Laura de Barros: Sobre Lei de Acesso à Informação e LGPD

25/11/2020

Muito se tem dito sobre eventual relação de contraposição entre a Lei de Acesso à Informação e

n-ingressa em vigor.

Inegável a inter-relação entre ambas.

Imperioso assinalar, porém, que, em linhas gerais, os dois instrumentos legislativos apresentam campos de incidência distintos: enquanto a LAI volta-se à disciplina das questões atinentes aos dados públicos — que, portanto, não são de propriedade, não integram a esfera de direitos de nenhum indivíduo isolada ou pessoalmente considerado —, a LGPD trata justamente dos dados pessoais, inseridos na esfera de intimidade e proteção do cidadão.

Materialmente, portanto, uma tem por foco dados públicos, outra, dados privados.

Mas as contraposições — e diferenças de incidência — não param por aí.

Enquanto a LAI busca regulamentar o exercício da transparência — instrumental e absolutamente condicionante de *accountability* e controle social —, a LGPD se ocupa da manipulação, da utilização, dos resultados pretendidos com o manejo de dados pessoais inerentes à esfera de intimidade das pessoas.

Para além disso, a LGPD é direcionada tanto aos entes públicos quanto aos privados (não obstante o foco talvez excessivo nestes), disciplinando a LAI atuação unicamente dos órgãos públicos e eventuais entidades privadas sem finalidade lucrativa parceiras, nos termos de seu artigo 2º [1].

Tal cenário já demonstra a existência de feixes de atuação — e competência, e repercussão — completamente dissociados entre as leis.

De se atentar, porém, para circunstâncias em que essa relação próxima da exclusão se transforma em desafiadora necessidade de compatibilização de normas, com a máxima

preservação dos valores norteadores da edição de cada um dos diplomas.

Nessa posição se encontra a definição de dados pessoais — tratada na LAI e estruturante da LGPD.

O conceito foi veiculado já em 2011 pelo artigo 31, §1º, da LAI: dados pessoais seriam aqueles relacionados à intimidade, à vida privada, à honra e à imagem das pessoas.

Tal "definição", marcada pela abstração e abertura, trazia certa dificuldade de caracterização mais efetiva desses dados — e carecia de qualquer preocupação com a finalidade de obtenção/manejamento/utilização dessas informações.

Ao longo dos anos em que é vigente e cada vez mais profundamente assimilada a LAI, chegou-se a uma série de conclusões de uma forma ou de outra assentadas na doutrina e na jurisprudência.

Entre elas, merece destaque a não caracterização de informações como nome, CPF, RG e endereço como informações pessoais protegidas por qualquer espécie de sigilo:

"*Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos — como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc. — condicionam o próprio intercâmbio humano na sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não se faz possível. Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles elementos identificadores usados nas relações de convivência privativas: a proteção é para elas, não para eles. Em consequência, simples cadastros de elementos identificadores (nome, endereço, RG, filiação etc.) não são protegidos. (...) Como se vê está aqui a possibilidade de se exigirem informações cadastrais relativas a nome filiação, endereço e número de inscrição no CPF ou CGC. Este tipo de dado (...), conforme fizemos ver anteriormente, embora privativo do sujeito, é condição de sua identificação para efeito dos intercâmbios sociais que ocorrem inclusive na vida privada. Destacados de intercâmbios privados, eles não estão protegidos pela privacidade. Isto vem sendo reconhecido pela jurisprudência, no caso até mais estrito do sigilo bancário, como se observa em diversos julgados, nos quais cadastros de que constem apenas os chamados dados pessoais (nome, endereço, filiação, número de registro) não são considerados objeto de sigilo*" (FERRAZ JUNIOR, Tércio Sampaio. "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado". Revista da Faculdade de Direito v. 88. São Paulo: 1993, pp. 449/54).

Tal lógica possibilita — e muitas vezes até condiciona — um efetivo controle sobre a ação pública, inclusive pela sociedade.

Realmente, a veiculação de informações como quadro societário de empresas contratadas pela Administração, CPF e endereço dos respectivos sócios muitas vezes assumem a condição de valiosa ferramenta no combate a desvios e conflito de interesses.

O mesmo se pode dizer quanto à ação de agentes públicos, cujas atividades e desempenho devem ser — ao menos potencialmente — acompanhadas por todo e qualquer cidadão.

Nesse sentido, digna de relato a já assentada posição — consagrada inclusive pelo Supremo Tribunal Federal em 2012 [2] — segundo a qual os salários de tais agentes devem ser disponibilizados nos portais da transparência das pessoas a que vinculados.

Registre-se também a determinação de acesso, pelos titulares de linhas telefônicas, aos dados cadastrais relacionados aos números dos quais recebam chamadas, por decisão do Tribunal Regional Federal da 5ª Região [3].

Mais recentes, dignas de menção ainda plataformas como as desenvolvidas pela Transparência Brasil "Tá de pé" [4] e "Tá de pé compras emergenciais" [5], voltadas à viabilização da *accountability* social das contratações públicas.

Delas constam informações como endereço, telefone, e-mail, capital social e lista de sócios dos fornecedores da Administração, com vistas justamente a impedir irregularidades e desvios.

Em cenários tais, incabível qualquer alegação de ofensa à privacidade dos indivíduos: uma vez se coloquem tais agentes/empresas em posição de contratados de um ente público, automaticamente se vem na posição de terem seus dados expostos — com vistas justamente á viabilização da fiscalização cidadã, à promoção e garantia da eficiência, da isonomia, da impessoalidade e da probidade administrativa.

Nesse aspecto, não há interesse particular ou pretensão de sigilo que possa ser oposta ao interesse público e à legitimidade da sociedade em conhecer profundamente e acompanhar *pari passu* o desempenho dos agentes e a execução dos contratos — e a postura adotada por seus sócios, inclusive quanto a eventuais conflitos de interesses.

As questões atinentes ao sigilo bancário também não podem ser invariavelmente articuladas como restrição à transparência.

Exemplo bastante eloquente disso foi a decisão prolatada por unanimidade pelo TSE no dia 20 de outubro, por provocação da Transparência Brasil e da Transparência Partidária apresentada em março, segundo a qual os extratos bancários dos partidos políticos deveriam ser disponibilizados na internet em tempo real [6].

Mais uma vez, reconheceu a Justiça a superioridade do interesse público com relação ao privado/individual/setorial.

Tais premissas continuam perfeitamente válidas nos dias atuais, pós edição da LGPD — que qualifica como dado pessoal a informação relacionada a pessoa natural identificada ou identificável.

O que muda com o novel diploma é justamente a sistematização de regras quanto à utilização dessas informações, à sua forma de gestão, e ao reconhecido direito fundamental do cidadão de saber quais dados a seu respeito estão sendo armazenados e com que finalidade.

Não que anteriormente questionamentos tais não se fizessem possíveis.

Contrariamente, o nosso ordenamento já contava com um microssistema de normas esparsas capazes de reprimir a má ou ilegítima utilização de dados pessoais, entre as quais se destacam o Código de Defesa do Consumidor (Lei nº 8.078/90), o Marco Civil da Internet (Lei 12.965/14) e o próprio Código Civil (Lei nº 10.406/02).

Tanto assim que já houve diversas ações propostas com vistas a questionar justamente alegados desrespeitos aos mesmíssimos valores e bens jurídicos de que trata a LGDP.

Cita-se, a título de exemplo, a ação proposta em fevereiro deste ano — portanto anteriormente à entrada em vigor a LGDP — pelas Defensorias Públicas da União e de São Paulo, pelo Instituto Brasileiro de Defesa do Consumidor (Idec), pela organização Artigo 19 e pelo coletivo Intervozes em face do Metrô de São Paulo [7], por meio da qual se pretendeu a produção antecipada de provas quanto a questões afetas à forma de utilização, armazenamento e destinação dos dados necessários ao reconhecimento facial dos usuários dos trens em processo de licitação.

Referida ação questionava a forma como os dados pessoais dos usuários seriam coletados e tratados; o protocolo de reação em caso de identificação de suspeito ou indivíduo procurado pela polícia; as bases de dados utilizadas a título de referência comparativa; o grau de confiabilidade e segurança do sistema e a eventual existência de estratégias de mitigação de riscos de vazamento.

O processo foi extinto em agosto do corrente ano, com a homologação das provas em seu âmbito produzidas [8] e, portanto, o reconhecimento da legitimidade e interesse inerente à disponibilização e controle de tais informações pela sociedade.

Sigilo *versus* dados pessoais

A circunstância de determinados dados pessoais não serem acobertados por sigilo não necessariamente lhes outorga a característica de dados públicos, ou de interesse público.

O fator determinante da possibilidade de sua eventual publicização dependerá da motivação para tanto: a justificativa para a exposição de dados pessoais é absolutamente lícita e proporcional em situações relacionadas, por exemplo, ao exercício da atividade de controle, ao desenvolvimento e implementação de políticas públicas, à realização de diagnósticos e estudos, com fins jornalísticos, acadêmicos ou estatísticos — ou, mais amplamente, e para fazer referência ao estabelecido no artigo 7, IX, da LGPD, à existência de legítimo interesse.

Assim, enquanto a regra geral da LAI consagra a publicidade e divulgação de dados e informações, o âmbito da LGPD impõe a abertura de dados (lembre-se, privados) única e exclusivamente em situações em que essa abertura se mostre legítima, proporcional e razoável.

Trata-se de conceituação que muitas vezes esbarrará em situações limites, com cenários pouco indefinidos e zonas interpretativas cinzentas.

Nesse contexto, ganhará destaque o papel da Autoridade Nacional de Proteção de Dados [9], incumbida, entre várias outras de enorme repercussão e importância, da missão de evitar que

todas as discussões atinentes à proteção ou abertura de dados vá desaguar no Judiciário — com as consequências perniciosas, tanto em termos temporais quanto de coerência e uniformização daí decorrentes.

O que tem que ficar claro e assente é a inadmissibilidade de manipulação, comercialização ou estudo de dados pessoais para fins comerciais, egoísticos ou ilegítimos — como se viu, por exemplo, no escândalo *Cambridge Analytica*, em que houve a comercialização e exploração de dados de cerca de 87 milhões de pessoas com vistas à manipulação de processos eleitorais em países como Estados Unidos e Reino Unido.

A questão foi tão acintosa que, para além da elaboração de um documentário de grande impacto mundial — "*The Great Hack*" — desencadeou a propositura, no final de outubro de 2020, de uma ação coletiva por mais de um milhão de usuários do Facebook no Reino Unido com vistas à sua responsabilização pelo fornecimento ilegal dos dados.

O grupo, referido pela designação "*Facebook, you own us*", alega ofensa ao *UK's Data Protection Act* de 1998, e pretende a responsabilização pecuniária da empresa — para além de uma multa já imposta pelo *Information Comission's Officer* em razão dos mesmos fatos, em novembro de 2019, no montante de mais de meio milhão de libras.

Cada vez mais evidente, portanto, a necessidade de tratamento e depósito responsável e seguro de dados e informações — os quais representam um dos mais importantes e sensíveis patrimônios pessoais dos dias atuais.

Conclusões

Tem-se, pois, que as lógicas de que partem os diplomas legais em consideração — LAI e LGPD — são opostas: enquanto uma adota como regra geral a publicidade e abertura, a outra parte da privacidade, a ser afastada por motivos determinados, justos e legítimos.

Tal cenário, porém, não leva a uma relação de estresse, de contraposição entre eles; contrariamente, o que se vê é um vínculo de complementariedade, como duas faces da mesma moeda.

Daí que a edição da lei mais recente veio a agregar — e muito — em termos de transparência, segurança da informação, promoção da verdade e combate às fake news: o simples fato de ter colocado todas as questões afetas à publicidade/privacidade/sigilo/proteção de dados em evidência já é suficiente para impulsionar um amadurecimento, tanto da comunidade jurídica quanto da sociedade em geral.

Além disso, tem-se hoje um panorama muito mais claro, previsível e digno de confiança, capaz de induzir um aprimoramento das relações e comunicações a partir de parâmetros mais objetivos e universais, avessos, portanto, a casuísmos e peculiaridades contextuais.

Há ainda um longo caminho a ser percorrido, com o aprimoramento das ferramentas de disponibilização e controle das informações. Mas ninguém pode negar a importância e evolução que representam esses primeiros passos.

[1] "*Artigo 2º — Aplicam-se as disposições desta lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres*".

[2] Conforme Suspensão de Segurança 3.902/SP; Recurso Extraordinário com Agravo 652.777/SP; Ação Originária 2.367/DF; Suspensão de Liminar 623.

[3] Apelação/Reexame necessário nº 15.896/SE (0002818/08.2010.4.05.8500).

[4] Acessível em https://www.transparencia.org.br/projetos/tadepe.

[5] Acessível em https://comprasemergenciais.transparencia.org.br/home.

[6] Decisão disponível em https://www.tse.jus.br/imprensa/noticias-tse/arquivos/tse-instrucao-0600292-29-voto-min-luis-felipe-salomao-em-20-10-2020/rybena_pdf?file=https://www.tse.jus.br/imprensa/noticias-tse/arquivos/tse-instrucao-0600292-29-voto-min-luis-felipe-salomao-em-20-10-2020/at_download/file.

[7] Processo nº 1006616-14.2020.8.26.0053, em trâmite perante a 1ª Vara da Fazenda Pública da Comarca de São Paulo.

[8] Foram produzias provas documentais relacionadas aos seguintes aspectos: 1) confiabilidade e eficiência do sistema de monitoração eletrônica a ser adotado; e 2) análise de impacto de proteção de dados, com a relação dos dados a serem coletados e tratados, e a base legal para essa coleta, a finalidade desse tratamento, análise à luz do princípio da minimização e da proporcionalidade.

[9] Conforme artigo 55-A da LGPD: "*Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da Administração Pública federal, integrante da Presidência da República. § 1º. A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da Administração Pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. §2º. A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até dois anos da data da entrada em vigor da estrutura regimental da ANPD. § 3º. O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias*".

Fonte: https://conjur.jumps.com.br/2020-nov-25/laura-barros-lai-lgpd/