LGPD: LEGAL GROUNDS FOR PRIVACY DESIGN

PROPOSTA PARA LIDAR COM CONTAS INAUTÊNTICAS

Ricardo Campos, Juliano Maranhão, Juliana Abrusio
Diretores do instituto LGPD

Uma forma de evitar que perfis em redes sociais e outros serviços virtuais sejam usados para prática ilícita é tornar possível a confirmação da identificação do responsável pela gestão destas contas inautênticas. Todavia, a exigência de que todos os usuários de redes sociais confirmem sua identidade e localização, no momento de abertura de cada conta seria desproporcional, sob a perspectiva da privacidade individual. Não está claro de que forma o custo gerado para coleta e processamento de todas essas informações seria adequado e necessário para o exercício da atividade.

Em sua esmagadora maioria, as redes sociais são frequentadas por pessoas autênticas que não utilizam a conta com finalidade ilícita ou de desinformação sistemática.[1] Prejudicar a privacidade de muitos, em função do ilícito praticado pela minoria parece excessivo. Vale lembrar que, há poucas semanas, o Supremo Tribunal Federal considerou inconstitucional, por desproporcional, a coleta de endereço e telefone de todos os usuários das empresas de telefonia móvel para fins estatísticos da Fundação IBGE. A exigência de confirmação da identificação para todos os usuários fere o princípio da necessidade previsto no art. 6º, III, da Lei Geral de Proteção de Dados Pessoais (LGPD), segundo o qual, o tratamento de dados pessoais[2] deve ser limitado ao mínimo necessário para atingir suas finalidades.

É inquestionável a legitimidade do combate aos difusores de desinformação, atrás da qual escondem-se, na maioria das vezes, crimes de diversas proveniências. Os dados que serão coletados dos usuários legítimos não contribuem para a identificação das contas inautênticas, e podem gerar riscos, caso os dados de identificação dos usuários legítimos sejam vazados ou utilizados de maneira indevida.

Há, contudo, uma forma de identificar os responsáveis por ilícitos sem interferir excessivamente no modelo de negócio e na privacidade dos usuários, já experimentado nas práticas internacionais: exigir a identificação apenas das contas sob suspeita de inautenticidade, seja por denúncias de usuários, seja pelo monitoramento e moderação feita pelas próprias plataformas.

A confirmação da identificação passa, assim, a ser seletiva, e colocada como condição para o exercício da defesa pelo usuário da conta suspeita. Enquanto o usuário não se identificar para se defender, sua conta ficará suspensa. Após longo período sem confirmação da identidade,

---

[1] Como aponta o estudo de Onur Varol e coautores, Online Human-Bot Interactions: Detection, Estimation, and Characterization, ICWSM 2017.

[2] A identificação do usuário necessariamente envolverá dados pessoais, de acordo com o artigo 5º, I, da LGPD.

a conta suspensa será excluída. Caso o usuário autentique sua identidade e recorra da suspensão de sua conta, o provedor da aplicação deverá decidir em definitivo sobre a exclusão, em prazo exíguo e hábil para conter prejuízos. Obviamente, por força constitucional, restará o recurso ao Poder Judiciário, pelo usuário indignado pela decisão adotada pela plataforma ou pela instituição de autorregulação.

O modelo também protege a liberdade de expressão na sociedade, uma vez que postagens defensáveis não encontrarão resistência quanto à confirmação de identificação por parte de seus autores. Esse modelo encaixa-se bem a uma estrutura de autorregulação, mas também é cabível exigi-lo diretamente como procedimento interno a ser adotado pelas provedoras de aplicação.

A solução proposta não demandará grandes adaptações em plataformas tecnológicas já existentes, já que muitas redes sociais já adotam procedimentos similares, especialmente para questões de infrações de direitos autorais por conteúdo postado por terceiros. Em outro exemplo, a rede social Twitter se reserva o direito de limitar ou até mesmo bloquear as contas de usuários que apresentem comportamento anômalo ou suspeito,[3] exigindo que estes usuários passem por um processo de verificação de seu e-mail ou conta de celular. Seria possível, então, adotar um mecanismo similar para exigir o envio dos documentos que comprovem a identidade do usuário, evitando o uso malicioso da conta até que seja possível identificar o responsável para fins de eventual responsabilização.

Esta abordagem, além de diminuir o ônus sob os usuários legítimos de boa-fé, e permitir o desenvolvimento de novos meios tecnológicos para o combate eficiente às contas inautênticas, está em linha com as práticas internacionais de enfatizar a responsabilidade do intermediário em criar mecanismos eficientes para evitar a lesão de direitos de terceiros. Um exemplo pode ser visto na regulação europeia de direito de autor e propriedade intelectual presente nas Diretivas 2001/29/CE, 2004/48/CE e 2019/790. Na Diretiva 2019/790 da União Europeia, por exemplo, o Artigo 17(4) estabelece a obrigação de que os provedores de serviço digital estabeleçam mecanismos para remover conteúdos protegidos por direito autoral em caso de solicitação do detentor dos direitos. O mesmo ocorre na terceira linha do art. 11 da Diretiva europeia 2004/48/CE e art. 8 inciso 3 da Diretiva europeia 2001/29/CE. [4]

Não se trata aqui de adotar o modelo de responsabilização por *notice and take down,* ou *notice and notice* (modelo canadense) em relação a casos como *fake news*, mas apenas de usar técnica semelhante para se tornar mandatória a confirmação da identificação, algo como *"notice and authentication"*, valendo notar, que essa autenticação será feita perante a plataforma,

[3] https://help.twitter.com/pt/managing-your-account/locked-and-limited-accounts
[4] Veja também nesse sentido o enunciado 59 da 2001/29/EG.

apenas, mantendo-se os dados adicionais resguardado perante terceiros. Mas é importante demarcar que a suspensão da conta até a identificação pode ocorrer não só por notificação, mas também pela iniciativa da própria plataforma em sua atividade moderadora de conteúdo e de atividades artificiais de contas voltadas para a propagação de desinformação, o que já ocorre.

Ou seja, com a identificação o problema é resolvido e o usuário defende sua postagem. Caso o usuário não se identifique (com prazo longo de suspensão para não prejudicar usuários de boa-fé), a conta será excluída. A conta também poderá ser identificada segundo interesse de agir da vítima, por meio de ordem judicial quebra do sigilo dos registros eletrônicos vinculados àquela conta, o que é possível por força da obrigação legal prevista no art. 15 do Marco Civil da Internet, que impõe o dever de guarda dos dados de registros de acesso à aplicação. Vale notar que, para casos configurados, em tese, como crimes, as autoridades ainda contarão com uma série de informações adicionais para a persecução criminal, em função dos relatórios periódicos enviados pelos provedores de redes sociais às autoridades para cumprir com seus deveres de transparência.

Poder-se-ia, nesse ponto, contra-argumentar que os criminosos não confirmarão sua identificação, terão a conta derrubada, e passarão, ato contínuo, para abertura de nova conta. Porém é importante lembrar que o expediente ilícito praticado pelos meios eletrônicos, notadamente pelas redes sociais, envolve a assim chamada “engenharia social”. Em outras palavras, o criminoso para concretizar seu desiderato, necessita de mais do que apenas uma conta de usuário. Exemplos: no caso de engodo, o criminoso precisa desenvolver uma aparência de verdade e credibilidade, com um histórico de postagens, tempo de conta, troca de mensagens etc. No caso de *fake news*, para realmente cumprir seu papel são necessários, pelo menos, três elementos: “persona” (conta de usuário), notícias falsas e engajamento. Esse último elemento demanda tempo, de modo que ter a conta derrubada frustraria, ou pelo dificultaria bastante, a prática de propagação de desinformação.

Por fim, é importante destacar que, no modelo geral aqui proposto e defendido, o intermediário não é responsabilizado como autor ou coautor da infração de terceiros que usam do serviço de sua plataforma, em consonância com as mais modernas posições jurídicas atualmente existentes, no Brasil (Marco Civil da Internet e jurisprudência consolidada) e no direito comparado. É responsabilizado, por culpa, apenas na omissão em não cumprir os deveres procedimentais ao seu alcance para a moderação da plataforma de comunicação. Por esse motivo, a plataforma não será responsabilizada civilmente por sua decisão acerca da manutenção ou exclusão da conta, ainda que sua decisão seja revertida posteriormente pelo Poder Judiciário.

PROPOSTA DE REDAÇÃO DO ARTIGO SOBRE CONTAS INAUTÊNTICAS

Art. X: O provedor de aplicação ou instituição de autorregulação deverá criar procedimento em plataforma digital, de fácil acesso e simples visualização, para apuração de denúncias contra contas supostamente inautênticas, incluindo mecanismo para confirmação da identificação dos usuários e que propicie oportunidade de defesa quanto a conteúdo postado ou atividade de impulsionamento e compartilhamento.

§ 1º Em caso de denúncia fundamentada de veiculação de desinformação ou, independentemente de denúncia, a gestão de moderação da plataforma identifique movimentação atípica e artificial ou suspeita de propagação sistemática de desinformação, o provedor de aplicação deverá, em até 48 horas, após avaliação preliminar do conteúdo, suspender a conta sob avaliação e notificar o usuário suspeito, por email e no próprio aplicativo, para que o mesmo providencie a confirmação de sua identificação pessoal, pelo fornecimento de dados adicionais.

§ 2º O titular de conta suspensa terá o direito de recorrer ao provedor de aplicação, em até 120 dias, devendo, para tanto, submeter-se ao procedimento de identificação nos termos do §1º deste artigo.

§ 3º Caso o usuário notificado não providencie os elementos de identificação pessoal requisitados no prazo acima indicado, a conta deverá ser removida da aplicação.

§ 4º Após recurso pelo usuário, cuja identificação for confirmada, o provedor de aplicação ou a instituição de autorregulação deverá adotar decisão final sobre remoção da conta em até 4 dias, sem prejuízo do direito de recurso ao Poder Judiciário.

§ 5º O provedor de aplicação não será responsabilizado por sua decisão de suspensão ou pela decisão final de manter ou excluir a conta suspeita, desde que adotados os procedimentos propostos neste artigo, ainda que sua decisão seja posteriormente revertida pelo Poder Judiciário.

§ 6º Observadas as garantias de proteção de dados pessoais e do devido processo legal, os provedores de aplicação deverão manter os dados de confirmação de identificação armazenados e compartilhá-los, em caso de requisição por autoridade competente, nos termos da Lei 12.965/2014.

§ 7º Durante o período legal de campanha eleitoral, o prazo para suspensão de contas suspeitas será de 24 horas e de decisão sobre recurso de usuário suspeito será de 48 horas.