Conflitos relativos à proteção de dados na rede mundial de computadores: bem imaterial *versus* Direito

https://doi.org/10.21814/uminho.ed.30.2

Amanda Cunha e Mello Smith Martins
Mestre
Universidade de São Paulo

1. Introdução

Ao realizar-se o enquadramento da questão jurídica analisada, passa-se necessariamente pela conceituação e pela classificação, momento no qual os dados pessoais podem ser entendidos sob duas perspectivas distintas. Por um lado, na condição de bem imaterial, o que, a princípio, permitiria a venda ou cessão dos dados, tidos como disponíveis. Por outro, na condição de direito (indisponível), correspondendo a ele um dever de proteção por parte dos responsáveis pela coleta, transmissão ou tratamento dos dados.

União Europeia e Estados Unidos são as duas maiores referências mundiais quanto a dados pessoais. Enquanto no primeiro caso a proteção de dados é tida como um direito fundamental, no segundo a visão adotada possui viés contratualista, no sentido de que, diferente dos direitos fundamentais, os dados seriam bens imateriais, passíveis de venda ou cessão.

O Brasil, por sua vez, está nos primeiros meses de vigência de sua própria legislação protetiva de dados, espelhada no Regulamento europeu de 2016. Episódios recentes no país, contudo, colocam à prova a suposta adoção da visão segundo a qual a proteção de dados pessoais seria um direito fundamental.

2. Proteção de dados: direito fundamental ou bem imaterial?

Nas considerações que inauguram o Regulamento Geral de Proteção de Dados da União Europeia (Regulamento EU 2016/679) já surge expressamente a natureza de bem imaterial dos dados pessoais, a título de premissa para tudo o que segue: "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental".

No Brasil, existe disposição semelhante na legislação protetiva de dados, colocando a liberdade e a privacidade como direitos fundamentais. O Supremo Tribunal Federal já havia se manifestado anteriormente reconhecendo de que a proteção de dados, em si, possui tal condição de direito fundamental, e o tema se tornou objeto de comitê específico em março deste ano.

O comitê tem como objetivo identificar e implementar medidas para ajuste de procedimentos da Corte à Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados, ou LGPD), "visando proteger direitos fundamentais da população, como liberdade, privacidade e livre desenvolvimento da personalidade".

Assim, pode-se dizer que o Brasil e a União Europeia são dois exemplos daquela segunda concepção de dados pessoais, atrelada à indisponibilidade, e colocada como um direito fundamental. Cumpre lembrar, contudo, que direito à proteção de dados, na condição de direito fundamental, é um conceito em constante e rápida evolução, e pode adquirir contornos diferentes dependendo do contexto envolvido. Nesse sentido, mesmo dentro do âmbito da União Europeia é possível encontrar visões distintas sobre a proteção de dados e sobre a privacidade, observando-se, em caso de divergência, as disposições da Carta dos Direitos Fundamentais da UE.

Os Estados Unidos, por outro lado, são comumente citados como exemplo da visão oposta, que privilegia a autonomia do indivíduo, permitindo que disponha sobre os dados livremente, inclusive quanto à sua cessão.

Cumpre questionar até que ponto Estados Unidos e União Europeia divergem quanto à qualificação dos dados pessoais, em um mundo cada vez mais conectado, e ultrapassado o episódio que deu origem ao *Safe Harbor Agreement*, com a interrupção abrupta da transferência de dados entre ambos.

De fato, o ocorrido em 2015 representou o ápice de tais divergências: conforme estas se tornaram um obstáculo para a continuidade das relações comerciais, impôs-se a necessidade de uma solução. A solução, convertida posteriormente no *EU-U.S. Privacy Shield*, garantiu certa segurança e estabilidade na transferência de dados, mas tratava-se de um equilíbrio delicado.

Os Estados Unidos vêm avançando na criação de uma legislação protetiva de dados aplicável em âmbito nacional, enquanto alguns estados, como a Califórnia, já contam com normas protetivas próprias, mais alinhadas às garantias europeias. Especificamente quanto ao CCPA (*California Consumer's Privacy Act*), embora exemplo relevante dessa tendência de harmonização, cumpre destacar o âmbito de aplicação restrito, cingindo-se aos residentes no estado.

3. O caso do WhatsApp: repercussão

Na prática, a classificação ou não da proteção de dados como um direito fundamental tem implicações práticas; exemplo disso é a recente polêmica suscitada pela alteração

dos termos de uso e política de privacidade do aplicativo de mensagens instantâneas WhatsApp. A divulgação pela empresa de que o uso do serviço seria condicionado à aceitação de novos termos de uso, implicando o compartilhamento de dados com o Facebook, alarmou os seus dois bilhões de usuários, e teve repercussões diversas.

O interessante aqui é o fato de que o WhatsApp não pretende impor a mudança igualmente em todos os países nos quais oferece os seus serviços – refletindo, na prática, as duas visões acima expostas. A empresa já esclareceu, por meio de comunicado divulgado em 07 de janeiro de 2021, que, exclusivamente no que se refere à União Europeia, não haverá tal compartilhamento de informações – ainda que outras mudanças nos termos de uso estejam previstas para ocorrer em breve.

Fora da União Europeia, a repercussão do compartilhamento de dados entre WhatsApp e Facebook foi bastante negativa, inclusive nos Estados Unidos, levando a empresa a adiar as mudanças na sua política para o dia 15 de maio. Com a divulgação da notícia de que, brevemente, os usuários que não aceitassem as novas condições seriam impedidos de utilizar o serviço, outras empresas ganharam destaque como alternativas mais seguras para a comunicação.

Em verdade, o compartilhamento de informações entre as empresas já vem ocorrendo desde 2016, mas o aplicativo oferece a opção de desabilitar esse tipo de tratamento dos seus dados. Trata-se, contudo, de *opt-out*, ou seja: aqueles usuários que não declararam expressamente o desejo de impedir o compartilhamento de suas informações, têm tido os seus dados tratados dessa maneira há anos.

Nos Estados Unidos, inclusive, o Facebook oferece ao usuário a opção de conectar sua conta do WhatsApp à conta da rede social, sob a justificativa de oferecer uma melhor experiência ao usuário em termos de publicidade direcionada e do uso de serviços como pagamento on-line (*Facebook Pay*).

A mudança, portanto, está na intenção de remover o *opt-out*, tornando o compartilhamento mandatório para que se utilize o serviço, o que vem sendo chamado pela imprensa brasileira de "consentimento forçado". Apesar de o Brasil e a União Europeia compartilharem a mesma concepção da proteção de dados como um direito fundamental, somente neste segundo caso a empresa declarou que não haverá tal obrigatoriedade.

A repercussão negativa no Brasil se evidencia pela existência de investigação sigilosa em curso no âmbito da Senacon (Secretaria Nacional do Consumidor) e, recentemente, foi alvo de notificação pelo Instituto Nacional de Defesa do Consumidor (Idec), que reportou ao Ministério da Justiça e à Autoridade Nacional de Proteção de Dados (ANPD) as mudanças pretendidas pela empresa, requerendo sua suspensão.

Na referida notificação, o Instituto também requer às autoridades que determinem que a empresa se abstenha de limitar o envio e leitura de mensagens pelos usuários que não aceitarem os novos termos, e, ainda, que a empresa seja impedida de

repassar dados a outras do mesmo grupo económico, com finalidade de publicidade, marketing, analytics e de melhoria do produto.

É mais provável que essa diferenciação de políticas por parte da empresa se dê como resultado de multas já aplicadas à empresa no âmbito da União Europeia, do que por uma preocupação com o respeito à ordem jurídica local. De fato, o Facebook já foi multado na Espanha e na Itália por induzir os usuários do WhatsApp a aceitar integralmente os novos termos de uso, e o Regulamento Geral de Proteção de Dados prevê multas elevadas em caso de violação. Isso vem sendo apontado como uma comprovação da efetividade das normas europeias.

Na esfera privada também é possível identificar reflexos das políticas de privacidade adotadas pelo Facebook e pelo WhatsApp: as empresas Apple e Google vêm reagindo à política de dados de suas concorrentes, criando suas próprias soluções de privacidade e proteção para seus consumidores.

O Google já vem testando sua alternativa de cookies no navegador Chrome desde fins de março: o FLOc (*Federated Learning of Cohorts*) foi criado para ser uma alternativa aos cookies utilizados hoje. A proposta é que, no lugar de um cookie de identificação pessoal, o FLOc é executado localmente, e agrupa os usuários conforme interesses comuns, sem compartilhar o histórico de navegação com o Google.

A Apple, por sua vez, lançou recentemente o sistema operacional iOS 14.5 para os seus produtos, o qual exige permissão do usuário para todos os aplicativos que coletam dados, e batizou a nova função de "*App Tracking Transparency*" (ATT). A empresa foi criticada publicamente por Mark Zuckerberg em janeiro, que acusou a Apple de ter sido motivada por "interesses competitivos", e cuja empresa, Facebook, obtém 97% dos seus lucros a partir da publicidade.

4. Schrems I e Schrems II: o exemplo da União Europeia

O frágil equilíbrio estabelecido pelo *Privacy Shield* já foi impactado recentemente pelo julgamento do caso Schrems II pelo Tribunal de Justiça da União Europeia, em 16 de julho de 2020: a Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, foi declarada inválida.

Em tal contexto, há negociações em curso entre o governo estadunidense e a Comissão Europeia para adaptar o *Privacy Shield* de forma a garantir que o nível de proteção seja adequado e em conformidade com as normas da União. A administração do presidente Joe Biden colocou o *Privacy Shield* como uma de suas prioridades – cujas disposições e requisitos devem continuar sendo observados pelas empresas estadunidenses que desejem transferir dados para ou da União Europeia.

Retomando a repercussão dos novos termos de uso do WhatsApp no Brasil, ao nosso ver, o Idec formulou questionamentos relevantes às autoridades protetivas

de dados nacionais – mas falhou no que se refere à motivação de suas demandas. O principal argumento apresentado foi o de que não estariam claras quais bases legais justificariam o compartilhamento de dados entre as empresas.

Equivoca-se, contudo, quem presume que o consentimento é a principal base legal para transferência de dados, inclusive internacional. A prática vem demonstrando que o legítimo interesse é mais frequentemente invocado como base legal apta a justificar o tratamento de dados pessoais, e, sobre tal aspecto (já de certo modo superado na União Europeia), ainda há bastante a evoluir no Brasil, em termos de doutrina e jurisprudência.

Os julgados Schrems I e Schrems II evidenciam que há outras questões para além das bases legais – em especial ao considerar que os dados representam ferramenta central à vigilância estatal. Os termos de uso e política de privacidade são constituídos por cláusulas contratuais padrão, assemelhando-se a contratos de adesão, e assim nos parece essencial que as autoridades brasileiras levem em consideração as discussões levadas a cabo no seio do TJUE.

Na decisão do caso Schrems II, além de ser declarado *inválido* o *Privacy Shield*, foram analisadas e *validadas* as cláusulas-tipo (Standard Contractual Clauses, SCC), e definido o âmbito de aplicação do RGPD. Quanto a este último tópico, a Corte concluiu pela aplicabilidade do Regulamento europeu ao tratamento de dados em países que não são membros da União, inclusive quando tal tratamento se der para finalidades de segurança e defesa nacional.

Mas até que ponto é possível garantir a aplicação extraterritorial de uma legislação protetiva de dados local? A pretensão extraterritorial do RGPD (assim como da LGPD brasileira) pressupõe a possibilidade de aplicação do regulamento globalmente, com o condão de, inclusive, obstar atos de vigilância por parte de agências estatais estrangeiras. Contudo, na prática, surgem situações que colocam em xeque tal aspiração extraterritorial. Normas jurídicas podem satisfazer os requisitos formais da proteção de dados, mas isto não significa que, na prática, estarão aptas a impedir a má utilização de dados pessoais, como no vaso da vigilância estatal sem legítimo interesse.

5. Para além das bases legais: outros problemas por trás dos termos de uso e políticas de privacidade

Atualmente, ao acessar a política de privacidade do WhatsApp, o usuário é informado de que, se "reside na região Europeia, o WhatsApp Ireland Limited fornece o WhatsApp" sob termos de uso e política de privacidade específicos. Fora do território da União, a empresa responsável por fornecer o serviço, e consequentemente pelos termos de uso, é o WhatsApp LLC.

Na versão disponibilizada aos usuários brasileiros, a utilização do serviço implica aceitar que a empresa pode "(...) coletar, usar, reter e compartilhar dados quando

acreditarmos em boa fé que isso se faz necessário para: (...); (c) detectar, investigar, prevenir e resolver atividades fraudulentas e ilícitas ou questões de segurança ou técnicas; ou (d) proteger os direitos, a propriedade e a segurança de nossos usuários, do WhatsApp, da família de empresas do Facebook ou de terceiros."

A utilização dos termos "prevenir", "investigar", "proteger" e "terceiros" deixa claro que já faz parte da política adotada pelo aplicativo o compartilhamento de dados em hipóteses diversas e bastante amplas. Nenhum desses termos é definido claramente pela empresa, que também deixa explícito que o compartilhamento de dados com o Facebook já é uma realidade desde 2014.

O Facebook utiliza as mesmas expressões em sua política de privacidade, deixando claro que a empresa compartilha "informações com autoridades responsáveis pela aplicação da lei ou em resposta a solicitações legais", e que as informações pessoais podem ser acessadas, preservadas ou compartilhadas com reguladores, autoridades ou "terceiros", nas mesmas hipóteses previstas nos termos do WhatsApp – ou seja, sem necessariamente haver um inquérito em curso ou ordem judicial.

Também é possível encontrar ressalvas quanto ao direito à exclusão de dados: "As informações que recebemos sobre você (incluindo dados de transações financeiras (...) podem ser acessadas e preservadas por um período maior quando forem objeto de uma requisição ou obrigação legal, investigação governamental, investigações de possíveis violações de nossos termos ou políticas, ou para de outra forma impedir danos."

Não estão claros quais os danos aptos a justificar a preservação de dados cujo titular solicitou a exclusão – nem tampouco há transparência para o usuário cujos dados são preservados, já que não lhe é dado conhecimento nem justificativa a respeito. Em caso de ordem judicial, há legítimo interesse indubitavelmente – mas também há maior transparência para a pessoa cujos dados estão sendo preservados e/ou compartilhados. No entanto, assim como o consentimento não é a principal base legal invocada para justificar o tratamento de dados, as decisões judiciais não são a única forma pela qual estados requisitam informações sobre cidadãos.

A coleta de dados pelo Estado sempre esteve ligada a duas questões principais: vigilância e controle. Diante disso, o compartilhamento de informações com "agências estatais" ou com "terceiros", sem que o usuário seja informado expressa e pontualmente a respeito dele, e esclarecido quanto às suas motivações, pode prejudicar mais do que o direito à proteção de dados.

A liberdade de expressão é outro direito fundamental intimamente ligado ao ambiente virtual – e o acesso do governo local ou do governo estadunidense a informações pessoais pode tolher o exercício desse direito. Não se trata de mera situação hipotética: recentemente foram realizadas prisões no Brasil, por conta de publicações em redes sociais que, supostamente, representariam ameaças à segurança nacional. Nenhuma das prisões foi mantida, mas o prejuízo à liberdade de expressão já foi concretizado.

Episódios semelhantes nos E.U.A. e no Reino Unido são relatados no documentário "Terms And Conditions May Apply" (2013), dirigido por Cullen Hoback, demonstrando que o compartilhamento de informações com agências estatais pode ser mais prejudicial às pessoas do que o compartilhamento entre duas empresas do mesmo grupo com fins publicitários. Em um mundo marcado pelas revelações de Edward Snowden, preocupações com vigilância e controle são incontestavelmente legítimas.

6. Conclusões

Christopher Kuner chama a atenção para as diferenças entre os planos do ser e do dever ser quanto à proteção de dados, e cumpre concordar com a afirmação de que, como qualquer direito fundamental, a proteção de dados não pode ser reduzida a um conjunto de procedimentos formais ou burocráticos.

A decisão do julgamento Schrems II pelo TJUE em 2020 levanta questões que não parecem ser ainda objeto de preocupação no Brasil – e isto, por sua vez, é alarmante. Na decisão, a Corte teceu críticas ao Privacy Shield com ênfase na sua limitação por conta de questões de segurança nacional ou aplicação da lei. O acordo foi considerado, portanto, incapaz de impedir o acesso de dados pessoais por agências governamentais e de inteligência.

A política de privacidade atual do WhatsApp, bem como a do Facebook, parece deixar as portas abertas para a vigilância estatal, indo de encontro com a concepção da proteção de dados como um direito fundamental. A preocupação brasileira com a mudança dos termos do WhatsApp é legítima, mas revela um entendimento ainda muito incipiente sobre a proteção de dados e sobre questões relacionadas, que extrapolam a letra da lei.

Mais do que transparência quanto às bases legais, impõe-se a transparência nos conceitos já utilizados nos termos de uso e políticas de privacidade, que possam implicar o compartilhamento de dados para finalidades de vigilância e controle estatal. Se o Brasil adota a visão segundo a qual a proteção de dados é um direito fundamental, espera-se que não apenas o WhatsApp aja de acordo em seus termos de uso, mas exige-se, também, que essa visão seja efetivamente incorporada no país.

A preocupação com o compartilhamento de dados entre duas empresas do mesmo grupo econômico para fins publicitários parece rasa diante dos direitos fundamentais colocados em risco. O Brasil pretendeu seguir a concepção europeia em sua legislação protetiva de dados – mas ainda há um longo caminho a percorrer antes que a condição de direito fundamental atinja o plano do ser. Enquanto isso, na prática, o país ainda está mais próximo da concepção contratualista estadunidense. É possível que isso explique, ao menos em partes, por que o WhatsApp não aplicará ao Brasil os mesmos termos que aplica à União Europeia.