ISSN 2447-1097

Direito & TI–Porto Alegre / RS www.direitoeti.com.br

EMERGENCY REQUEST DISCLOSURE: A POLÍCIA JUDICIÁRIA E AS SOLICITAÇÕES DE EMERGÊNCIA ÀS APLICAÇÕES DE INTERNET

Alesandro Gonçalves Barreto[1]

RESUMO

O artigo analisa tema de grande relevância para momento, qual seja, a possibilidade de obtenção de dados junto aos provedores de Internet para fazer cessar situações que envolvam risco de morte ou ameaça de grave lesão a terceiros. Diversas empresas de internet, em obediência à legislação americana, fornecem canais de comunicação com o intutito de repassar dados emergenciais à polícia. Cabe-nos amoldar essas possibilidades a fim de ter eficiência no atendimento de uma ocorrência policial.

Palavras-chave*: Emergência. Risco. Provedores. Internet.*

INTRODUÇÃO

A *Internet* tem demandado à polícia novos desafios na investigação de crimes cometidos em meio virtual. Longe são os tempos em que esse atendimento se restringia a um local de crime real. Hoje, em diversas ocorrências, esse local passou a ser virtual. A identificação do registro de conexão[i] ou de acesso a aplicações de *Internet*[ii], em que pese outros elementos informativos colhidos, é ponto crucial na individualização da autoria e materialidade delitiva desses delitos.

Nesse diapasão, o Marco Civil da *Internet*, ao estabelecer princípios, garantias e deveres para o uso da *Internet* no Brasil, condicionou o fornecimento desses registros e das comunicações privadas à expedição de ordem judicial[iii].

Por conseguinte, as investigações necessitarão de representação ao Poder Judiciário visando identificar, por exemplo, os protocolos de *internet*[iv] utilizados por determinado usuário. Excepcionalmente, há situações em que as aplicações de *internet* repassam dados diretamente aos órgãos encarregados da investigação criminal. Passaremos, então, a fazer análise dessa reserva, de emergência.

1 Delegado de Polícia Civil do Estado do Piauí e coautor dos livros Inteligência Digital e Manual de Investigação Cibernética à Luz do Marco Civil da Internet, ambos da Editora Brasport. Coordenador do Núcleo de Fontes Abertas da Secretaria Extraordinária para Segurança de Grandes Eventos nos Jogos Olímpicos e Paralímpicos Rio 2016. delbarreto@gmail.com.

ISSN 2447-1097

1. SOLICITAÇÕES DE EMERGÊNCIA

Nas situações de perigo de morte ou danos físicos graves a alguém, as aplicações de *internet* fornecem diretamente às autoridades policiais os dados necessários para fazer cessar esse risco iminente. Algumas delas fornecem informações ainda nos casos de terrorismo ou de criança e adolescente envolvido em situação de risco.

As solicitações de emergência somente podem ser realizadas por órgãos de persecução penal, não devendo, todavia, ser requerida diretamente por advogado ou representante legal. Para evitar fraudes ou pedidos desnecessários, urge a utilização de *e-mail* institucional.

Os provedores de *internet* fornecem essas informações baseados no ECPA – *Eletronic Communications Privacy Act*[v]. A lei de Privacidade das Comunicações Eletrônicas regula as expectativas de privacidade do cidadão americano, além da interceptação telefônica e telemática.

A excepcionalidade do fornecimento dos dados diretamente através dessas solicitações facilita, de sobremaneira, a celeridade no atendimento desse tipo de ocorrência. Imaginemos uma situação, por exemplo, de uma postagem em que haja risco de morte de usuário de determinada rede social. Caso fosse representado judicialmente para identificar o protocolo de internet atrelado ao conteúdo, talvez não houvesse tempo de atendimento adequado à vítima.

2. PROCEDIMENTO JUNTO ÀS APLICAÇÕES DE INTERNET

Como regra, solicitações devem ser bem claras e pontuais sobre a natureza da emergência, a necessidade de urgência no recebimento, a inexistência de outro meio mais célere para obtenção do dado e, quando possível, devem ser anexados arquivos ou *URLs* relacionadas ao fato. É importante frisar que esses requerimentos devem ser feitos excepcionalmente a fim de evitar pedidos desnecessários e que não sejam abrangidos pela reserva.

Passamos, então, a fazer uma análise de algumas redes sociais e de buscadores que disponibilizam aos órgãos investigativos meios hábeis a essas solicitações de emergência.

a) Google – a plataforma se limita a fornecer dados para fazer cessar as situações de emergência. As informações são repassadas diretamente nos casos de danos físicos graves a alguém, risco

de morte, sequestro ou ameaças de bomba. Há necessidade de demonstração da correlação entre o fornecimento de informações e impedimento do dano[vi].

b) Microsoft – as solicitações de emergência são limitadas às situações de sequestro, risco de morte, ameaças de bomba e de terrorismo. O pedido deve conter um resumo da emergência e ser redigido em papel timbrado e assinado pela autoridade policial[vii].

c) Facebook – a aplicação de internet disponibiliza, através da plataforma Records[viii], um meio para solicitar as informações de emergência nos casos que envolvam perigo iminente a uma criança, risco de morte ou de lesões graves para qualquer pessoa.

d) Yahoo – a empresa disponibiliza um formulário[ix] *online* para os casos de informações de emergência. Seu preenchimento deve ser claro no sentido de demonstrar que se trata de excepcionalidade. A demanda deve pontuar o risco de morte ou perigo de lesão grave, bem como a relevância dos dados para a solução do caso.

e) Twitter – a aplicação de Internet aceita os pedidos de emergência desde que haja boa-fé por parte do postulante e que os dados fornecidos devam evitar danos nas situações que envolvam risco de morte ou sérios danos a alguém. O método mais eficiente para fazer a denúncia é através do preenchimento de formulário *online*[x]. Há a opção de envio da solicitação através de fax[xi], desde que esteja em papel timbrado com as informações da autoridade policial, natureza da emergência e identificação de quem está sofrendo, nome do usuário e *url* do Twitter relacionadas às contas cujas informações são necessárias para evitar a situação urgente, informações dos *tweets* e sua correlação com a emergência.

f) LinkedIn – fornece as informações de emergência desde que haja indicação de situação excepcional e de boa-fé do requerente. O formulário de solicitação deve conter: nome do investigador e da instituição na qual está lotado, matrícula, e-mail e telefone de contato[xii]. Deve-se, ainda, descrever a natureza da emergência e demonstrar que o meio de solicitação normal é insuficiente para o caso sob investigação. Por fim, o solicitante deve individualizar o usuário da plataforma ou nome e respectivo endereço de e-mail e ainda relacionar as informações necessita para sanar a situação de emergência.

g) Pinterest – a empresa atenderá pedidos de informações de usuários do Pinterest nos casos de perigo de morte ou de lesões físicas graves desde que haja uma solicitação por e-mail[xiii]. As solicitações deverão ser encaminhadas através de formulário *online*[xiv].

h) Snapchat – o fornecimento dos dados do usuário em situação de emergência é condicionado aos casos de risco de morte ou lesão de natureza grave. A empresa disponibiliza atendimento tanto

por e-mail quanto por telefone[xv]. O pedido deve ser feito através de e-mail institucional, detalhando a situação de risco e as informações que serão úteis para resolvê-la. Para tanto, deverá indicar o nome do usuário, e-mail ou endereço de telefone do usuário Snapchat em que o conteúdo foi divulgado.

CONSIDERAÇÕES FINAIS

As relações sociais têm cada vez mais migrado para o ambiente virtual. Essa digitalização de nossas vidas demanda uma polícia capacitada para seu atendimento. Outrora, o atendimento emergencial de risco de morte ou lesão grave era feito pelo 190 ou 197. Hodiernamente, em alguns cenários, as vítimas estão situadas no Brasil enquanto os arquivos encontram-se hospedados em servidores espalhados pelo planeta e aplicações de internet sediadas nos Estados Unidos.

A polícia judiciária tem ao seu alcance a solicitação de emergência para obtenção de dados de usuários que estejam em situação de risco. Esse mecanismo permite ao policial o acesso às informações de usuário, protocolos de internet, dentre outros que auxiliam na interrupção do ato lesivo a determinada pessoa.

Insta realçar que essas solicitações só devem ser utilizadas em caráter extraordinário. Eventuais abusos cometidos nessas solicitações irão intricar futuros procedimentos circunstanciais.

Essa flexibilização dos provedores de *internet* em razão da legislação americana permite à polícia judiciária respostas rápidas e pontuais nessa nova realidade. Caberá ao policial conhecer e se adequar aos mecanismos colocados à sua disposição para rápida solução da ocorrência.

REFERÊNCIAS

18 U.S. Code § 2702 - Voluntary disclosure of customer communications or records. Legal Information Institute. Disponível em: <https://www.law.cornell.edu/uscode/text/18/2702>. Acesso em: 14. dez. 2016.

Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14. dez. 2016.

FACEBOOK. Central de Segurança. Informações para Autoridades Policiais. Disponível em: <https://www.facebook.com/safety/groups/law/guidelines/>. Acesso em: 14. dez. 2016.

GOOGLE. Transparency Report. Disponível em: <https://www.google.com/transparencyreport/userdatarequests/legalprocess/>. Acesso em: 14. dez. 2016.

LINKEDIN. Data Request Guideline. Atualizado em 05 mai. 2015. Disponível em: <http://help.linkedin.com/ci/fattach/get/6682760/1479502696/redirect/1/filename/Law_Enforcement_Guidelines_11_15_2015_9C7C.pdf>. Acesso em: 14. dez. 2016.

MICROSOFT. Law Enforcement Request Reports. Disponível em: <https://www.microsoft.com/about/csr/transparencyhub/lerr/>. Acesso em: 14. dez. 2016.

PINTEREST. Law Enforcement Request Guidelines. Disponível em: <https://help.pinterest.com/en/articles/law-enforcement-guidelines>. Acesso em: 14. dez. 2016.

SNAPCHAT. Law Enforcement Guideline. Última atualização: 11 out. 2016. Disponível em: <https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf>. Acesso em: 14. dez. 2016.

YAHOO. Law Enforcement Response Guidelines. Disponível em: <https://transparency.yahoo.com/law-enforcement-guidelines/us>. Acesso em: 14. dez. 2016.

TWITTER. Diretrizes para Autoridades Policiais. Disponível em: <https://support.twitter.com/articles/297661#14>. Acesso em: 14. dez. 2016.

[i] O conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados.

[ii] O conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

[iii] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

[iv] Código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais

[v] 18 U.S.C. § 2702 (b)(8): Exceptions for disclosure of communications.—A provider described in subsection may divulge the contents of a communication— to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for Disclosure of Customer Records.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

[vi] Email de contato da Google: juridicobrasil@google.com / lis-latam@google.com

[vii] Email de contato da Microsoft: lelatam@microsoft.com

[viii] www.facebook.com/records.

[ix] https://s.yimg.com/dh/ap/tyc/pdf/Yahoo_Emergency_Disclosure_Request_Form.pdf.

[x] https://support.twitter.com/forms/lawenforcement

[xi] Telefone de contato do Twitter para solicitações de emergência: 00 1 415-222-9958 a/c: Trust & Safety - Legal Policy.

[xii] O modelo de solicitação pode ser encontrado em http://help.linkedin.com/ci/fattach/get/6682760/1479502696/redirect/1/filename/Law_Enforcement_Guidelines_11_15_2015_9C7C.pdf

[xiii] lawenforcement@pinterest.com

[xiv] https://help.pinterest.com/en/law-enforcement

[xv] O formulário preenchido deve ser encaminhado através do e-mail lawenforcement@snapchat.com. Em horário não comercial, o requerimento pode ser feito através do telefone +1 310-684-3062. O modelo de formulário encontra-se disponível em https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf.