A RESPONSABILIDADE DO COMPLIANCE OFFICER NA PROTEÇÃO DE DADOS PESSOAIS

Liability of the compliance officer in the protection of personal data

Revista de Direito e as Novas Tecnologias | vol. 3/2019 | Abr - Jun / 2019
DTR\2019\35399

Fabiani Oliveira Borges da Silva
Especialista em Direito Processual Civil pela UNIFACS. MBA em Direito Eletrônico pela Escola Paulista de Direito EPD. Aluna da Especialização em Compliance pelo IBCCrim – Coimbra. Formação avançada em Ciberespaço pela Unifoj – Coimbra. Membro do Instituto Brasileiro de Direito da Informática, do Instituto Brasileiro de Direito Digital – IBDDIG e da ISOC (Internet Society) Brasil. Advogada militante.
fabianiborges@ebqadvogados.com.br

Área do Direito: Digital
Resumo: As novas tecnologias apresentam relações sociais inéditas, decorrentes de profundas mudanças nos hábitos e comportamentos humanos. Em um mundo hiperconectado, em que toda a sociedade parece se erguer e movimentar a partir da coleta e tratamento de dados, torna-se necessário o estudo sobre os reflexos jurídicos de questões intrínsecas ao uso dessas informações. Assim, em um cenário novo, aparentemente dividido entre economia compartilhada e capitalismo de vigilância, inúmeras questões jurídicas são trazidas à baila. A mais recente, e talvez mais pertinente, delas é a proteção dos dados pessoais, decorrente do direito à privacidade, sobre os quais se ergueu essa sociedade da informação. O surgimento de ecossistemas legais de proteção de dados pessoais, especialmente na União Europeia (GDPR) e no Brasil (LGPD), demanda não apenas a conformidade com tais normativos, mas a compreensão da extensão da responsabilidade do Compliance Officer, não apenas diante da (im)possibilidade de atuação como Data Protection Officer ou do Encarregado de Dados, mas também da própria delimitação da atividade daquele profissional nesse contexto inédito que se descortina, sendo essa a proposta do presente artigo.

Palavras-chave: Compliance – Responsabilidade – Proteção de dados pessoais – Direito digital – Privacidade
Abstract: The new technologies present unprecedented social relationships, resulting from profound changes in human habits and behaviors. In a hyper connected world, where all society seems to rise and move from the collection and processing of data, it is necessary to study the legal reflexes of questions intrinsic to the use of this information. Thus, in a new seemingly divided scenario between shared economy and capitalism surveillance, numerous legal issues are brought into play. The most recent and perhaps most pertinent of these is the protection of personal data arising from the right to privacy on which this information society has been built. The emergence of legal ecosystems of personal data protection, especially in the European Union (GPDR) and in Brazil (LGPD), demands not only compliance with such laws, but also an understanding of the extent of the Compliance Office´s liability, not only about the (im)possibility action of Data Protection Officer or the Data Keeper, but also the delimitation of the activity of that professional in this unpublished context that is unfolding, being the aim of this article.

Keywords: Compliance – Liability – Data protection – Digital law – Privacy

Para Luís (guerreiro glorioso) Fernando (que segue em frente com coragem), meu pequeno menino Nando, por me ensinar, todos os dias, a apreender a se reinventar.

Sumário:

1.Introdução

As[1] duas últimas décadas foram tão ou mais importantes para a humanidade quanto a Revolução Industrial. Os avanços inexoráveis da tecnologia trouxeram uma série de mudanças comportamentais nunca antes experimentadas, apresentando reflexos em todas as esferas sociais e negociais. A cibercultura[2] nunca esteve tão maciçamente difundida quanto se observa agora, e seus impactos são de todo o tipo de ordem.

Não se olvida que o mundo vive a era da informação, a quarta revolução, a era digital ou Revolução 4.0, enfim, não restam dúvidas acerca do quão impactado pela tecnologia a sociedade está. Se, até a década de 1990, o computador pessoal parecia um imenso avanço, vê-se que aquele momento fora apenas o primeiro passo para a hiperconectividade, em um mundo em que aparelhos, roupas, eletrodomésticos, carros, enfim, tudo e todos parecem estar conectados.

Há alguns anos, inclusive, Eric Schmidt e Jared Cohen[3] profetizavam que em pouco tempo todos no planeta estariam conectados, e mais de cinco bilhões de pessoas iriam aderir ao mundo virtual, fazendo surgir o boom da conectividade. Este, por sua vez, traria ganhos de mais diversos tipos, desde a produtividade até a qualidade de vida, passando por saúde e educação, proporcionando acesso a todos os usuários, não apenas aos mais afortunados economicamente, mas também àqueles que estivessem na base da pirâmide social.

Alvin Toffler[4] também pontuou sobre a emersão de uma nova civilização, que traria (trará) consigo novos arranjos familiares, modos de trabalho, de expressão do amor e convivência diferentes daquilo que a sociedade já conhecia, inclusive uma nova economia, novos conflitos políticos, e até mesmo uma consciência alterada, em sintonia com um amanhã do qual muitos estariam tentando escapar através de inúteis tentativas de restaurar um passado que já não existe mais. É essa alvorada da civilização o evento principal para a compreensão dos anos que virão, e esse movimento é tão significativo quanto a descoberta da agricultura e da Revolução Industrial, que seria denominada Terceira Onda, caracterizada pela Informação, em uma era eletrônica, que ele anuncia como Aldeia Global.

E essa nova realidade de hiperconexão, como se apresenta? Embora inevitavelmente imagens de filmes de ficção científicas venham à mente dos que se deparam com tais reflexões, é preciso delimitar – e prever – o que de fato é realidade já em uso, e o que se pode esperar para um futuro próximo, em termos de avanços da tecnologia.

Obviamente, a internet[5] é o pano de fundo dessas mudanças, pois é a partir de seu surgimento que se pode observar o fenômeno da vida on-line e dos novos modelos de negócios. Se a rede mundial de computadores é, por assim dizer, o pai dessas transformações, a força computacional pungente seria a mãe.

Com o aumento da capacidade de processamento dos dados pelos computadores é que se observa o fenômeno da Big Data, ou seja, a capacidade computacional de obter e processar grande volume de dados. E, a partir dela, vê-se o contexto da economia compartilhada e do capitalismo de vigilância, os quais se valem de uma mineração das informações produzidas pelos usuários de dispositivos computacionais, para o possível o fomento econômico dos dados.

Segundo Pierre Levy[6], o volume de informações armazenadas cresce em ritmo acelerado e, portanto, os conhecimentos e habilidades necessários a entender a esfera da "tecnociência" igualmente evoluem na mesma velocidade, a ponto de não mais haver dissociação entre memória pessoal e saber, perante essa escala crescente de dados.

É a partir dessa contextualização que se torna possível a compreensão do caminho que a proteção de dados pessoais tomou. A urgência na criação de garantias legais à privacidade nesse sentido ganhou força com as informações sobre monitoramento de

cidadãos e governos – revelados por Edward Snowden, no Wikileaks – além dos grandes vazamentos e controle de temas, inclusive eleições, – como no caso da empresa Cambridge Analytica, fazendo a sociedade se preocupar com trânsito tão intenso de dados e, principalmente, com a destinação e uso dos mesmos.

A consciência do legislador sobre a privacidade e proteção dados dos usuários – para os mais diversos fins, então, surge com vistas à proteção da privacidade daqueles, considerando o grande crescimento dos maiores players desse cenário: as empresas de tecnologia.

Assim, vistas muitas vezes como um empecilho à inovação, a proteção e a privacidade de dados ganham status de direito personalíssimo com a regulação europeia, que acaba balizando a lei brasileira e outras ao redor do planeta, criando um ecossistema legal muito interessante.

Nesse sentido, ao disciplinar a responsabilidade pelo tratamento (uso, coleta, armazenamento, transferência etc.) dos dados, vê-se que tanto o GDPR quanto a LGPD trazem uma série de condutas a ser adotadas no meio empresarial, para estar em conformidade com as normas.

Mas onde reside o papel do Compliance Officer nesse novo cenário? Será que ele deve englobar as funções do Data Protection Officer (Oficial de Proteção de Dados, doravante indicado apenas como DPO) ou do Encarregado de Dados? Essa cumulação de funções é possível ou não? As competências do compliance limitam-se à nomeação dessas figuras ou se estendem à gestão da segurança da informação e no due diligence de novos negócios? São respostas pretendemos trazer ao longo deste ensaio.

A metodologia utilizada neste artigo foi, essencialmente, a pesquisa bibliográfica em livros, artigos na internet e leis, que serviu para traçar a contextualização histórica dos efeitos da tecnologia e da economia de vigilância; delimitar o bem jurídico da privacidade como o objetivo das tutelas legais da proteção de dados pessoais e, a partir dos marcos legislativos surgidos sobre o assunto, poder verificar o escopo das atribuições inerentes ao DPO/Encarregado de Dados. Após a identificação das competências deles é que se consegue estabelecer um comparativo entre suas atribuições e as competências do Compliance Officer, para então responder às perguntas anteriormente elencadas, concluindo o propósito do presente trabalho.

2.Breve escorço histórico e contextualização

O estudo do tema é interdisciplinar, e o viés jurídico perpassa, necessariamente, pela compreensão de alguns conceitos de tecnologia, exigindo, quer do operador do Direito, quer do estudioso do compliance, conhecimentos de ciências da informação, engenharia e segurança da informação, inclusive das suas próprias limitações nas áreas afins.

Sem sombra de dúvidas, um dos maiores desafios nos estudos de tecnologia e direito, para além da mudança cultural que se enfrenta em inúmeras instituições – tal qual aquela vista na implantação dos mecanismos de conformidade após a Lei Anticorrupção – a própria necessidade de união de esforços multidisciplinares.

Há uma fala comum entre os operadores da área jurídica de que "estudaram Direito para não estudar Matemática", como inclusive destaca Augusto Marcacini[7]:

"Direito e tecnologia, à primeira vista, poderiam ser comparados a duas substâncias que jamais se misturam. Como água e óleo. O Direito é uma ciência humana, e seus estudiosos, salvo poucas exceções, não costumam – ou, ao menos, não costumavam – despertar muito interesse pelas ciências exatas. Há até uma vela piada, costumeiramente contada nas Faculdades de Direito, segundo a qual, perguntado ao aluno primeiranista por que ele escolheu o curso, tem-se como resposta: 'porque eu não gosto de Matemática.'

Na verdade, não há ramo do conhecimento que não possa ser relacionado com o Direito. O Direito regula a vida em sociedade. Isso significa dizer que cada aspecto do universo humano – a família, a vizinhança, o trabalho, os bens, o comércio e os negócios, a política, a ciência e o avanço tecnológico – merece sua atenção".

Todavia, necessária é a superação dessa ideia preconcebida para poder adentrar-se no mundo da tecnologia. Compreender os novos modelos de negócios é de suma importância, tanto para os operadores de compliance quanto aos de direito – em que pese esses mundos se reúnam em um só – para que se tenha domínio das implicações legais decorrentes.

Desmitificar que o conhecimento de tecnologia demanda conhecimentos de matemática, linguagem de programação e códigos computacionais é imperioso, pois o Direito Digital, ramo que trata das questões jurídicas originadas das relações sociais surgidas nas novas tecnologias, requer a compreensão do que são esses novos modelos, como funcionam, e não sobre sua arquitetura computacional em si.

Apenas com o advento da massificação de uso da internet é possível delinear o atual cenário social, e não apenas com a força computacional crescente. Assim, se de um lado, nas últimas décadas, o mundo passou a produzir computadores com maior capacidade de armazenamento, do outro, essas máquinas passaram a se comunicar com o advento da rede mundial de computadores.

A facilidade de acesso, especialmente através de celulares e outros dispositivos portáteis, foi o campo fértil para a produção de uma quantia antes inimaginável de informações, no qual toda produtividade passou a ser coletada, processada, estruturada e vendida com todo tipo de finalidade, da melhoria na oferta de serviços ao consumidor – com propostas individualizadas de produtos e serviços – a alegadas experiências personalizadas.

Esse imenso volume de pessoas usando outro grande volume de dispositivos conectados à internet é o solo fértil das mudanças econômicas e sociais experimentadas nos últimos 20 anos. Se lá nos anos 1990 para muitos a ideia de que a rede mundial se limitava a comunicação à distância, na década seguinte a ideia de que internet era a ferramenta edificante de outros negócios ganhou força e fez surgir empresas que vislumbraram oportunidades e modelos de negócios nunca outrora vistos.

Nesse sentido, o escopo primário a ser compreendido é o de que somos hoje uma sociedade da informação, através do Big Data – a inevitável consequência de um rolo compressor tecnológico com vida de própria da qual somos apenas espectadores[8] – e sua mineração de dados, que estruturou uma economia de vigilância com um varejo dos dados pessoais[9].

Esse capitalismo de vigilância nada mais é senão a venda dos dados que fornecemos, em sua grande parte gratuitamente, às grandes empresas de tecnologia, como Google, Facebook, Apple, Amazon – os quatro maiores cavaleiros – e tantas outras. E não há inocência no mundo empresarial, o e-mail gratuito que a Google oferece é pago pelos dados que ela coleta sobre a vida do usuário, com a concordância dele quando deu o seu aceite nos termos de uso, muito provavelmente sem lê-los, entregando sua vida e alma pela conta com aquela empresa.

Tampouco as empresas disruptivas ou de economia colaborativa o são. O aplicativo Uber, que conecta passageiros a motoristas, não se remunera apenas dos (baixos) valores das corridas, mas do volume de informações produzidos por cada usuário.

Sobre o assunto, a Ministra Nancy Andrighi[10], do Superior Tribunal de Justiça pontuou, com clareza, o caráter de consumo existente entre o usuário e tais serviços gratuitos:

"Civil e consumidor. Internet. Relação de consumo. Incidência do CDC. Gratuidade do serviço. Indiferença. Provedor de pesquisa. Filtragem prévia das buscas.

Desnecessidade. Restrição dos resultados. Não cabimento. Conteúdo público. Direito à informação. 1. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração', contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. 3. O provedor de pesquisa é uma espécie do gênero provedor de conteúdo, pois não inclui, hospeda, organiza ou de qualquer outra forma gerencia as páginas virtuais indicadas nos resultados disponibilizados, se limitando a indicar links onde podem ser encontrados os termos ou expressões de busca fornecidos pelo próprio usuário. 4. A filtragem do conteúdo das pesquisas feitas por cada usuário não constitui atividade intrínseca ao serviço prestado pelos provedores de pesquisa, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não exerce esse controle sobre os resultados das buscas. 5. Os provedores de pesquisa realizam suas buscas dentro de um universo virtual, cujo acesso é público e irrestrito, ou seja, seu papel se restringe à identificação de páginas na web onde determinado dado ou informação, ainda que ilícito, estão sendo livremente veiculados. Dessa forma, ainda que seus mecanismos de busca facilitem o acesso e a consequente divulgação de páginas cujo conteúdo seja potencialmente ilegal, fato é que essas páginas são públicas e compõem a rede mundial de computadores e, por isso, aparecem no resultado dos sites de pesquisa. 6. Os provedores de pesquisa não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente da indicação do URL da página onde este estiver inserido. 7. Não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa. 8. Preenchidos os requisitos indispensáveis à exclusão, da web, de uma determinada página virtual, sob a alegação de veicular conteúdo ilícito ou ofensivo – notadamente a identificação do URL dessa página – a vítima carecerá de interesse de agir contra o provedor de pesquisa, por absoluta falta de utilidade da jurisdição. Se a vítima identificou, via URL, o autor do ato ilícito, não tem motivo para demandar contra aquele que apenas facilita o acesso a esse ato que, até então, se encontra publicamente disponível na rede para divulgação. 9. Recurso especial provido." (STJ, 2012, on-line, grifamos)

Assim, parece pacífico que a venda de dados seja a mola propulsora do capitalismo de vigilância, e não há sites com videntes 24 horas para descobrir, em questão de fração de segundos, os desejos de consumo dos usuários de internet, mas tão somente algoritmos preditivos criados para, com base no perfil daquele, oferecer serviços e produtos.

Um caso clássico sobre o tema é o da Target[11], uma rede de varejo norte-americana, que conseguiu descobrir a gravidez de uma adolescente antes mesmo dos pais dela, através de estatísticas e análises preditivas. Ao perceber que a empresa enviava propagandas sobre produtos para gestantes e bebês à adolescente, o pai buscou satisfações na empresa, ao argumento de que ela estaria estimulando a filha a engravidar. Porém, logo depois a menina contou aos pais que, de fato, estava gestante.

A escalada dos dados é tão vertiginosa que ela não passa a ser desejada apenas pelas empresas, mas também por governos e políticos[12]. Quando Edward Snowden vem a público, no caso do Wikileaks, falar sobre o monitoramento de cidadãos pela agência americana de segurança NSA, não foi difícil perceber a relevância do Big Data, tampouco ser surpresa as notícias de uso indevido de dados pela Cambridge Analytica nas eleições americanas e, até mesmo, nas eleições brasileiras.

A preocupação na proteção de dados é relevante, existe e reside no fato de que "Os Quatro Cavaleiros estão nadando em dados que lhes damos de graça, 24 horas por dia e

sete dias por semana, e que são analisados por algumas das pessoas mais inteligentes, criativas e determinadas que já pisaram neste planeta".[13] Ou seja, poucos jogadores dominam um tabuleiro inteiro de informações importantes e relevantes, dando destinação aos dados dos usuários que sequer sabem como e por quem eles estão sendo utilizados.

Para além da proteção da privacidade dos usuários, a governança por algoritmos pode ser distorcida, quando consideramos a análise das vidas das pessoas por números e estatísticos. Nessa era do algoritmo, decisões importantes nas vidas dessas pessoas – a exemplo da escolha de um curso ou escola, acesso a crédito bancário, cotação de seguros – são realizadas por modelos matemáticos que, em tese, deveriam levar a uma maior justiça, eis que a fórmula seria aplicada para todos, em uma única regra.

Porém, o que se vê na prática é bem diferente. Os algoritmos – as fórmulas matemáticas usadas atualmente – não são regulamentados, nem transparentes, e não permitem contestação, mesmo quando claramente estão errados. E isso acaba reforçando a discriminação, como o crédito bancário é negado em razão do endereço do requerente, ou uma professora ser analisada como má profissional apenas pelas notas dos alunos, sem avaliar o seu contexto em sala de aula, ou mesmo pessoas negras serem associadas em mecanismos de buscas a macacos ou falta de beleza[14].

Concretamente tem-se um crescente número de empresas explorando, cada vez mais, dados produzidos pelos próprios titulares, mapeando todas as informações sobre o comportamento pessoal deles, escrutinando as migalhas e rastros deixados pelos hábitos de trabalho, consumo, vida pessoal no cotidiano uso da internet[15].

O pano de fundo, portanto, está colocado. O uso desenfreado e sem finalidade específica de dados pessoais coletados não deveria mais ser permitido, a privacidade do cidadão é o bem jurídico a ser tutelado e protegido. Mas quem e como controlar a coleta e uso dos dados pessoais? Como regular o mercado sem podar a inovação tecnológica? Como conter algoritmos preconceituosos ou maléficos? É a partir dessas perguntas que o mundo passa a delinear os escopos legislativos sobre o tema.

3.Ecossistemas legais

O cenário da coleta de dados desenfreada, de algoritmos opacos, de investidas de autoridades governamentais na vida privada dos cidadãos, sob o argumento da segurança nacional, parece ser terreno fértil para a criação de dispositivos legais que, de alguma maneira, conseguissem assegurar o direito à privacidade.

Em que pese a necessidade de regulações sobre proteção de dados pessoais não ser nova, as mudanças no processamento (Big Data) e controle das informações (empresas privadas), somadas à ideia de uniformização nas regras de proteção de dados pessoais é que dão o tom da criação dos ecossistemas legais.

Sem sombra de dúvidas, a OCDE – Organização para a Cooperação e Desenvolvimento Econômico – tem um papel pungente no tema. As guidelines da OCDE têm grande influência na criação das atuais leis de proteção de Dados[16]:

"[...] Nota-se, por tanto, que as guidelines da OCDE também experimentaram um movimento pendular do consentimento: a sua emergência, o questionamento e a reafirmação como ponto focal da dinâmica regulatória.

De outro lado, ainda se buscava fazer ajustes em termos de interoperabilidade legal entre os países-membros. E, nesse sentido, mais do que haver uniformidade normativa, o processo de revisão aponta para a necessidade de ações coordenadas para a aplicação e fiscalização das leis de proteção de dados pessoais, por ser isto também um elemento crucial para o livre fluxo informacional transfronteiriço.

Resulta, portanto, de mais de 3 (três) décadas a proeminência das guidelines da OCDE,

as quais vieram a influenciar as mais diversas legislações de proteção de dados do mundo. Esse processo teve como fio condutor a elevação do titular dos dados pessoais como principal ator da dinâmica normativa sobre proteção de dados pessoais. A replicação de muitos direitos acima elencados nas mais diversas legislações, que convergem para o papel de destaque que o consentimento do titular dos dados desempenha nesse arranjo normativo, é elucidativa para a compreensão de como até hoje foram estruturadas as normas sob tal temática".

O ano de 2018, em particular, pode ser considerado decisivo no âmbito legislativo da proteção de dados, eis que três grandes leis foram sancionadas ou entraram em plena eficácia como adiante se explica.

Inicialmente destaca-se a California Consumers Act Privacy, lei estadual norte-americana que foi sancionada em junho último pelo governador da Califórnia, Jerry Brown. O mais curioso desse caso é o fato de se tratar de norma de proteção de dados no país com talvez maior resistência a legislações sobre nova tecnologias, sob o argumento de poda da criatividade na inovação.

A lei entrará em plena eficácia no dia 1º de janeiro de 2020, exigindo das empresas uma conformidade com a norma, sob pena de multas pecuniárias por evento violador, como explica Julia Cheng[17]:

"A Lei de Privacidade do Consumidor da Califórnia de 2018 (CCPA) é um conjunto de leis de privacidade de dados que se aplica a todas as empresas, dos EUA ou estrangeiras, que coletam, processam e divulgam os dados dos residentes da Califórnia. Assinado em lei em 28 de junho de 2018, o CCPA deve entrar em vigor em 1º de janeiro de 2020. O CCPA se aplica a empresas com fins lucrativos que coletam informações pessoais de residentes da Califórnia (consumidores) e (1) receitas brutas anuais gerais maiores de US$ 25 milhões, (2) comprar, receber, vender ou compartilhar informações pessoais de mais de 50.000 consumidores, famílias ou seus dispositivos; ou (3) obter 50% ou mais de suas receitas anuais com a venda das informações pessoais dos consumidores da Califórnia. Sob o CCPA, 'informação pessoal' é definida de forma bastante ampla, como qualquer informação que possa ser usada para identificar um indivíduo, como identificadores pessoais únicos, transações comerciais, atividades de navegação na Internet, etc. Para cumprir, as empresas são obrigadas a fornecer mais especificidades em suas políticas de privacidade quanto ao tipo e fonte das informações pessoais coletadas, seus usos e se elas estão sendo divulgadas ou vendidas a terceiros e suas identidades. Os consumidores terão o direito de 'recusar' as informações pessoais que estão sendo vendidas, solicitar que suas informações pessoais sejam excluídas e receber serviços e preços iguais de uma empresa, mesmo que exerçam seus direitos de privacidade sob a CCPA. Por último, mas não menos importante, o CCPA exige o desenvolvimento de mecanismos de conformidade voltados ao consumidor e protocolos relacionados. Considerando que o CCPA pode ser aplicado pelo Procurador Geral da Califórnia, os consumidores da Califórnia também terão um novo direito de ação privado em certos casos, quando as informações pessoais forem comprometidas. Potenciais danos estatutários podem variar de US$ 100 a US$ 750 por incidente de consumidor e até US$ 7.500 por violação de CCPA. Como a Califórnia está na vanguarda das leis de privacidade de dados nos EUA, e a CCPA ainda está evoluindo, conforme a legislatura da Califórnia acaba de aprovar várias emendas à CCPA em 31 de agosto de 2018, as empresas que coletam, processam e divulgam os dados dos moradores da Califórnia encorajados a procurar aconselhamento jurídico em conformidade".

Outro fato curioso sobre a CCPA são as propagandas de divulgação dela, de uma criatividade ímpar. Em uma delas, há uma foto de Mark Zuckberger sorrindo, dizendo que ele comprou quatro casas para garantir sua privacidade, com o dinheiro que ele ganhou vendendo a privacidade dos usuários do Facebook. Outra tem a foto do Willy Wonka – personagem do famoso filme A fantástica fábrica de chocolate – em um meme que viralizou na rede, em que pede que o usuário lhe conte mais sobre como proteger a privacidade dele, sendo que o próprio sai vendendo seus dados para todos. Bom, parece

que a propaganda nesse caso não é enganosa.

A CCPA é de extrema relevância neste estudo, especialmente por ser a norma que regerá as regras "dentro da casa" de alguns grandes players de tecnologia, já que a Califórnia, no Vale do Silício (Silicon Valley), é sede dos gigantes da área, como Google, Facebook, Microsoft, Twitter, LinkedIn, Intel, HP, Mozilla, Tesla, WhatsApp, Apple e outros. Ou seja, é a lei nascida na casa das empresas que mais coletam e tratam dados, e que pretende colocar ordem no quintal delas, devendo ser um grande observatório de embate entre o escopo normativo e a real conduta daquelas.

Ousa-se dizer, contudo, que o grande marco legislativo de 2018 foi a entrada em plena eficácia o GDPR – General Data Protection Regulation (EU 679/2016), a lei que regula a proteção de dados pessoais na União Europeia.

A norma europeia, publicada em 27.04.2016, entrou em efetiva aplicação em 25.05.2018, concedendo um hiato de dois anos para que setores público e privado adequassem-se às regras. E essas não são poucas. Com 173 Considerandas e 99 artigos, trouxe um verdadeiro mundo novo de conceitos, aplicações e figuras próprias e virou alvo de estudos, principalmente em razão da sua aplicação extraterritorial.

É do GDPR que se extraem os conceitos de Data Protection Officer (DPO), Data Protection Authority – Autoridade de Proteção de Dados (DPA), aplicação material e territorial, controlador, princípios de privacy by design (privacidade desde a concepção) e privacy by default (privacidade por padrão), transferência internacional de dados, e sanções[18]. Em suma, um novo modelo legal para balizar o tema e com aplicação de alcance extraterritorial.

O GDPR parece ser o estopim, então, da corrida em busca de uma legislação brasileira pelo tema, quer pelo alcance extraterritorial da norma europeia – que forçou os países sem marcos regulatórios sobre o tema a adotar medidas protetivas, em razão do impedimento de transferência de dados entre a União Europeia e aqueles que não adotassem o mesmo grau de zelo com os dados pessoais, ou seja, uma medida de alcance comercial – quer pelo desejo manifesto do Brasil em fazer parte da OCDE, que exige de seus membros proteção similar à que é garantida pelo GDPR.

Nesse sentido, em que pesem as normas setoriais existentes sobre o tema, os poucos dispositivos existentes no Marco Civil da Internet[19] não havia qualquer lei semelhante no País, sendo certo que a após a plena eficácia do GDPR viu-se avançar no Congresso Nacional Projetos de Lei que tramitavam há oito anos sem despertar muito interesse do legislador.

Com efeito, a reboque do GDPR, em agosto de 2018 o Presidente Temer sancionou a Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018, criando as diretrizes de proteção de dados em um escopo legal inédito até então no País, mas muito claramente copiado da norma europeia. Por tal razão, aqueles que se preparam para a entrada em vigência completa do GDPR contam com uma leve vantagem sobre aqueles que aguardaram a LGPD ser sancionada.

Após a sanção, muito se discutiu acerca do veto presidencial no que tange à criação a Autoridade Nacional de Proteção de Dados (ANPD), sob alegação de vício de iniciativa – o Legislativo não possui legitimidade para criar cargos e funções no Executivo. Porém, a urgência da criação da ANPD se mostrou cada vez mais relevante – especialmente pela sua função consultiva e diretiva durante a vacância da LGPD – considerando a necessidade de um órgão com poder deliberativo, consultivo e sancionador, de caráter autônomo e imparcial, considerando a pretensão brasileira de entrada na OCDE.

A ausência da ANPD inicialmente criou um clima de que a Lei "não pegaria", fala comum no Brasil diante de estranhamentos iniciais com novos regramentos. Tal mentalidade foi ultrapassada rapidamente – antes mesmo da Medida Provisória 869/2018 – diante da atuação contundente do MPF, do Distrito Federal, que montou um grupo de trabalho

vanguardista na fiscalização e aplicação de normas de proteção de dados, muito antes da plena eficácia da LGPD, diga-se. Ou seja, o mindset rapidamente mudou da descrença no novo marco regulatório para uma crescente busca pela conformidade com ele.

Ao apagar das luzes, o Governo Temer criou a Medida Provisória 869, de 274 de dezembro de 2018, criando a ANPD e disciplinando sua composição e funcionamento, e ampliando o prazo de vacatio legis de fevereiro de 2020 para agosto daquele ano. E, em suma, empresas públicas[20] e privadas terão até agosto de 2020 para se adequar a LGPD, sob pena de pagamento de multas – que variam de 2% sobre o faturamento a R$ 50.000.000,00 por evento – e outras sanções administrativas.

Mas a pergunta que não quer calar parece ser: o que o Compliance tem a ver com isso? Como no próximo tópico será abordado, vê-se que tudo e mais um pouco.

4.Responsabilidade do compliancer officer

Nos últimos dois a três anos, nunca antes na história do Brasil se viu tamanho palco para os inúmeros debates sobre medidas anticorrupção, especialmente em decorrência direta das revelações da Operação Lava-Jato. Parece ter havido um boom, uma corrida, das empresas pela implantação de programas de compliance em suas estruturas, muito provavelmente por conta dos benefícios, em eventuais acordos de leniência, obtidos pela demonstração do dever de casa devidamente realizado[21].

Mas o Compliance não pode ser delimitado ao tema anticorrupção[22]:

"No mundo corporativo atual encontramos geralmente diversas equipes de auditores internos, especialistas em gerenciamento e monitoramento de riscos corporativos. Conhecemos especialistas de compliance, em controles internos, gestores de qualidade, segurança da informação, especialistas em prevenção a fraudes e à lavagem de dinheiro e outros profissionais de gestão de riscos e controles, sempre trabalhando em conjunto para ajudar suas empresas a gerenciar os tão falados riscos operacionais.

Cada uma dessas especialidades em questão tem uma perspectiva única e, em certos casos, são personalizadas e determinadas habilidade bem específicas, na busca em agregar valor às organizações. [...]

As responsabilidades devem ser claras e bem definidas para que cada área responsável pela gestão de riscos e controles conheça seus limites e obrigações na estrutura organizacional, pois é comum pessoas agirem da mesma forma e obterem resultados diferentes, sendo preocupante, por isso, devemos alinhar melhor os processos de gestão para que possamos completar os trabalhos uns dos outros".

Nesse sentido, diante do ecossistema legal criado para as normas de proteção de dados, especialmente em função do GDPR e da LGPD há de se ampliar o horizonte do compliance, no que tange à gestão de risco, inclusive para, ousa-se dizer, criar uma área de atuação: o Compliance Digital. Este, como adiante se verá, terá um escopo de atuação maior que a proteção de dados em si, porém se destaca de pronto esse item, pela urgência de adequação que a norma exige.

As dinâmicas trazidas pelas legislações de proteção de dados têm implicações diretas na atuação das pessoas jurídicas, quer de direito público, quer de direito privado, tanto no que concerne a sua atividade interna quanto ao que diz respeito aos seus relacionamentos com outras empresas e pessoas.

Ao longo do segundo semestre de 2018, após a plena eficácia do GDPR e sanção da LGPD, uma pergunta diuturna que se ouvia durante eventos de capacitação e discussão dos temas era a possibilidade de cumulação da função de DPO ou do Encarregado de Proteção de Dados na pessoa do Compliance Officer.

Inicialmente, cumpre dizer que na prática a figura do DPO (GDPR) e Encarregado (LGPD) tem basicamente as mesmas funções. E a exigência da norma brasileira quanto à necessidade do Encarregado ser uma pessoa física deixou de existir com Medida Provisória 869 de dezembro próximo passado.

Nesse sentido, valem os esclarecimentos de Bruno Bioni e Renato Leite Monteiro:

"O DPO é a pessoa que atuará como canal de comunicação perante os titulares dos dados pessoais e aos órgãos reguladores. Ele deverá supervisionar todas as práticas de tratamento de dados pessoais dentro da organização e verificar se estas estão em conformidade com a futura Lei Geral e setoriais de proteção de dados pessoais.

Para isso, o DPO deverá ter condições de realizar Privacy Impact Assessments (PIA), relatórios de impacto à privacidade e proteção de dados pessoais decorrente das atividades dentro da organização. O DPO deverá, também, estar diretamente envolvido no desenvolvimento de produtos, serviços e na formulação de políticas públicas para que a proteção da privacidade seja delas um valor de concepção, por meio de metodologias conhecidas como privacy by design e data protection by design".[23]

Enquanto a definição e as atribuições do DPO estão disciplinadas nos arts. 37 a 39 do GDPR[24], as atribuições do Encarregado de Dados são aquelas definidas no art. 41 da Lei 13.709/2018[25], cujo rol de atribuições deve ser ampliado pela ANPD.

Luís Fernando Prado, em artigo sobre o tema, elenca uma série de responsabilidades do DPO, nas mais diversas áreas, do serviço de marketing direto e indireto à advocacia, passando pela contabilidade, setor de turismo, call center, redes sociais e empresas de um mesmo grupo econômico[26]:

"As funções do DPO estão elencadas, de forma não taxativa, no artigo 39 do GDPR e incluem:

Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações, nos termos da regulamentação de proteção de dados aplicável;

Controlar a conformidade das atividades de tratamento de dados pessoais com as leis e políticas internas de proteção de dados aplicáveis, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

Prestar consultoria, quando tal lhe for solicitado, sobretudo quanto à avaliação de impacto sobre a proteção de ados, controlando a sua realização; e

Servir como ponto de contato com a autoridade de proteção de dados competente e com ela cooperar.

Para além dessas, a partir de uma análise integrada do GDPR, podemos extrair ao menos três mais: (i) servir como ponto de contato com titulares de dados, conforme artigo 31, 7; (ii) conservar o registro de tratamento de dados pessoais previsto no art. 30, se assim solicitado pelo responsável ou subcontratante; e, (iii) emitir parecer sobre a necessidade de realização de avaliação de impacto, incluindo, também, considerações sobre o que deve constar em seu teor.

Perceba-se, por fim, que as funções do DPO não incluem qualquer ato no sentido de garantir cumprimento ao GDPR (e demais legislações de proteção dados aplicável), pois essa é uma obrigação exclusiva dos agentes de tratamento de dados. Portanto, não deve o DPO ser responsabilizado pelo descumprimento do GDPR por parte do respectivo responsável pelo tratamento ou subcontratante, sendo a responsabilidade pessoal do encarregado limitada ao bom exercício de sua função consultiva em matéria de proteção de dados junto àquela parte (agente de tratamento de dados) que o contratou".

Com efeito, não parece adequada a cumulação da função do DPO ou do Encarregado de Dados com a do Compliance Officer. Inicialmente, frise-se, que as atribuições daqueles devem estar subordinas diretamente à Presidência da empresa, enquanto as do último costumam estar vinculadas aos Conselhos Administrativos.

A autonomia da atividade do DPO é mais ampla, inclusive no que tange a algumas obrigações, como a de reportar à DPA ou à ANPD vazamentos de dados pessoais de usuários, expressa recomendação de não realização de coleta de dados quando verificada a possibilidade de infração às normas de proteção. No caso do DPO (GDPR), inclusive, há impedimento de demissão dele quando, correta a sua atuação, há vazamento dados.

Observa-se que o escopo de atuação – e de responsabilização pessoal, inclusive – do DPO é mais específica que àquelas inerentes ao Compliance Officer. A cumulação das atividades, em que pese inexista impedimento legal, não é recomendável.

Não é demais ressaltar que o DPO ou Encarregado possui autuação de caráter específico e direto vinculado à segurança da informação, enquanto a obrigação do CCO é de olhar a proteção à privacidade e aos dados pessoais de maneira mais ampla.

A responsabilidade do Compliance Officer na proteção de dados parece, portanto, ser mais genérica, porém longe de ser menos importante.

Embora as atribuições sejam diferentes, elas não se contrapõem, ao reverso, complementam-se e demandarão um trabalho inter e multidisciplinar, exigindo esforços de coalizão e integração entre áreas de gestão de risco, segurança da informação, tecnologia e jurídica.

Isso porque há inúmeras red flags para os profissionais da área. O compliance digital deve começar com o mapeamento dos dados tratados[27] pela empresa. E aqui máxime atenção, o dever de guarda e proteção dos dados envolvem, pela norma brasileira, não apenas os dados digitais, mas os em meio físico também. Então a conformidade não pode se limitar a banco de dados e arquivos digitais, menosprezando arquivos físicos em papel ou outro meio.

Outro ponto importante a ser destacado é a necessidade de adequação de toda a vida documental da empresa, e isso envolve termos e políticas internas de conduta, políticas de privacidade, contratos de empregados, fornecedores, colaboradores, contratos com prestadores de serviço, de execução interna ou externa. E esse mapeamento não é estático, é dinâmico, ou seja, deve existir durante todo o ciclo de vida do dado.

O monitoramento da proteção dos dados pessoais não encerra no levantamento de todas as possibilidades de vazamento, ele deve existir enquanto durar a coleta, o tratamento e armazenamento do dado, tanto interna quanto externamente. Observe-se que não basta a empresa utilizar a ISO/IEC 27002 (normas internacionais de Segurança da Informação), se a sua folha de pessoal (com dados pessoais dos seus empregados) é executada por uma empresa externa de contabilidade, e ela não tem sequer backup de seus arquivos.

A responsabilidade do Compliance Officer se estende ainda ao due diligence na aquisição de outras empresas, no sentido de conseguir identificar possíveis contaminações de dados e documentos na aquisição. Tal regra deve valer, ainda, para atividades pontuais da empresa, tais como ações de marketing, em que costumeiramente são utilizados bancos de dados externos de agências de publicidade, que, quando da integração aos documentos internos, contaminam toda a base de dados da empresa.

De suma importância destacar ainda que deve ser do Compliance Officer o fomento da cultura institucional de proteção de dados, nas suas mais diversas gamas de possibilidades, desde a elaboração de termos de consentimento de monitoramento dos dispositivos dos funcionários em ambiente de trabalho, aos de ciência de políticas

internas de segurança que impeçam uploads ou downloads de documentos restritos, passando pela conscientização de não compartilhamento de logins e senhas entre os usuários, até a obrigação de uso de senhas fortes – principalmente por ocupantes de cargos que têm acesso amplo a estrutura de dados e informações institucionais.

Sem a conscientização ampla, em cascata, com forte reverberação e confirmação das estruturas mais altas e complexas para as mais simples, de toda a empresa não haverá conformidade com a LGPD. Observe-se caso prático narrado obtido[28] no curso da construção deste artigo: um funcionário de uma empresa de saúde, encantado com as belezas de uma paciente, abre o prontuário eletrônico dela, para, utilizando uma rede social, assediá-la. Essa registrou o assédio e encaminhou à empresa, que, por seu turno, demitiu, com justa causa, o funcionário.

Apesar de uma solução sem maiores consequências para a empresa, à luz da LGPD o comportamento do funcionário poderia ser caracterizado como vazamento de dados pessoais (sensíveis, inclusive, considerando a natureza dos dados contidos em prontuário médico[29]), implicando não apenas as sanções pecuniárias e administrativas do marco legal, como também eventuais condenações por danos morais decorrentes da exposição e assédio à paciente.

Por fim, mas não menos importante, há de se criar, ainda na cultura de compliance da empresa – e de responsabilidade direta do DPO – é a disseminação dos princípios do privacy by design e privacy by default, que nada mais são senão o fomento da privacidade desde concepção – do serviço ou produto – especialmente nas empresas de inovação tecnológica, e a implantação da privacidade por padrão – em produtos e serviços – quando identificados problemas relativos à proteção de dados neles[30].

É um tipo de regulamentação de natureza técnica, pois traz itens de controle que dependem de ajustes na plataforma de TI das organizações, especialmente no que diz respeito à governança de dados. E isso exige tempo e investimento para serem implantados. Também traz exigências documentais, que requerem a atualização de termos de uso, políticas de privacidade e cláusulas de contratos, além do mapeamento do fluxo dos dados, e mudanças estruturais que vão além da alteração na redação dos contratos, como a criptografia de bases de dados, a implementação de novos direitos, como o direito ao esquecimento, e a indicação de um Data Protection Officer (DPO), que será o responsável em proteger os dados nas grandes empresas.

Tamanhas alterações podem aumentar também os trabalhos de auditoria durante transações e, consequentemente, o tempo médio para efetivar operações. Diante disso, as empresas devem começar a pedir mais prazo para não se colocarem em uma situação de exposição e serem autuadas na fase de due diligence, o que poderia desvalorizá-las.

Para os advogados que tratam com operações que, de alguma forma, são reguladas pelo GDPR, é recomendado elaborar uma matriz comparativa durante o processo de due diligence e a rastreabilidade de dados não só dentro da empresa, em contratos e política de privacidade, mas também na sua estrutura externa, com terceiros e fornecedores.

Note-se, portanto que estar em conformidade com o GDPR e LGPD é uma tarefa que demanda múltiplos aspectos, atores e fatores, em uma mudança de pensamento legal, cultural e estrutural que permita a coalização de áreas e disciplinas distintas em prol do bem jurídico maior: a privacidade.

Assim, a responsabilidade do Compliance Officer na proteção de dados não se resume a atos únicos e isolados de implantação de novos documentos legais ou softwares de segurança, ao reverso, demanda um novo capítulo de atuação na gestão e governança das empresas, de caráter multidisciplinar, e, mormente possa ser atrelada ao cotidiano do DPO/Encarregado, é de escopo maior, mais extenso, de fomento e formação de novas culturas e comportamentos no sentido da proteção de dados pessoais dos cidadãos.

5.Conclusão

O tema é inesgotável, porque não há como prever todas as circunstâncias empresariais que surgirão na proteção da privacidade e dos dados pessoais, mas inequivocamente, a necessidade de integração entre as equipes de Compliance, Jurídico, Segurança de Informação e Tecnologia é imperativa e absoluta.

Se o Compliance Officer não parece ser o profissional ideal para assumir a vaga do Encarregado de Dados ou do DPO, na aba do chapéu dessa área da empresa também parece não caber tal compromisso. Entretanto, a necessidade de interação multidisciplinar de ambos remete à ideia de que um sombreiro ou chapéu complementar será mais útil na finalidade de dar cumprimento à conformidade que as novas legislações de dados exigem.

Não escapa da responsabilidade do Compliance Officer o dever de diligenciar a adequação da instituição às normas de segurança da informação. E essa responsabilidade somente poderá ser exercida em interoperabilidade com o DPO/Encarregado.

Note-se que o escopo da GDPR e LGPD exige um mapeamento dos dados e de seu ciclo de vida, a identificação dos papéis de controlador e processador, a delimitação das responsabilidades de cada agente de tratamento de dados, a análise de impacto a coleta e tratamento dos dados, um canal de comunicação expresso entre titulares e empresa e entre esta e DPA/ANPD, cujas atribuições são inerentes à especificidade do DPO/Encarregado.

Assim, uma vez identificados pelo DPO/Encarregado os eventuais gaps na proteção de dados pessoais, a atuação conjunta com o CCO é mais que necessária, eis que é daí que surgirá os necessários pontos de mudança, reestruturação, repactuação de documentos internos e externos da empresa, de forma a torná-la compliant com o GDPR e a LGPD.

Os desafios são imensos, decerto, especialmente para empresas nacionais ou multinacionais com atuações extraterritoriais, que demandam adequação para ambas as legislações, tanto a europeia quanto a brasileira. Elas deverão fazer um esforço hercúleo para adaptação, porém, se em conformidade com o GDPR – em plena vigência desde maio de 2018 – pouco ou quase nada terão de fazer para cumprir a LGPD em 2020.

A mudança de pensamento, de mindset – para utilizar o jargão frequente do atual mundo corporativo, é urgente e o período de vacância legislativo não deveria ser utilizado para comuns discussões "se a lei vai ou não pegar". Ao reverso, é curto para programar um programa de compliance digital efetivo, inclusive.

Essa mudança de perfil do Compliance Officer deverá dar o tom nos próximos anos, especialmente por conta das evoluções tecnológicas que se avizinham, como a internet das Coisas[31] (IoT – Internet Of Things), na qual objetos – roupas, eletrodomésticos, eletrônicos, brinquedos etc. – estão conectados à internet e também coletam dados e informações; e do tecnologia Blockchain[32] (grande banco de dados no qual se registram informações com segurança, como um livro-razão digital e público), que promete ser o grande salto evolutivo dos próximos 20 anos.

Não há dúvidas, portanto, que a responsabilidade do Compliance Officer na proteção de dados revela-se multidisciplinar e, cada vez mais, exigirá do profissional da área não apenas a conformidade com normas, leis, e regulamentos, mas a compreensão da tecnologia e dos novos modelos de relações jurídicas e de negócios trazidos pela inovação.

9.Referências

ASSI, Marcos. Governança riscos e compliance. São Paulo: Saint Paul, 2017.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

CASTELLS, Manuel. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

GALLOWAY, Scott. Os quatro. Trad. Cristina Yamagami. São Paulo: HSM, 2017.

LÉVY, Pierre. As tecnologias da inteligência. O futuro do pensamento na era da informática. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 2011.

LÉVY, Pierre. Cibercultura. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 2014.

MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato et al (Coord.). Comentários ao GDPR. São Paulo: Revista dos Tribunais, 2018.

MASSO, Fabiano Del et al (Coord.). Marco Civil da Internet: Lei 1296/2014. São Paulo: Revista dos Tribunais, 2014.

MARCACINI, Augusto Tavares Rosa. Direito e tecnologia. São Paulo: Estúdio Editores, 2014.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

O'NEIL, Cathy. Weapons of math destruction. Nova York: Crown Publishing Group, 2016. E-book.

PINHEIRO, Patricia Peck; ROCHA, Henrique. Advocacia digital. São Paulo: Revista dos Tribunais, 2018.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

SCHIMIDT, Eric; COHEN, Jared. A nova era digital. Como será o futuro das pessoas, das nações e dos negócios. Trad. Ana Beatriz Rodrigues, Rogério Durst. Estados Unidos: Intrínseca, 2013.

SINCLAIR, Bruce. IoT Internet of Things. Como usar a Internet das Coisas para alavancar seus negócios. Trad. Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2018.

TAPSCOTT, Don; TAPSCOTT, Alex. Blockchain revolution. Como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. Trad. colaborativa. São Paulo: Senai, 2016.

TOFFLER, Alvin. A terceira onda. Trad. João Távora. Rio de Janeiro: Record, 2014.

TRAY CORP. Target: entenda como a loja monitora o comportamento do consumidor. Disponível em: [www.traycorp.com.br/conteudo/target-e-o-comportamento-do-cliente/]. Acesso em: 03.01.2019.

VERISSIMO, Carla. Compliance: incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2018.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Disponível em: [https://papers.ssrn.com/sol3/Data_Integrity_Notice.cfm?abid=2594754]. Acesso em: 07.01.2018.

---

1 Artigo apresentado ao Instituto Brasileiro de Ciências Criminais (IBCCRIM) e ao Instituto de Direito Penal Econômico e Europeu (IDPEE), da Faculdade de Direito da

Universidade de Coimbra, como parte dos requisitos para obtenção do título de Especialista em Compliance. Orientadora: Prof.ª Me. Isis Hochmann de Freitas.

2 LEVY, Pierre. Cibercultura. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 2014. p. 21-28.

3 SCHIMIDT, Eric; COHEN, Jared. A nova era digital. Como será o futuro das pessoas, das nações e dos negócios. Trad. Ana Beatriz Rodrigues, Rogério Durst. Estados Unidos: Intrínseca, 2013. p, 21.

4 TOFFLER, Alvin. A terceira onda. Trad. João Távora. Rio de Janeiro: Record, 2014. p.19-21.

5 CASTELLS, Manuel. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 7.

6 LEVY, Pierre. As tecnologias da inteligência. Trad. Carlos Irineu da Costa. 3. ed. São Paulo: Editora 34, 2014. p. 121.

7 MARCACINI, Augusto Tavares Rosa. Direito e tecnologia. São Paulo: Estúdio Editores, 2014. p. 5-6.

8 ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Disponível em: [https://papers.ssrn.com/sol3/Data_Integrity_Notice.cfm?abid=2594754]. Acesso em: 07.01.2018.

9 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense. 2019. p. 3-107.

10 BRASIL. Superior Tribunal de Justiça (3. Turma). Recurso Especial 1316921/RJ. Civil e Consumidor. Internet. Relação De Consumo. Incidência do CDC. Gratuidade do Serviço. Indiferença. Provedor de Pesquisa. Filtragem prévia das buscas. Desnecessidade. Restrição dos Resultados. Não-Cabimento. Conteúdo Público. Direito à Informação. Relatora: Min. Nancy Andrighi, 29.06.2012. Disponível em: [https://stj.jusbrasil.com.br/jurisprudencia/22026857/recurso-especial-resp-1316921-rj-2011-0307909 Acesso em: 07.01.2019.

11 Tray Corp. Disponível em: Target: entenda como a loja monitora o comportamento do consumidor. Disponível em: [www.traycorp.com.br/conteudo/target-e-o-comportamento-do-cliente]. Acesso em: 03.01.2019.

12 MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva. 2014. p. 83-120.

13 GALLOWAY, Scott. Os quatro. Trad. Cristina Yamagami. São Paulo: HSM, 2017. p. 259.

14 O'NEIL, Cathy. Weapons of math destruction. Nova York: Crown Publishing Group, 2016. E-book, p. 13-15.

15 PASQUALE, Frank. The black box society. Cambridge: Harvard University Press, 2015. E-book, p. 21.

16 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 121-122.

17 CHENG, Julia. Lei de Proteção de Dados na Califórnia. Disponível em: [www.cots.adv.br/artigo/lei-de-protecao-de-dados-na-california]. Acesso em: 04.01.2019.

18 MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato et al (Coord.). Comentários ao GDPR. São Paulo: Revista dos Tribunais. 2018. p. 16-19.

"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;

II– proteção da privacidade;

III– proteção dos dados pessoais, na forma da lei; [...]."

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I– inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

VIII– informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX– consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X– exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI– publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII– acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII– aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet."

19 MASSO, Fabiano Del et al (Coord.). Marco Civil da Internet: Lei 1296/214. São Paulo: Revista dos Tribunais, 2014. p. 83-176.

20 PINHEIRO, Patrícia Peck. Proteção de dados pessoais. Comentários à Lei 13.709/2018 (LGPD). São Paulo. Saraiva Educação. 2018. p. 84-90.

21 VERISSIMO, Carla. Compliance. Incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2018. p. 71-30.

22 ASSI, Marcos. Governança riscos e compliance. São Paulo: Saint Paul, 2017. p. 84.

23 BIONI, Bruno R.; MONTEIRO, Renato L. O papel do Data Protection Officer: por que o Brasil precisa formar profissionais em proteção de Dados Pessoais. Disponível em: [www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-papel-do-d Acesso em. 07.01.2019.

24 MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato et al (Coord.). Comentários ao GDPR. São Paulo: Revista dos Tribunais. 2018. p. 127.

25 "Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1ºA identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2ºAs atividades do encarregado consistem em:

I– aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II– receber comunicações da autoridade nacional e adotar providências;

III– orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV– executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados."

26 MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato et al (Coord.). Comentários ao GDPR. São Paulo: Revista dos Tribunais. 2018. p. 135-136.

27 "Art. 5º Para os fins desta Lei, considera-se:

I– dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

III– dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV– banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V– titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI– controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII– operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII– encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

VIII– encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de DadosIX – agentes de tratamento: o controlador e o operador;

X– 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;

XI– 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;

XII– consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII– bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV– eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV– transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI– uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII– relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII– 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;

XVIII– 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; e

XIX– autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

XIX– autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.”

28 PALMA, Pedro. Adequação LGPD [mensagem pessoal]. Mensagem recebida pela autora de [pedro@clivaleiguatemi.com.br] em 07.11.2018.

29 Dados pessoais sensíveis estão disciplinados no art. 5º, II da LGPD e art. 9º da GDPR.

30 PINHEIRO, Patricia Peck; ROCHA, Henrique. Advocacia digital. São Paulo: Revista dos Tribunais, 2018. p. 105-106.

31 SINCLAIR, Bruce. IoT Internet of Things. Como usar a Internet das Coisas para alavancar seus negócios. Trad. Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2018. p. 19.

32 TAPSCOTT, Don; TAPSCOTT, Alex. Blockchain revolution. Como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. Trad. colaborativa. São Paulo: Senai, 2016. p. 34.