Paulo SantarÃ©m: A rastreabilidade no PL de Fake News

Na proposta de enfrentamento à desinformação (vulgo fake news), a controvérsia mais empacada quanto ao Projeto de Lei nº 2630/2020 (Lei Brasileira da Liberdade, Responsabilidade e Transparência na Internet) trata da rastreabilidade de mensagens instantâneas. Previsto no artigo 10 do texto aprovado pelo Senado e em análise na Câmara dos Deputados, o chamado "encaminhamento em massa" é defendido por pesquisadores como Pablo Ortellado, jornalistas como Pedro Dória e juristas como Ivar Hartmann e Kettemann e Ricardo Campos.

A demanda pela solução de ilegalidades tem sido colocada como força contraposta ao ideal de uma criptografia forte. Alegou-se, em muitas oportunidades, que alguma exceção à proteção de dados seria necessária para viabilizar o trabalho da segurança pública.

Um impasse político decorre da seguinte polarização: de um lado, o exame judicial e a punição de ilícitos civis e penais dependeriam de alguma autoridade, se necessário, no curso de uma investigação, poder ler qualquer mensagem ou informação criptografada. De outro lado, qualquer comprometimento da criptografia é rechaçado como destruidor de direitos individuais e da própria segurança pública, do respeito a direitos individuais e até mesmo da democracia.

Segundo um estudo de Harvard publicado em 2018 ("Abordagens políticas ao debate da criptografia"), a superação desse impasse depende de substituirmos situações hipotéticas pela consideração de questões práticas do mundo real. Pois, fora dos seriados ficcionais, não há relatos reais de uma mensagem secreta cuja revelação seria o único meio para salvar vidas e prender criminosos.

Uma abordagem pragmática precisa indagar sobre: 1) evidências empíricas dos benefícios de uma porta dos fundos; 2) a inexistência de outras soluções tecnológicas disponíveis; e 3) se o Direito autoriza a exigência desse tipo de brechas de segurança.

Os possíveis benefícios da vulnerabilidade devem ser mensuráveis a partir de estatísticas sobre o número de crimes não resolvidos ou criminosos que não foram processados em razão de as principais evidências disponíveis estarem criptografadas. Dados dos Estados Unidos apontam só 3,2% de escutas telefônicas frustradas por criptografia forte. Até o momento, nenhum levantamento desse tipo parece ter sido feito no Brasil.

Alternativas tecnológicas parecem existir. Casos como o *iPhone* em San Bernardino e o Inquérito 4781 no STF mostram ser possível investigar ilícitos sem exigir por lei fraquezas embutidas em sistemas e *apps*. Além de as pessoas nem sempre usarem todo o aparato disponível, as medidas de segurança largamente oferecidas exigem constante atualização e solução de falhas recém-descobertas.

E, se levado a sério (como adaptado por Bruno Bioni e Rafael Zanatta), o arcabouço constitucional que assegura sigilo de dados e comunicações, liberdade de expressão e de acesso à informação, e presunção de inocência, não combina com a imposição de fragilidades tecnológicas como uma regra geral. A generalização tirânica (adjetivo do jurista Lênio Streck) de uma medida contrária ao livre aprimoramento de mecanismos de proteção de dados é desproporcional e desnecessária: atingiria indistintamente todo mundo (incluindo agentes políticos, juízes e as forças policiais) e não garantiria o sucesso das investigações. Diversamente dos sistemas engessados pela lei, praticantes de ilícitos dolosos teriam incentivos claros para inovar nas formas de atuação e escapar impunes.

Basta de exercícios mentais sobre exemplos alegóricos ou caricatos. Quem defende a ideia de um monitoramento sistemático de metadados de mensagens em grupo, ou qualquer outra proposta que fragilize a segurança oferecida por criptografia forte, precisa começar a responder perguntas práticas, com base em números da vida real.

Um ponto silente não declarado seria a intenção de derrubar o presidente Jair Bolsonaro no contrapé. A demonstração de que uma rede de desinformação se armou em seu favor seria o caminho para afastá-lo da presidência. Nessa linha, a rastreabilidade poderia ser o fio no labirinto que nos guiaria de volta à democracia. Como se frases despreocupadas em informar não estivessem sendo ditas e repetidas, em toda sua gravidade, à razão de mais de uma por dia, e publicamente. A ideologia bolsonarista ecoa na população. A estratégia de desestruturar nosso ordenamento jurídico não é razoável, nem promissora. Ou como ponderou Danilo Doneda (IDP), *"temo que a gente esteja perdendo muito tempo com soluções para o passado, para as eleições de 2018"*.

Precisamos de políticas públicas preocupadas com problemas concretos da vida social no Brasil. Nossa polícia precisa deixar de reproduzir o racismo estrutural, na mesma medida em que as pessoas que vestem as fardas têm o direito de serem expostas ao risco tão alto de morrer. Em um cenário de abusos, matança e violência, com recursos limitados e pouco ou nenhum treinamento para lidar devidamente com as inovações da sociedade da informação, será mesmo que a resposta passa pela previsão legal de menos garantias jurídicas para toda a população brasileira (com potencial para perseguição de grupos vulneráveis, como lembrou Raquel Saraiva)? Pela imposição jurídica de um esquema tecnológico sabidamente falho e que não se sabe efetivo? Pela desconsideração de meios investigativos particularizados e menos abrangentes do que a obrigação de produzir permanentemente provas mesmo antes de qualquer acusação?

Tais aspectos absolutamente práticos têm sido ruidosamente ignorados. Eu e Diego Canabarro enumeramos dez. Até o momento, o silêncio segue sendo a nossa resposta. Parece que ao desenterrar a cabeça das nuvens de hipóteses irreais, a defesa teórica do artigo 10 do PL 2630 teme se ver muito distante da realidade. Pode ser doloroso para algumas teorias, mas a política não pode deixar de cair na real: só a criptografia forte permite, ao mesmo tempo, a efetiva proteção legítima de dados e a tomada de medidas democráticas de segurança pública e satisfação de direitos individuais violados.