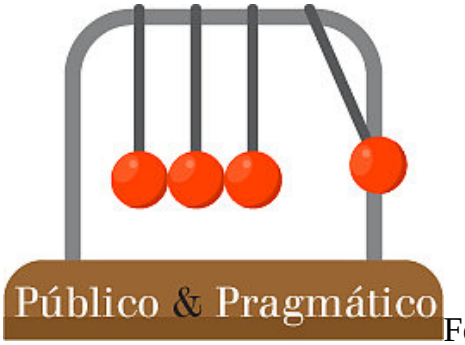
Privacy by design e LGPD: impactos e desdobramentos

A noção de *privacy by design (PbD)* surgiu na década de 1990 no Canadá, a partir dos estudos de Ann Cavoukian, comissária para Informação e Privacidade de Ontário entre 1997 e 2014, e traduz sistemas e ferramentas que levam em consideração, desde a sua concepção, a noção de privacidade, de proteção à



Foi adotada como padrão internacional em outubro de 2010 por meio de resolução proposta pela comissária canadense e unanimemente aprovada pelas autoridades especializadas em proteção à privacidade de diversos países reunidos em Jerusalém, por ocasião da *32ª International Conference of Data Protection and Privacy Commissioners.*

Suas origens remotas constam dos primeiros diplomas pensados com vistas à proteção dos referidos bens jurídicos: nos Estados Unidos, digno de registro o relatório *"Records, Computers and the Rights of Citizens"*, lançado em 1973 pelo Departamento de Saúde, Educação e Bem Estar, que trouxe os denominados *Fair Information Principles* [1]; na Europa, a pioneira *Euro*pean *Convention of Human Rights*, de 1950, cuja Seção 8 estabelece que *"todos têm o direito ao respeito à privacidade e vida familiar, à sua casa e correspondência"* [2]; e o *European Union Directive on Data Protection*, de 1995, segundo o qual todos os integrantes do bloco devem aprovar leis nacionais de proteção de dados e constituir sua autoridade nacional dela encarregada.

Nesse diapasão, cumpre registrar diferença sensível entre os sistemas dessas duas referências (EUA e Europa) no que tange à proteção de dados e privacidade: enquanto a maior preocupação americana é o manuseio de dados por agentes públicos, o sistema europeu tem seu foco concentrado sobre a atividade privada.

O sistema norte-americano, que não traz expressa menção à privacidade em sua Constituição, é composto por uma série de documentos/*acts* esparsos, enquanto o europeu conta com um diploma básico [3], centralizador e concentrador de todo o assunto — o *General Data Protection Regulation* (GDPR).

Tal quadro reflete a cultura de confiança/desconfiança dos dois países quanto a esses atores.

Independentemente dos influxos culturais a que estão submetidas as sociedades (no Brasil, verifica-se uma marcante desconfiança para com as instituições em geral, em especial as públicas [4]), é certo que a coleta, manuseio e "consumo" de dados pessoais devem ser objeto de cuidadosa disciplina.

A não incorporação dessa lógica — de respeito e resguardo à privacidade em todas as etapas do processo que envolva de alguma forma o processamento de dados — viabilizou, por exemplo, o escândalo envolvendo a *Cambridge Analityca* e o Facebook, conforme se vê do documentário *"The Great Hack"* (em português *"Nada é privado: o escândalo da Cambridge Analytica")*.

A ideia de *privacy by design* traz um *plus*, uma maior sofisticação com relação à de *privacy by default* [5] : enquanto esta última traduz hipóteses em que há automática proteção de dados, porém de forma uniforme, padronizada e de prateleira, a primeira pressupõe uma maior personalização, uma individualização no modo de coletá-los, armazená-los, manuseá-los e eventualmente transferi-los.

O GDPR europeu representa uma das mais importantes referências no assunto, trazendo os sete princípios fundamentais orientadores dessa arquitetura de sistema — e de políticas, inclusive públicas — e que devem, portanto, ser invariavelmente observados:

1) Proatividade, exigindo uma postura positiva, ativa da entidade responsável pela coleta/manipulação/manutenção/dispensa dos dados.

Sua lógica de incidência é sempre preventiva, voltada a evitar desvios e vazamentos, devendo incorporar a premissa de utilização de dados não identificáveis, exceto nas hipóteses em que sejam absolutamente indispensável a identificação — sendo sempre possível ao titular negar o fornecimento das informações a ele atinentes sem que isso lhe subtraia a capacidade de utilizar o serviço/programa.

Não se pode esperar que vazamentos ocorram para que as áreas competentes sejam instadas a agir, ou controlar os danos: o que se espera é que existam antecipadamente ferramentas desenvolvidas justamente para inviabilizar a sua ocorrência;

2) Privacidade como princípio, como padrão, devendo as suas exceções serem claras e expressamente anunciadas e submetidas à escolha do titular. A abordagem deve, nesses termos, seguir sempre uma lógica de *opt in* (caso o titular pretenda relativizar a sua privacidade, deve agir positivamente, sair da zona de conforto e manifestar assertivamente essa decisão/escolha);

3) Proteção à privacidade assimilada e incorporada desde a concepção, do desenho dos sistemas/políticas até o eventual descarte;

4) Plena funcionalidade dos sistemas/políticas. Segundo esse princípio, não se pode admitir, na equação privacidade x eficiência, uma relação de soma zero, em que o aumento de um redundaria em necessário decréscimo do outro. Exige-se, contrariamente, uma relação de soma positiva, ou de "ganha-ganha", em que o aprimoramento de um leve ao do outro, em uma perspectiva de constante evolução;

5) Segurança de dados do início ao fim do ciclo de pré-coleta-manuseio-utilização-manutenção-descarte, devendo todas e cada uma dessas etapas contar com mecanismos seguros e confiáveis de proteção;

6) Visibilidade e transparência, de forma que todos os elementos de todas as fases do processo sejam acessíveis a quem quer que pretenda acessá-los. Está inserida nesse contexto, inclusive, a denominada transparência algorítmica (relacionada à estrutura dos programas adotados, aos seus códigos-fonte e critérios assumidos pela tecnologia para discriminar, "fazer opções" e "tomar decisões"), além da possibilidade de submissão dos coletores de dados a auditorias;

7) Respeito à privacidade do usuário/cidadão como valor fundamental, cuja proteção deve ser tomada como absoluta prioridade.

Outro aspecto inerente ao PbD é o prestígio às estratégias e rotinas com relação às leis e normas: não obstante tenham estas uma importância inegável, a rapidez de espraiamento de informações por meio eletrônico e o potencial de dano dele decorrente demanda postura de prevenção de erros e vazamentos, de modo a evitar a sua ocorrência a todo o custo, como grande prioridade.

Realmente, a previsão de sanções e medidas de recomposição apresenta-se de baixa efetividade em se tratando de vazamento de dados — daí o privilégio das estratégias (arquitetura *PbD*) face a leis, e prestígio da atuação prática, preventiva e proativa em detrimento da elaboração pura e simples de instrumentos normativos. Mais importante que a existência de dispositivos legais é a criação de uma cultura de proteção de dados.

A grande questão que se coloca é a adoção do conceito pela LGPD — a qual defendemos enfaticamente, com fundamento no seu artigo 46, §2º, segundo o qual as medidas de segurança, técnicas e administrativas aptas a proteger dados pessoais *deverão ser adotadas desde a fase de concepção do produto ou do serviço até a sua execução*.

Resta saber como o dispositivo será traduzido na prática, qual a configuração das providências e políticas a partir dele desenvolvidas.

Nesse âmbito, dois aspectos surgem: 1) A quem se direciona a norma? Qual o seu destinatário na esfera da Administração Pública?; 2) como fica a questão da sua efetividade, tendo em vista a ausência de sanções administrativas, ao menos até agosto?

Conforme artigos 1º e 3º da lei, sujeitam-se aos seus ditames todas as pessoas físicas e jurídicas de direito público ou privado — sendo o discrímen determinante de sua incidência a ação de coletar/manipular/armazenar dados pessoais de quem quer que seja, desde captados em território nacional, e com exceção dos destinados às finalidades elencadas no artigo 4º [6].

Daí que, para além dos entes públicos, devem observar as estratégias em prol da privacidade — inclusive as relacionadas ao PbD — todas as entidades parceiras ou contratadas pela Administração direta ou indireta, conforme dinâmica estabelecida nos artigos 26 e 39.

Nesse cenário, despontam dois personagens fundamentais: o controlador (*pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais)* e o operador (*pessoas com as mesmas características e que realizam tratamento de dados pessoais em nome do controlador)*.

A responsabilidade de ambos é definida pelos artigos 42 a 45 da lei, respondendo tanto um quanto outro, em linhas gerais, por eventuais desvios e vazamentos.

As sanções são estabelecidas a partir de artigo 52 da lei: 1) advertência; 2) multa simples; 3) multa diária; 4) bloqueio de dados pessoais envolvidos na violação; 5) eliminação dos referidos dados; 6) suspensão parcial do funcionamento do banco de dados por até seis meses, prorrogável por igual período; 7) suspensão do exercício de tratamento de dados por até seis meses, igualmente prorrogável; 8) proibição total ou parcial de tratar dados.

As multas referidas nos itens 2 e 3 não são passíveis de aplicação em face de entes públicos, por expressa disposição legal (§3º). Não fosse isso, há impeditivos de ordem lógica a essa incidência: não faria sentido, em se considerando o orçamento público sob uma perspectiva holística, simplesmente "tirar de um bolso para colocar em outro".

Há, porém, outras sanções que, por sua natureza, e considerados os interesses públicos a serem preservados, não seriam aplicáveis à Administração: o bloqueio/eliminação compulsória de dados pessoais e a proibição total ou parcial de tratar dados.

Ora, não se pode imaginar o efetivo, eficaz e eficiente exercício da atividade administrativa sem o tratamento de dados — consideradas as atribuições mais comezinhas como lançamento/cobrança de tributos ou alocação de alunos/pacientes em vagas escolares/hospitalares.

Mais do que isso, parece-nos de questionável constitucionalidade a imposição de penalidade por órgão integrante da Administração federal (ANPD) a outro ente federativo, com a criação de uma relação de verticalidade, de subordinação entre as esferas.

Para além dessa discussão, há ainda outra, relacionada à efetividade da lei, tendo em vista a inaplicabilidade das sanções até (pelo menos) agosto de 2021.

Nesse particular, defendemos que, não obstante despidos da total magnitude legalmente atribuída, os dispositivos têm razoável impacto e eficácia, funcionando como diretrizes, como norte para um gerenciamento de dados responsável e comprometido com os direitos e garantias fundamentais.

Nas palavras de Celso Lafer, *"a sanção não é o único argumento para a observância da norma, pois o destinatário a cumprirá com mais efetividade se acreditar que ela é boa, justa e oportuna"* (1988, p. 59/60)

É essa a lógica de incidência das normas de *soft law*, em que, não obstante a ausência de sanções, há inegável legitimidade, repercussão jurídica e contribuição para a mudança de cultura.

A mudança cultural, aliás, é, ao nosso ver, um dos grandes frutos da LGPD: a partir de sua aprovação, vem sendo travada uma série de discussões a respeito do tema e aspectos correlatos, com notável evolução de toda a sociedade brasileira.

Que possamos com cada vez mais propriedade e profundidade compreender a importância da proteção da privacidade — e da sua necessária compatibilização com os reclamos pela incorporação definitiva das noções afetas ao governo eletrônico e da Administração Pública eletrônica.

Referências bibliográficas

CAVOUKIAN, Ann. Privacy by design. The seven foundational principles. Implementation and mapping of fair information practices. Disponível em https://www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf. Acesso em 26/5/2021.

SULLIVAN, Bob. "La difference" is stark in EU, U.S. privacy laws. NBC News. Disponível em https://www.nbcnews.com/id/wbna15221111. Acesso em 28/5/2021.

LAFER, Celso. A reconstrução dos direitos humanos: um diálogo com o pensamento de Hannah Arendt. São Paulo: Companhia das Letras, 1988.

[1] 1) Ciência dos dados e informações, de modo a inviabilizar registros de dados pessoais secretos; 2) Possibilidade de o indivíduo ter acesso às informações sobre ele coletadas e o respectivo uso; 3) Impossibilidade de utilização de informações com finalidade diversa da que justificou sua coleta sem expresso consentimento de seu titular; 4) Possibilidade de correção de dados e informações coletados por seu titular; 5) Qualquer organização que crie, monitore, use ou dissemine dados pessoais deve assegurar a confiabilidade das informações e impedir eventuais desvios e mau usos.

[2] Tradução livre de *"Everyone has the right to respect for his private and Family life, his home and his correspondence."*

[3] Há, contrariamente, uma série de diplomas com esse objeto: The Privacy Act; Fair Credit Reporting Act; Family and Educational Rights and Privacy Act (FERPA); Video Privacy Protection Act; Diver"s Policy Act; The Health Insurance Portability and Accountability Act (HIPAA); Gramm-Leach-Blibey Act Children"s Online Privacy Protection Act (COPPA); Genetic Information Non-Discrimation Act (GINA)

[4] O estudo Latinobarômetro mais recente (2018) indicou o patamar mais baixo, desde 1995, em termos de confiança na democracia e nas instituições em grande parte da América Latina, inclusive no Brasil. Maiores informações em https://www.latinobarometro.org/latOnline.jsp.

[5] No Brasil, adota-se a tradução "privacidade por padrão"; em Portugal, porém, a expressão adotada é "privacidade por defeito" — o que pode conduzir a compreensões equivocadas do assunto.

[6] Dentre as quais se inserem as *atividades de investigação e repressão de infrações penais*. Nesse diapasão, é interessante trazer à baila, a título ilustrativo, o caso Reporters Committee for Freedom of the Press vs. US Department of Justice, em que se discutia a possibilidade de disponibilização de registros de condenações criminais do FBI via internet, com base na LAI americana (FOIA). Na ocasião, as informações eram historicamente disponibilizadas ao público nos fóruns locais, mas decidiu a Suprema Corte pela não razoabilidade de sua disponibilização de forma eletrônica, centralizada e aberta, ao fundamento de que *o fato de um evento não ser unicamente privado não leva a que os sujeitos não tenham interesse na limitação do seu acesso universal*. Em âmbito nacional, o assunto é objeto do RE 1.301.250, com repercussão geral reconhecida (Tema 1.148).

Date Created
04/07/2021