Proteção de dados pessoais na sociedade globalizada – Parte II

Por Renato Afonso Gonçalves*

No artigo antecedente traçamos um panorama histórico da proteção de dados pessoais, culminando com a edição do Regulamento Geral de Proteção de Dados – RGPD europeu, e da Lei Geral de Proteção de Dados – LGPD brasileira.

Como visto, o RGPD europeu, Regulamento (UE) 2016/679, constitui talvez o mais importante diploma de proteção de dados na atualidade, na medida em que busca o necessário equilíbrio entre o desenvolvimento de um enorme mercado digital e a proteção de dados pessoais, gerando reflexos inclusive para aquelas nações que mantém relações comercias com a Europa. Esse diploma é fruto do processo de amadurecimento das experiências no tratamento da matéria no campo legislativo, regulatório e jurisprudencial.[i]
Trata-se do reconhecimento de que a matéria adquire enormes proporções relativas a aspectos econômicos, sociais e culturais.

O RGPD, que entrou em vigor em 25 de maio de 2018, é composto por 173 Considerandos e 99 Artigos, o que denota não só a grande extensão do diploma mas a preocupação do legislador europeu em detalhar o seu conteúdo visando a facilitação de sua aplicação, muito embora esteja prevista uma abertura legislativa e regulamentar para os Estados-Membros aprimorarem a sua aplicação em seus respectivos territórios.[ii]

Desta feita o Regulamento Europeu trata de fixar o âmbito de aplicação material e territorial das regras; fixar definições, princípios e condições para o tratamento das diferentes categorias de dados pessoais; conferir direitos dos titulares de dados pessoais; fixar regras atinentes aos responsáveis pela manipulação e seus subcontratantes; estabelecer regras para a transferência internacional de dados pessoais; fixar mecanismos públicos e administrativos de controle e sanções para a violação de seus preceitos; e normatizar a proteção de dados no âmbito das relações de trabalho.

Em apertadíssima síntese procuraremos apontar os principais aspectos do novel diploma europeu.

Atente-se
que o objetivo do RGPD é “contribuir
para a realização de um espaço de liberdade, segurança e justiça e de uma união
econômica, para o progresso econômico e social, a consolidação e a convergência
das economias a nível do mercado interno e para o bem-estar das pessoas
singulares”.[iii]
Com isso, não se trata de proibir as atividades econômicas no mundo digital, ao
contrário, trata-se de garantir que essas atividades sejam exercidas tendo como
pressuposto o respeito ao direito fundamental à proteção de dados, o que, por
consequência, também garante uma leal concorrência entre os agentes econômicos.
Como expressa o Considerando 7 do RGPD, deverá ser “reforçada a segurança jurídica e a segurança prática para as pessoas
singulares, os operadores econômicos e as autoridades públicas”.

O diploma
em exame estabelece um conceito amplo aos “dados pessoais”[iv],
que são considerados qualquer informação relativa a uma pessoa singular
identificada ou identificável (pessoa singular que possa ser identificada,
direta ou indiretamente, em especial por referência a um identificador, como
por exemplo um nome, um número de identificação, dados de localização,
identificadores por via eletrônica ou a um ou mais elementos específicos da
identidade física, fisiológica, genética, mental, económica, cultural ou social
dessa pessoa singular).

A mesma
amplitude foi empregada para a conceituação de tratamento de dados como uma
operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre
conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais
como a recolha, o registo, a organização, a estruturação, a conservação, a
adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação
por transmissão, difusão ou qualquer outra forma de disponibilização, a
comparação ou interconexão, a limitação, o apagamento ou a destruição.***[v]***
Com isso percebe-se que o RGPD ampliou de sobremaneira o seu espectro de
incidência, afetando atividades profissionais ou comerciais que tenham como
pressuposto ou instrumento de desenvolvimento alguma forma de manipulação de
dados pessoais.

Atente-se
que o RGPD estabeleceu uma categorização de dados pessoais e espectros de
proteção diferenciados, conforme se manifeste a expressão da privacidade ou
intimidade do sujeito. São o que a doutrina denomina de dados pessoais sensíveis
(intimidade), ou não sensíveis (privacidade). Por essa razão o Artigo 9º do
RGPD estabelece como regra geral que é “proibido
o tratamento de dados pessoais (sensíveis) 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 pessoa”.As exceções previstas no número
2 do Artigo 9º implicam um nível de proteção mais rigoroso e, por conseguinte,
de maior responsabilização por suas violações.

Outro
aspecto relevante é o que se refere ao tratamento lícito[vi]
de dados pessoais, que somente se dá se o respectivo titular tiver dado o devido consentimento para uma ou mais finalidades específicas, tais como a fase pré-contratual ou de execução de um contrato; para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança[vii],
hipótese não aplicável se o tratamento de dados for efetuado por autoridades públicas na prossecução das suas atribuições por via eletrônica.

Assim, o
tratamento de dados pessoais só pode se dar de forma lícita, leal e transparente, almejando finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. Os dados devem ser adequados, pertinentes e limitados às finalidades pretendidas (minimização de dados) para as quais são tratados, devendo ser mantidos exatos, atualizados, e conservados de uma forma que permita a identificação de seus titulares durante o período necessário para as finalidades para as quais são tratados (limitação de conservação), podendo ser conservados por longos períodos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica, histórica ou para fins estatísticos.

A
segurança ganha centralidade no RGPD, visando proteger os dados pessoais de tratamento não autorizado ou ilícito, bem como de sua perda, destruição ou danificação acidental, com a adoção de medidas técnicas ou organizativas adequadas, razão pela qual se prevê a responsabilização de todos os corresponsáveis pela manipulação, exigindo-se o registro de todas as atividade de tratamento e gestão de riscos, com a nomeação de um encarregado e a notificação às autoridades competentes sobre eventuais violações.

Para dar
efetividade às suas regras, o RGPD estabelece poderosas sanções à sua violação, permitindo que os Estados-membros regulem a matéria sempre para ampliar o espectro de efetividade. É o que dispões o seu Artigo 58, conferindo a cada autoridade de seus Estados-Membros o poder de correção através de advertências, repreensões, determinação para a adoção de procedimentos específicos, retirada de certificações, aplicação de vultosas multas pecuniárias (Artigo 83[viii]),
e determinação de suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

Por
derradeiro, chama-se a atenção para o aspecto da territorialidade que visa

proteger os dados pessoais de residentes europeus em qualquer lugar do mundo. O Artigo 3º do RGPD prescreve que o diploma é aplicado ao tratamento de dados de residentes europeus, independentemente de o tratamento ocorrer dentro ou fora da União Europeia.

Prevê ainda a sua aplicação quando o responsável pelo tratamento ou subcontratante, não estabelecidos na União, ofertar bens ou serviços na União, ou pretender o controle do comportamento do titular, desde que esse comportamento tenha lugar na União Europeia. Por essas razões todas as pessoas que estabeleçam algum tipo de relação econômica com União Europeia devem necessariamente observar o RGPD.

Em consequência desse cenário, têm-se que o mesmo se dá em relação à transferência de dados de pessoas que residem na Europa. É o que determina o Artigo 44 do RGPD, ao prescrever que "qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento".

Feita uma rápida análise do RGPD, passemos à nova LGPD brasileira.

Como visto, a LGPD veio integrar o arcabouço legislativo existente até 2018 para a proteção de dados pessoais, reforçando, por conseguinte, a proteção brasileira à privacidade, intimidade, honra, imagem e dignidade da pessoa humana.

Há muito tempo a sociedade brasileira ansiava por um diploma específico na matéria, e a edição do RGPD europeu precipitou a sua aprovação, na medida em que se tornou estratégico e vital para a nossa economia o estabelecimento de níveis de proteção semelhantes ao europeu, de forma a contribuir para a competitividade internacional das empresas brasileiras.

Inicialmente note-se que LGPD entrará em vigor apenas em fevereiro de 2020, justamente para que a sociedade e o mercado brasileiros se adaptem às novas exigências.

Trata-se de uma lei que institui princípios a serem observados na matéria, estipulados no rol exemplificativo do Artigo 6º, e que contempla a figura da boa-fé, delineada e consolidada no direito civil.

Destarte,
os princípios expressos na LGPD são: *finalidade* – o tratamento deve ser realizado para propósitos legítimos, específicos, e sem possibilidade de manipulação incompatível com essas finalidades; *adequação* – o tratamento deve ser compatível com as finalidades informadas ao titular; *necessidade* – o tratamento deve ser limitado ao mínimo necessário para a realização das finalidades; *livre acesso* – deve ser garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como o acesso à integralidade dos seus dados; *qualidade dos dados* – deve ser garantida a exatidão, clareza, relevância e atualização dos dados; *transparência* – deve ser garantida a prestação de informações claras e facilmente acessíveis pelos titulares; *segurança* – deverão ser adotadas medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados; *prevenção* – deverão ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; *não discriminação* – impossibilidade de tratamento para fins discriminatórios; *responsabilização e prestação de contas* – demonstração de medidas eficazes para observar e comprovar o cumprimento das normas de proteção de dados pessoais.

Esses
princípios orientam toda atividade manipuladora de dados pessoais e se unem ao dever de *privacy by design* e *privacy by default*. *Privacy by design* ou privacidade desde a concepção, é um conceito atinente à engenharia de sistemas, e que leva em conta a privacidade durante todo o processo de construção e execução (adotando por exemplo a pseudonimização e cifragem), respeitando os valores humanos em todo o processo. *Privacy by default* ou proteção por padrão, implica que os manipuladores devem garantir que os dados pessoais sejam tratados com a mais elevada proteção da privacidade (somente dados necessários devem ser tratados por um período de conservação curto e com acessibilidade limitada) para que, por padrão, os dados pessoais não sejam disponibilizados a um número indefinido de pessoas. O RGPD, em seu Artigo 25 positivou e delineou bem esses conceitos, o que não ocorreu com a LGPD. No entanto, a conjugação dos Artigos 6º e 46 da LGPD nos permite inferir que esses princípios/conceitos foram adotados pela nossa lei.

Assim
como o RGPD, a nossa lei trata de fixar o âmbito de sua aplicação material e territorial, estabelecendo definições, princípios e condições para o tratamento das diferentes categorias de dados pessoais. Também confere direitos aos titulares de dados pessoais, fixando regras aos responsáveis pela manipulação e seus subcontratantes, e delineando os mecanismos públicos e administrativos de controle e sanções para a violação de seus preceitos.

Ao contrário
do RGPD, nossa lei positivou o direito fundamental à autodeterminação informativa (Art. 2º, II), o que em nossa opinião é um aspecto positivo, pois consolida na cultura jurídica pátria esta importante conquista da humanidade frente às novas tecnologias.

A novel

lei brasileira de proteção de dados pessoais passa ser a *lei geral* na matéria, que irradia comandos para todas as áreas do direito e deve ser aplicada e interpretada de forma sistemática a partir dos preceitos constitucionais da matéria. Portanto, a LGPD possui um caráter matricial que impactará múltiplos setores da economia e da atividade estatal.

Desta feita, como regra geral, qualquer manipulação, coleta ou processamento de dados pessoais realizada no território nacional, cujos titulares se encontrem no Brasil, estão submetidas à lei brasileira, independentemente da localização ou nacionalidade de quem as manipula. Excetuam-se de sua aplicação a manipulação feita por pessoa natural para fins particulares; realizada para fins jornalísticos ou artísticos ou acadêmicos; realizada para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, hipóteses que serão objeto de normas próprias, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular.

A manipulação de dados pessoais de crianças e adolescentes foi contemplada na LGPD, que trata do assunto no Artigo 14, lembrando que nessas hipóteses a lei deve ser aplicada e interpretada em consonância com o Estatuto da Criança e do Adolescente – ECA, e o Código Civil. Ao contrário do RGPD, a nossa lei não fixou a idade limite para que o titular dos dados promova o consentimento de forma autônoma, fixando apenas que 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"(§ 1º do Artigo 14). Assim, entendemos que deve ser aplicado Art. 2º do ECA, que considera criança a pessoa até doze anos de idade incompletos.

Na esteira do RGPG, a lei brasileira não se furtou de enfrentar a questão da anomização de dados, ou seja, a 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. Como salientado, esses dados não são considerados como pessoais salvo quando o processo de anonimização puder ser revertido, utilizando exclusivamente meios próprios ou mediante esforços razoáveis, considerando-se fatores objetivos, como custo e tempo para reverter o processo de anonimização (pseudoanomização).

Outro aspecto digno de nota é o que se refere à responsabilização civil pela lesão à dados pessoais, matéria tratada de forma bastante similar à disposta pelo Código de Defesa do Consumidor – CDC. Aliás, o texto do novel diploma fez bem em enfatizar que lesões à dados pessoais nas relações de consumo serão apuradas em integração com o CDC (Artigo 45 da LGPD).

Assim,

reconhecendo a possibilidade da ocorrência de danos patrimoniais, morais, individuais ou coletivos pelos agentes de tratamento, o Artigo 40 da LGPD estabelece a regra geral de solidariedade entre o controlador e operador quando este descumprir as obrigações da legislação de proteção de dados ou quando ele não tiver seguido as instruções lícitas do controlador. Os controladores também são solidários quando estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados.

As exceções à essa regra de solidariedade estão dispostas no Artigo 43 da LGPD. São elas: quando o agente de tratamento (controlador ou operador) provar que não realizou o tratamento de dados pessoais que lhes é atribuído; quando provar que, embora tenha realizado o tratamento de dados pessoais que lhe é atribuído, não houve violação à legislação de proteção de dados; ou provar o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.À essa sistemática a lei reserva a possibilidade de ação de regresso, e a tutela coletiva em juízo com a aplicação do CDC e da Lei de Ação Civil Pública.

Outra medida semelhante ao preconizado no CDC, é a que prevê a inversão do ônus da prova em favor do titular dos dados, quando for verossímil a alegação, houver hipossuficiência para fins de produção de prova, ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Ao contrário do RGPD que prevê prazo de 72 horas, a LGPD apenas prevê o dever de o controlador comunicar, em prazo razoável, à Autoridade Nacional e ao titular sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. Neste ponto falhou a nossa lei pois não há elementos para a definição de prazo razoável, que possivelmente ficará ao encargo de regulamento da Autoridade Nacional. Nesta hipótese, a Autoridade Nacional poderá adotar medidas semelhantes ao *recall* consumerista, como a ampla divulgação do fato em meios de comunicação (hipótese bastante constrangedora para a imagem do controlador), bem como outras medidas que entender necessárias para reverter ou mitigar os efeitos do incidente.

Quanto à transferência internacional de dados pessoais (Artigos 33 ao 36) a lei brasileira seguiu a esteira do RGPD, possibilitando-a apenas para aqueles países ou organizações internacionais que proporcionarem grau de proteção de dados pessoais adequado ao previsto na LGPD ou quando o controlador oferecer e comprovar a conformidade, através de disposições contratuais, normas corporativas, selos, certificados e códigos de conduta regularmente emitidos, com conteúdo definido ou verificado pela Autoridade Nacional.

Outro requisito indispensável para a transferência internacional de dados pessoais é a necessidade de consentimento específico do titular dos dados, que deve se dar em destaque e de forma distinta de outras finalidades.

Por
derradeiro, no que se refere às sanções administrativas a LGPD caminhou bem ao fixar grandes montas. Assim, de acordo com cada caso concreto a Autoridade Nacional, após conclusão de procedimento administrativo e garantida a ampla defesa, pode fixar a advertência; multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 por infração; multa diária; publicização da infração e bloqueio dos dados pessoais a que se refere a infração até a sua regularização.

Como
visto, o mundo digital alcançou um grau de desenvolvimento extraordinário. A crescente dependência tecnológica da humanidade só faz crescer a quantidade e o fluxo de dados pessoais disponíveis para as tecnologias disruptivas. Proteger a privacidade, intimidade, imagem e dados pessoais é uma tarefa indispensável para o necessário equilíbrio no mundo da pós-modernidade.

Por isso,
à exemplo do que aconteceu na Europa, a sociedade civil e as empresas brasileiras deverão se adaptar à LGPD, como uma necessidade premente do crescente mundo globalizado da economia digital.

Assim, as
empresas deverão instituir ou rever a forma como recolhem, manipulam, armazenam e processam dados pessoais. Essa adaptação é muito valiosa em todos os sentidos, desde a consolidação da confiabilidade dessas empresas perante consumidores e clientes, até a possibilidade de condições igualitárias de concorrência internacional. Nesse sentido, proteção de dados e *compliance* são pressupostos básicos da atividade empresarial no século XXI.

A LGPD em
muitos aspectos se aproxima, porque em certa medida foi inspirada, do RGPD europeu. No entanto, no que pese representar um bom começo, pensamos que a novel lei deixou a desejar em muitos aspectos, não regulando ou regulando de maneira insuficiente, matérias como: dados pessoais nas relações de trabalho; no espectro de investigações criminais e infrações administrativas; videovigilância; direito ao esquecimento; biotecnologia; perfirização; subcontratação; aspectos técnicos de segurança, conduta e certificação; cooperação e coerência; liberdade de expressão e informação; documentos públicos; tratamento efetivado por entidades religiosas, entre outras.

É verdade
que caberá à doutrina e à jurisprudência superar eventuais lacunas e antinomias decorrentes dessa situação. A própria criação da Autoridade Nacional de Proteção de Dados vinculada à administração direta, junto à Presidência da República, evidencia o mar de dificuldades que surgirão pela frente. Era imperiosa a criação de autarquia especial com mais independência institucional, funcional e financeira, para a adequação de nosso sistema aos padrões internacionais.

Muito
possivelmente assistiremos os conflitos de interesses econômicos decorrentes da aplicação da LGPD baterem às portas dos tribunais superiores como ocorreu com o marco civil da internet e as relações em torno do *whatsapp*, que discute os limites da intervenção estatal no desenvolvimento e uso da criptografia. A lei do cadastro positivo é o exemplo mais nítido e flagrante de conflito com a LGPD, sobretudo no que diz respeito ao tema do consentimento do titular dos dados pessoais.

Questões
como aquelas que envolviam a atividade da *Cambridge Analytica* no processo do *Brexit* e nas eleições americanas, começam a ser suscitadas no Brasil com as denúncias de proliferação de *fake news* nas eleições presidências de 2018. A influência jurídica americana que trata o tema à luz do direito de propriedade contrasta com a concepção europeia de enquadrar o direito à proteção dos dados pessoais no âmbito dos direitos humanos. A esquizofrenia vivida no mundo jurídico pátrio (*civil law* x common law) influenciará de sobremaneira o futuro da LGPD.

O Brasil
passa por uma profunda crise política, econômica, social e institucional poucas vezes vista em nossa história. Autoritarismos de agentes públicos, desrespeito flagrante à ordem constitucional e aos direitos humanos, ódio e intolerância, brotam, noite e dia, nas ruas e principalmente no mundo digital.

É nesse
cenário que nasce a LGPD. Um bom começo, que poderia ser melhor. Um futuro a ser construído por linhas tortuosas, que exigirá do mundo jurídico muito trabalho e superação para a efetivação da proteção integral dos dados de caráter pessoal no Brasil.

*__Renato Afonso Gonçalves__, advogado, é doutorando em Ciências Histórico-Jurídicas na Faculdade de Direito da Universidade de Lisboa.

---

[i]Atente-se para
os paradigmáticos acórdãos do Tribunal de Justiça da União Europeia: Digital Rights Ireland, de 2014 – Processos C-293/12 e C-594/12; Google Spain SL e Google Inc, de 2014 (Processo C-131/12); e Maximillian Schrems, de 2015 – Processo C-362/2014. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPÉIA. Disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

[ii]À guisa de
exemplificação, em Portugal foi editada a Lei nº 58/2019, de 08 de Agosto de 2019, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção
das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à

livre circulação desses dados. Disponível em: https://www.cnpd.pt/.

[iii]Considerando 2
do RGPD.

[iv]Artigo 4º, 1, do
RGPD.

[v]Artigo 4º do
RGPD.

[vi]Artigo 6º do
RGPG.

[vii]O Artigo 8º do
RGPD exige o consentimento dos pais ou responsáveis para a manipulação de dados pessoais de pessoas menores de 16 anos. De outra parte o regulamento permite que as leis dos estados-membros possam reduzir esse limite, que não pode ser inferior a 13 anos.

[viii]Podem variar de
10 milhões de euros ou 2% do faturamento anual global da empresa, a 20 milhões de euros ou 4% do faturamento anual global da empresa.