Marcelo Bulgueroni: País está atrasado na proteção de dados pessoais

29/01/2013

Nos dias 9 e 10 de janeiro deste ano, um usuário do Twitter, utilizando o apelido "@nbdu1nder" publicou em um website clandestino dados pessoais de diversos nomes da política brasileira, sob a justificativa de fazer "justiça" com referência a situações de corrupção do poder público. Foram divulgados telefones fixos, celulares, endereços residenciais, CPF e RG, entre outros dados, de personalidades como José Genoino, José Dirceu e o ex-presidente da República Luís Inácio Lula da Silva. Esse tipo de prática, com pessoas famosas ou não, é bastante comum internacionalmente como método de desmoralização pública dos alvos.

O evento da publicação desses dados imediatamente abriu um intenso debate na mídia acerca da legalidade ou não da prática desse "hacker" —seria uma conduta ilegal publicar dados pessoais de indivíduos na internet, gerando claro incômodo e mesmo exposição a perigo em consequência disso?

Ainda que a prática claramente onere as pessoas que tiveram seus dados expostos, temos que analisar a legislação brasileira para determinar se houve violação. Pelo que temos em vigor, crime na publicação dos dados não há, pois o parágrafo 1º-A do artigo 153 do Código Penal é o que mais se aproxima à divulgação sem justa causa de informações sigilosas ou reservadas, assim definidas em lei. Voltaremos a essa definição a seguir.

Em abril deste ano, entra em vigor a Lei 12.737, de 30 de novembro de 2012, também conhecida por "Lei Carolina Dieckmann"[1], dedicada à proteção da privacidade. O fato ocorrido é anterior, mas caso estivesse em vigor o único crime que o "hacker" poderia ter cometido seria o de "invasão de dispositivo informático alheio", previsto no artigo 154-A, se é que se utilizou desse expediente para acessar os dados. A divulgação desses dados, que é que nos interessa, entretanto, não seria prevista. Os parágrafos 3º e 4º, responsáveis por tratar da divulgação dos dados obtidos, referem-se somente a dados sigilosos, definidos em lei. Ainda há o projeto do Marco Civil para considerar, que na forma em que segue sendo discutido não tratará desse assunto específico, oferecendo apenas uma proteção genérica à intimidade e privacidade em seu artigo 7º.

Não há definição em lei que diga que dados pessoais sejam sigilosos ou reservados. E, na prática, não o são, como podemos constatar ao avaliar a situação e utilização prática desses dados.

O endereço residencial e comercial de cada cidadão é encontrado na correspondência que trafega de mãos em mãos, quando não também em websites, redes sociais, listas telefônicas. Até no registro WHOIS de um domínio, algo bastante comum nos dias de hoje, se pode ter acesso ao nome completo do proprietário do domínio, seu endereço, e-mail e telefone de contato principal.

Dados um pouco mais sensíveis, como CPF, RG, CNPJ e outros já não são encontrados tão facilmente, mas são muitas vezes fornecidos de livre e espontânea vontade por usuários de internet que, ávidos por se conectarem a um novo portal de serviços, concordam com termos e condições de uso que preveem expressamente o compartilhamento de todas as informações fornecidas com outros parceiros comerciais do portal em que se cadastra, sem quaisquer restrições de confidencialidade. Isso quando o portal pede autorização, pois é comum o compartilhamento, autorizado ou não, desses dados.

Dados Pessoais não são sigilosos, pois, circulam, sendo exigidos por partes terceiras livremente para as mais diversas transações, sem qualquer requisito legal quanto à sua guarda e manuseio. Diferentemente de determinados dados específicos, como os pertinentes ao sigilo bancário, protegido expressamente por lei e que não podem ser acessados sem ordem judicial ou autorização do proprietário.

Mas como situar esse dado, sensível ainda que não sigiloso, e diferenciá-lo dos dados essencialmente públicos? Basta um tratamento legal adequado. Tratamento específico dado, apenas para dar alguns exemplos, em toda a União Europeia desde 1995, quando foi publicada a Diretiva[2] relacionada a esse tema, na Argentina desde 2000[3] e pelo Uruguai desde 2008 [4], sendo estes últimos dois exemplos oficialmente reconhecidos pela União Europeia como tendo proteção compatível com os níveis europeus para intercâmbio protegido de informações pessoais.

O Brasil não conta com qualquer dispositivo legal para a proteção e disciplina do acesso a dados pessoais. Temos alguns projetos de lei em (lenta) tramitação no Congresso Nacional, mas a melhor proposta seria um Anteprojeto de Lei para a proteção de dados pessoais e privacidade, de autoria do Executivo[5], já disponível para consulta na Internet. Esse projeto deverá ser apresentado ainda no primeiro trimestre deste ano para avaliação pelo Congresso.

Como o Legislativo idealmente deve agir como um espelho da sociedade, é redobrada a expectativa que o ocorrido neste janeiro possa acelerar a recuperação de um atraso de quase vinte anos na proteção de dados pessoais no Brasil, em meios informáticos ou não.

[1] http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:PT:HTML

[3] http://www.jus.gob.ar/media/33481/ley_25326.pdf

[4] http://www.datospersonales.gub.uy/wps/wcm/connect/829161004d0a999d861fcefd6066fd91/Descarg

[5]http://www.acessoainformacao.gov.br/acessoainformacaogov/publicacoes/anteprojeto-lei-protecao-dados-pessoais.pdf

Fonte: https://conjur.jumps.com.br/2013-jan-29/marcelo-bulgeroni-pais-atrasado-protecao-dados-pessoais/