casos são obtidos por tratamentos secundários, distantes da finalidade inicial para a qual os dados foram coletados, diversas vezes sequer possíveis ou conhecidos no momento da coleta dos dados.

Mais especificamente, quando se impõe amarras expressas no tratamento, especialmente se reportando ao princípio da finalidade[638], coloca-se em cheque muitas práticas atualmente frequentes que extraem valor e benefícios diante

635 "Big data and mass surveillance are difficult to reconcile with the mandate of the European Union under Article 16 TFEU in the area of privacy and data protection." HIJMANS, Hielke. **The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU**. Springer International Publishing, 2016. p. 81

636 "The continuous repurposing and making use of already processed or inherent data sets, has made the traditional consent models insufficient and obsolete in big data." Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016.

637 Vale mencionar também os artigos 3, 8 e 11 do Marco Civil da Internet que também abordam a tutela da privacidade no mundo virtual.

638 REGULAMENTO (UE) 2016/679: Artigo 5º. Princípios relativos ao tratamento de dados pessoais 1. Os dados pessoais são: (...) b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n. 1 («limitação das finalidades»); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»).

de uma utilização secundária, muitas vezes inimaginável quando da coleta dos dados que estão sendo objeto de análise:

> In the EU context there is a further consequence: purpose limitation is a substantive principle of EU data protection law, included in Article 8 Charter, which means, in essence, that collection of data should take place for a specific purpose.
>
> (...) However in a big data context, personal data collection takes place for unspecified purposes and on a massive scale[639].

Em que pese ser o consentimento um instituto relevante a garantir ao indivíduo o protagonismo do controle de seus dados pessoais, essa assertiva tem causado relevantes impasses ao avanço tecnológico[640], diante de práticas já presentes e difundidas, a justificar a constatação de que "a própria emergência do consentimento como vetor central para a proteção dos dados pessoais carregou consigo seus complicadores" [641].

Na sociedade da informação, onde já se afirmou que a privacidade morreu[642], não é raro se deparar com autores defendendo uma revisitação da tutela da privacidade[643], de forma que o consentimento não seria suficiente[644] para suprir integralmente os anseios desta nova realidade trazida pela tecnologia, especialmente com o big data[645].

---

639 HIJMANS, Hielke. **The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU**. Springer International Publishing, 2016. p. 99.

640 "Por vezes, aliás, tem-se a sensação de que cresce a distância entre o velocíssimo mundo da inovação tecnológica e aquele lentíssimo do planejamento sócio-institucional". RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008. p. 42.

641 BIONI, Bruno R. **Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet**. 2016. Dissertação (Mestrado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016. p. 147.

642 Disponível em: <http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#46c9c18fdfbd>. Acesso em: 01 dez. 2016.

643 MAYER-SCHONBERGER, Viktor; CUKIER, op. cit., p. 173.

644 "In this chapter I have been arguing that consent-based privacy models are inadequate in the face of contemporary information practices and the emerging corporate–state nexus that has created such a striking surveillance infrastructure on the internet". AUSTIN, L.M. Enough About Me: Why Privacy is About Power, not Consent (or Harm) In Sarat, A. (ed.) **A World without Privacy: What Law Can and Should Do?** Cambridge: Cambridge University Press, 2014. p. 189.

645 "In the context of Big Data, there is growing skepticism regarding the effectiveness of informed consent in the context of personal data processing (...)". CUSTERS, Bart. **Click here to consent forever: Expiry dates for informed consent.** Big Data & Society, 2016. DOI: 10.1177/205395171562493.

Em extenso relatório divulgado pela Comissão Europeia em janeiro de 2017, concluiu-se que o instituto do consentimento tem se tornado um pesado fardo a ser carregado pelas empresas e não necessariamente é capaz de prover a proteção almejada à privacidade dos cidadãos[646]. Stefano Rodotà já teceu críticas ao consentimento, quando asseverou, por exemplo, que para se ter acesso a determinado bem ou serviço é necessário fornecer os seus dados pessoais[647]. Revela-se uma faceta imprópria da utilização do instituto, visto que, em razão da assimetria de poder entre o fornecedor do bem ou serviço e o aderente, não haverá escolha[648] ao aderente senão por "consentir". Em outras palavras:

> Pode-se acrescentar, de modo mais geral, que o usuário de serviços informáticos e telemáticos se encontra em tal situação de disparidade de poder em relação aos fornecedores de tais serviços que, a rigor, não se pode falar em consentimento livremente manifestado para transações referentes à privacidade[649].

Há que se mencionar ainda a possibilidade de se transferir toda a responsabilidade pelas consequências danosas do tratamento de dados para o indivíduo que teria consentido com aqueles riscos previstos nos termos do serviço[650].

---

646 "Based on these issues relating to the scope, the consent mechanism and enforcement, competent authorities interviewed by Deloitte pointed out that this provision causes an unnecessarily high burden for businesses, while the usefulness for citizens is not optimal". **Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector**. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology by Deloitte, 2017. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=41232>. Acesso em: 11 jan. 2017.

647 RODOTÀ, Stefano. op. cit., p. 76.

648 "There is also the issue of the extent to which individuals have meaningful choices about what information they disclose. Typically, individuals cannot use a service unless they agree to the terms of use, which, in addition to being complex or legalistic, frequently present a "take it or leave it" approach. Under such an approach, the user must agree to provide personal data for all of the purposes the organization represents – even if some are not directly related to the service – in order to access the service. This substantially limits the ability of the individual to protect their personal data by giving meaningful consent. Generally, the emphasis on consent based on overly complex privacy policies that provide few real options and few limitations on collection and use diminish the effectiveness of privacy protections that are intended to support the individual's role in controlling his or her own personal data". Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 20 nov. 2016.

649 RODOTÀ, Stefano. op. cit., p. 52-53.

650 "Consent is related to the concept of informational self-determination. The autonomy of the data subject is both a pre-condition and a consequence of consent: it gives the data subject influence over the processing of data. However, as explored in the next chapter, this principle has limits, and there are cases where the data subject is not in a position to take a real decision. The data controller may want to use the data subject's consent as a means of transferring his liability to the individual". Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016.

Big data e novas formas de licitude de tratamento de dados do titular

Em determinadas situações, no que diz respeito ao big data, o consentimento livre, informado, expresso, em cláusula apartada e destacada, renovado quando em contratos de longa duração e com finalidades estritas e restritas certamente se mostra impróprio para tratar de toda e qualquer atividade que envolva o tratamento de dados pessoais, especialmente na sociedade da informação, mostrando-se um instituto, certas vezes, "anêmico" [651].

Aliás, a própria regulamentação europeia, que trata dos dados pessoais, reconhece que o consentimento, apesar de protagonista, não é o único fundamento a iluminar com licitude o tratamento dos dados pessoais, a saber:

> Therefore, consent is recognised as an essential aspect of the fundamental right to the protection of personal data. At the same time, consent under the Charter is not the only legal ground enabling the processing of personal data; the Charter explicitly recognises that the law may lay down other legitimate grounds, as is the case with Directive 95/46/EC[652].

O novo regulamento 2016/679 do Parlamento Europeu e do Conselho, que revogou a Diretiva 95/46/EC, traz a mesma ressalva[653], entendendo pela possibilidade de que outros institutos ou circunstâncias específicas[654] legitimem a coleta e análise de dados pessoais sem, necessariamente, existir consentimento do titular. Note-se que o mencionado regulamento de 2016 não trata diretamente do termo big data, porém faz referência a práticas e situações em que se pode inferir que esta modalidade de tratamento de dados está sendo abordada:

---

651 AUSTIN, L.M. Enough About Me: Why Privacy is About Power, not Consent (or Harm) In SARAT, A. (ed.) A World without Privacy: What Law Can and Should Do? Cambridge: **Cambridge University Press**. 2014. p. 131–189.

652 Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016.

653 "Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar".

654 Moreover, taking into account the sensors and smart devices in big data, other types of usable and practical user positive actions, which could constitute consent (e.g. gesture, spatial patterns, behavioral patterns, motions), need to be analyzed. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016.

> (50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. (...)

Percebe-se, neste turno, que o regulamento 2016/679, apesar de reforçar o consentimento com regra geral, traz casos específicos, como o acima destacado, onde outras questões em jogo justificariam a licitude do tratamento dos dados[655].

Na esteira da novel regulamentação sobre dados pessoais na Europa, a Comissão Europeia elaborou, em janeiro de 2017, proposta de revogação da Diretiva 2002/58 que versa exclusivamente sobre comunicações eletrônicas, onde reconhece que as regras atualmente existentes não acompanharam[656] as inovações tecnológicas dos últimos anos colocando o consentimento como um dos exemplos nesse sentido e propondo novas formas de tutela da privacidade e controle dos dados pessoais.

Este novo esboço de regulamentação na Europa, que trata exclusivamente sobre comunicações eletrônicas, em que pese ampliar a tutela dos dados pessoais, flexibiliza[657] a regra geral do consentimento em casos específicos, como, por exemplo, quando o usuário de um navegador de internet define as sua regras básicas de privacidade para utilização de cookies, entendendo que tal configuração definiria as suas preferências gerais de navegação na rede, sendo então desnecessário que, em todos os sítios visitados, houvesse uma nova e incômoda mensagem requerendo o consentimento do usuário, como ocorre atualmente.

---

655 "Nessa conjuntura, uma abordagem normativa mais flexível seria necessária, o que foi endereçado, mesmo que não voluntariamente para tais desafios mais contemporâneos, por algumas legislações ao redor do mundo através de exceções à regra do consentimento. Previsões legais para o tratamento adicional dos dados pessoais sem qualquer tipo de consentimento ulterior do titular, como dos interesses legítimos na Diretiva da União Europeia, são um bom exemplo disso". BIONI, Bruno. XEQUE-MATE. **O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. USP-Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. 2016.

656 "Accordingly, the Directive has not kept pace with technological developments, resulting in a void of protection of communications conveyed through new services". Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>. Acesso em: 11 jan. 2017.

657 "A «disposição sobre cookies», que obriga os utilizadores da Internet a responder incessantemente a pedidos de consentimento, será racionalizada. As novas regras permitirão aos utilizadores controlar melhor os seus parâmetros, proporcionando uma maneira fácil de aceitar ou recusar os cookies e outros identificadores de rastreio das suas atividades em caso de risco para a privacidade. A proposta esclarece que não é necessário consentimento relativamente a cookies não invasivos da privacidade utilizados para melhorar as pesquisas na Internet (memorização do histórico de compras, por exemplo). A introdução de cookies por um determinado sítio para contagem do número de visitantes do sítio deixará de necessitar de consentimento". Disponível em: <http://europa.eu/rapid/press-release_IP-17-16_pt.htm>. Acesso em: 11 jan. 2017.

Importante ressaltar ainda, no Brasil, uma tímida passagem constante no Anteprojeto de Lei de Proteção de Dados Pessoais, atualmente Projeto de Lei 5276 / 2016, que em seu artigo 9º, parágrafo 7o., assevera que "O órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos". O PL 5276 estabelece que o consentimento passa a ser apenas uma das nove maneiras a autorizar a coleta, uso e tratamento dos dados pessoais, incluindo a figura dos legítimos interesses[658]. O consentimento livre e inequívoco passa a funcionar como regra geral e o expresso apenas em determinadas situações específicas, como quando se tratar de informações sensíveis.

Menciona ainda no parágrafo 7º, do artigo 9º , que o "órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos", o que pode ser de grande valia no contexto do big data, cotejando com os legítimos interesses envolvidos, diante de suas especificidades, especialmente no caso de tratamentos secundários, distante da finalidade inicial, sempre respeitando os direitos e liberdades fundamentais do titular.

Nota-se que o PL 5276 estabelece freios e contrapesos de maneira bastante rígida e evidente, tais como a transparência e o direito de oposição do titular[659], solicitação de relatório de impacto à privacidade[660], dentre outros. Traz diversas formas de tratamento lícito de dados pessoais, tais como os legítimos interesses, sem olvidar da autodeterminação informativa e dos valores cardeais do sistema, como a dignidade da pessoa humana[661], garantindo o exercício e a proteção da

658 Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. (...) IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevaleceram interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titula for menor de idade.

659 Art. 10, §2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.

660 Art. 10 §4º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo.

661 "A dignidade da pessoa humana, como valor e princípio, compõe-se dos princípios da liberdade privada, da integridade psicofísica, da igualdade substancial (art. 3°, III, CF) e da solidariedade social (art. 3°, I, CF). Tais princípios conferem fundamento de legitimidade ao valor social da livre iniciativa (art. 1°, IV, CF), moldam a atividade econômica privada (art. 170, CF) e, em última análise, os próprios princípios fundamentais do regime contratual regulados pelo Código Civil". TEPEDINO, Gustavo. Normas Constitucionais e Direito Civil na Construção Unitária do Ordenamento. In: **Temas de Direito Civil – Tomo III.** Rio de Janeiro: Renovar, 2009. p. 14.

privacidade às pessoas naturais, ao mesmo tempo em que não marginaliza por completo a inovação tecnológica visivelmente presente nas práticas do big data.

Neste contexto, o consentimento livre e inequívoco passa a funcionar como regra geral e o expresso apenas em determinadas situações específicas, como quando se tratar de informações sensíveis, o que permite a ponderação dentro do contexto do big data, na medida em que haveria o cotejo com os legítimos interesses envolvidos, porém sem ter como letra morta os direitos fundamentais do titular, garantindo unicidade e coerência normativa ao ordenamento[662].

Cumpre destacar que este caminho tem sido traçado pelo sistema jurídico Europeu desde a Diretiva 95\46\CE[663] e, mais recentemente, através de seu novo regulamento 2016/679, já destacado alhures, quando faz referência a práticas e situações as quais se pode inferir que o big data está sendo retratado[664].

Novas formas a legitimar o tratamento de dados pessoais parece ser o caminho seguido na Europa[665], onde a sua regulamentação está na vanguarda[666], sem, no entanto, passar ao largo dos direitos e garantias fundamentais dos indivíduos, especialmente a privacidade.

---

662 TEPEDINO, Gustavo. O direito civil-constitucional e suas perspectivas atuais. In: **Temas de Direito Civil – Tomo III**. Rio de Janeiro: Renovar, 2009. p. 21-40.

663 Artigo 7º. Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se (...) ou f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.

664 (50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. (...)

665 "Previsões legais para o tratamento adicional dos dados pessoais sem qualquer tipo de consentimento ulterior do titular, como dos interesses legítimos na Diretiva da União Europeia, são um bom exemplo disso". BIONI, Bruno. XEQUE-MATE. **O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, 2016.

666 Nas palavras do vice-presidente da Comissão Europeia: "As nossas propostas assegurarão a confiança no mercado único digital que as pessoas esperam. Pretendo garantir a confidencialidade das comunicações eletrônicas e a proteção da vida privada. O nosso projeto de regulamento «Privacidade e Comunicações Eletrônicas» estabelece um justo equilíbrio entre um elevado nível de proteção dos consumidores e, simultaneamente, perspectivas de inovação para as empresas". Disponível em: <http://europa.eu/rapid/press-release_IP-17-16_pt.htm>. Acesso em: 11 jan. 2017.

Conclusão

O big data urge por abordagem lúcida no debate democrático contemporâneo no processo, especialmente no aprimoramento da legislação brasileira, esta que, sem dúvidas, tem se espelhado[667] no sistema europeu, notadamente quando se percebe ter a privacidade status constitucional no ordenamento pátrio.

A presença dos legítimos interesses, como uma das formas de conferir licitude ao tratamento de dados pessoais, revela-se um caminho possível, pois constitui uma verdadeira cláusula geral, dispondo de conteúdo fluido, mutável e adaptável com as mais variadas situações, muitas delas que, diante da constante evolução da tecnologia, surgirão no futuro e sequer são possíveis de imaginar neste momento.

Gustavo Tepedino, tratando dos desafios impostos pelas novas tecnologias, defende a utilização das cláusulas abertas para solucionar questões difíceis:

> Diante da multiplicação de situações trazidas pelas novas tecnologias, muda-se radicalmente a técnica legislativa, valendo-se o legislador de inúmeras cláusulas gerais - as quais permitem ao intérprete amoldar as previsões normativas às peculiaridades do caso concreto -, e os princípios, dotados de força normativa, tornam-se fundamentais para determinação dos ordenamentos aplicáveis aos casos concretos, cada vez mais inusitados[668].

Neste sentido, o professor italiano Pietro Perlingieri sustenta de maneira contundente a necessidade da utilização de cláusulas gerais quando se tratar da tutela das situações subjetivas existenciais, advogando que deve haver a "elasticidade da tutela" e que nenhuma forma de tutela dos direitos da personalidade deveria ser exaustiva, visto que "deixaria de fora algumas manifestações e exigências da pessoa que, em razão do progresso da sociedade, exigem uma consideração positiva" [669].

Cumpre salientar que os legítimos interesses aparecem em diversas passagens dos mais relevantes projetos de lei em trâmite no parlamento, sendo crucial, no entanto, que existam sistemas de "freios e contrapesos"[670], evitando-se um cheque

---

667 "Ao mesmo tempo, a Diretiva Europeia 95/46/EC, que já está em vigor há mais de 15 anos e serviu de ponto de partida do Anteprojeto apresentado pelo Ministério da Justiça (…) ". GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 388.

668 TEPEDINO, Gustavo. Normas Constitucionais e Direito Civil na Construção Unitária do Ordenamento. In: **Temas de Direito Civil. Tomo III**. Rio de Janeiro: Renovar, 2009. p. 17.

669 PERLINGIERI, Pietro. **O direito civil na legalidade constitucional**. Rio de Janeiro: Renovar. 2008. p. 765.

670 "Do contrário, a regra geral do consentimento tornar-se-ia exceção, tamanha a elasticidade e as diversas facetas que a hipótese camaleão dos interesses legítimos poderia alcançar. Um sistema de

em branco e o esvaziamento do consentimento com regra geral, sendo garantida a privacidade[671], através do controle dos dados pessoais nas mãos de seu titular.

Ou seja, sob o pretexto dos legítimos interesses a dar licitude ao tratamento de dados, não se pode olvidar da dignidade da pessoa humana como fundamento da república, da direta aplicação das normas constitucionais e da necessidade imperiosa de se garantir unidade ao ordenamento jurídico[672], sob pena da criação de um microssistema[673] incoerente e absolutamente inconstitucional.

Com base em tudo que foi exposto, não há dúvidas de que a criação de uma legislação que regulamente a proteção de dados pessoais no Brasil é fundamental[674], pois, ao contrário do que pode parecer, o vácuo legislativo constitui verdadeiro empecilho à efetiva tutela da privacidade nos tempos modernos[675], além de trazer imensa insegurança jurídica[676], especialmente quando eventuais

---

freios e contrapesos deve ser arquitetado para tanto". BIONI, Bruno. XEQUE-MATE. **O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil.** USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. 2016.

671 "No entanto, apesar da flexibilidade dos seus critérios, em função das peculiaridades e circunstâncias que envolvem cada caso, deverá a privacidade ter pontos de referência implacáveis: a dignidade humana e o respeito à personalidade de cada indivíduo servirem de guia, como valores constitucionais primordiais e unificadores de todo o sistema". KLEE, Antonia Espínola Longoni; MARTINS, Guilherme Magalhães. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965 / 2014). In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. (Org.). **Direito & Internet III – Tomo I**. São Paulo: Quartier Latin, 2015.p. 299.

672 TEPEDINO, Gustavo. Normas Constitucionais e Direito Civil na Construção Unitária do Ordenamento. In: **Temas de Direito Civil. Tomo III.** Rio de Janeiro: Renovar. 2009. p. 19.

673 TEPEDINO, Gustavo. O Código Civil, os chamados microssistemas e a Constituição: premissas para uma reforma legislativa. In: **Problemas de Direito Civil-Constitucional.** Rio de Janeiro: Renovar, 2000. p. 5.

674 "Por fim, constata-se que o Marco Civil da Internet possui disposições relativas à proteção de dados pessoais e de comunicação de forma imprecisa e incompleta, o que, provavelmente, somente será integralizado quando da promulgação da Lei de Proteção de Dados e Privacidade". GIACCHETTA, André Zonaro. MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 391.

675 GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 390.

676 "Ao contrário do que alguns entusiastas libertários poderiam achar, a ausência de leis nesse âmbito não representa a vitória da liberdade e do laissez-faire. Ao contrário, a ausência de uma legislação que trate das questões civis da rede leva, ao contrário, a uma grande insegurança jurídica". LEMOS, Ronaldo. O marco civil como símbolo do desejo por inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord). **Marco Civil da Internet.** São Paulo: Atlas, 2014. p. 10.

conflitos forem levados ao Poder Judiciário, que poderá decidir da forma que quiser, com base apenas em verdadeiro vácuo legislativo, que não contempla a possibilidade de novas formas de tratamento de dados, como o big data.

Há que se considerar a especificidade do contexto no qual o big data se insere, não se revelando, à primeira vista, razoável que o pano de fundo regulatório a legitimar o tratamento de dados pessoais seja inteiramente homogêneo, horizontal, fulcrado quase que integralmente na regra do consentimento, sem que haja previsão de estados de fato específicos e que possam fugir à regra geral. Este é nitidamente o caso do big data, em que os resultados úteis da análise dos dados surgem, muitas vezes, distantes da finalidade inicial para as quais foram coletados[677].

Tal contexto revela uma clara hipótese em que os institutos jurídicos clássicos se mostram obsoletos diante da evolução informática e do contexto social do século XXI, devendo ser revisitados e reconstruídos à luz dos valores cardeais do sistema, promovendo a livre iniciativa e o progresso social e tecnológico, sem esvaziar a proteção da dignidade humana, conforme lição de Gustavo Tepedino:

> As categorias do direito privado devem ser reconstruídas, a partir do surgimento de situações jurídicas inteiramente novas, advindas com a revolução tecnológica dos últimos cinquenta anos. Basta pensar na engenharia genética, na procriação in vitro, na extraordinária massa de informações pessoais colhidas mediante exame de DNA e na circulação de dados propiciados pelas redes de informática. Cabe à doutrina do direito civil estabelecer parâmetros para tutelar a pessoa humana diante dos novos bens jurídicos que se tornam objeto de situações existenciais suscitadas pelo avanço da cibernética e da tecnologia[678].

677 "In the era of big data, however, when much of data's value is in secondary uses that may have been unimagined when the data was collected, such a mechanism to ensure privacy is no longer suitable". MAYER-SCHONBERGER, Viktor; CUKIER, op. cit., p. 173.

678 TEPEDINO, Gustavo. Normas Constitucionais e Direito Civil na Construção Unitária do Ordenamento. In: **Temas de Direito Civil – Tomo III**. Rio de Janeiro: Renovar, 2009, p. 15.