UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

OS DIREITOS DOS TITULARES DE DADOS NO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU (RGPD) E NA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD)

RODRIGO CAMPOS RIBEIRO

Rio de Janeiro
2019/2

RODRIGO CAMPOS RIBEIRO

OS DIREITOS DOS TITULARES DE DADOS NO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU (RGPD) E NA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD)

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor LL.M. Allan Nascimento Turano.

Rio de Janeiro

2019/2

Ribeiro, Rodrigo Campos
R484d Os direitos dos titulares de dados no regulamento geral de proteção de dados europeu (RGPD) e na lei geral de proteção de dados brasileira (LGPD) / Rodrigo Campos Ribeiro. -- Rio de Janeiro, 2019.
77 f.

Orientador: Allan Nascimento Turano.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Naciona de Direito, Bacharel em Direito, 2019.

1. privacidade. 2. proteção de dados pessoais. 3. titulares de dados. 4. direitos dos titulares de dados. 5. lei de proteção de dados. I. Turano, Allan Nascimento, orient. II. Titulo.

RODRIGO CAMPOS RIBEIRO

OS DIREITOS DOS TITULARES DE DADOS NO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU (RGPD) E NA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD)

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor LL.M. Allan Nascimento Turano.

Data da Aprovação: ___ / ___ / _____.

Banca Examinadora:

_____

Orientador - Professor Allan Nascimento Turano

_____

Membro da Banca

_____

Membro da Banca –

Rio de Janeiro

2019/2

AGRADECIMENTOS

É com grande satisfação que celebro mais uma conquista acadêmica em minha vida. E, seja na vitória ou na derrota, sempre há a oportunidade de agradecer a todos aqueles que compartilharam essa experiência de vida comigo, assim agradeço:

a Deus, primeiramente, por ter me dado permissão para vivenciar esse momento e experimentado mais uma graduação, agradeço muito a oportunidade de cursar Direito em uma grande instituição como a FND e junto com pessoas voltadas para a busca de uma Sociedade muito melhor;

à minha mãe Rosa Ângela, que foi fundamental na minha formação e que compartilhou comigo os principais momentos da minha vida, uma mãe que lutou para criar os três filhos da melhor forma possível e que sempre desejou cursar Direito, obrigado por construir comigo esse sonho e por permitir que seus filhos sejam felizes com suas escolhas;

ao meu irmão Gabriel, que foi sempre um exemplo de dedicação ao trabalho e à família, obrigado por sempre ter orgulho das minhas conquistas e por admirar a dedicação e a paixão que sempre tive pelo aprendizado e ensino;

ao meu irmão Rafael, que compartilhou comigo momentos de alegria e tristeza e que, de alguma forma, apesar da pouca idade, sempre se mostrou um jovem maduro e comprometido com propósitos maiores de vida, obrigado por sua dedicação e carinho e por compartilhar comigo sua paixão pelos games e animes;

ao Professor Allan Nascimento Turano, que me auxiliou muito na definição de um recorte adequado para o tema e me socorreu durante o árduo caminho de realização do trabalho. Agradeço pela oportunidade de crescimento e aprendizado. Um trabalho que foi difícil, mas, sem dúvida, muito recompensador ao final;

à minha grande amiga Dra. Alessandra de Paula, pelos maravilhosos momentos na Letras e na vida, por todo o exemplo e dedicação ao curso de Letras, obrigado pelo amor ao magistério que me contagia, obrigado por permanecer na minha vida;

ao meu grande amigo Dr. Rodolfo Mascarenhas, que dividiu comigo momentos incríveis das ciências jurídicas e da vida como um todo, obrigado por compartilhar comigo essa fase tão importante das nossas vidas e por passar momentos agradáveis nas padarias da Tijuca e do Centro do Rio, obrigado por ser esse cara incrível e por me inspirar diariamente a superar os desafios impostos pela área do Direito;

ao meu amigo Murilo Gouveia, que me diverte com seu humor particular e me comove com sua paixão pelo exercício da advocacia, obrigado por me inspirar com sua dedicação ao trabalho e com sua luta diária para seguir em frente independentemente de todas as dificuldades presentes;

ao meu amigo Fábio Ferrer, pelo exemplo de trabalho, dedicação e comprometimento com a FND, obrigado pela manobra Ferrer e pela possibilidade de compartilhar muitos bons momentos ao seu lado, obrigado por ser esse cara incrível que nos ensina e inspira sempre;

ao meu amigo Guilherme Klein, por geralmente apresentar um contraponto nas discussões, por me permitir ver o mundo com um olhar novo e crítico, obrigado por ser um exemplo de um bom advogado e por compartilhar comigo as angústias do término da graduação;

ao meu grande amigo Dr. Pedro Castagna, pelos momentos de discussão e debate no Direito, pelo exemplo de vida, pelos debates políticos e ideológicos, obrigado por ser uma pessoa tão importante na minha vida;

ao meu amigo doutorando em música pela UFRJ, Vinícius Macedo, que na maior parte do curso de Direito compartilhou comigo as angústias e as alegrais de fazer parte de uma das maiores faculdades do Brasil, obrigado por me ensinar a ser uma pessoa melhor e a compreender que há momentos para tudo na vida, obrigado por dividir comigo o poder transformar da arte, em especial da música, e por me inspirar sempre na busca por um mundo melhor;

à minha grande amiga Bárbara Abreu, pelos momentos de alegria, de tristeza, de angústia, de segredos, de confissões, de sonhos, obrigado por ser uma parceira de vida,

obrigado por dividir comigo o que você tem de melhor, obrigado por mostrar que é possível viver uma amizade de forma intensa;

à minha chefe atual Dra. Elza Rodrigues Aguiar, pelo ótimo convívio e pelo exemplo de liderança e coordenação, obrigado por sua sinceridade e clareza, por seu altruísmo e por sua dedicação a uma área tão difícil dentro da nossa empresa, obrigado por ser uma fonte de eficiência e trabalho e por conduzir tão bem o nosso departamento e as coordenadorias a ele anexas;

à minha amiga Priscilla Mouta, por seu amor a linda arte literária, por compartilhar comigo a sua sinceridade e o seu carinho, obrigado por estar ao meu lado e dividir comigo as angústias da vida;

à minha ex-chefe Dra. Tereza Robichez de Carvalho, pelo apoio nos anos iniciais de empresa, pela serenidade e tranquilidade que sempre lidou com as situações mais complexas, pelo incentivo à melhor realização das tarefas;

aos meus colegas da área jurídica, em especial, LG, Fred, Priscilla, Denise, Ana, Maria, Juliana, Rayane, Roberta e Noeli, muito obrigado por compartilharem comigo todos os dias as inúmeras tarefas que a empresa nos propõe;

aos demais colegas e professores que tive ao longo dessa jornada, que foram fundamentais na construção do conhecimento.

À todos, deixo aqui a minha eterna Gratidão!

“Li e aceito a política de privacidade”

(Termo de aceite da política de dados)

“Os que sonham de noite, nos recessos poeirentos das suas mentes, acordam de manhã para verem que tudo, afinal, não passava de vaidade. Mas os que sonham acordados, esses são homens perigosos, pois realizam os seus sonhos de olhos abertos, tornando-os possíveis.”

(T. E. Lawrence)

“Aqueles que passam por nós, não vão sós, não nos deixam sós. Deixam um pouco de si, levam um pouco de nós.”

(Antoine de Saint-Exupery)

RESUMO

A chamada sociedade da informação trouxe um novo olhar para a privacidade. Com o advento das novas tecnologias da informação, fez-se necessária a revisão de normativos que delimitam os poderes dos responsáveis pelo tratamento de dados e asseguram os direitos dos titulares desses dados. O Regulamento Geral de Proteção de Dados europeu é um marco importante de mudança na forma como os Estados pretendem assegurar os direitos constitucionais ligados à proteção dos dados, ele inspira a Lei Geral de Proteção de dados brasileira e busca estabelecer práticas internacionais comuns. Os direitos dos titulares de dados presentes nos dois recentes normativos são o objeto principal de estudo desse trabalho e se justifica pela importância que o tema tem diante da evolução da internet, da possibilidade de mercantilização dos dados pessoais, das novas tecnologias de tratamento de dados e das inúmeras possiblidades de troca de informações pessoais entre particulares e entre pessoas físicas e jurídicas. O método descritivo foi escolhido para apresentar as características presentes nos dois normativos e pelo método dialético contrapor as particularidades entre eles e as demais fontes jurídicas existentes.

Palavras-chave: Privacidade; Proteção de Dados Pessoais; Titulares de dados, Direitos dos titulares de dados

ABSTRACT

The so-called information society has brought a new look at privacy. With the advent of new information technologies, necessary revision of the normatives presented itself, one that would determine the powers of data controllers and also guarantee the rights of data subjects. The European General Data Protection Regulation is an important milestone in the way states intend to enforce constitutional data protection rights; it inspired the Brazilian General Data Protection Act and seeks common practices. The copyright of the data subjects presented in the last two norms are the main object of this study, which justifies itself because of the increased importance that the theme has gain in the face of the internet evolution, the possibilities of commercialization of personal data; the new technologies of data processing; and the numerous possibilities for exchanging personal information between individuals, and between individuals and companies. The descriptive method was chosen to present the characteristics observed in the two normatives, and the dialectical method was used to identify the particularities between them and other existing legal sources.

Keywords: Privacy; Protection of personal data; Data subjects, Data subjects rights

SUMÁRIO

INTRODUÇÃO

Os avanços gerados pela internet e as novas tecnologias da informação suscitaram uma nova forma de tratamento e compartilhamento de dados. A rede mundial de computadores possui recursos únicos que viabilizam o rastreamento e a mercantilização dos dados pessoais gerando um mercado de dados e um interesse econômico de diversos grupos.

Nesse cenário tecnológico, as empresas detentoras de grandes bancos de dados compreenderam rapidamente que a informação se tornou um dos bens mais valiosos do mundo moderno. O tratamento apropriado desses dados obtidos dentro e fora da web pode gerar uma compreensão de padrões de comportamento que possibilitam o oferecimento de produtos e serviços personalizados e direcionados.

O problema desse novo "universo personalizado" está nas possíveis violações de direitos pessoais que o tratamento inapropriado de dados pode gerar. As empresas que, em última análise, buscam ampliar seus lucros precisam compreender que há limites para a atuação do tratamento de dados.

Uma das formas de limitar uma atuação desregulada desses agentes de dados é por meio de legislações específicas sobre o tema. O Regulamente Geral de Proteção de Dados europeu é um desses normativos que regulamentam a proteção de dados pessoais impondo restrições para a prática de tratamento de dados e de compartilhamento de informações pessoais. No contexto brasileiro, surge, no final do ano de 2018, uma esperada Lei Geral de Proteção de Dados que tem basicamente o mesmo objetivo central do GDPR de proteger os direitos fundamentais dos titulares de dados nesses processos de tratamento de dados.

Este trabalho busca entender os aspectos gerais e legais que permitem ao GDPR e à LGPD assegurar os direitos dos titulares de dados em um cenário de proteção de dados. Para tal, através de um método descritivo e dialógico, busca-se apresentar elementos estruturais dos normativos em diálogo com situações reais e hipotéticas. A aplicação do Regulamento já é uma realidade e os exemplos extraídos das diversas autoridades nacionais dos países membros da União europeia representam um caminho possível de interpretação das lides que serão geradas na aplicação da LGPD.

A difusão do acesso à internet no Brasil, apesar de ainda limitada em muitos aspectos, configura um elemento relevante para o aumento de compartilhamentos e tratamentos de dados em diversos segmentos. Em seguida, vale ressaltar mais detalhadamente o papel econômico dos dados que são viabilizados por meio de recursos tecnológicos de rastreamento, identificação e direcionamento personalizado de informações. Além da apresentação de alguns casos ilustrativos de violação de direitos.

Após esse capítulo introdutório, busca-se, no capítulo II do trabalho, uma análise mais específica sobre os direitos dos titulares de dados presentes no capítulo III do GDPR, intitulado “Direitos dos titulares de dados”. Esse capítulo apresenta oito direitos: (i) direito à informação dos dados pessoais; (ii) direito de acesso aos dados pessoais; (iii) direito de retificação; (iv) direito ao apagamento; (v) direito à limitação do tratamento; (vi) direito à portabilidade dos dados; (vii) direito de oposição e (viii) direito de objeção quanto a decisões individuais automatizadas.

Antes de detalhar a forma como cada direito é apresentado no Regulamento, buscou-se inicialmente apresentar brevemente a influência que a GDPR exercer sobre a Lei brasileira e delimitar sua aplicabilidade além de destacar o princípio da transparência como guia para uma melhor compreensão da relação entre os titulares de dados e os responsáveis pelo tratamento de dados. Há de se destacar que os direitos presentes no GDPR são norteados pela proteção de direitos fundamentais dos indivíduos detentores dos direitos dos dados e em um conflito entre os interesses de mercado e esses direitos individuais, o Regulamento optou por favorecer os direitos dos titulares de dados.

Após a análise dos direitos no Regulamento, o estudo direciona seus esforços para uma análise da Lei Geral de Proteção de Dados (Lei 13.709 de 14 de agosto de 2018), no capítulo III da lei são apresentados os direitos dos titulares de dados, são eles: 1) confirmação da existência do tratamento; 2) acesso aos dados; 3) correção de dados incompletos, inexatos ou desatualizados; 4) anonimização, bloqueio ou eliminação de dados desnecessários; 5) portabilidade dos dados; 6) eliminação dos dados pessoais; 7) informações sobre o compartilhamento de dados; 8) informações sobre a possibilidade de não fornecer o consentimento; e 9) revogação do consentimento. Assim como no GDPR, busca-se apresentar

os fundamentos e princípios da lei brasileira e detalhar a incidência de cada direito presente no normativo.

Por fim, faz-se necessário um comparativo entre as normas por meio de um quadro de análise comparativa. Desse modo, observa-se no detalhamento ilustrativo de cada direito analisado, evidências de influencias do normativo anterior, GDPR, na constituição dos direitos presentes na lei brasileira.

O presente trabalho, assim, busca, de forma geral, apresentar uma perspectiva do tema dos direitos dos titulares de dados no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados. O trabalho não esgota, de modo nenhum, todas as nuances que envolvem um tema tão vasto, trata-se de uma tentativa de colaboração para uma reflexão inicial sobre o tema.

I. ASPECTOS INTRODUTÓRIOS SOBRE O DIREITO E A PROTEÇÃO DOS TITULARES DE DADOS

A internet, pelo menos nas grandes cidades, é uma realidade no cotidiano dos brasileiros. O acesso à rede mundial de computadores se tornou parte importante da vida das pessoas e, com isso, novas formas de interação social foram desenvolvidas. É inegável, que atualmente a maneira como as pessoas se relacionam foi drasticamente alterada pela possibilidade de estarem diariamente e quase que ininterruptamente conectadas na internet.

Essa conexão constante e a naturalização das interações na rede gera, todavia, uma falsa percepção da realidade virtual. É como se o usuário, por utilizar tanto a internet, não compreendesse as importantes distinções que há entre a rede mundial de computadores e o cotidiano "real" de interações sociais. Essa percepção equivocada das particularidades virtuais impede muitas vezes que o usuário tenha plena consciência de seus próprios deveres e direitos presentes nessas interações na rede.

Um dos pontos ainda negligenciados por uma parte dos usuários é a segurança dos dados. Em geral, as pessoas não se preocupam com os riscos presentes na livre exposição de seus dados pessoais e não compreendem de que forma essas informações podem gerar algum prejuízo.

Inicialmente é importante entender que, mesmo que não haja um pagamento imediato na maioria das redes sociais, os dados pessoais fornecidos livremente pelos usuários possuem um grande valor econômico. Aliás, o fato de não haver um pagamento imediato sobre as informações coletadas corrobora para alimentar a percepção de um universo na rede semelhante ao mundo não virtual. Vale destacar que o aspecto econômico dos dados é tão relevante que as empresas hoje consideradas mais valiosas do mundo estão diretamente ligadas com a monetização de dados pessoais e com o controle de informações dos seus clientes.

Em seguida, é preciso compreender que cabe a cada usuário da rede ponderar na exposição dos dados públicos divulgados. A realidade virtual não é um espaço idêntico ao mundo não conectado, é fundamental que o usuário entenda que os dados não protegidos na

rede possuem um grande potencial de permanência e de reaproveitamento. Os dados produzidos servem para realimentar outros bancos de dados que cruzam informações e geram uma identidade virtual que até mesmo o titular[1] dos dados desconhece. Atualmente a proteção dos dados é possível por meio de ferramentas tecnológicas e jurídicas que impedem que os controladores das redes tenham liberdade para tratar[2] os dados de forma indiscriminada.

1.1 O acesso à internet no Brasil

As pessoas estão cada vez mais conectadas e dependentes dos inúmeros recursos gerados pelo avanço da internet.[3] O *Whatsapp*, o *Instagram*, o *Youtube*, o *Linkedin* e o *Facebook* são ferramentas hoje consideradas, para muitos, indispensáveis. Mais que uma necessidade, o acesso à rede de computadores se tornou uma política pública[4] fomentada pelo próprio Estado,[5] como se pode observar, por exemplo, pela disposição regulamentar do Decreto das Telecomunicações que em seu art. 2º, prevê entre os objetivos gerais das políticas públicas a *expansão do acesso à internet em banda larga fixa e móvel, com qualidade e velocidade adequadas*.[6]

No Brasil, a presença da internet impacta diretamente na forma como nos comunicamos, o livre exercício do direito à liberdade de expressão presente na Constituição de 88[7] é potencializado pela rede. Atualmente uma parte considerável dos brasileiros possuem acesso à

[1] Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V, LGPD).
[2] Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X, LGPD).
[3] INTERNET das coisas, integração de serviços e interação social: o que esperar da Web 4.0. Disponível em: https://rockcontent.com/blog/web-4-0/. Acesso em: 10 out. 2019.
[4] PNBL – Programa Nacional de Banda Larga. Decreto 7.175 de 12 de maio de 2010. O PNBL foi revogado pelo Decreto nº 9.612 de 17 de dezembro de 2018 que institui políticas públicas de telecomunicações.
[5] Como afirma Silvado Pereira da Silva, um bom exemplo disso é o Programa Nacional de Banda Larga (PNBL), a principal iniciativa de política pública brasileira neste campo nas últimas décadas. Trata-se de um programa do Governo Federal que tinha como objetivo principal massificar o acesso a serviços de conexão à internet em banda larga. SILVA, Silvado Pereira da. Políticas de acesso à Internet no Brasil: indicadores, características e obstáculos. **Cadernos Adenauer XVI (2015) nº 3**. Disponível em: http://ctpol.unb.br/wp-content/uploads/2019/04/2015_SILVA_Acesso-Internet.pdf. Acesso em: 30 out. 2019, p. 165.
[6] Decreto 9.612 de 17 de dezembro de 2018, que institui políticas públicas de telecomunicações.
[7] "é livre a manifestação do pensamento, sendo vedado o anonimato; e IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença." (Art. 5º, IV e IX, CFRB/88).

internet, segundo importantes institutos de pesquisa,[8] o Brasil possui uma rede de acesso contabilizando aproximadamente 70% de domicílios com acesso à internet.

> "O percentual de domicílios que utilizavam a Internet subiu de 69,3% para 74,9%, de 2016 para 2017, representando uma alta de 5,6 pontos percentuais. Nesse período, a proporção de domicílios com telefone fixo caiu de 33,6% para 31,5%, enquanto a presença do celular aumentou, passando de 92,6% para 93,2% dos domicílios. Essas são algumas informações da PNAD Contínua TIC 2017, pesquisa domiciliar do IBGE que investiga o acesso à Internet e à televisão, além da posse de telefone celular para uso pessoal."[9]

O crescimento da infraestrutura e as diversas tecnologias inteligentes alavancam o crescimento dos usuários no Brasil. Segundo dados do IBGE[10] em pesquisa[11] realizada em 2017,[12] há um aumento de usuários em todos os seguimentos. O celular continua sendo o equipamento mais utilizado para acessar a rede, aproximadamente 98,7% dos usuários que possuem um acesso à internet utilizam esse aparelho. Número surpreendente diante das dimensões continentais do Brasil e de suas inúmeras diferenças sociais.

> "Os resultados desta pesquisa corroboram que a utilização da Internet nos domicílios vem crescendo rapidamente. (...) em 98,7% dos domicílios em que havia utilização da Internet no País, o telefone móvel celular era utilizado para este fim em 2017, continuando a se aproximar da totalidade, visto que, em 2016, este percentual estava em 97,2%."[13]

Apesar das possibilidades quase "infinitas" de acesso a inúmeros sites e informações, grandes empresas controladoras[14] de um número bem restrito de redes sociais e portais centralizam a maior parte dos acessos. As redes sociais são um desses centros preferenciais de atividades na rede. Em pesquisa[15] recente, foi verificado que a população brasileira está ativa nas redes sociais. Aproximadamente 62% dos brasileiros participam de uma rede social com uma frequência considerável. As principais redes acessadas, segundo a pesquisa *Digital in*

---

[8] Fonte: PNAD Contínua 2017 – IBGE. Informativo.
[9] AGÊNCIA IBGE - PNAD, 2018
[10] Órgão de pesquisa. - órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (Art. 5º, XVIII, LGPD).
[11] A pesquisa de dados estatísticos é um tratamento autorizado pela LGPD brasileira, conforme art. 7º, IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (art. 7º, IV, LGPD).
[12] Fonte: PNAD Contínua 2017 – IBGE. Informativo.
[13] pág. 5, PNAD, 2017
[14] Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, LGPD).
[15] Digital in 2018: The Americas – "62% da População Brasileira está ativa nas Redes Sociais" – Exame Online/2018.

2018: The Americas, foram *Youtube*, com 60% de acesso, o *Facebook* com 59%, o *Whatsapp* com 56% e o Instagram com 40%. Os números mostram que o acesso às redes sociais no Brasil continua crescendo e que se torna relevante na tomada de decisão do usuário. Por exemplo, no caso das últimas eleições presidenciais do Brasil, em 2018, uma pesquisa do Datafolha[16] indica que 61% dos eleitores se informaram pelo *Whatsapp* e 57% pelo *Facebook*.

O acesso à internet se consolida como uma ferramenta necessária para o desenvolvimento e o exercício dos direitos fundamentais. Conforme indica Silvado Pereira da Silva:

> "Em diversos países, o acesso à Internet vem sendo tratado como um serviço fundamental, diretamente ligado ao exercício de direitos e, paralelamente, uma ferramenta inevitável para o desenvolvimento social."[17]

Apesar do grande avanço estrutural da internet no Brasil, há ainda muitas diferenças na forma como os usuários acessam a rede. Ainda estamos longe de uma uniformidade no serviço e, se considerarmos que a internet hoje é fundamental para o pleno exercício de Direitos Fundamentais, há ainda entre 30% e 40% de brasileiros que não possuem o acesso em casa. A exclusão digital aumenta de acordo com a classe social do usuário, quanto mais baixa a classe, mais excluído digitalmente ele se torna. Assim a internet se torna por um lado um mecanismo de acesso a direitos, e por outro, mais uma ferramenta de exclusão e de desigualdade social.

Mesmo com todas as desigualdades de acesso, as redes sociais se tornam uma mídia de grande impacto na vida dos brasileiros. Nessa performance, cada usuário cede parte de seus dados pessoais gerando um banco de dados potencialmente tratáveis por essas redes.

O direito dos titulares de dados presentes na Lei Geral de Proteção de Dados, no Regulamento Geral de Proteção de Dados europeu, nas demais legislações, na doutrina e na jurisprudência será o objeto principal de análise nesse trabalho.

---

[16] Disponível em: https://g1.globo.com/politica/eleicoes/2018/eleicao-em-numeros/noticia/2018/10/03/datafolha-quantos-eleitores-de-cada-candidato-usam-redes-sociais-leem-e-compartilham-noticias-sobre-politica.ghtml. Acesso em: 10 out. 2019

[17] SILVA, Silvado Pereira da. Op. cit. p. 155.

1.2 A mercantilização dos dados

O tratamento de dados feito atualmente por essas redes sociais, segundo alguns autores, gerou uma nova fase tecnológica para a internet. A chamada web 3.0 que gerencia de forma eficaz uma quantidade imensa de dados e consegue criar um perfil vasto, inteligente e confiável de informações. Considerando um breve histórico da internet, na web 1.0, o usuário era apenas um mero "expectador", sua participação era mais passiva, apenas visualizando uma grande quantidade de informações. Na web 2.0, por outro lado, surge a possibilidade de interação do usuário, que além de receber as informações poderia também inserir dados, por exemplo, nas redes sociais.

> "Em termos de recursos e ferramentas, a Web 1.0 utilizava sites estáticos de conteúdo, com imagens e textos imóveis. Os sites desenvolvidos durante esta fase consideravam o usuário um elemento passivo, receptor, como um telespectador diante de notícias (...). A Web 2.0 surge com uma nova perspectiva de produção de conhecimento online, capaz de eliminar fronteiras físicas como o tempo e o espaço, propiciando a construção de um espaço democrático caracterizado pelas trocas virtuais e pelo compartilhamento, tendo como foco a aprendizagem do usuário. (...) novas tecnologias possibilitem que as máquinas sejam dotadas de ferramentas inteligentes e, assim, sendo capaz de raciocinar, inferindo o conteúdo dos documentos armazenados em seu banco de dados."[18]

A inteligência, aliás, proporcionada pelos chamados algoritmos[19] é a chave para o tratamento eficaz dos dados. Os sistemas inteligentes codificados no algoritmo revolucionaram a forma como a internet controla as informações. Sem esses sistemas automatizados as redes sociais não seriam capazes de relacionar, quase que de forma imediata, a busca em um site de compras, por exemplo, com a posterior propaganda de produtos similares na *timeline*[20] do *Facebook*. Os parceiros comerciais do Facebook fornecem informações através de seus próprios sistemas de algoritmo e elas são selecionadas e direcionadas de forma personalizada para o usuário.

Essas informações são um "grande negócio", um negócio que movimenta bilhões.[21] O Facebook, a maior rede social do mundo com cerca de 2.23 bilhões de MAUs (*monthly active*

---

[18] LOTH, Adriana Falcão et al. As tendências e desafios da Web 3.0 à luz da gestão do conhecimento. **RISUS - Journal on Innovation and Sustainability**, São Paulo, v.10 n.1, p37-47, Mar/Maio, 2019. Disponível em: https://revistas.pucsp.br/risus/article/download/ 41810/27983. Acesso em: 10 out. 2019, p. 40.

[19] O que 'diabos' é um algoritmo? Uma tecnologia extraterrestre...? Disponível em: https://becode.com.br/o-que-e-algoritmo/. Acesso em: 10 set. 2019

[20] Linha do tempo. A página do Facebook onde as publicações do usuário são organizadas.

[21] FACEBOOK obtém receita de US$ 15 bilhões no 1º trimestre de 2019 – 24/04/2019.

users – usuários ativos mensais),[22] consegue tratar os dados pessoais inseridos diariamente com o fim de criar uma experiência personalizada para o usuário e atender às demandas de seus parceiros comerciais.

> "Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação. E, com a possiblidade de organizar tais dados de maneira escalável (e.g., Big Data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e codificação. Há uma "economia de vigilância" que tende a posicionar o cidadão como um mero expectador das suas informações."[23]

Os dados se tornaram um "bem de consumo", as informações geradas diariamente e constantemente pelos milhões de usuários das redes sociais são úteis e potencialmente lucrativas para a geração de diversos tipos de negócios.

As redes sociais e a internet como um todo conseguem maximizar o valor agregado aos dados. Segundo Bruno Bioni, estudioso na área de privacidade e proteção de dados, esse valor está relacionado a forma como os usuários dessas redes modificam sua relação com o consumo de bens. Isso é algo novo na relação de consumo, pois antigamente os consumidores eram, na maior parte das vezes, passivos diante dessa relação, sem muitas ferramentas práticas e úteis de manifestação da experiência de consumo. Os consumidores atuais se tornam agentes ativos, pois produzem bens de consumo com as informações disponibilizadas.

> "O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa, que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do prosumer. O consumidor não apenas consome (consuption), mas, também, produz o bem de consumo (production)."[24]

Assim, a rede mundial de computadores com todo esse valor agregado pelos consumidores/usuários propicia a mercantilização dessas informações direcionando o marketing de parceiros estratégicos ligados às redes sociais. Aliás, mais de 60% da receita de

---

[22] The 21 most popular social media sites in 2019. Disponível em: https://buffer.com/library/social-media-sites. Acesso em: 14 set. 2019.
[23] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. *E-book*. p. 38-39.
[24] BIONI, Bruno Ricardo. Op. cit. p. 40.

publicidade e marketing nos EUA atualmente são controladas apenas por duas empresas, o Facebook e Google.[25]

Considerando a fonte da própria empresa, o Facebook e sua família de aplicativos,[26] consegue diariamente o acesso de 2,1 bilhões de pessoas e mensalmente cerca de 2,7 bilhões de acessos de usuários distintos.[27] Os dados gerados nesses acessos são contratualmente cedidos para a rede de Mark Zuckerberg que os usa para fins diversos.

Sendo assim, de fato, no Brasil há o crescimento no número de usuários das redes sociais e consequentemente o aumento da geração de dados pessoais nessas redes, algo que possibilita a negociação dos dados com a consequente vinculação de propagandas direcionadas nas redes.

Vale destacar que não é somente nas relações digitais diretas que há a mercantilização dos dados. Atualmente as corporações compreenderam o valor das informações e estabelecem políticas de armazenamento e cruzamento de dados mesmo para aqueles que não efetuam um negócio online. Por exemplo, grandes redes de farmácia no Brasil oferecem descontos de produtos para os usuários previamente cadastrados. O cliente é informado que precisa fazer um cadastro com seu CPF para obter o desconto e, caso possua algum plano de saúde, poderá obter mais vantagens na compra dos medicamentos. O cruzamento de dados ocorre de forma explícita, visto que, os planos de saúde têm total interesse nas informações de compra dos clientes e podem estabelecer qual a probabilidade de beneficiários do plano de saúde possuírem determinada doença.

Diante desse cenário, a proteção dos direitos dos titulares de dados se torna mais do que necessária, o Regulamento Geral europeu sobre a proteção de dados e a Lei Geral de Proteção de Dados tratam desse tema em um capítulo específico e destacam todos os recursos que os titulares possuem para intervir em uma área tomada por interesses econômicos.

---

[25] Este ano, gigantes da tecnologia devem obter metade de toda a receita mundial de publicidade na internet e mais de 60% nos EUA, de acordo com empresa de pesquisas. Disponível em: https://g1.globo.com/tecnologia/noticia/google-e-facebook-mostram-poder-de-duopolio-em-anuncios-digitais-rivais-perdem-forca.ghtml. Acesso em: 8 ago. 2019.

[26] Família de Aplicativos nesse exemplo é o *Facebook*, *Instagram*, o *Whatsapp* e o *Facebook Messenger*.

[27] Facebook cresce em Receita e usuários, mas teme multa de até US$ 5 bi. Link. Estadão.

1.3 O rastreamento dos dados

Como visto, na era da informação, os dados dos usuários da rede possuem um grande valor. Os "rastros" que são deixados na rede determinam de forma muito precisa o perfil daqueles que irão consumir os produtos oferecidos pelos parceiros comerciais das redes sociais.

O percurso que cada indivíduo percorre em seu equipamento de conexão pode ser mapeado pelos chamados *cookies*, um tipo de ferramenta tecnológica capaz de rastrear as informações dos usuários e indicar para a empresa os hábitos de navegação e utilização da máquina conectada à internet. Com os cookies a publicidade pode ser direcionada, as redes sociais irão apenas vincular propagandas que se adequam ao perfil indicado pelo *cookie*.

> "Nesse sentido, a ciência mercadológica percebeu que a Internet poderia propiciar uma abordagem publicitária mais efetiva. Por meio de diversas ferramentas tecnológicas, dentre as quais se destacam os cookies, tornou-se possível rastrear a navegação do usuário e, por conseguinte, inferir seus interesses para correlaciona-los aos anúncios publicitários. Por meio do registro da navegação dos usuários cria-se um rico retrato das suas preferências, personalizando-se o anúncio publicitário."[28]

Com a consolidação dos celulares como os principais dispositivos de acesso à internet, surgiu a possibilidade de traçar os hábitos de navegação de forma dinâmica. Os celulares permitem um retrato constante da movimentação dos usuários, de seus hábitos, eles se transformam em um dispositivo de controle constate de todas as ações realizadas pelo usuário.

> "Essa onipresença da Internet permitiu, de forma acoplada com a possibilidade de monitoramento da localização geográfica (global positioning system/GPS) dos smartphones, que as publicidades também sejam direcionadas com base em tal informação. Leva-se, assim, em conta, a proximidade física do potencial consumidor ao bem de consumo ofertado, como, por exemplo, seria o caso de um restaurante. Esse é um dos motivos pelos quais o aplicativo Waze, que captura a geolocalização de seus usuários, foi adquirido pela Google pela quantia expressiva de US$ 1,3 bilhão; ou ainda, por que uma rede social permite ao usuário marcar os locais que frequenta – "check-in". Tais dados de geolocalização são extremamente valiosos. Não é portanto, uma mera coincidência que surja um anúncio publicitário, cujo bem

[28] BIONI, Bruno Ricardo. Op. cit. p. 43.

> de consumo esteja bem próximo geograficamente do cidadão ao utilizar um smarthphone do potencial consumidor é uma (nova) estratégia mercadológica."[29]

Além do controle da navegação, do controle geográfico, diversas ações aparentemente simples dos usuários na rede contribuem para montar esse grande perfil do usuário. Por exemplo, no envio de ícones que expressam emoções na rede, os chamados *emoticons*, é possível identificar o estado emocional do usuário e com isso direcionar propagandas específicas para determinados estados de humor. Em determinadas situações, usuários felizes possuem hábitos de consumo distintos de usuários tristes. A emoção humana é também um dado relevante, pois ela influencia na forma como o usuário consome.

> "Ao se comunicar com alguém por meio de um ícone de expressão – os chamados emoticons; ao responder à sua rede social como está se sentindo ou nela emitir uma opinião sobre determinado assunto; ao interagir com um aplicativo de música para que ele forneça faixas musicais de acordo com o seu humor, as pessoas fornecem um rico retrato das suas emoções."[30]

O retrato construído por essas ações revela muito dos hábitos dos usuários. As empresas que possuem essas informações são capazes de estimular práticas que as beneficiam. Os dados coletados e estruturados são capazes de traçar o perfil de consumo e tornar o consumidor vulnerável diante das ações publicitárias altamente personalizadas.

Observando a política de dados da rede social *Linkedin* é possível perceber que a política de transferência de dados é necessária para a mercantilização do serviço oferecido pela rede:

> "Usaremos os dados coletados (tais como seu perfil, os perfis que você visualizou ou os dados fornecidos por meio de carregamentos da lista de endereços ou de integrações com parceiros) para ajudar outros a encontrarem o seu perfil, sugerir conexões a você e a terceiros (por exemplo, usuários que possuem contatos ou experiências de trabalho em comum) e permitir que você convide terceiros para se tornarem usuários e se conectarem com você. Você também pode habilitar o nosso uso da sua localização precisa ou a proximidade com terceiros para certas tarefas (ex.: para sugerir outros Usuários na sua área com quem você pode se conectar, calcular o tempo de deslocamento até um novo emprego ou notificar conexões de que você está em um evento profissional)."[31]

---

[29] BIONI, Bruno Ricardo. Op. cit. p. 45.
[30] BIONI, Bruno Ricardo. Op. cit. p. 45.
[31] Política de Privacidade do Linkedin, disponível em: https://www.linkedin.com/legal/privacy-policy?_l=pt_BR. Acesso em: 10 set. 2019.

O “pacto” proposto pelas redes sociais é a troca dos seus dados pessoais pelo oferecimento de um serviço. O usuário contratualmente permite que a rede social compartilhe o seu comportamento na rede com seus parceiros comerciais. Essa “troca”, em um primeiro momento, pode parecer algo vantajoso para o usuário que estaria “apenas” cedendo os dados pessoais produzidos diariamente na sua rede. Não há inicialmente nenhum prejuízo financeiro imediato para o usuário e, em tese, nenhum risco no compartilhamento dessas informações para os parceiros da rede social.

A política de dados do *Facebook*, *Instagram*, *Messenger* e outros produtos e recursos oferecidos pelo *Facebook* não é muito diferente e está disponível para a visualização em um link público da rede social.[32] A forma como ela é apresentada é interativa, com um layout em forma de site, com cores variadas e um visual atrativo para o usuário comum. Essa política é dividida em alguns itens que explicam quais informações serão coletadas e como essas informações são compartilhadas.

O *Facebook* e seus produtos basicamente controlam automaticamente todos os dados incluídos pelos usuários da rede, desde as informações presentes no cadastro realizado para criar a conta até a localização, a data e os filtros da foto incluída em seus aplicativos. O que é fornecido pelo usuário é contratualmente cedido para os interesses da empresa, porém, há uma ressalva para algumas proteções especiais. O *Facebook* indica que as preferências políticas, religiosas, raciais, étnicas ou filosóficas podem estar sujeitas a uma proteção especial dependendo da legislação do país.

Além disso, a rede coleta as informações das suas conexões, seus contatos, suas páginas visitadas, seus grupos, registro de chamadas, históricos de SMS. Tudo é coletado, segundo o Facebook, para que o programa consiga de forma mais fácil conectar você a outras pessoas. Os dados de uso também são coletados, as visualizações, o tempo de uso, as interações e, dentro do tópico das informações que o usuário insere, também são controladas todas as transações financeiras, como a compra de um jogo, por exemplo.

O *Facebook*, então, basicamente monitora a maior parte das “coisas que você e outras pessoas fazem e fornecem”. Além dessas informações, o *Facebook* também identifica o

[32] Disponível em: https://pt-br.facebook.com/privacy/explanation. Acesso em: 14 ago. 2019.

dispositivo que se conecta a sua rede, se é um celular, um notebook ou desktop e de qual modelo eles pertencem. Eles alegam que é uma forma de melhorar o conteúdo de anúncios que será veiculado na sua *timeline*. Os anunciantes parceiros também fornecem informações sobre o usuário, através de APIs,[33] SDKs[34] e o pixel do *Facebook*, que são basicamente ferramentas que compartilham dados entre sites e softwares dos parceiros. É uma forma automatizada de compartilhar todas as suas ações realizadas fora do *Facebook*, mas nas ferramentas desses parceiros.

Basicamente as informações são utilizadas para personificar a venda de produtos e oferecer o conteúdo apropriado para cada usuário. Dessa forma, o algoritmo do site cruza os dados, por exemplo, do *Instagram*, com os contatos do *Messenger* e sugere que você faça parte de um grupo no Facebook que já possui membros dessas listas dos demais produtos do *Facebook*. A rede social controla sua localização, de acordo com as informações que são recebidas pelo *Facebook*, e orienta produtos próximos de seus parceiros.

1.4 O direito à privacidade

A privacidade surge como direito bem antes desse cenário conectado que estamos inseridos atualmente. É recente esse instituto jurídico e é reconhecido geralmente pelo trabalho feio por Samuel Warren e Louis Brandeis,[35] em 1890. Esses operadores do Direito da época entenderam que haveria uma espécie de "Direito de estar só" e que não deveria ser violado por interesses ligados à informação. O estudo surge de um caso concreto, em que jornalistas, se valendo da recente criação da máquina fotográfica, registraram em uma festa momentos íntimos e constrangedores dos ali presentes. Desse episódio surge então o entendimento de que os jornalistas não poderiam ter vinculado as imagens registradas na festa de forma arbitrária. O entendimento dos autores é de que, de alguma forma, há um direito que impede a vinculação dessas informações e protege a plena constituição da imagem e da personalidade dos indivíduos.

---

[33] API – Application Programming Interface (Interface de Programação para Aplicativos). É basicamente um conjunto de bibliotecas, métodos, funções e/ou objetos que tem como principal função interligar dois softwares distintos, compartilhar informações.

[34] SDK – Sotware Development Kit (Kit de Desenvolvimento Integrado). São kits para implementação de determinadas funcionalidades, um modelo de código, por exemplo.

[35] WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. **Harvard Law Review**, 1890. p. 193-220.

A personalidade pode significar um conjunto de características que diferencia uma pessoa da outra como indica Bruno Bioni, ou ainda, como preceitua Caio Mário da Silva Pereira, "a aptidão genérica para adquirir direitos e contrair deveres. (...) aptidão hoje reconhecida a todo ser humano, o que exprime uma conquista da civilização".[36] Ainda de acordo com a atualização do livro do civilista mineiro, direitos inerentes a essa personalidade, são direitos que se projetam da natureza dessa personalidade.

> "Entendemos que o poder do indivíduo sobre si mesmo se exprime nos direitos inerentes à própria personalidade, direito à vida, à honra, ao respeito, à integridade física e moral, ao nome etc., direitos que se projetam sobre as manifestações dessa personalidade, como o trabalho físico ou mental. O direito ao próprio corpo é um complemento do poder sobre si mesmo, mas deve ser exercido no limite da manutenção da sua integridade."[37]

O reconhecimento desses direitos é fundamental para que possamos buscar a proteção da privacidade e dos direitos ligados aos titulares de dados pessoais. Assim como Warren e Brandeis em seu estudo inovador no final do século 19 entenderam que o uso da tecnologia de fotografar não poderia ultrapassar um direito, as novas tecnologias da internet e das redes sociais possuem uma limitação jurídica imposta pelo reconhecimento de direitos inerentes à personalidade.

Reconhece-se, então, a privacidade como um direito a ser protegido e essa proteção perpassa a necessidade de entendimento do tratamento que é feito atualmente pelos dados coletados peles agentes de tratamento.[38] O titular de dados, mesmo que não entenda juridicamente que há um direito inerente a sua personalidade, precisa compreender e avaliar os riscos envolvidos no tratamento de seus dados pessoais. Além disso, como a proteção de dados é um campo recente, com uma legislação nova e uma jurisprudência ainda não consolidada, não sabemos ainda quais limites serão impostos para a (re)utilização dos dados coletados.

O processamento de dados tem um potencial enorme de atingir esse direito à personalidade restringindo direitos fundamentais dos titulares de dados.

---

[36] PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**: introdução ao direito civil: teoria geral de direito civil. Atual. Maria Celina Bodin de Maoraes. (versão digital). 30. ed. rev. atual. Rio de Janeiro: Forense, 2017. v. 1. p. 182.
[37] PEREIRA, Caio Mário da Silva. Op. cit. p. 54
[38] Agentes de tratamento: o controlador e o operador (art. 5º, IX, LGPD).

> "(...) as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses signos identificadores do cidadão. Trata-se de um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações."[39]

1.5 Casos de violação de direitos

Não é somente o marketing direcionado que se valerá dos dados do usuário. Em entrevista veiculada no *Youtube*,[40] antevendo um pouco de como será a aplicação da nova Lei Geral de Proteção de Dados do Brasil,[41] Bruno Bioni alerta para o impedimento por parte dos provedores da reutilização de dados para fins diversos daqueles que o foram tratados.[42] Por exemplo, no caso de um aplicativo de corrida, seria natural e aceitável que o aplicativo indicasse equipamentos ligados à corrida para que o titular possa comprar, um tênis ou um relógio. Entretanto, não seria razoável, nem aceitável, que os dados tratados no aplicativo de corrida fossem enviados para as seguradoras de saúde gerando assim um perfil informacional que eventualmente afetará o valor do plano contratado.

O grande alerta dos estudiosos de segurança de dados, como Bruno Bioni, é nesse sentido. Não sabemos ainda os limites do tratamento de dados, hoje um desconto na farmácia parece ser irrecusável, mas se as informações dos remédios comprados pelo usuário são tratadas pelo plano de saúde, os descontos da farmácia podem se converter em outro tipo de taxação.

Um outro exemplo citado sobre a exposição de dados sensíveis dos titulares de dados, foi o caso da *Netflix*, em que a empresa no intuito de melhorar o algoritmo de indicação de filmes para os usuários permitiu que programadores tivessem acesso à seu banco de dados de forma "anômima" (omitindo informações pessoais como nome e *email*),[43] porém, os

---

[39] BIONI, Bruno Ricardo. Op. cit. p. 100.
[40] Proteção de Dados – Bruno Bioni – Youtube – Palavra do Professor – Verbo. 14/11/2018. Disponível em: https://www.youtube.com/watch?reload=9&v=jeh9Y9li_4k. Acesso em: 20 set. 2019.
[41] Lei nº 13.709, de 14 de agosto de 2018. (em vigor em 14 de agosto de 2020)
[42] Art. 5º, b), GDPR.
[43] O considerando 26 do Regulamento europeu faz referência ao afastamento da proteção de dados em caso de anonimização. (26) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa

pesquisadores que receberam o banco de dados cruzaram os esses dados com um outro banco de dados de informações sobre cinema, o IMDB (*Internet Movie Data Base*).[44] Desse modo, eles conseguiram tornar os dados anteriormente anônimos em dados pessoais perfeitamente identificáveis gerando um vazamento do banco de dados da Netflix.

Tal "problema" é alertado por Bruno Bioni, que indica, pautado na nova LGPD, que a anonimização[45]dos dados pode sofrer uma reversão, como ocorreu com o caso acima:

> "A proteção dos dados pessoais, como um novo direito da personalidade, dirige-se a todo e qualquer dado em que se denota o prolongamento de um sujeito. Dados pessoais não se limitam, portanto, a um tipo de projeção imediata, mas também, a um referencial mediato que pode ter ingerência na esfera de uma pessoa. Por essa lógica, qualquer dado pessoal anonimizado detém o risco inerente de se trasmudar em um dado pessoal. A agregação de diversos pedaços de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico."[46]

Mais um exemplo de falha na proteção dos dados informados pelo titular foi o caso que ocorreu recentemente, nos EUA, com a empresa *moviepass*, uma empresa de assinatura de ingressos de cinema. O usuário se cadastra no serviço oferecido pela empresa e, com isso, tem direito a assistir uma quantidade determinada de sessões em diversos cinemas cadastrados. Ocorre que, por uma falha de segurança registrada por empresas especializadas, a empresa expôs[47] o cartão de crédito de milhares de assinantes. A empresa moviepass já vinha sofrendo uma série de problemas financeiros e parece que a exposição desses dados registrados na reportagem em agosto de 2019 contribuiu para que em setembro deste ano a empresa decretasse o fim de suas atividades, como consta no site atual da empresa.[48] No Brasil, há

---

singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação. (Considerando 26, GDPR)

[44] Disponível em: https://www.imdb.com/. Acesso em: 22 out. 2019.

[45] Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. (art. 5º, XI, LGPD).

[46] BIONI, Bruno Ricardo. Op. cit. p. 110.

[47] Disponível em: https://www.theverge.com/2019/8/20/20825725/moviepass-credit-card-numbers-exposed-sensitive-customer-data. Acesso em: 02 nov. 2019.

[48] "As a result, it pains us to inform you that effective at 8 a.m. E.T. on September 14, 2019, we must interrupt service for all current MoviePass™ subscribers" Disponível em: https://www.moviepass.com/. Acesso em: 02 nov. 2019.

serviços similares que também oferecem assinaturas mensais que disponibilizam ingressos para cinema, como é o caso do *primepass*.[49]

Recentemente outras multas pesadas foram aplicadas no Reino Unido. A Agência de privacidade do Governo britânico (ICO)[50] aplicou na companhia aérea British Airways uma multa de 230 milhões de dólares[51]. A rede hotéis Marriott também amargou uma multa de 123 milhões de dólares[52] aplicada também pela ICO, ambas por violarem a privacidade de seus clientes.

Na Alemanha, um caso curioso de uma aplicação de uma multa no valor de 1,5 mil dólares a um policial, para fins pessoais pesquisou pela placa do carro o número de telefone do proprietário do veículo. Um tratamento de dados extremamente singular e particular, mas que, mesmo assim, está enquadrado no campo de aplicação do Regulamento.

É notório que a proteção de dados se tornou um fator de grande importância no Brasil e no mundo, esse trabalho busca, assim, identificar quais as principais ferramentas que os titulares de dados possuem, de acordo com as principais legislações, para assegurar seus direitos.

[49] Disponível em: https://primepass.club/. Acesso em: 02 nov. 2019.
[50] ICO – Information Commissioner's Office
[51] Disponível em: https://tiinside.com.br/tiinside/08/07/2019/british-airways-recebe-multa-de-uss-230-milhoes-por-violacao-de-dados/. Acesso em: 02 nov. 2019.
[52] Disponível em: https://olhardigital.com.br/noticia/rede-marriott-encara-multa-de-us-123-milhoes-por-vazamento-de-dados/87800. Acesso em: 02 nov. 2019.

II. OS DIREITOS DOS TITULARES DOS DADOS E O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O tema da proteção da privacidade e tratamento de dados está "na moda". A visibilidade recente gerada pelo vazamento de dados do caso *Cambridge Analytica*,[53] a aprovação do GDPR (*General Data Protection Regulation* - Regulamento Geral de Proteção de Dados) da União Europeia, e mais especificamente no cenário brasileiro, a aprovação da LGPD (Lei Geral de Proteção de Dados) criaram um verdadeiro *frenesi* relacionado ao tema.

É nesse cenário recente de valoração do tema, que o Regulamento europeu busca parametrizar as bases do que promete ser nos próximos anos um campo de disputas entre titulares de dados e empresas responsáveis pelo armazenamento e tratamento desses dados. O Regulamento dedica um capítulo inteiro com 12 artigos que tratam especificamente de todos os direitos que os titulares de dados possuem na proteção de suas informações pessoais.

O capítulo III do Regulamento, que centraliza essas informações, intitulado de "Direitos do titular dos dados", está dividido em cinco seções e doze artigos e, para este estudo, pode ser compreendido em oito blocos de direitos, são eles: (i) direito à informação dos dados pessoais; (ii) direito de acesso aos dados pessoais; (iii) direito de retificação; (iv) direito ao apagamento; (v) direito à limitação do tratamento; (vi) direito à portabilidade dos dados; (vii) direito de oposição e (viii) direito de objeção quanto a decisões individuais automatizadas. Esses direitos delimitam os recursos estruturados pelo Regulamento que os titulares possuem para exigir que os agentes de dados cumpram a legalidade. É certo que não é somente no capítulo III que os direitos dos titulares estão presentes, o Regulamento é repleto de considerações sobre a forma como os dados devem ser tratados e como os titulares podem agir em determinadas situações.

Apesar disso, é através desse capítulo que iremos focar todos esses direitos e as possíveis nuances que eles podem apresentar. Para isso, iniciaremos esse capítulo falando de

[53] "O mundo parou para assistir o depoimento de Mark Zuckerberg ao Senado norte-americano na última terça-feira (10). O motivo do encontro foi tratar sobre a privacidade dos dados de seus usuários, necessidade que surgiu após o escândalo da Cambridge Analytica, quando informações de milhões de pessoas foram destinadas à campanha que elegeu Donald Trump como presidente dos Estados Unidos." ROSA, Natalie. Cambridge Analytica – Os principais momentos do depoimento de Mark Zuckerberg. Canaltech.com (online). 11/04/2018. Disponível em: https://canaltech.com.br/redes-sociais/cambridge-analytica-os-principais-momentos-do-depoimento-de-mark-zuckerberg-111626/. Acesso em: 20 out. 2019.

forma mais geral sobre o GDPR e o seu âmbito de aplicação para em seguida, de fato, adentrar sobre cada direito apresentado.

2.1 A influência e a aplicação do GDPR

A Sociedade vem sendo, cada vez mais, forçada a compreender os riscos relacionados com o tratamento inadequado dos dados e, sobretudo, com a violação da privacidade e dos direitos dos titulares dos dados. O caso do *Cambridge Analytica* mostrou que o *Facebook* está longe de ser um "local" seguro e que os dados dos usuários podem ser expostos e utilizados para fins diversos. O próprio CEO do Facebook precisou ir até o Senado norte-americano para assumir a culpa sobre os vazamentos ocorridos, "Foi um erro meu e peço desculpas. (...) Está claro agora que não fizemos o suficiente para prevenir estas ferramentas de serem usadas para danos".[54]

No caso do GDPR, os números recentes de aplicação da lei mostram que as notificações de vazamentos de dados aumentaram.[55] O Regulamento acaba forçando as empresas europeias a notificarem suspeitas de vazamento de dados para que não sejam punidas pela violação do normativo.

Isso, por si só, deve gerar um maior cuidado, por parte das instituições, com a segurança da informação e dos dados dos usuários de seus sistemas. Conforme indica o estudo, "De maio de 2018 a janeiro deste ano, empresas europeias já fizeram 41.502 notificações sobre ameaças ou incidentes de vazamento de dados, conhecidos como "data breach."". O direito à notificação de um provável vazamento de dados é um dos direitos previstos no Regulamento e é um desdobramento do direito à transparência. Essas informações permitem que os usuários e as autoridades competentes tenham a oportunidade de agir diante de possíveis vazamentos de dados.

[54] ROSA, Natalie. Op.cit. p. 01.
[55] LEORATTI, Alexandre. Com GDPR, número de notificações de vazamento de dados ultrapassa 41 mil casos.

O objeto central desse normativo é a proteção de dados de pessoas naturais, com atenção ao tratamento dos dados e a circulação das informações. O art. 1º[56] do GDPR assegura o respeito aos direitos e liberdades fundamentais que englobam a proteção dos dados pessoais. A delimitação dos âmbitos de aplicação material e territorial da lei estão presentes nos seus art. 2º[57] e 3º. Há a indicação que o GDPR se aplica tanto para o tratamento automatizado quanto para o tratamento não automatizado dos dados, o que indica a preocupação da amplitude da lei. Certamente o maior uso hoje do tratamento dos dados é voltado para o automatismo dos algoritmos que possibilitam um tratamento rápido e personalizado de uma infinidade de dados. Assim, a lei prevê uma grande quantidade de operações relacionadas a esse tratamento, como destaca Renato Ópice Blum, em seus comentários da lei

> "Como se pode depreender, por se tratar de Lei Geral, basicamente toda operação que trate dados pessoais estará sujeita ao Regulamento, contemplando desde relações de consumo, interações por meio da internet, questões envolvendo relações de emprego, tratamento de dados de crianças e adolescentes, a estas não se limitando."[58]

O objeto vai além dos domínios da própria União Europeia, a lei prevê que os dados dos europeus, por exemplo armazenados e tratados no Brasil, devem respeitar o GDPR. Assim o normativo não só influencia a LGPD brasileira, mas acaba por ter aplicabilidade direta para as relações comerciais internacionais entre Brasil e Europa.

2.2 O princípio da transparência

A seção 1 do capítulo III do GDPR, que inclui o art. 12, é intitulada como "Transparência e regras para o exercício dos direitos dos titulares dos dados", e destaca que o operador deve apresentar de forma clara o que deve ocorrer no tratamento de dados. Por exemplo, no inciso 3 do art. 12:

---

[56] "Artigo 1.º Objeto e objetivos - 1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais. 3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais." (Art. 1º, GDPR).

[57] 1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. (art. 2º, GDPR)

[58] BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coordenação). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 27.

> "3. O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 15.o a 20.o, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informa o titular dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da data de recepção do pedido. Se o titular dos dados apresentar o pedido por meios eletrônicos, a informação é, sempre que possível, fornecida por meios eletrônicos, salvo pedido em contrário do titular. (art. 12, 3, GDPR)"

O GDPR reforça muito, em diversos artigos, essa determinação de permitir o acesso ao usuário das informações referentes ao tratamento de seus dados. Por exemplo, no inciso 7, ele indica que não basta somente apresentar os dados, é preciso que eles estejam com um layout claro, visível, inteligível. O Regulamento indica que as informações referentes ao tratamento obtenham um destaque.

> "7. As informações a fornecer pelos titulares dos dados nos termos dos artigos 13.o e 14.o podem ser dadas em combinação com ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e claramente legível, uma perspectiva geral significativa do tratamento previsto. Se forem apresentados por via eletrônica, os ícones devem ser de leitura automática." (art. 12, 7, GDPR).

O *Google*, como exemplo, apresenta uma política de privacidade com links, vídeos explicativos e destaque para informações relevantes. Sua política, aliás, foi atualizada em 15 de outubro de 2019. O recurso de vídeo pode facilitar bastante o entendimento dos dados que são tratados. Essas empresas que têm grande parte de sua receita ligada ao tratamento de dados têm um compromisso ainda maior de explicar aos usuários como são realizadas essas operações.

> "A transparência não é um direito em si próprio. É, em realidade, um princípio geral que se atrela ao direito de informação e que se coloca ao lado dos princípios da licitude e da lealdade, na forma do que dispõe o artigo 5º, item 1 "a"; os dados pessoais são a)objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados."[59]

O princípio da transparência deve permear todas as ações dos agentes de dados, cabe aos profissionais responsáveis a devida clareza sobre todos os acontecimentos relevantes com o tratamento e armazenamento das informações.

[59] BLUM, Renato Opice; MALDONADO, Viviane Nóbrega. Op. cit. p. 92.

2.3 O Direito à informação dos dados pessoais

O GDPR, no seu art. 13 e 14, elenca as informações que devem estar disponíveis para o titular. O direito à informação pode ser entendido como um desdobramento do direito à transparência. Os agentes de tratamento, segundo o Regulamento, não podem negar aos titulares determinadas informações sob risco de serem responsabilizados sobre as omissões.

Há uma divisão relevante na seção 2 do capítulo III com relação aos direitos de informação e acesso aos dados, o direito à informação é subdivido em dois artigos, o art. 13 trata do direito à informação que é obtido junto ao titular e o art. 14 trata do direito que não é obtido junto ao titular. O direito de acesso do titular de dados é apresentado no art. 15. Por exemplo, um tratamento realizado diretamente com o titular dos dados e um tratamento que se vale de dados já recolhidos por terceiros. É uma forma de forçar os agentes a manter um histórico confiável e completo dos dados que podem ser tratados e, sobretudo, uma maneira de garantir que um dado coletado por um agente de tratamento A e transferido para um agente de tratamento B seja perfeitamente identificado, caso o titular dos dados busque as informações junto ao agente de tratamento B. Feitas essas considerações e entendendo, de certo modo, que os art. 13 e 14 são complementares, é possível agrupar as informações que são fornecidas ao titular dos dados em três grupos: 1) informações sobre a identidade dos agentes de tratamento; 2) informações sobre a finalidade do tratamento e as 3) informações sobre o destinatário dos dados, caso haja.

As informações sobre a identidade dos agentes de tratamento são: “a) A identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante e o b) Os contatos do encarregado da proteção de dados, se for caso disso;”[60] O titular dos dados tem direito de saber as informações básicas sobre a identidade e o contato do responsável pelo tratamento.

Por exemplo, em uma rápida pesquisa no site de buscas do *Google*[61] é possível encontrar a política de dados[62] do jornal francês *Le Monde*, o item 2 da política de dados,

[60] Arts. 13 e 14, GDPR.
[61] Disponível em: www.google.com.br. Acesso em: 10 nov. 2019.
[62] Disponível em: https://www.lemonde.fr/confidentialite/. Acesso em : 02 nov. 2019.

intitulado “2. Quem é o responsável pelos tratamentos realizados no presente documento?”[63] deixa claro o respeito ao GDPR e mais especificamente ao direito do titular a obter a identidade do encarregado da proteção de dados. No caso específico há a referência a uma empresa, a *Sociedade editora du Monde*, com o devido endereço, registro comercial, capital social e representante legal, além de um encarregado pela proteção dos dados do grupo *Le monde*, senhora Juliette Boukobza.[64]

Com relação à finalidade do tratamento, o Regulamento indica que o agente deve informar: “c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;”[65] Trata-se de mais uma informação assegurada pela lei, também relacionada com o direito à transparência.

Considerando ainda nosso exemplo sobre o jornal francês *Le Monde*. O item 4 de sua política de dados, intitulado “4. Para quais finalidades nós utilizamos os seus dados?” [66] faz um detalhamento de todas as finalidades relacionadas aos dados coletados. Há uma lista com quatro grandes finalidades com dezenas de subitens relacionados, esses grupos são: 4.1 Operações necessárias ao fornecimento de produtos e serviços, 4.2 Operações de marketing e de prospecção comercial relativas às publicações, produtos e serviços do grupo *Le Monde*, 4.3 Operações ligadas à parceiros comerciais e 4.4Finalidades associadas a inclusão de cookies no seu navegador.[67]

E por fim, com relação somente ao direito à informação, o titular deve ter acesso às informações referentes aos destinatários, “e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;”.[68] Trata-se de um direito de saber o caminho que o dado pode percorrer.

---

[63] “2. Qui est le responsable des traitements mentionnés dans le présent document ?”
[64] “Le responsable des traitements mentionnés par le présent document est la Société éditrice du Monde, société anonyme à directoire et conseil de surveillance au capital de 124 610 348,70 €, dont le siège social est situé 80, boulevard Auguste-Blanqui, 75013 PARIS, immatriculée au registre du commerce et des sociétés de Paris sous le n° 433 891 850 et dont Monsieur Louis Dreyfus, président du directoire, est le représentant légal. La Société éditrice du Monde est une entité du Groupe Le Monde.” Disponível em: https://www.lemonde.fr/confidentialite/. Acesso em: 04 nov. 2019.
[65] Arts. 13 e 14, GDPR.
[66] 4. Pour quelles finalités utilisons-nous vos données ?
[67] “4.1. Opérations nécessaires à la fourniture de produits ou services, 4.2. Opérations de marketing et de prospection commerciale relatives aux publications, produits et services du Groupe Le Monde, 4.3. Opérations liées à des partenariats commerciaux, 4.4. Finalités associées au dépôt de cookies sur votre navigateur.”
[68] Arts. 13 e 14 da GDPR.

No caso da condenação do *Google*, a sentença da CNIL foi fundamentada pela falta de transparência da política de dados do *Google*. Os itens 119, 120 e 121, mostram que no item 4 da política apresentada pelo portal o período de conservação de dados não é está claro.

> "119. Com relação às informações sobre períodos de conservação dos dados, a estrutura apresentada indica que a página "Como as informações são coletadas pelo Google" está organizada em quatro categorias: (i) informações conservadas até que você as suprima; (ii) informações que serão expiradas com o tempo; (iii) informações conservadas até que sua conta do Google seja excluída; (iv) informações mantidas por longos períodos de tempo por razões específicas.
> 120. No entanto, observa-se que em se tratando da última categoria, somente há informações muito gerais sobre o objetivo da retenção e nenhuma duração precisa. Os critérios utilizados para determinar essa duração não são indicados. Essas informações estão entre as que devem ser emitidas a pessoas nos termos do artigo 13 (2) (a) do Regulamento.
> 121. Por fim, se a empresa alega que várias ferramentas de informação são disponibilizadas aos usuários concomitantemente e após a criação de sua conta, a estrutura restrita mostra que esses métodos não permitem atender aos requisitos de transparência e informações dos artigos 12 e 13 do RGPD."[69] [70]

Por exemplo, em caso recente, o órgão de controle francês *Comission Nationale Informatique & Libertés* (CNIL) aplicou uma multa milionária ao *Google.*[71] A alegação do órgão que multou a companhia americana em 50 milhões de euros foi de "falta de transparência, informação insuficiente e falta de consentimento válido sobre personalização de anúncios". Isso mostra que o objeto da lei se direciona para companhias que tratam os dados europeus independentemente da sua nacionalidade ou localização física, basta que o cidadão ou organização europeia sejam vítimas de um tratamento inadequado de dados.

O caso do *Google* é um sinal claro de que os dados não serão tratados como antigamente e que a Europa está disposta a enfrentar grandes empresas que dominam o

---

[69] "119. S'agissant de l'information relative aux durées de conservation, la formation restreinte relève que la page "Comment des informations collectés par Google sont-elles conservés" comporte quatre catégories: (i) informations conservées jusqu'à ce que vous le supprimiez; (ii) informations assorties d'un délai d'expiration; (iii) informations conservées jusqu'à la supression de votre compte Google; (iv) informations conservées pendant de longues périodes pour des raisons precises. 120. Elle constate néanmoins que s'agissant de la dernière catégorie, seules des explications très générales sur la finalité de cette conservation sont founies et aucune durée précise ni les critères utilisés pour déterminer cette durée ne sont indiqués. Or cette information figure parmi celles devant êtrre obligatoirement délivrées aux personnes en application du a) du 2 de l'article 13 du Règlement. 121. En dernier lieu, si la société fait valoir que de multiples outils d'information sont mis à la disponsition des utilisateurs concomitamment et après la création de leur compte, la formation restreinte relève que ces modalités ne permettent pas d'atteindre les exigences de transparence et d'information issues des articles 12 et 13 du RGPD (GDPR)."

[70] Sentença que condenou o Google ao pagamento de 50 milhões de euros. CNIL – *Comission Nationale Informatique & Libertés*, 2019.

[71] PACETE. Luiz Gustavo. **Multa aplicada ao Google é emblemática para a GDPR**. 22/01/2019. Meio e Mensagem (online). Disponível em: https://www.meioemensagem.com.br/home/midia/2019/01/22/multa-aplicada-ao-google-e-divisor-de-aguas-para-a-gdpr.html. Acesso em: 25 out. 2019.

mundo tecnológico e econômico. As empresas que mais faturam no mundo precisam adaptar suas práticas, segundo Dani Dilkin, diretor de uma empresa de consultoria de negócios.

> "(...), em maio do ano passado. Na última sexta-feira, 18, a mesma denúncia recaiu sob o YouTube, Netflix, Spotify, Apple e Amazon em uma lista apresentada pela Autoridade Austríaca de Proteção de Dados. (...) a sanção aplicada ao Google reforça o rigor com o qual o tema será tratado na União Europeia e em outras regiões."[72]

No caso das grandes corporações, a lei prevê uma multa de até 4%[73] do faturamento[74] global da companhia, o que no caso do Google seria um valor bilionário, pois segundo a revista Época Negócios[75] em 2017 a empresa Alphabet que controla o *Google* teve um faturamento acima de 100 bilhões de dólares. No Brasil a multa é menos impactante para companhias como o *Google*, o teto da lei brasileira é de até R$ 50.000.000,00.

Os agentes de dados precisam ser transparentes sobre a forma como esses dados estão sendo analisados, mas também precisam informar objetivamente sobre esses dados. O princípio da transparência é, de certo modo, mais abrangente, uma espécie de boa-fé que os agentes devem ter, já o direito a informações é mais concreto e específico com um rol de informações que podem ser fornecidas.

2.4 O Direito de acesso aos dados pessoais

O direito de acesso que o titular de dados possui está presente no art. 15 e reforça os demais direitos presentes no capítulo III, por exemplo, no inciso I, há a indicação que o titular pode ter acesso resumidamente às seguintes informações: 1) as finalidades do tratamento; 2) as categorias dos dados; 3) destinatários ou categorias de destinatários; 4) o prazo previsto de

---

[72] PACETE. Luiz Gustavo. Op. cit. pág. 01.

[73] "Art. 83 - 5. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o nº 2, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado (art. 83, 5, GDPR).

[74] No Brasil, a Lei Geral de Proteção de Dados (LGPD) prevê uma multa de até 2% do faturamento anual, mas limitada a um teto de R$ 50 milhões. Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (...) II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração (art. 52, LGPD).

[75] GOOGLE, Amazon e Apple batem recorde em seus balanços. Época Negócios. 02/02/2018. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2018/02/google-amazon-e-apple-batem-recorde-em-seus-balancos.html. Acesso em: 11 ago. 2019.

conservação dos dados, e os critérios para esses prazos; 5) o direito de solicitar ao responsável prelo tratamento a retificação, o apagamento ou a limitação do tratamento; 6) o direito de apresentar reclamação a uma autoridade de controle; 7) informações sobre a origem dos dados e 8) se há decisões automatizadas.

Considerando que no direito à informação a finalidade dos dados já foi apresentada, a alínea b) trata do acesso ao tipo de categoria em que o dado está parametrizado.[76] É um direito de acesso a forma como o dado é organizado, ou seja, a maneira como os agentes de dados tratam esses dados e os organizam para obter determinados resultados. É um acesso a estrutura operacional de tratamento do dado.

Os destinatários também foram apresentados no direito à informação, seguindo, assim para a alínea d) que trata de uma categoria bem relevante, o acesso ao prazo previsto de conservação dos dados.[77]

2.5 Direito de retificação

O direito de retificação é apresentado pelo Regulamento de forma muito sintética, ele está concentrado no caput do art. 16:

> "Art. 16 O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional." (Art. 16, GDPR).

As observações referentes a retificação dizem respeito ao tempo que deve ser razoável e justificável e a retificação propriamente dita permitindo ao titular dos dados efetuar as correções necessárias para manter a integridade das informações. Na maioria dos bancos de dados gerados pela internet é normalmente possível e relativamente simples a retificação ou alteração dos dados fornecidos pelo titular.

---

[76] "b) As categorias dos dados pessoais em questão." (GDPR, art. 15).
[77] "d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo." (art. 15, GDPR).

Por exemplo, no *Facebook* é possível editar as informações do usuário, nas configurações pode se editar as informações da conta, e na página principal do perfil é possível, através dos links com a informação "editar", alterar ou retificar s informações prestadas. O mesmo acontece com demais redes sociais como o *Linkedin* e o *Whatsapp* que possuem formas disponíveis aos usuários para alterarem suas informações.

2.6 Direito de apagamento de dados

O Direito de apagamento dos dados está presente no art. 17 do Regulamento, "Direito ao apagamento dos dados (direito a ser esquecido)", e permite ao titular dos dados obter do responsável pelo tratamento a exclusão de seus dados.[78] Há alguns motivos específicos que permitem ao titular solicitar a exclusão desses dados, são eles:

> "a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8º, n. 1." (GDPR. Art. 17).

O primeiro motivo diz respeito à manutenção da finalidade inicial relacionada com a recolha ou o tratamento. Um dado recolhido para um determinado fim não pode ser reutilizado, sem prévia autorização do titular dos dados, para uma finalidade distinta, se isso ocorrer, o titular poderá solicitar exclusão dos seus dados.

É o reforço de que um determinado dado coletado deve ser destinado para um fim específico, é um direito do titular que esse fim seja respeitado. Podemos imaginar diversos exemplos para o desvio de finalidade, por exemplo, um restaurante que oferece um cadastro de descontos para seus clientes e nesse cadastro ele contabiliza o peso que cada cliente consome diariamente. Nesse caso, a finalidade deve ser específica para a promoção

[78] "Artigo 17. O Direito ao apagamento dos dados («direito a ser esquecido») 1.O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada." (art. 17 GDPR).

específica, caso esse dado seja disponibilizado para uma clínica, por exemplo, interessada nos clientes que consomem as maiores quantidades, esse tipo de transferência dos dados é considerada ilegal, e é um direito do titular exigir que esse dado seja apagado.

O tratamento de dados deve respeitar uma finalidade específica e, em regra, ter a concordância do usuário. Um princípio indicado pela lei é o "não reaproveitamento" dos dados para um fim incompatível com o originalmente determinado.

> "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, nº 1 («limitação das finalidades»)." (GDPR, art. 5º, 2016).

Dessa forma, não seria possível o cruzamento de dados de forma indeterminada e incompatível com o consentimento inicial. Aliás, no que diz respeito ao tratamento mais propriamente, o art. 6º[79] vai nos apresentar esse consentimento como uma importante limitação para o tratamento de dados.

> "O consentimento, provavelmente a principal hipótese para o tratamento de dados pessoais, é definido no GDPR como manifestação de vontade, livre, específica, informada e explícita, pela qual a titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento, devendo conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina." (GDPR, art. 5º, 2016).

Segundo Carlos Roberto Gonçalves,[80] "o consentimento pressupõe a capacidade das partes para vender e comprar e deve ser livre e espontâneo, sob pena de anulabilidade". A lei brasileira segue essa condição de consentimento livre, a LGPD define consentimento em seu *art. 5º, XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica.* A Comissão Europeia disponibiliza um artigo para orientar a interpretação do consentimento[81],

---

[79] "Art. 6º. Licitude do tratamento 1.O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas." (art. 6º, GDPR).

[80] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**. Vol. 1: parte geral. 12ª Ed. São Paulo: Saraiva, 2014. p. 48.

[81] Grupo de Trabalho do artigo 29º - Article 29 Working Party; Guidelines on consent under Regulation 2016/679. Grupo de trabalho do art. 29º - Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/679(disponível em português em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Acesso em:14 jul. 2019).

essas orientações, segundo o próprio documento, "fornecem uma análise exaustiva do conceito de consentimento previsto no Regulamento."

Destaca-se nas orientações um exemplo bem significativo de como o novo Regulamento pode impedir o tratamento inadequado de dados. O exemplo 1[82] é de "um aplicativo de celular para edição de imagens que solicita aos utilizadores que ativem a localização por *GPS* para fins de prestação de serviço. O aplicativo também informa que utilizará os dados recolhidos para fins de publicidade comportamental". Tais solicitações não são necessárias para a prestação do serviço do aplicativo de edição de imagens fotográficas, o usuário só pode utilizar o aplicativo se consentir com tal utilização, o que torna o consentimento não livre e, logo, ilegal.

Por exemplo, se fizermos um teste na loja de aplicativos do *Android*[83] e buscarmos um aplicativo de edição de imagens, podemos selecionar, por exemplo, da empresa InShot Inc. o aplicativo "Editor de Fotos – Montagem de Fotos e Colagem. O aplicativo está em português e apresenta avaliação de 4,7/5,0 (avaliado por quase 200 mil usuários), o desenvolver tem um endereço de Hong Kong. O aplicativo após instalado não solicita nenhum consentimento, todavia, se acionarmos a política de privacidade ela está em inglês, dela é possível depreender que, de fato, não há o armazenamento e o tratamento de PII (*Personally Identifiable Information*),[84] somente no caso de contato do usuário com o desenvolver do aplicativo.

> "A única situação em que podemos obter acesso às suas informações de identificação pessoal é quando você decide pessoalmente enviar seus comentários por e-mail ou fornecer um relatório de erro. As informações de identificação pessoal que podemos obter nessa situação são estritamente limitadas ao seu nome, endereço de e-mail e apenas sua resposta à pesquisa. (Política de privacidade - InShot Inc.)".[85]

Apesar do aplicativo alegar por sua política (em inglês) que não tratará seus dados pessoais, parece haver um desrespeito à transparência e a clareza. As políticas dos aplicativos devem, respeitando diversos dispositivos tanto do Regulamento europeu quanto da Lei brasileira, ao menos, serem apresentadas no idioma oficial do país.

---

[82] [exemplo 1] – Grupo de Trabalho do artigo 29º. Última redação revista e adotada em 10 de abril de 2018, pág 6.
[83] Google Play (Loja de aplicativos do Sistema Operacional Android).
[84] Informações de Identificação Pessoa.
[85] The only situation we may get access to your PII is when you personally decide to email us your feedback or to provide us with a bug report. The PII we may get from you in that situation are strictly limited to your name, email address and your survey response only. (Privacy Policy – InShot Inc. – EDITOR de Fotos – Montagem de Fotos e Colagem.

Se não há interesses justos para o tratamento, não deve ocorrer o tratamento, e, caso ocorra, é um direito do titular também exigir o apagamento dos dados ali tratados. A finalidade não deve ser alterada durante o tratamento, o consentimento deve persistir e o fim deve justo e o tratamento de dados deve respeitar a legalidade.

Em decorrência de uma decisão judicial o dado também deve ser apagado e, por fim, o direito ao apagamento de dados em situações que envolvam menores de 16 anos sem o devido consentimento dos responsáveis.

2.7 Direito à limitação de tratamento

O art. 18 trata do Direito à limitação de tratamento, esse direito não é o mesmo que o direito ao apagamento, nele o titular dos dados pode, por um motivo específico elencado no referido artigo, impedir temporalmente ou qualitativamente um determinado tratamento.

O Considerando 67 especifica melhor quais são as situações de limitação de tratamento:

> "Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições." (Considerando 67, GDPR).

As situações previstas no art. 18 que justificam o direito do titular são: a) a inexatidão dos dados pessoais;[86] b) o tratamento ilícito;[87] c) os responsáveis não precisarem mais dos dados pessoais[88] e d) oposição aos motivos do tratamento.[89]

[86] "a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão." (art. 18, 1, GDPR).
[87] "b)O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização." (art. 18, 1, GDPR).
[88] "c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial." (art. 18, 1, GDPR).
[89] "d) Se tiver oposto ao tratamento nos termos do artigo 21.o, n.o 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados." (art. 18, 1, GDPR).

2.8 Direito à portabilidade dos dados

A portabilidade é mais um direito presente no rol do capítulo III e diz respeito a possibilidade do titular de dados de solicitar ao responsável pelo tratamento de dados os seus dados em um formato estruturado podendo transferir esses dados para um outro responsável.

O direito à portabilidade impede que os agentes de tratamento, em situações específicas, criem uma situação de "aprisionamento de informações", e o titular não consiga migrar livremente para outros serviços que possam lhe parecer mais favoráveis. Há um termo em inglês, vendor lock-in. Esse direito de portabilidade já se manifesta no Brasil e ficou muito conhecido na possibilidade de troca de operadora de telefonia móvel.

> "O objetivo dessa norma é proteger o titular de dados da situação conhecida como vendor lock-in, que, em português pode ser traduzida por "aprisionamento tecnológico". Tal circunstância acaba por compelir o usuário e permanecer vinculado a um determinado controller, já que os custos para possível troca seriam excessivamente elevados e capazes de desmotivar a substituição."[90]

2.9 Direito de oposição

O direito de oposição, previsto na seção 4 do capítulo III, no art. 21, faz referência à possibilidade que o titular de dados tem de se opor ao tratamento de dados para efeito de comercialização, ou por motivos relacionados à licitude do tratamento.

A possibilidade de se opor a esses tratamentos é um direito que surge em decorrência dos princípios gerais que regem o próprio regulamento. Há algumas particularidades presentes no artigo, por exemplo, a possibilidade presente no inciso 3[91] do titular se opor somente ao tratamento para efeitos de comercialização direta.[92]

---

[90] BLUM, Renato Opice; MALDONADO, Viviane Nóbrega. Op. cit. p. 105.

[91] "3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim." (art. 21,GDPR).

[92] A comercialização direta é entendida, no Regulamento Geral sobre a Proteção de Dados, como qualquer ação, por parte de uma empresa, destinada a comunicar material publicitário ou de comercialização, dirigida a pessoas específicas. A sua empresa/organização deve informar as pessoas, no seu aviso de privacidade ou pelo menos no momento da primeira comunicação com as mesmas, de que irá utilizar os seus dados pessoais para efeitos de comercialização direta e de que estes têm o direito a opor-se gratuitamente. Sempre que uma pessoa se opõe ao tratamento dos dados pessoais para efeitos de comercialização direta, a sua empresa/organização deixa de poder efetuar o tratamento dos seus dados pessoais para esse efeito. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/what-happens-if-someone-objects-my-company-processing-their-personal-data_pt. Acesso em: 22 out. 2019.

Há a possibilidade do agente de dados se negar a atender o direito de oposição do titular, nesse caso, ele precisa demonstrar que o tratamento deve prevalecer frente aos interesses, direitos e liberdades do titular de dados.

Um exemplo relatado pela comissão europeia é o caso das empresas da área de seguros que, muitas vezes, necessitam dos dados do titular para exercer seus próprios direitos:

> "No setor dos seguros, é muito frequente os dados pessoais serem necessários para a defesa de ações judiciais no caso de medidas antifraude ou antibranqueamento de capitais. Nesses casos, as companhias de seguros podem recusar-se a atender ao pedido de oposição de uma pessoa com base em motivos que prevalecem sobre os direitos e as liberdades deste." (Comissão Europeia).[93]

Apesar disso, cabe ao responsável pelo tratamento a comprovação de que, de fato, não é possível o atendimento ao direito de oposição do titular, o Considerando 69 do Regulamento esclarece essa exigência na negativa dos responsáveis.

> "No caso de um tratamento de dados pessoais lícito realizado por ser necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou ainda por motivos de interesse legítimo do responsável pelo tratamento ou de terceiros, o titular não deverá deixar de ter o direito de se opor ao tratamento dos dados pessoais que digam respeito à sua situação específica. Deverá caber ao responsável pelo tratamento provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados." (GDPR, Considerando 69).

Considerando a prática comum de ofertas de anúncios relacionadas com a comercialização direta, é provável, que o direito de oposição se manifeste de forma mais presente nos casos de impedimento de comercialização direta. Assim, é possível que um titular exercendo seu direito, se oponha ao tratamento que geraria nossas possibilidades de comercialização direta.

Por exemplo, é relativamente comum nas redes sociais a vinculação de propagandas de produtos recém-pesquisados. Nesse caso, trata-se de material publicitário com o fim claro de comercialização direta e, segundo o art. 21, o titular de dados poderia se opor às propagandas que estão diretamente vinculadas com o tratamento de seus dados pessoais.

---

[93] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/what-happens-if-someone-objects-my-company-processing-their-personal-data_pt. Acesso em 10 nov. 2019

Nesse aspecto, a oposição, caso seja popularizada e entendida como uma forma comum dos titulares de dados de evitarem propagandas direcionadas, pode gerar uma dificuldade de monetização dos agentes econômicos envolvidos, visto que atualmente a publicidade na internet está pautada fortemente na comercialização direta e pessoal. Assim, o direito à oposição, apesar de aparentemente simples, deve ser observado e analisado com o fim de compreender se, de fato, os titulares terão interesse em limitar essa prática comum no tratamento de dados.

2.10 Direito de objeção quanto a decisões individuais automatizadas

Por fim, o último direito apresentado no capítulo III, é o direito de objeção quanto a decisões individuais automatizadas. O art. 22 limita a atuação de decisões automatizadas que atualmente são muito presentes em diversas relações de consumo. Por exemplo, é perfeitamente possível que na abertura de contas bancárias digitais um software verifique que o cliente não atenda aos requisitos necessários estabelecidos pelo banco. Nesse caso, o titular de dados tem o direito de se opor a essa decisão e buscar uma análise mais específica.

Esse direito busca diminuir os problemas relacionados com o tratamento automatizado de determinadas dados em situações específicas, permitindo que o titular possa esclarecer melhor a composição dos dados solicitados e buscar uma melhor compreensão de sua situação real. O tratamento automatizado pode limitar o direito do titular estabelecendo barreiras excessivas para o exercício de um direito.

> "O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar." (art. 23, I, GDPR).

As informações coletadas para o tratamento automatizado podem surgir de diversas fontes, o objetivo do Regulamento é proteger o titular de dados da construção de um perfil com uma interpretação muito restritiva e potencialmente prejudicial. Um caso conhecido que ocorreu nos EUA, publicado em um artigo do NYT[94] em 2012, foi do tratamento de dados realizado pela empresa Target, uma empresa varejista dos EUA, que através da análise de dados do comportamento de consumo identificou a gravidez de uma jovem antes mesmo que

[94] *New York Times*.

seu pai soubesse. Segundo a reportagem esse tipo de tratamento de dados gerou um lucro para empresa que conseguia saber o momento da gravidez de suas clientes e com isso lançava uma agressiva campanha de marketing de produtos específicos para gestantes. Esse caso só ocorreu porque há um tratamento automatizado e a construção de um perfil com os dados dessas clientes. O Regulamento busca, de certo modo, em determinadas situações, limitar a criação desses perfis.

De forma ilustrativa, o episódio da série *Netflix*, "Queda Livre",[95] mostra como o tratamento de dados pode ser prejudicial para o titular de dados, a jovem Lacie ativa nas redes sociais, busca atingir os melhores conceitos definidos pela interação entre os usuários do programa. As notas obtidas influenciam diretamente na vida real de Lacie, por exemplo, na compra de um imóvel, no aluguel de um veículo, na compra de passagens aéreas. O episódio mostra que o tratamento automatizado pelos algoritmos já determina o destino da personagem principal, Lacie, sua nota baixa no aplicativo a restringe de uma série de direitos disponíveis apenas para aqueles que possuem boas avaliações. Essa alegoria nos mostra os danos em potencial que podem ser causados ao titular de dados por um tratamento ilegal e abusivo.

[95] BLACK MIRROR. **Queda Livre (Nosedive)**. Dirigido por Joe Wright. Escrito por Carlie Brooker, Rashida Jones & Mike Schur. 1º episódio da 3ª temporada. Londres: Netflix, 2016.

III. OS DIREITOS DOS TITULARES DOS DADOS NA NOVA LEI GERAL DE PROTEÇÃO DE DADOS

A nova Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018, que entra em vigor em agosto de 2020, promete causar uma mudança radical nas práticas relacionados ao tratamento e armazenamento de dados no Brasil. Essa Lei, aliás, já vem influenciando uma série de medidas em entidades públicas e privadas que buscam, desde agora, se adequar às inúmeras exigências impostas pela LGPD.

Antes de buscar o diálogo entre as fontes e a jurisprudência brasileira que possa perpassar o tema da proteção de dados pessoais, vale observar a estrutura da nova Lei, a LGPD está dividida em 65 artigos e 10 capítulos, se comparada com o RGPD a lei brasileira é mais sintética e mais objetiva. No que diz respeito especificamente ao nosso recorte sobre os direitos dos titulares, há na Lei especificamente no capítulo III, nove direitos explícitos, são eles: 1) confirmação da existência do tratamento; 2) acesso aos dados; 3) correção de dados incompletos, inexatos ou desatualizados; 4) anonimização, bloqueio ou eliminação de dados desnecessários; 5) portabilidade dos dados; 6) eliminação dos dados pessoais; 7) informações sobre o compartilhamento de dados; 8) informações sobre a possibilidade de não fornecer o consentimento; e 9) revogação do consentimento.[96]

Assim como ocorre no Regulamento europeu, há uma série de direitos que não estão diretamente previstos no capítulo III, e que podem ser entendidos a partir das disposições preliminares da lei, dos fundamentos previstos nos arts. 1º e 2º. Eles tratam dos direitos: à liberdade; à liberdade de expressão, de informação, comunicação e de opinião; à privacidade; ao livre desenvolvimento da personalidade, à autodeterminação informativa, à intimidade, à honra e à imagem, do consumidor, dentre outros. São direitos mais gerais que podem também ser extraídos da Constituição e de outros normativos. É uma forma da Lei reforçar esses ideais

[96] "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa." (art. 18, LGPD).

e garantir que os fundamentos presentes nos direitos dos titulares de dados dialogam com princípios legais e constitucionais. Esses fundamentos serão melhor compreendidos nos itens 3.1 e 3.2 deste trabalho.

3.1. Os fundamentos e a aplicabilidade da LGPD

O capítulo primeiro da Lei trata das disposições preliminares, nele há a definição de alguns termos importantes para a LGPD, a indicação dos fundamentos e, sobretudo, a delimitação da aplicabilidade do normativo. O art. 1º[97] dispõe sobre o objeto central da Lei que é o tratamento de dados pessoais, seja por pessoa natural ou pessoa jurídica de direito público ou privado. Essa definição é muito similar ao do Regulamento europeu, e expressa de forma clara que a lei regulamentará a forma como os dados devem ser tratados. O art. 2º apresenta os fundamentos da proteção de dados, são eles:

> "I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." (art. 2º, LGPD).

Esses fundamentos nos orientam na melhor interpretação da norma. A Lei busca indicar o caminho que deve ser seguido para compreender os valores que devem ser considerados no momento do tratamento e armazenamento de dados pessoais. O inciso I, o respeito à privacidade,[98] reforça o entendimento de que há um campo privado que deve ser respeitado pelo operador de dados, o inciso II trata do direito que o cidadão tem de se informar sobre o que é feito com os dados pessoais tratados pelos operadores. A falta de clareza dos operadores dos dados fere essa premissa, os usuários precisam ter acesso sobre o que, de fato, é tratado de suas informações pessoais.

A liberdade de expressão como um reforço do texto constitucional, e o entendimento de que é um fundamento da rede mundial de computadores a liberdade de opinião, de informação

---

[97] "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." (art. 1º, LGPD).

[98] Podemos comparar a LGPD à Lei 12.965/2014, conhecida como marco civil da internet, que em seu art. 3º também tem como princípio a proteção da privacidade.

e de comunicação. Algo também reforçado pelo marco civil[99] da internet. O quarto fundamento, inciso IV, é o da inviolabilidade da intimidade, da honra e da imagem do usuário. Por exemplo, na famosa série *Black Mirror*, há vários episódios que tratam da questão da privacidade, um deles é o *Shut up and Dance*[100] que relata a invasão de hackers nos computadores dos usuários, esses usuários acabam sendo chantageados por esses invasores que possuem dados sensíveis de sua intimidade. O episódio mostra a fragilidade da intimidade exposta na rede, o personagem principal é filmado em uma situação constrangedora e, sob ameaça de exposição pública, realiza uma série de tarefas impostas pelos criminosos. A Lei então busca reforçar a proteção desses direitos.

A preocupação presente no Regulamento e na Lei é, sem dúvida, a viabilidade da proteção da privacidade frente a um mercado que, em tese, necessita dessas informações para continuar em desenvolvimento. Assim, a Lei também assegura o desenvolvimento econômico, tecnológico, a inovação, e também a livre iniciativa, a livre concorrência e o direito do consumidor. Os incisos V e VI são um contraponto necessário para compreender a complexa relação entre os agentes de tratamento dos dados e os titulares de dados. E por fim, o inciso VII, é um fundamento mais geral, abrangente, de menor densidade normativa, os Direitos Humanos, a dignidade e o exercício da cidadania.

O art. 3º reforça que a Lei se aplica a qualquer operação de tratamento de dados,[101] trata-se de uma ratificação do art. 1º, mas com uma delimitação da aplicabilidade da norma. A primeira delimitação é territorial, "I - a operação de tratamento seja realizada no território nacional;". A lei se aplica aos tratamentos realizados no Brasil, mesmo que por pessoas físicas ou jurídicas de nacionalidades diferentes.

---

[99] "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal." (Lei nº 12.965/2014).

[100] Manda quem Pode (em português).

[101] "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei."

O inciso I indica que a lei se aplica, no momento do tratamento, a uma operação realizada no território brasileiro. Por exemplo, um indivíduo com um notebook que trata dados de diversos lugares, mas que está fisicamente localizado no Brasil deve seguir os preceitos da LGPD. A lei se aplica a uma empresa estrangeira que trata dados de estrangeiros, mas que está localizada no Brasil. O inciso I trata da localização física do operador dos dados.

O parágrafo 2º do artigo 3º excetua a aplicação do inciso I em situações em que estrangeiros não estabelecem uma comunicação direta com agentes de tratamento brasileiros, é um caso, por exemplo, de um estrangeiro que tem seus dados tratados por agentes estrangeiros e está aqui no Brasil apenas para turismo. Nesse caso, a norma afasta a sua aplicabilidade desde que haja, no país de origem do titular, uma proteção de dados equivalente à brasileira. "§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei."[102]

O inciso II acrescenta que mesmo que o tratamento não seja realizado no Brasil, se tiver por destino um indivíduo localizado no território nacional a Lei também se aplica. "II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;". Assim a Lei ganha, como o GDPR, um aspecto extraterritorial, uma jurisdição abrangente que busca proteger os brasileiros de tratamentos fora do Brasil.

Por exemplo, em uma eventual violação do tratamento dos dados pela empresa *Google*, seria possível aplicar a LGPD. Mesmo que os servidores da companhia não estejam localizados no Brasil e que o tratamento seja realizado nos EUA, a justiça brasileira poderia sancionar a empresa e, assim como fez a CNIL francesa, forçar o *Google* a se adequar a LGPD.

O inciso III considera também a possibilidade de o dado ter sido coletado no território nacional e ser tratado em outro território. Seria uma ampliação da aplicação do inciso I que trata especificamente do momento do tratamento. Assim, "III - os dados pessoais objeto do

[102] "IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei." (art. 4º, IV, LGPD).

tratamento tenham sido coletados no território nacional.", a norma também se aplica aos dados apenas coletados no Brasil e tratados no exterior.

Então, a lei se aplica também aos dados, mesmo que apenas coletados no Brasil e tratados no exterior. Há uma ressalva para essa aplicação territorial, o art. 3º, § 1º: "*Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta*." O recorte, assim como ocorre com o tratamento, é temporal e espacial, no momento da coleta o titular dos dados precisa estar em território nacional para que a lei seja aplicada.

3.2. Princípios que norteiam a LGPD

O Art. 6º da LGPD estabelece uma série de princípios que devem ser observados no tratamento de dados. Além o princípio da boa-fé presente no caput do artigo, há dez princípios explícitos indicados e explicados nos incisos que se seguem do referido artigo.

O princípio da Finalidade,[103] também destacado pelo GDPR, é um dos princípios que norteia a Lei e vai impedir o reaproveitamento arbitrário e com fim totalmente diversos do tratamento de dados. O respeito à finalidade, como já indicou Bruno Ricardo Bioni, vai impedir que um banco de dados compartilhe as informações destinadas a um fim diverso. Por exemplo, um site ligado à área de Educação que possui informações sobre o desempenho de seus alunos coleta e trata dados com o fim de gerenciar as atividades educacionais e orientar a melhor forma de alcançar objetivos específicos. O desvio de finalidade estaria constituído se o site resolvesse compartilhar dados com fins diversos, por exemplo, para agências de empregos que buscam profissionais com o melhor desempenho educacional. Há um desvio de finalidade, os dados recolhidos não se destinavam a alimentar informações relacionadas a vagas de empregos. No caso, a agência de empregos deve gerar seu próprio banco de dados especificando para o titular dos dados, de forma clara, qual a finalidade das informações solicitadas.

[103] "I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades." (art. 6º, LGPD).

A adequação[104] e a necessidade[105] são princípios que impedem que agentes de tratamento exijam informações que estão distantes de sua finalidade. Um aplicativo de jogo eletrônico, por exemplo, não deve exigir informações pessoais que ultrapassem a sua margem possível de atuação. Determinados jogos eletrônicos se valem do sistema de posicionamento global (GPS) como uma dinâmica necessária para o funcionamento do software, o famoso jogo *Pokemon GO*[106] é um exemplo de utilização do recurso. Entretanto, o próprio jogo *Pokemon Go* não pode se valer dessas informações para fins diversos do estritamente necessário, pelo princípio da finalidade, e não pode exigir outras informações incompatíveis, como renda mensal, hábitos de compras em outros jogos, pelos princípios da adequação e necessidade.

A LGPD prevê que o titular dos dados tenha livre acesso a seus dados tratados. Não é mais possível que os agentes de tratamento mantenham banco de dados secretos e inacessíveis ao titular de dados. O acesso deve ser gratuito e facilitado permitindo que o titular compreenda perfeitamente quais dados estão armazenados e de que forma estão sendo tratados. Em caso de eventuais incorreções, é possível que o titular dos dados realize de forma simples as devidas correções. Além disso, é fundamental que todo o processo seja permeado pela transparência por parte dos agentes de tratamento.

A lei estabelece três princípios expressos que indicam a forma como os dados devem ser tratados: 1) o princípio do livre acesso,[107] 2) o princípio da qualidade dos dados[108] e 3) o princípio da transparência.[109]

---

[104] "II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (art 6º, LGPD).
[105] "III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados." (art 6º, III, LGPD).
[106] O APP *Pokemon Go* está na lista dos 10 aplicativos que mais faturaram no Apple Store e Google Play no Brasil em 2018. Disponível em: https://www.tecmundo.com.br/software/140320-netflix-garena-free-fire-apps-faturaram-brasil-2018.htm. Acesso em: 20 out. 2019.
[107] "IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais." (art 6º, IV, LGPD).
[108] "V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento." (art 6º, V. LGPD).
[109] "VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial." (art 6º, VI, LGPD).

O tratamento de dados não pode ser feito de forma a facilitar qualquer tipo de discriminação, ilicitude ou abusividade, é o que indica o princípio da não discriminação.[110] A forma como os dados são tratados devem respeitar os valores que norteiam o respeito aos direitos humanos e a dignidade da pessoa humana. Não é razoável e nem aceitável que o tratamento seja uma forma de favorecer práticas não aceitáveis pelo normativo brasileiro.

E, por fim, o bloco de princípios relacionados com os deveres de segurança e prestação de contas por parte dos agentes de tratamento: 1) o princípio da segurança;[111] 2) o princípio da prevenção[112] e 3) o princípio da responsabilização e prestação de contas.[113] São princípios que indicam que o agente de tratamento tem responsabilidade sobre a segurança dos dados e deve zelar pelos dados administrados. Caso ocorra um vazamento de dados e seja identificado que os agentes de tratamento tinham condições técnicas para proteger os dados eles serão responsabilizados.

Vazamentos de informações se tornaram comuns em uma sociedade moderna que cria diariamente uma quantidade imensa de dados que alimentam bancos de dados públicos e privados. Recentemente foi noticiado um caso de vazamento de um banco de dados administrado pela Secretaria de Cultura e Economia Criativa do Estado de São Paulo.[114] O caso é considerado grave, pois expôs a documentação dos candidatos, como fotocópias de CPF, carteira de identidade, comprovante de endereço e telefone. A LGPD tem como objetivo reforçar que os agentes de tratamento criem medidas de segurança de seus dados capazes de evitar ou minimizar situações similares.

Ainda sobre a segurança e a eventual responsabilização dos agentes de tratamento, o art. 45[115] da LGPD estabelece uma relação direta com o Código de Defesa do Consumidor e o

---

[110] "IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos." (art 6º, IX, LGPD).
[111] "VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão." (art 6º, LGPD).
[112] "VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais." (art 6º, LGPD).
[113] "X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." (art 6º, LGPD).
[114] Disponível em: https://congressoemfoco.uol.com.br/midia/ex-secretario-da-cultura-de-sp-nega-responsabilidade-por-vazamento-de-dados-pessoais/. Acesso em: 05 nov. 2019.
[115] "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente."

Código Civil e indica que as regras de responsabilização civil não são afastadas, cabendo ao lesado se valer delas para a manutenção do seu direito. Trata-se de um artigo mais genérico que reforça a possiblidade de responsabilização dos agentes. O art. 44,[116] por outro lado, é mais específico, e faz referência a irregularidade propriamente do tratamento de dados, ou seja, pelos princípios da prevenção e da segurança o tratamento deve ocorrer de um modo adequado, com um resultado e um risco esperado, com técnicas atuais de tratamento e com a devida prestação de contas dos procedimentos adotados.

3.3. Direito de confirmação da existência de tratamento

O primeiro direito apresentado no art. 18 que trata especificamente sobre os direitos dos titulares diante do tratamento dos controladores é o direito a confirmação da existência do tratamento. O titular dos dados tem o direito de questionar se há um tratamento sendo realizado.

Conforme ilustra o portal sobre a proteção de dados da empresa pública Serpro,[117] a confirmação é um dos direitos básicos do titular dos dados. A empresa Serasa Experia[118] reforça a necessidade de adequação das empresas quanto à possibilidade de novos serviços de informação de dados solicitados pelos titulares. Segundo o Gerente de Gestão de dados do Serasa, Lucas Oliveira, é importante que essas empresas se adaptem a essas demandas:

> "É preciso considerar que os titulares poderão solicitar desde a confirmação da existência de tratamento dos dados até a sua revogação. O leque de opções é bastante amplo e, por isso, deve-se construir todas as jornadas de atendimento claras para garantir por onde essas solicitações vão ser recebidas, quais áreas serão responsáveis e como será feita a resposta ao titular."[119]

3.4. Direito de acesso aos dados

---

[116] "Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado."

[117] Disponível em: https://www.serpro.gov.br/lgpd/cidadao/quais-sao-os-seus-direitos-lgpd. Acesso em: 15 nov. 2019.

[118] Disponível em: https://www.serasaexperian.com.br/conteudo_lgpd/jornada-de-adequacao-como-se-preparar-para-a-lgpd. Acesso em: 17 out. 2019.

[119] OLIVEIRA, Lucas. Op. Cit. pág. 01.

O direito de acesso aos dados é entendido como a possibilidade que os titulares de dados têm de acessar seus dados pessoais em posse dos agentes de tratamento. Os responsáveis pelo tratamento devem gerir uma forma simples, rápida e sem custos adicionais para que o titular tenha livre acesso aos seus dados armazenados.

Se considerarmos a maioria das redes sociais presentes na internet, há geralmente a possibilidade de acessar as informações básicas inseridas pelo usuário em seu cadastro, além disso, é possível ter aceso também aos dados inseridos ou compartilhados pelo usuário em seu perfil na rede e também a um controle das informações prestadas por terceiros que se vinculam ao titular dos dados. O direito ao acesso é uma manifestação mais ampla da possibilidade que os usuários têm de saber exatamente quais dados estão em tratamento e solicitar que esses dados sejam disponibilizados pelos agentes.

Há um prazo estabelecido pela Lei para a informação sobre o tratamento e a disponibilização do acesso, segundo o art. 19,[120] em formato simplificado, o acesso ou a informação sobre o tratamento devem ser disponibilizados imediatamente,[121] caso seja uma informação mais completa o prazo estabelecido é de 15 dias.

3.5. Direito de correção de dados inexatos

A Lei estabelece mais um direito que é derivado dos inúmeros princípios que regem o normativo. Além da possibilidade de informação sobre o tratamento e acesso dos dados há um inciso específico sobre a correção dos dados incompletos, inexatos ou desatualizados. Trata-se de um direito que o titular possui de ajustar suas informações no banco de dados dos responsáveis pelo tratamento.

Esses direitos enumerados até agora são uma decorrência lógica da relação transparente que deve existir entre os titulares e os responsáveis pelos dados. O art. 18 apenas enumera essas ações para tornar mais claro o exercício efetivo dos direitos dos titulares.

---

[120] "Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular."

[121] Segundo o §4º, do art.19 da LGPD, é possível que a Autoridade Nacional estabeleça novos prazos.

Os três primeiros direitos apresentados podem ser equiparados, de certo modo, ao remédio constitucional habeas data, presente no art. 5º, LXXII da CRFB/88.[122] Nesse remédio busca-se assegurar o direito ao acesso ou à retificação a banco de dados de entidades governamentais ou de caráter público. A Lei dialoga com a Constituição, nesse sentido, e, por via administrativa, por meio de petição à autoridade nacional[123] ou organismos de defesa do consumidor[124] garante o direito de acesso à informação e às devidas correções.

3.6. Direito de anonimização, bloqueio ou eliminação de dados

A anonimização, o bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei é o direito que o titular de dados tem de requisitar de tornar seus dados pessoais inacessíveis ao tratamento de dados. Ele está presente no inciso IV,[125] do art. 18, esse termo, anonimização, já conceituada pela Lei, se refere a um procedimento que afasta a identidade do titular de dados. Desse modo, os dados pessoais ficam diluídos no banco de dados servindo para um tratamento não pessoal. Vale ressaltar, como já visto em um caso com um banco de dados da *Netflix*, que é possível, em situações específicas, a identificação de dados anonimizados, ou seja, dependendo do método utilizado a anonimização pode não ser totalmente eficaz.

Além da anonimização, é possível o bloqueio ou eliminação de dados que não são considerados mais necessários para o tratamento. Por exemplo, em uma situação em que a empresa realizou uma determinada campanha de preenchimento de informações para um sorteio, findo a realização do evento, os dados obtidos exclusivamente para esse fim poderiam ser eliminados.

---

[122] "LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo."

[123] "§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional." (art. 18, §1º, LGPD).

[124] "§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor." (art. 18, §8º, LGPD).

[125] "IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei." (art. 18, IV, LGPD).

O inciso VI do art. 18,[126] trata de um caso específico de eliminação de dados relacionado ao consentimento do titular. O titular de dados que consentiu com o tratamento pode simplesmente revogar o consentimento, art. 18, IX, ou solicitar a eliminação desses dados. O titular deve possuir o controle sobre os dados pessoais coletados e escolher qual a melhor alternativa para a proteção de seus dados.

3.7. Direito de portabilidade dos dados

A portabilidade de dados, assim como ocorre no Regulamento europeu, é também um direito viabilizado pela LGDP. O inciso V do art. 18,[127] é claro ao determinar que, exceto com relação a segredos comerciais e industriais é direito do titular de dados transferir seus dados para um outro fornecedor de serviços ou produtos.

Esse direito corrobora com a necessidade de uma padronização por parte dos agentes de dados no tratamento das informações. A concorrência entre as empresas responsáveis por esse tratamento será também influenciada pela forma como esses dados são tratados. A portabilidade de dados, além de gerar a proteção ao dado em si, também gera uma oportunidade para o cliente escolher, de fato, a melhor empresa fornecedora de produtos ou serviços.

Por exemplo, se considerarmos um serviço de venda de livros digitais, como ocorre com o portal da *Amazon*[128] que vende livros diretamente para o leitor de livros digitais, o *kindle*, seria possível, segundo a Lei, transferir informações referentes a compras para um portal concorrente. Esse direito de portabilidade impede que o cliente fique "preso"[129]a um serviço que detém informações que dificilmente seriam obtidas fora desse serviço. No caso dos livros, essas informações seriam relevantes para a construção do perfil do usuário e a indicação de leituras próprias, considerando que o leitor esteja interessado em ler principalmente os livros indicados pelo algoritmo do programa.

---

[126] "VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei." (art. 18, VI, LGPD).
[127] "V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial."
[128] Disponível em: https://www.amazon.com.br/Livros/b?ie=UTF8&node=6740748011. Acesso em: 17 set. 2019
[129] Termo em inglês para essa situação é Vendor *lock-in*.

Evitar o abuso de poder gerado pelas grandes companhias que detém uma quantidade significativa de dados também deve ser uma preocupação da Lei:

> "Orla Lynksey também destacou que, em um cenário de grandes companhias coletando e gerindo grandes quantidades de dados, um dos impactos fundamentais do controle dessas informações é na concorrência nesses mercados. O abuso de poder de mercado pela administração de quantidades excessivas de dados deve ser considerado na análise de fusões, recomendou a professoara, que citou como exemplo a compra do WhatsApp pelo Facebook em 2014. Na Europa, as autoridades concorrenciais entenderam que não haveria problema pelo fato de as redes sociais supostamente não concorrerem entre si."[130]

3.8. Direito de informação sobre o compartilhamento dos dados

As informações referentes ao compartilhamento dos dados realizado por um controlar devem ser informadas para o titular de dados. É mais um direito apresentado pela Lei, no inciso VII do art. 18,[131] que pretende traçar um rastro das informações não permitindo que os dados fiquem sem um histórico devido.

Essas informações protegem o titular e trazem mais segurança para a coleta de dados e os futuros tratamentos que podem ser realizados. Trata-se de um controle da trajetória que o dado seguiu, desde sua origem até o tratamento atual. A partir da compreensão da Lei, caso isso já não seja realizado, os responsáveis de dados terão a responsabilidade de indicar a origem e de manter atualizadas as informações sobre os compartilhamentos realizados.

Podemos imaginar uma situação em que um titular de dados é abordado na rua para uma pesquisa de satisfação sobre determinado serviço, é provável e natural que esse dado seja direcionado para a empresa que presta o serviço e que ele seja tratado para indicar quais aspectos do negócio podem ser reforçados ou modificados. É possível também que haja alguma outra empresa que preste um serviço complementar que tenha interesse nessas informações e deseja realizar um outro tratamento de dados. Se o titular não tiver o histórico do compartilhamento que ocorre entre as empresas, será muito difícil compreender de que

---

[130] PORTABILIDADE dos dados pessoais é um direito do cidadão. **Convergência Digital**. 18/09/2019. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=51755&sid=4. Acesso em: 10 nov. 2019.

[131] "VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados."

forma os dados pessoais fornecidos na pesquisa estão atualmente disponíveis em um outro banco de dados e sendo tratados por uma outra empresa.

3.9. Direito de informação do consentimento e de sua revogação

A definição de consentimento é apresentada pela Lei como a manifestação livre, informada e inequívoca para uma finalidade específica. O art. 7º, I,[132] nos informa que o tratamento de dados somente pode ocorrer mediante consentimento do titular, esse consentimento segundo o art. 8º, *caput* ,[133] deve ser por escrito ou por meio que demonstre a manifestação de vontade do titular. O ônus da prova do consentimento é do controlador de dados[134] e é, como já visto, para uma finalidade específica sendo nulas as autorizações genéricas.[135] Se o consentimento for obtido por meio escrito, a cláusula que o justifica deve estar em destaque,[136] caso haja vício do consentimento o tratamento de dados é vedado.[137]

É possível perceber que a lei, antes mesmo de adentrar propriamente no capítulo referente aos direitos dos titulares faz inúmeras referências ao consentimento como um elemento fundamental para a realização o tratamento de dados. É um direito do titular exigir que seus dados pessoais só sejam tratados com sua autorização e para a efetivação desse direito a LGPD estabeleceu que a informação do consentimento não pode estar escondida ou disfarçada. O titular de dados precisa ter a plena consciência de que cabe a ele, num primeiro momento, decidir sobre o tratamento ou não dos dados e as consequências do aceite ou da recusa.

Muitos aplicativos e sites exigem o acesso a áreas restritas, por exemplo, do celular, como agenda, GPS ou SMS. Caso o usuário se negue a permitir o acesso, o aplicativo não funciona e não permite que o usuário conclua a instalação do software. Essas exigências do

---

[132] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular."
[133] "Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular."
[134] § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. (art. 8º, §2º, LGPD)
[135] § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (art. 8º, §4º, LGPD)
[136] § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. (art. 8º, §1º, LGPD)
[137] § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento. (art. 8º, §3º, LGPD)

aplicativo precisam ser claras e justificadas, não basta exigir o consentimento sem explicar para o titular dos dados qual é exatamente a necessidade e a aplicabilidade dessa função.

> "Quando tratar dados pessoais for condição para fornecimento de produto ou serviço ou para exercício de um direito, você deve ser avisado sobre isso e sobre os meios pelos quais pode exercer seus direitos como titular. E se as informações fornecidas tiverem conteúdo enganoso ou abusivo, ou não forem apresentadas previamente com transparência e clareza, o consentimento será considerado nulo.[138]

É evidente que se o consentimento possui uma finalidade específica e ocorre uma mudança de finalidade, o tratamento se torna inválido para aquele consentimento inicial, conforme indica o art. 9º, § 2º[139] da Lei. A clareza e a transparência são os princípios que regem o livre consentimento, sendo também inválido o consentimento que ocorre com conteúdo enganoso ou abusivo.[140]

A Lei também trata do consentimento, art. 11, II, [141] necessário ao tratamento de dados sensíveis. Nesse caso, o consentimento parece ainda mais importante, visto que, os dados sensíveis têm um maior potencial de lesão ao direito dos titulares. Um tratamento diferenciado apresentado pelo normativo é a situação de crianças e adolescentes que devem ter o consentimento de pelo menos um dos pais ou do responsável legal[142].

Com relação propriamente ao capítulo III, o consentimento surge inicialmente no inciso VI, que se refere à eliminação de dados pessoais tratados com consentimento e, sem seguida, nos dois incisos referentes à informação de consentimento, inciso VIII[143] e a revogação do consentimento, inciso IX.[144]

---

[138] Disponível em: https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei. Acesso em: 15 nov. 2019.
[139] "§2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações."
[140] "§1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca."
[141] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: II - sem fornecimento de consentimento do titular (...)."
[142] "§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal." (art. 14, §1º, LGPD).
[143] "VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa." (art. 18, VIII, LGPD).
[144] "IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei." (art. 18, IX, LGPD).

O titular de dados tem o direito de revogar o consentimento a qualquer tempo, de acordo com o art. 8º, §5º da LGPD. Essa revogação deve ser por manifestação expressa do titular em um procedimento gratuito e facilitado.

3.10. Quadros comparativos entre a LGPD e a GDPR

QUADRO COMPARATIVO DOS DIREITOS ESPECÍFICOS DOS TITULARES PRESENTES NA LGPD E GDPR (PRESENTES NO CAPÍTULO III)		
Direitos dos titulares de dados	**GDPR**	**LGPD**
Direito à informação dos dados pessoais	Os agentes de tratamento, segundo o Regulamento, não podem negar aos titulares determinadas informações sob risco de serem responsabilizados sobre as omissões (arts. 13 e 14)	É o direito a confirmação da existência do tratamento. (art. 18, I)
Direito de Acesso	O direito de acesso que o titular de dados possui. (art. 15)	O direito de acesso aos dados é entendido como a possibilidade que os titulares de dados têm de acessar seus dados pessoais em posse dos agentes de tratamento. (art. 18, II)
Direito de retificação dos dados	O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. (art. 16)	Trata-se de um direito que o titular possui de ajustar suas informações no banco de dados dos responsáveis pelo tratamento. (art. 18, III)

Direito de anonimização (limitação de tratamento)	O titular de dados pode solicitar a limitação do tratamento em situações específicas: a) a inexatidão dos dados pessoais; b)o tratamento ilícito; c) os responsáveis não precisarem mais dos dados pessoais e d)oposição aos motivos do tratamento. (art. 18)	Trata-se de um direito de anonimizar, bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade com a Lei (art. 18, IV)
Direito à portabilidade de dados	Trata-se da possibilidade de solicitar ao responsável pelo tratamento de dados os seus dados em um formato estruturado podendo transferir esses dados para um outro responsável. (art. 18)	É direito do titular de dados transferir seus dados para um outro fornecedor de serviços ou produtos. (art. 18, V)
Direito à eliminação dos dados pessoais (direito ao esquecimento	Trata-se do direito de obter do responsável pelo tratamento a exclusão de seus dados (art.17)	Trata-se do direito do titular de dados de solicitar a eliminação desses dados (art. 18, VI)
Direito de revogação do consentimento	Direito de retirar o consentimento em que se baseia o tratamento dos dados (art. 17)	O titular de dados tem o direito de revogar o consentimento a qualquer momento (art. 18, IX c/c art. 8º §5º)
Direito de oposição	Trata-se do direito de se opor ao tratamento de dados para efeito de comercialização, ou por motivos relacionados à licitude do tratamento (art. 21)	O titular de dados pode opor-se ao tratamento com fundamento em uma das hipóteses de dispensa de consentimento (art. Art. 18, §2)

QUADRO COMPARATIVO DOS DIREITOS GERAIS DOS TITULARES PRESENTES NA LGPD E GDPR		
Direitos Gerais dos Titulares de Dados	**GDPR**	**LGPD**
Direito fundamental à liberdade (liberdades fundamentais)	Art. 1º, 2, "O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais."	Art. 1º "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade"
Direitos Humanos e liberdades fundamentais	Art. 45, 2. a), "O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais"	Art. 2º, VII "VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."
Direito ao não tratamento de dados de forma discriminatório (dados sensíveis)	Art. 9º, I, "É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma	Art. 5º, II, "dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;" Obs: No caso da LGPD há

	pessoa” Considerando 71: “direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos”	uma restrição para o tratamento de dados sensíveis.
Direito à privacidade	Considerando 4, “presente regulamento respeita todos os direitos fundamentais e observa as liberdade e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar”	Art. 2º “A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade;”
Direito à liberdade de expressão e informação	Considerando 4, “presente regulamento respeita todos os direitos fundamentais e observa (...) a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação	Art. 2º “III - a liberdade de expressão, de informação, de comunicação e de opinião;”
Direito de ação, de petição ao tribunal e/ou órgão de controle	Considerando 4, “o direito à ação e a um tribunal imparcial,	Art 41, § 2º “As atividades do encarregado consistem em:

	Considerando 141, “Os titulares dos dados deverão ter direito a apresentar reclamação a uma única autoridade de controlo única, particularmente no Estado-Membro da sua residência habitual, e direito a uma ação judicial efetiva,”	I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; Art. 50, caput, “Os controladores e operadores, no âmbito de suas competências, (...) os procedimentos, incluindo reclamações e petições de titulares,” Art. 55-J, V, “Compete à ANPD: apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;”

CONCLUSÃO

A Lei brasileira foi fortemente influenciada pelo Regulamento europeu e provavelmente os operadores do direito no Brasil se valerão das inúmeras orientações propostas pelas autoridades nacionais europeias. Nesse sentido é importante o diálogo entre os normativos e a compreensão da aplicação do Regulamento por parte desses entes de fiscalização. O Regulamento, por si só, também já possui a aplicabilidade extraterritorial e pode ser perfeitamente aplicado no território brasileiro em função de negócios realizados entre empresas brasileiras e titulares de dados protegidos pelo regulamento.

As empresas brasileiras ou estrangeiras que já estão de acordo com o Regulamento europeu devem ficar atentas a possíveis determinações específicas da Autoridade Nacional que será responsável pela fiscalização do tratamento de dados no Brasil. De forma geral, a Lei brasileira dialoga muito bem com o Regulamento e impõe princípios gerais que podem ser equiparados, todavia, a realidade brasileira pode exigir ajustes específicos.

Sobre a diferenciação entre os normativos, as empresas já adaptadas ao Regulamento devem se atentar ao § 2º do artigo 12 da LGPD, que traz uma possibilidade de aplicação da Lei para dados em uma situação específica de criação de perfil comportamental do titular de dados. A Autoridade Nacional deverá esclarecer melhor que tipo de dados serão considerados nessa situação.

Os direitos dos titulares de dados, tanto na GDPR quanto na LGPD, não estão limitados aos capítulos específicos que tratam do tema. Há diversos princípios gerais presentes nos normativos que se constituem como direitos, além de outras referências sobre a forma como deve ser o tratamento de dados e as limitações impostas aos operadores de dados.

Alguns direitos precisam ainda de uma regulamentação da Autoridade Nacional, como é o caso de prazos e requerimentos. Nesse sentindo, o titular de dados e os responsáveis pelos dados deverão seguir a orientação da agência reguladora para o efetivo cumprimento dos preceitos legais.

Há muitas similaridades presentes entre os normativos, os quadros comparativos ilustram algumas delas e reforçam a inspiração da Lei brasileira em valorizar os direitos fundamentais frente aos interesses econômicos ligados ao tratamento de dados. Se comparada com o GDPR, a Lei brasileira é formalmente mais sintética, apresenta menos artigos e menos capítulos, explorando de forma mais geral os aspectos da proteção de dados. Apesar disso, a Lei consegue apresentar os fundamentos que norteiam sua efetiva aplicação. Há ainda alguns termos que precisam de maior esclarecimento por parte da Autoridade Nacional como é o caso da possibilidade de reversão da anonimização de dados prevista no caput do art. 12 da LGDP. No mesmo artigo há ainda a expressão "com esforços razoáveis" que sem um maior esclarecimento da Autoridade Nacional se torna ampla e imprecisa.

A existência de normativos gerais de proteção de dados não transforma a sociedade de forma automática, os direitos dos titulares de dados presentes nos normativos só poderão ser, de fato, concretizados com o comprometimento dos titulares, das empresas e dos órgãos de controle.

Grandes empresas que tratam dados pessoais já foram punidas com fundamento no Regulamento Europeu, como é o caso do *Google*, do *Facebook*, da *British Airways*, da rede de *Hoteis Marriott*, dentre outras. É possível que a Lei brasileira exija que as práticas adotadas por essas multinacionais sejam adaptadas para a realidade da LGPD e que mantenham nível de segurança de dados igual ou superior ao normativo europeu.

Apesar de entender que em muitos aspectos esses normativos gerais possuem um viés protetivo do titular de dados, as empresas têm um papel importante na dinâmica da Lei. Cabe às empresas demonstrar a viabilidade do efetivo atendimento a esses direitos. Não é (e não pode ser) um desejo do legislador brasileiro, a inviabilidade de negócios que necessitam dos dados pessoais. A empresa precisa fortalecer sua estrutura tecnológica, seu corpo jurídico e seu relacionamento com os clientes, mas, ao mesmo tempo, gerar justificativas válidas para o possível não atendimento de determinadas demandas.

Os desafios gerados pela LGPD são inúmeros, as empresas brasileiras, a sociedade e, sobretudo, os titulares de dados pessoais devem, cada vez mais, compreender os riscos

gerados pela falta de uma regulamentação forte na área de proteção de dados e aplicar os direitos presentes no normativo.

REFERÊNCIAS

ARTIGO 12: Direito à privacidade. **Nações Unidas**. 28/11/2018. Disponível em: https://nacoesunidas.org/artigo-12-direito-a-privacidade/. Acesso em 29 jul. 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. *E-book*.

BLACK MIRROR. **Manda Quem Pode (Shut Up and Dance)**. Dirigido por James Watkins. Escrito por Carlie Brooker & William Bridges. 3º episódio da 3ª temporada. Londres: Netflix, 2016.

_____. **Queda Livre (Nosedive)**. Dirigido por Joe Wright. Escrito por Carlie Brooker, Rashida Jones & Mike Schur. 1º episódio da 3ª temporada. Londres: Netflix, 2016.

BLUM, Renato Opice & MALDONADO, Viviane Nóbrega (Coordenação). Comentários ao GDPR: **Regulamento Geral de Proteção de Dados da União Europeia**. São Paulo: Thomson Reuters Brasil, 2018.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 nov. 2019.

_____. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor – CDC. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 30 jul. 2019.

_____. **Lei 10.406 de 10 de janeiro de 2002** que institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 10 jul. 2019.

_____. **Lei 12.527 de 18 de novembro de 2011** que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 2016 da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 12 jul. 2019.

_____. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 30 jul. 2019.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (Marco civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htmhtm. Acesso em: 30 out. 2019.

_____. **Lei nº 13.709, de 14 de agosto de 2018** – Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 24 jul. 2019.

_____. **Lei nº 13.853, de 8 de julho de 2019,** que dispõe sobre a proteção de dados pessoais e altera a Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 24 jul. 2019.

_____. Superior Tribunal de Justiça. **Recurso Ordinário em Mandado de Segurança: RMS 55109 PR**. Quebra de sigilo telemático. Cumprimento incompleto de ordem judicial. Aplicação de multa diária à empresa responsável pelo fornecimento de dados (Facebook). T5 – Quinta turma, julgado em 7/11/2017. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/522273587/recurso-ordinario-em-mandado-de-seguranca-rms-55109-pr-2017-0215256-6?ref=serp. Acesso em: 31 jul. 2019.

_____. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 4815 DF**. Relatora Ministra Cármen Lúcia. 10/06/2015. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=293336. Acesso em: 04 ago. 2019.

_____. Supremo Tribunal Federal. **Repercussão Geral no Recurso Extraordinário 1.037.396 SP**. Proteção aos Direitos da personalidade. Liberdade de expressão e de manifestação. Plenário, julgado em 01/03/2018. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=14588363. Acesso em: 01 ago. 2019.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à privacidade hoje**: perspectiva histórica e o cenário brasileiro. Agosto de 2017. Sequência (Florianópolis), u. 76, p. 213-240. Ago.2017. Disponível em: http://www.scielo.br/pdf/seq/n76/2177-7055-seq-76-00213.pdf Acesso em: 04 ago. 2019.

CAPELAS, Bruno. Facebook cresce em receita e usuários, mas teme multa de até US$ 5bi. Link. **Estadao.com**. 24/04/2019. Disponível em: https://link.estadao.com.br/noticias/empresas,facebook-cresce-em-receita-e-usuarios-mas-teme-multa-de-ate-us-5-bi,7000280295. Acesso em: 30 jul. 2019.

CASTRO, Saulo. Quais as diferenças entre API e SDK. **Medium.com**, 4 set. 2018. Disponível em: https://medium.com/@saulocastrolp/quais-s%C3%A3o-as-diferen%C3%A7as-entre-api-e-sdk-d050e60d46e. Acesso em: 28 jul. 2019.

CNIL – Comission Nationale Informatique & Libertés. **Délibération de la formation restreinte nº SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société**. GOOGLE LLC. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001_21-01-2019.pdf. Acesso em: 25 out. 2019.

DATAFOLHA: quantos eleitores de cada candidato usam redes sociais, leem e compartilham notícias sobre política. **G1.com**. [on-line]. 03/10/2018. Disponível em: https://g1.globo.com/politica/eleicoes/2018/eleicao-em-numeros/noticia/2018/10/03/datafolha-quantos-eleitores-de-cada-candidato-usam-redes-sociais-leem-e-compartilham-noticias-sobre-politica.ghtml/. Acesso em: 10 out. 2019.

DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, **relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 25 out. 2019.

EDITOR de Fotos – **Montagem de Fotos e Colagem**. (aplicativo disponível no Google play). Inshot Inc. Política de Privacidade – Privacy Policy. Acesso em: 27 out. 2019.

ELDER, Jeff. As multas do GDPR se espalham pela Europa. **Avast Blog (online)**. 20/08/2019. Disponível em: https://blog.avast.com/pt-br/gdpr-fines. Acesso em: 26 out. 2019.

EXAME online. 62% da População Brasileira está Ativa nas Redes Sociais. **Exame online**. [on-line]. 19/10/2018. Disponível em: https://exame.abril.com.br/negocios/dino/62-da-populacao-brasileira-esta-ativa-nas-redes-sociais//. Acesso em: 14 out. 2019.

FACEBOOK obtém receita de US$ 15 bilhões no 1º trimestre de 2019. **canaltech.com**. [on-line]. 24/04/2019. Disponível em: https://canaltech.com.br/resultados-financeiros/facebook-obtem-receita-de-us-15-bilhoes-no-1o-trimestre-de-2019-137867/. Acesso em: 28 jul. 2019.

_____. pagará multa recorde de US$ 5 bilhões por violação de privacidade. **G1**.Globo.com. [on-line]. 24/07/2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/facebook-pagara-multa-de-us-5-bilhoes-por-violacao-de-privacidade.ghtml. Acesso em: 28 jul. 2019.

_____. Política de Dados. **Facebook, Instagram, Messenger e outros**. 2019. Disponível em: https://pt-br.facebook.com/privacy/explanation. Acesso em: 30 jul. 2019.

GAETAN, R. GDPR: quelles sont les implications du règlement européen pour les entreprises? 01/10/2019. **Le Big Data**.fr. Diponible: https://www.lebigdata.fr/gdpr-reglement-europeen. Accés en: 24 out. 2019.

GENERAL. **Data protection Regulation shows results, but work needs to continue**. Comission Europeenne – base de données des communiqués de presse. Brussels, 24 July 2019. Disponível em: <https://europa.eu/rapid/press-release_IP-19-4449_en.htm?locale=FR>. Acesso em: 20 out. 2019.

GDPR, **General Protection Privaty Regulation**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 20 out. 2019.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**. Vol. 1: parte geral. 12ª Ed. São Paulo: Saraiva, 2014.

GOOGLE, Amazon e Apple batem recorde em seus balanços. **Época Negócios**. 02/02/2018. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2018/02/google-amazon-e-apple-batem-recorde-em-seus-balancos.html. Acesso em: 26 out. 2019.

_____. Privacidade & termos. **Como o Google retém os dados que coletamos**. Disponível em: https://policies.google.com/technologies/retention?hl=pt-BR. Atualizada em 15/10/2019. Acesso em: 27 out. 2019.

GRUPO de Trabalho do Artigo 29º - (Article 29 Working Party; Guidelines on consent under Regulation 2016/679). **Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/679**. Disponível em português em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Acesso em: 27 out. 2019.

HOSTERT, Ana Cláudia. Proteção de dados pessoais na internet: **A necessidade de Lei Específica no ordenamento jurídico brasileiro**. 2018. Monografia (Bacharel em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2018. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/188181/TCC%20-%20ANA%20CL%C3%81UDIA%20HOSTERT%20%282%29.pdf?sequence=1&isAllowed=y. Acesso em: 30 jul. 2019.

INTERNET das coisas, integração de serviços e interação social: o que esperar da Web 4.0. **Rockcontent.com**. 09/01/2018. Disponível em: https://rockcontent.com/blog/web-4-0/. Acesso em 30 jul. 2018.

LEAL, Livia Teixeira. Internet e morte do usuário: a necessária superação do paradigma da herança digital. **Revista Brasileira de Direito Civil**, v. 16, p. 181-197, 2018. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/237. Acesso em: 12 jul. 2018.

LEORATTI, Alexandre. Com GDPR, número de notificações de vazamento de dados ultrapassa 41 mil casos. **Jota.info online**. 06/02/2019. Disponível em: https://www.jota.info/pesquisa-empirica/gdpr-vazamento-de-dados-41-mil-casos-06022019. Acesso em: 20 out. 2019.

LOTH, Adriana Falcão et al. As tendências e desafios da Web 3.0 à luz da gestão do conhecimento. **RISUS - Journal on Innovation and Sustainability**, São Paulo, v.10 n.1, p37-47, Mar/Maio, 2019. Disponível em: https://revistas.pucsp.br/risus/article/download/41810/27983. Acesso em: 10 out. 2019.

LUA, Alfred. 21 Top Social Media Sites to Consider for your Brand. **Buffer Marketing Library**. 24/01/2019. Disponível em: https://buffer.com/library/social-media-sites. Acesso em: 31 jul. 2019.

MONTEIRO, Renato Leite. Qual o impacto direto do GDPR em empresas brasileiras? **Cio.com.br**. 25/05/2018. Disponível em: https://cio.com.br/qual-e-o-impacto-direto-do-gdpr-em-empresas-brasileiras/. Acesso em 02 nov. 2019.

NUNES, Simone Lahorgue & TURANO, Allan Nascimento. Nova lei de proteção de dados pessoais e atividade jornalística. **Levy & Salomão Advogados**. 15/08/2018. Disponível em: http://www.levysalomao.com.br/Publicacoes.aspx?a=boletim&p=nova-lei-de-protecao-de-dados-pessoais-e-atividade-jornalistica&idioma=pt-br. Acesso em: 02 nov. 2019.

OLIVEIRA, Lucas. Jornada de adequação: Como se preparar para a LGPD. Serasa Experian. Disponível em: https://www.serasaexperian.com.br/conteudo_lgpd/jornada-de-adequacao-como-se-preparar-para-a-lgpd. Acesso em: 20 set. 2019.

OLIVEIRA, Jaqueline Simas. Google é multado em 50 milhões de euros na França por violação ao GDPR. **Jota.info**. 2401/2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/google-e-multado-em-50-milhoes-de-euros-na-franca-por-violacao-ao-gdpr-24012019. Acesso em: 26 out. 2019.

PACETE. Luiz Gustavo. Multa aplicada ao Google é emblemática para a GDPR. 22/01/2019. **Meio e Mensagem (online)**. Disponível em:

https://www.meioemensagem.com.br/home/midia/2019/01/22/multa-aplicada-ao-google-e-divisor-de-aguas-para-a-gdpr.html. Acesso em: 25 out. 2019.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**: introdução ao direito civil: teoria geral de direito civil. / Atual. Maria Celina Bodin de Maoraes. (versão digital). 30. ed. rev. atual. Rio de Janeiro: Forense, 2017. v. 1.

PNAD contínua. **Pesquisa Nacional por Amostra de Domicílios Contínua 2017**. TIC – Tecnologia da Informação e Comunicação. Informativo sobre o Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2017. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 30 jul 2019.

_____. Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país. **Agência IBGE de notícias**. 18/12/2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais. Acesso em: 28 jul. 2019.

PORTABILIDADE dos dados pessoais é um direito do cidadão. **Convergência Digital**. 18/09/2019. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=51755&sid=4. Acesso em: 10 nov. 2019.

QUEROL, Ricardo de. Zygmunt Bauman: "As redes sociais são uma armadilha". **El País**, 8 jan. 2016. Disponível em: https://brasil.elpais.com/brasil/2015/12/30/cultura/1451504427_675885.html. Acesso em: 12 jul. 2019.

ROHR, Altieres. Como a 'Web 3.0' criou um caos na privacidade. **G1**. Globo.com. 01/05/2018. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-web-30-criou-um-caos-na-privacidade.html. Acesso em: 31 jul. 2019.

ROSA, Natalie. Cambridge Analytica – Os principais momentos do depoimento de Mark Zuckerberg. **Canaltech.com (online)**. 11/04/2018. Disponível em: https://canaltech.com.br/redes-sociais/cambridge-analytica-os-principais-momentos-do-depoimento-de-mark-zuckerberg-111626/. Acesso em: 20 out. 2019.

SERRA, Nathália Conde. **Proteção de dados pessoais e Facebook**: Análise sobre privacidade de dados na Internet. 2018. Monografia (Bacharel em Direito) – Universidade de Brasília, Brasília, 2018. Disponível em: http://bdm.unb.br/bitstream/10483/22020/1/2018_NathaliaCondeSerra_tcc.pdf. Acesso em: 28 jul. 2019.

SILVA, Silvado Pereira da. Políticas de acesso à Internet no Brasil: indicadores, características e obstáculos. **Cadernos Adenauer XVI (2015) nº 3**. Disponível em: http://ctpol.unb.br/wp-content/uploads/2019/04/2015_SILVA_Acesso-Internet.pdf. Acesso em: 30 out. 2019.

SILVERMAN, Craig. Facebook removed over 2 billion fake accounts, but the problem is getting worse. 24/05/2019. **Bruzzfeed.news**. Diponível em: https://www.buzzfeednews.com/article/craigsilverman/facebook-fake-accounts-afd. Acesso em: 02 ago. 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** (coord. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, 2008.

TRATADO da União Europeia. **Jornal Oficial das Comunidades Europeias**. 29/07/1992. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:11992M/TXT. Acesso em: 20 out. 2019.

UCHINAKA, Fabiana. No Limite. Facebook abre as portas da moderação de conteúdo para mostrar quem decide o que é certo ou errado na rede. 07/06/2019. **Tecnologia.uol.com.br**. Disponível em: https://tecnologia.uol.com.br/reportagens-especiais/como-e-o-centro-de-moderacao-de-conteudo-do-facebook/. Acesso em: 07 ago. 2019.

UNIVERSAL declaration of human rights. 1948. Portuguese. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 29 jul. 2019.

VIEIRA, Sergio. Acordo Mercosul-EU deve baratear produtos, mas forçar eficiência e produtividade. **Agência Senado**. 10/09/2019. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2019/08/acordo-mercosul-ue-deve-baratear-produtos-mas-forcar-eficiencia-e-produtividade. Acesso em: 02 nov. 2019.

WARREN, Samuel D,; BRANDEIS, Louis, D. The right to privacy. **Harvard Law Review**. V. IV, n.5, December, 1890. Disponível em: https://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 04 ago. 2019.