Gustavo Pedrina: Vigilância invasiva aos poucos é instalada no Brasil

Nos próximos dias o Rio de Janeiro sediará 19º Congresso Internacional de Direito Penal, com o tema central *Sociedade da Informação e Sistema Penal*. O Brasil tem a chance de, pela presença de tantos e tão importantes especialistas, tornar-se centro de debates de um ramo nascente do Direito: o informático de proteção da intimidade dos usuários da internet.

O maior meio de intercâmbio de informações atual é eletrônico: diariamente bilhões de e-mails são trocados, mensagens são postadas em contas de redes sociais, fotos são carregadas, livros e músicas são lançados. Vivemos na sociedade da informação. E, Manuel Castells faz questão de enfatizar a importância de estudar as mudanças tecnológicas em relação aos contextos culturais, condições históricas e intervenções políticas. As estruturas sociais são construídas de acordo com o espaço-tempo que vivemos, mas com os avanços que presenciamos, o próprio conceito de estado-nação é afetado pelas novas fronteiras que estamos descobrindo com a tecnologia.[1]

Assistimos uma transformação do conceito de poder. Se para Castells o poder está na capacidade de influenciar assimetricamente na decisão de um outro ator, a posse de uma coleção imensa de dados tem papel objetivamente claro nisto: a sociedade da informação passa a depender cada vez mais da acumulação de informações sobre pessoas e organizações. Essas informações são objeto de cobiça por parte de governos e particulares interessados tanto em ganhos políticos quanto financeiros. Como escreveram Eugenio Raul Zaffaroni e Edmundo Oliveira “A tecnologia tornou as pessoas senhores do universo, mas eles também devem ser senhores do seu próprio destino (…)O mundo moderno confronta a lei com a necessidade de restabelecer a paz e a segurança, sem ferir a justiça, sem violar os direitos humanos”[2], nada mais verdadeiro na Sociedade da Informação.

No começo de 2012 um episódio de curiosidade massiva ocorreu com a atriz Carolina Dieckmann, que viu fotos suas nua serem espalhadas pela internet. Só então a discussão quanto a invasão de caos armazenados em dispositivos digitais ganhou algum protagonismo no Brasil. Disciplinou-se, ainda em 2012, pela lei 12.735, as penas para a invasão de dispositivos eletrônicos, introduzindo no ordenamento jurídico a tipificação de delitos eletrônicos justamente no capítulo que trata dos crimes contra a liberdade individual.

Os novos tipos penais atuam para a expansão do direito penal, colocando no centro da pretensão punitiva os “hackers” particulares e tutelando principalmente a intimidade do cidadão, mas não a segurança dos dados e a privacidade do usuário. Víctor Gabriel Rodríguez apontou, antes mesmo da edição da lei, um equívoco nisto: “delitos como o hacking ou mera invasão de sistema informático, (…)não constituem por si próprios ofensa à intimidade, mas à rede de computadores. Sua criação como tipo autônomo teria de fixar um bem jurídico tutelado ou colocado em risco e, no nosso entendimento, a intimidade não o pode ser, isoladamente.”[3]

O que se deve avaliar é, principalmente, a abrangência das leis que estão em vigor para regular a internet: a quem se aplicam e em qual medida suas punições alcançam os agentes particulares e, principalmente, os governamentais. Não basta uma lei que puna os hackers particulares mas deixe livre os agentes estatais que pratiquem abusos semelhantes ou mais graves. Na União Européia, a *European Court of Justice(ECJ)*

2023 - www.conjur.com.br - Todos os direitos reservados.

a mais alta corte do bloco, acaba de invalidar a diretiva 2006/24/EC, norma que regulava o tema, justamente por seu caráter excessivamente abrangente, dando aos governos mais dados do que precisam para conduzir investigações criminais. Não se pode, segundo a corte, coletar dados indiscriminadamente de todos os cidadãos de uma jurisdição. É assim para o sigilo telefônico e também deve ser para o sigilo de dados. Viola-se o princípio da proporcionalidade ao estender a todos a exceção que deve ser aplicada na condução de investigações a alguns[4].

O novo Marco Civil da internet brasileira traz exatamente este mesmo dispositivo que obriga o armazenamento dos dados, numa cópia da agora ultrapassada lei europeia. A tutela equivocada destes dados pode fornecer, a quem detenha conhecimento suficiente para decifrá-los[5], a localização e os hábitos de qualquer usuário da internet, colocando em risco seu direito à segurança[6], presunção de inocência[7], à vida privada (privacidade)[8] e à livre expressão[9], todos direitos fundamentais, constantes da declaração universal dos direitos do homem.

Qual será então a solução normativa? R. Brownsword defende, por exemplo, que antes de estabelecermos normativas para o sigilo de dados, é preciso que se defina claramente os princípios que dão origem a este direito. Segundo ele, privacidade, processamento adequado de dados pessoais e confidencialidade são as raízes principiológicas do direito ao sigilo de dados, mas nem elas encontram definição clara.[10]

O que está em discussão aqui é um problema de segurança moderna. A quebra do sigilo de dados é capaz de expor fragilidades e diminuir a confiança em organizações e governos, o que é um problema de primeiro plano na atualidade, que, de apesar de sua importância, ainda é discutido em círculos bastante restritos.

No Brasil há um equivoco bastante comum: imaginamos que este é um problema de países ricos e desenvolvidos, o que não é verdade. O Exército brasileiro monitorou, por exemplo, as manifestações que tomaram as ruas do país em junho de 2013, inclusive com uma técnica de espionagem semelhante à utilizada pela NSA. Um software de fabricação nacional, em uso pelo Centro de Defesa Cibernética do Exército, filtrou informações postadas nas redes sociais e serviu para identificar os manifestantes que assumiram a linha de frente dos protestos contra a Copa do Mundo. Os dados produzidos foram enviados à Polícia Federal e às Secretarias de Segurança Pública nos estados onde ocorriam as manifestações. Estas informações foram noticiadas pelo *O Globo*, repassadas sem qualquer sombra de anormalidade general José Carlos dos Santos, chefe do Centro de Defesa Cibernética do Exército brasileiro. É bastante elucidativo o fato de que 23 destes manifestantes monitorados tenham sido posteriormente indiciados pelo judiciário fluminense. Assim como é preocupante que a “inteligencia” da policia tenha até investigado até o escritor Mikail Bakunin.

2023 - www.conjur.com.br - Todos os direitos reservados.

Os agentes estatais brasileiros cometem erros, como cometem os agentes do mundo todo. Mas aqui podemos observar a figura do “tira hermeneuta” tantas vezes lembrado. O problema é que o Brasil, diferente dos EUA, por exemplo, não mantém uma Corte Especial de Vigilância, responsável por autorizar ou não os grampos: qualquer juiz de primeiro grau pode autorizar, com base na lei lei 9.296/1996, tanto a quebra do sigilo telefônico de um suspeito, como pode, no mesmo pedido, requisitar a quebra do sigilo do “fluxo de comunicações em sistemas de informática e telemática”. A diferença é que a quebra do sigilo de dados expõe a intimidade do indivíduo em um grau ainda maior do que a quebra do sigilo telefônico, desde há muito critica no Brasil.

Com uma vigilância tão intensa os seus dados sabem mais de você do que você mesmo. A coleção indiscriminada de dados de suspeitos e não suspeitos pode dar aos Estados um poder desproporcional. Quando uma investigação é conduzida com dispositivos de geolocalização atuando em aplicativos do celular do suspeito, uma nova barreira é rompida: o sigilo de dados é algo muito maior do que a vigilância física ou telefônica.

Sem nos darmos conta, a sociedade de vigilância imaginada por George Orwell em 1949, na publicação de seu “1984” era inspirada nos regimes nazista e stalinista instala-se pouco a pouco, inclusive em sociedades democráticas como a brasileira, num cenário de controle social potencialmente muito maior do que o imaginado há 60 anos.

[1] CASTELLS, Manuel. Communication Power. Oxford University Press, New York, 2013. P.10

Ver também em CASTELLS, Manuel, Internet Galaxy: reflections on the internet, business and society. Oxford University Press. Oxford, 2001. P. 18

[2] ZAFFARONI, Eugenio Raul, OLIVEIRA, Edmundo, Criminology and Criminal Policy Movements. University Press of America: Lanham, 2013. P. 2

[3] RODRÍGUEZ, Víctor Gabriel, Tutela da Intimidade: perspectivas da atuação penal na sociedade da informação. São Paulo: Atlas, 2008. P.232

[4] “the Court is of the opinion that, by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.” Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, ECJ, 08/04/2014. Disponível em: http://www.mcgarrsolicitors.ie/wp-content/uploads/2014/04/CP140054EN.pdf

[5] O que vem sendo chamado de “datability”, a habilidade de possuir e manejar grandes quantidades de dados.

2023 - www.conjur.com.br - Todos os direitos reservados.

[6] Artigo 3º da Declaração Universal dos Direitos do Homem, ONU, 1948.

[7] Idem, Artigo 11.

[8] Ibidem, Artigo 12.

[9] Idem. Ibidem, Artigo 19.

[10] BROWNSWORD, Roger. Consente in data protection law:Privacy, Fair Processing and Confidentiality. In: DE HERT, Paul, GUTWIRTH, Serge, Data Protection in the case law of Strasbourg and Luxemburg: Constitucionalization in action, In: DE HERT, Paul, GUTWIRTH, Serge, NOUWT, Sjaak, POULLET, Yves, Reinventing data protection?. Springer: Bruxelas, 2014.P.97-98

Date Created
03/09/2014

2023 - www.conjur.com.br - Todos os direitos reservados.