O impasse das contas inautênticas na regulação das redes

09/06/2020

Dentre as propostas presentes no projeto de lei sobre *fake news* e emendas substitutivas apresentadas gerou forte polêmica a obrigatoriedade de confirmação de identidade na abertura de contas nas redes sociais.

A exigência de que todos os usuários de redes sociais confirmem sua identidade e localização, no momento de abertura de cada conta parece desproporcional, sob a perspectiva da privacidade individual.

Seus defensores apoiam-se em dois argumentos principais. Primeiro, que a Constituição proíbe o anonimato. Segundo que a confirmação da identidade no momento de abertura da conta seria a única forma de impedir a atividade das chamadas contas inautênticas, aquelas direcionadas à propagação de desinformação nas redes.

Quanto ao primeiro argumento, é importante esclarecer que não há na Constituição a imposição obrigação geral de identificação como condição para qualquer manifestação pública de pensamento. A vedação ao anonimato aparece como ressalva à manifestação pública como condição para preservar a possibilidade de responsabilização do discurso ilícito, lesivo à honra à imagem e a vida privada.[1] Mas não se pode, em nome da privacidade, anular o próprio anonimato, que é uma ferramenta importante para o exercício da liberdade de expressão.

Quanto ao segundo argumento, embora não haja dúvidas quanto aos vilões a serem combatidos, é fundamental partir da premissa de que, em sua esmagadora maioria, as redes sociais são frequentadas por pessoas autênticas que não utilizam a conta com finalidade ilícita ou de desinformação sistemática.[2] 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[3] deve ser limitado ao mínimo necessário para atingir suas finalidades.

Há, contudo, uma forma de identificar os responsáveis por ilícitos sem interferir excessivamente no modelo de negócio ou na privacidade dos usuários e assegurando o mandamento constitucional de preservar a responsabilização do discurso ilícito: 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 fica suspensa. Após período sem confirmação da identidade, a conta suspensa é 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.

A solução não demandaria 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,[4] 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. [5]

Não se trata aqui de adotar 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 seria feita perante a plataforma, apenas, mantendo-se os dados adicionais resguardado perante terceiros, a não ser que o ofendido valha-se de ordem judicial para 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. A suspensão da conta até a identificação poderia ocorrer não só por denúncia, mas também pela iniciativa da própria plataforma em sua atividade moderadora de conteúdo e de atividades artificiais e atípicas de contas cuja autenticidade recai fundada suspeita.

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". No caso de engodo, o agente 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.

Nesse modelo, o intermediário não seria 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, o intermediário seria 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 deveria ser responsabilizada civilmente por sua decisão acerca da manutenção ou exclusão da conta, ainda que sua decisão seja revertida posteriormente pelo Poder Judiciário.

[1] MARANHÃO, Juliano; CAMPOS, Ricardo. Fake news e autorregulação regulada das redes sociais no Brasil: fundamentos constitucionais. In: Fake news e Regulação. Coordenadores: Georges Abboud; Nelson Nery Jr. e Ricardo Campos. 2ª edição, São Paulo: Thomson Reuters Brasil, 2020.

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

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

[4] https://help.twitter.com/pt/managing-your-account/locked-and-limited-accounts

[5] Veja também nesse sentido o enunciado 59 da 2001/29/EG.

Fonte: https://conjur.jumps.com.br/2020-jun-09/direito-tecnologia-impasse-contas-inautenticas-regulacao-redes/