Quintiere: Reflexões sobre o Protecting Household Privacy Act

No dia 1º deste mês, entrou em vigor no estado de Illinois, nos Estados Unidos, o denominado *Protecting Household Privacy Act* (EUA, 2022). Inicialmente, referido ato normativo trouxe em seu bojo os conceitos de comunicação eletrônica, *household*, dispositivo eletrônico doméstico (*household electronic device*), dado eletrônico doméstico (*household electronic data*) e de órgão de aplicação da lei (

O primeiro desses termos, consistente na chamada

comunicação eletrônica, deve ser entendida como aquela de qualquer origem, transmissão, emissão, transferência ou recepção de sinais, sinais, dados, escritos, imagens, vídeo, áudio ou inteligência de qualquer natureza por telefone, incluindo telefones celulares ou um fio, internet, sem fio, rádio, eletromagnético, sistema foto-eletrônico ou foto-óptico, televisão a cabo, fibra óptica, satélite, micro-ondas, com base na internet ou sem fio.

O termo *household*, ou, em tradução livre, de utilização familiar, de acordo com a lei, foca no local de utilização de dispositivos eletrônicos objeto de regulamentação, consistindo esse em qualquer residência, seja a que comporte família única, seja aquela que comporte mais de um núcleo familiar, incluindo, mas não se limitando, a uma única casa de família, casa, apartamento, casa móvel, trailer, prédio, condomínio, duplex, casa geminada ou outros aposentos, usados ou pretendidos para ser usado como uma habitação e imediatamente envolvente área.

Por sua vez, o *household electronic device* diz respeito a qualquer dispositivo, principalmente àquele destinado ao uso dentro de uma família que seja capaz de facilitar qualquer comunicação eletrônica, não estando incluídos dispositivos pessoais de computação e dispositivos de *gateway* digital. Para fins de interpretação do referido ato normativo, "dispositivo de computação pessoal" significa um dispositivo pessoal, podendo ser citados como exemplos um computador, telefone celular, *smartphone* ou *tablet* ; e "dispositivos digitais de *gateway*" podem ser exemplificados por um modem, roteador, ponto de acesso sem fio ou decodificador de sinais de cabo atendido por um provedor de serviços a cabo.

O termo "dados eletrônicos domésticos" compreende qualquer informação ou entrada fornecida por uma pessoa a um dispositivo eletrônico doméstico. Por fim, por agência de aplicação da lei se entende qualquer agência do estado de Illinois ou de uma subdivisão política cuja atividade seja lastreada em lei visando à manutenção da ordem pública e o cumprimento das leis.

A Seção 10 disciplina que, em regra, é proibida a utilização de dados eletrônicos domésticos. Nesse sentido, exceto o disposto na Seção 15, uma agência de aplicação da lei não deve obter dados eletrônicos domésticos ou, ainda, direcionar a aquisição de dados eletrônicos domésticos de um terceiro.

Disciplinando as exceções ao regramento da Seção 10, a Seção 15 dispõe que a lei não proíbe que uma agência obtenha dados eletrônicos domésticos nas seguinte situações: 1) mediante expedição de mandado nos termos da Seção 108-4 do Código de Processo Penal de 1963; 2) para responder a uma chamada de serviços de emergência sobre o usuário ou possuidor de um dispositivo eletrônico doméstico; 3) em uma situação de emergência, 4) com o consentimento do proprietário ou possuidor do dispositivo eletrônico doméstico.

As alíneas "a", "b", "c" e "d" caracterizam somo situação de emergência aquela que: a) envolve um perigo claro e de morte iminente ou de grande dano corporal a uma pessoa ou pessoas resultante de um sequestro ou detenção de refém pela força ou ameaça de uso iminente de força; b) em que não houve prévio aviso da situação de emergência para o investigador ou policial, impossibilitando a aprovação judicial prévia, devendo existir circunstâncias que razoavalmente façam com que o oficial conclua pela existência de risco caso se espere a decisão judicial prévia; c) os dados eletrônicos domésticos são necessários para prevenir a morte iminente ou grande dano corporal a uma pessoa ou pessoas; e d) os dados devem e podem ser acessados antes de um mandado para prevenir a morte iminente ou de grave dano a uma pessoa ou grupo de indivíduos.

O parágrafo quinto da Seção 15 do *Protecting Household Privacy Act* disciplina que, para a obtenção de dados eletrônicos domésticos, o juiz deve, em sua decisão, explicitar que a providência teria sido deferida caso fosse pedida em momento posterior ao pleito da autoridade, existe situação de emergência, conforme definido no subparágrafo C do parágrafo terceiro da Seção 15.

De acordo, ainda, com a Seção 15, se um pedido de aprovação da diligência então feita for negado, os dados eletrônicos domésticos obtidos serão considerados inadmissíveis de acordo com a Seção 30, do mesmo diploma normativo.

A Seção 20, por sua vez, dispõe que caso a agência, após regular coleta de dados, não registrar acusações criminais, os mesmos devem ser destruídos no prazo máximo de 60 dias contados da coleta. O mesmo dispositivo, nos parágrafos primeiro e segundo, assevera que os dados não serão destruídos, caso o supervisor da agência entenda como cabível a retenção do material coletado em virtude da: 1) suspeita razoável de que a informação contém evidências de atividades criminosas; ou 2) relevância dos dados para alguma investigação em curso.

A Seção 25, ao abordar a divulgação de informações pelas autoridades policiais e/ou agências dos dados coletados, assevera que se uma agência de aplicação da lei obtiver os dados eletrônicos domésticos nos termos da Seção 15, não deve divulgar qualquer informação obtida, com exceção da troca de informações entre agências governamentais e desde que a informação seja relevante para um procedimento ou investigação; ou com o consentimento legal do proprietário, ou pessoa em posse real, permanente ou provisória, do dispositivo eletrônico domiciliar.

No que tange à divulgação dos dados eletrônicos domésticos para agências governamentais, o subitem "b" da Seção 25 dispõe que tal divulgação deve ocorrer de modo a se resguardar, dentro do razoável, a intimidade dos envolvidos, devendo ocorrer a comunicação do mínimo necessário para cumprimento da diligência entre agências.

De acordo com a Seção 30, se o tribunal decidir que uma agência de aplicação da lei obteve dados eletrônicos domésticos relativos a uma pessoa ou seus efeitos em violação desta lei, referida informação será presumidamente considerada inadmissível em qualquer processo judicial ou administrativo.

No mesmo dispositivo foi destacado que o Estado pode superar essa presunção de inadmissibilidade , comprovando: 1) a aplicabilidade de alguma das exceções reconhecidas à regra de exclusão da Quarta Emanda à Constituição dos Estados Unidos; ou, ainda, 2) da Seção 6 do artigo I da Constituição de Illinois, bem como demonstrando, por meio de evidências, que o policial estava agindo de boa-fé e razoavelmente compreendeu que um ou mais das exceções da Seção 15 da norma aqui analisada, existiam no momento em que os dados eletrônicos domésticos foram obtidos.

Após delimitar o escopo de aplicação da norma a partir da Seção 35, dispondo que interpretações ampliativas quanto ao acesso a dados eletrônicos domésticos não serão admitidas, a Seção 40 destaca que qualquer pessoa ou entidade que fornece dados eletrônicos domésticos em resposta a uma solicitação de qualquer agência de aplicação da lei, justificada na referida lei, deverá tomar medidas razoáveis para garantir a confidencialidade, integridade e segurança de quaisquer dados eletrônicos domésticos durante a transmissão para qualquer agência de aplicação da lei, e para limitar qualquer produção de dados eletrônicos domésticos a informações que atendam à solicitação da agência de aplicação da lei.

A Seção 50, por sua vez, disciplinando eventuais conflitos de normas, informa que, no caso de qualquer conflito entre essa lei e qualquer lei federal ou estadual aplicável, a norma que estabelece o padrão mais elevado para obter informações deve prevalecer. Além disso, disciplina expressamente que intimações realizadas pelo júri para obtenção de dados domésticos em momento anterior ao advento da lei de Illinois devem ser consideradas válidas.

Conhecida como *Protecting Household Privacy Act*, a lei restringe o compartilhamento de dados do dispositivo ao exigir um mandado de busca e apreensão ou permissão do proprietário do dispositivo como regra, com algumas exceções em cenários de emergência, conforme visto acima.

O objetivo da lei é definir limites para quando os fabricantes de tais dispositivos entreguem os dados às autoridades, em vez de deixá-los nas mãos de empresas de tecnologia como Amazon.com Inc. para definir seus próprios padrões.

Seu foco no compartilhamento de dados com a polícia destaca uma tensão legal sobre as expectativas de que as casas das pessoas sejam um espaço privado, mesmo quando elas usam dispositivos que podem documentar suas conexões sociais e registrar seu paradeiro.

Peter Hanna, consultor jurídico da *American Civil Liberties Union de Illinois*, em recente entrevista para a *Bloomberg Law* [1], refletindo sobre os problemas que esses dispositivos trazem para a privacidade, destacou o seguinte: *"Se eu planejo um crime em uma esquina e alguém me ouve, não tenho expectativa de privacidade lá"*.

De acordo com o que é conhecido como *third-party doctrine* (doutrina de terceiros, em tradução livre), a Suprema Corte dos Estados Unidos decidiu que as pessoas não podem esperar privacidade em informações voluntariamente compartilhadas com terceiros. A doutrina emergiu de uma decisão de 1976 em *Estados Unidos v. Miller* sobre registros bancários e uma decisão de 1979 em *Smith v. Maryland* envolvendo telefonemas.

Além disso, a nova lei em Illinois pode *"complicar os esforços de conformidade"* para empresas que também estão sujeitas à Lei de Comunicações Armazenadas, pois os requisitos do *Protecting Household Privacy Act* não se enquadram perfeitamente na estrutura da legislação federal conhecida como *Stored Communications Act* [2], circunstância que pode gerar diversos problemas no que tange a aplicação da referida lei.

Isso tudo se deve ao fato de que a lei de Illinois é aplicável aos dados de dispositivos conectados, mas não os de computação, como um computador, *tablet* ou telefone celular. A lei estadual também exclui dispositivos de "*gateway* digital", como modems e roteadores de internet ou decodificadores de cabo. A lei federal, por sua vez, se aplica aos dados armazenados, independentemente do dispositivo ao qual estejam associados, segundo Goodwin.

Antes que as pessoas concordem em compartilhar seus dados domésticos com a polícia, elas devem entender quais informações estão compartilhando. Nesse sentido, cada vez mais é necessário que os fabricantes de dispositivos esclareçam em suas políticas de privacidade quais informações estão sendo coletadas e quando, seja por ativação intencional ou por um modo sempre ligado.

Nesse sentido, após o estudo feito no presente tópico, é possível concluir preliminarmente que a prova, em um momento civilizatório no qual, cada dia mais, a quantidade de dados e metadados dos indivíduos estão disponíveis por toda a rede, passará (não exclusivamente, mas em sentido complementar, no mínimo) a ser produzida pelo Estado de forma eletrônica, podendo ser utilizadas tanto técnicas estáticas como preditivas (com as ressalvas relativas ao avanço tecnológico e o estágio normativo atuais) de coleta, assim como já ocorreu no estado de Illinois. Nesse contexto, é essencial o estabelecimento de critérios objetivos para que o acusado, de um lado, não seja tolhido de usar de forma concreta o seu direito ao silêncio, evitando-se a produção abusiva de indícios e prova.

Referências bibliográficas

Chaker, Vania (21 September 2018). "*Your Spying Smartphone: Individual Privacy Is Narrowly Strengthened in Carpenter v. United States, The U.S. Supreme Court's Most Recent Fourth Amendment Ruling"*. Journal of Tech Law. Retrieved 21 September 2018.

Chaker, Vania (6 August 201). *"Chimaera I: Chimaera Unleashed: The Specter of Warrantless Governmental Intrusion Is a Phantom that Has Achieved Greater Life in the Ether of Internet Communications"*. Journal of Tech Law. 23. Retrieved 6 August 2019.

EUA. Protecting Household Privacy Act. Disponível em: <https://aboutblaw.com/0ZD. Acesso em: 03.01.2022.

EUA. Stored Communications Act. Disponível em:< https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap121-sec2701.pdf>. Acesso em: 03.jan. 2022.

Kerr, Orin S. (2009). *"The Case for the Third-Party Doctrine"* (PDF). Mich. L. Rev. 107 (4): 561–602. Archived from the original (PDF) on October 7, 2009.

[1] A entrevista pode ser acessada através do seguinte link: *Law Curbing Police Access to Home Data Tests Privacy Boundaries* https://news.bloomberglaw.com/privacy-and-data-security/law-curbing-police-access-to-home-data-tests-privacy-boundaries. Disponível em: 03.jan.2022.

[2] O *Stored Communications Act* (SCA), promulgado em 1986, fornece proteção estatutária de privacidade para clientes de provedores de serviços de rede. A SCA controla como o governo pode acessar informações de contas armazenadas de entidades como Provedores de Serviços de Internet (ISPs). Essas informações de conta geralmente incluem e-mail, bem como informações de assinante e cobrança. Especificamente, o SCA estabelece o processo que os policiais estaduais e federais devem seguir para que possam forçar a divulgação desses registros pelo provedor.

Date Created
05/01/2022