Novo Projeto de Lei das Fake News 3063/2020: 10 pontos que merecem atenção antes de qualquer votação

O que o legislativo brasileiro não pode desconsiderar ao tratar de um PL sobre a possível desinformação na Internet.

Em 02 de junho de 2020 foi apresentado um novo Projeto de Lei que institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. A norma projetada destina-se às redes sociais e serviços de "mensageria privada" que ofertam serviços de Internet, com o escopo de desestimular o abuso ou a manipulação destes, dando causa a danos individuais ou coletivos.

Não se aplica ao provedor de aplicação de redes sociais com menos de dois milhões de usuários registrados. Logo, é evidente o foco da Legislação para grandes aplicações como Twitter, Facebook, WhatsApp, Instagram e outros grandes serviços populares no Brasil e mundo, campos de batalha digital em período eleitoral. Sua aplicabilidade também se dá a empresas estrangeiras, desde que haja pelo menos uma integrante do grupo econômico presente no Brasil.

Os objetivos são contemplados no artigo 3 o ., como o fortalecimento do processo democrático com base no combate ao comportamento "inautêntico", distribuição artificial de conteúdo e fomento à diversidade de informações. Em seu artigo 4º, define o que seria uma conta "inautêntica", conta essa, criada ou usada com o propósito de assumir identidade inventada ou de terceiros para enganar o público, ressalvados o direito à pseudonímia, bem como o explícito ânimo humorístico ou de paródia. Do mesmo modo, descreve o que

seriam “contas automatizadas”, como contas geridas por qualquer programa de computador ou tecnologia para simular, substituir ou facilitar atividades humanas na distribuição de conteúdo em aplicações de internet ou aquelas geridas por ação preponderantemente humana e que complementam a atuação automatizada da conta, ainda que esporadicamente.

A legislação projetada preocupa-se com a criação de “redes de distribuição artificial”, caracterizadas como sendo um comportamento coordenado e articulado de contas automatizadas ou por tecnologia não fornecida pelo provedor de aplicação, com o fim de implantar de forma artificial a distribuição de conteúdos.

No artigo 5º, simplesmente informa que os provedores de aplicação de internet deverão adotar medidas para vedar contas inautênticas, contas automatizadas cujo caráter automatizado não foi comunicado aos referidos provedores. Ainda, em seu artigo 6 o , inclui diversas atividades e deveres para as redes sociais, dentre as quais medidas que demandam levantamento de dados
excessivos e desnecessários para o efetivo combate às Fake News. Chega a anotar como obrigatório relatório com o “número total de redes de distribuição artificial” detectadas. Ora, será preciso uma perícia em informática acurada, e ainda assim, receia-se que será temeroso demais às redes sociais terem que rotular um grupo de perfis como uma “rede de distribuição artificial”.

O usuário passa a ter o direito de ser notificado pela própria rede social, sempre que ocorrer um processo de análise de conteúdos e contas violadoras. Este poderá, nos termos do art. 8º, contestar eventual denúncia de conteúdo irregular. Do mesmo modo, são previstos recursos das decisões, nos termos do art. 9º do Projeto de Lei.

A norma assegura que em caso de conteúdos que tenham sido equivocadamente identificados como irregulares ou violadores

dos padrões do provedor de aplicações, caberá ao mesmo reparar o dano, informando o erro de maneira destacada e garantindo a exposição da correção, no mínimo, aos usuários inicialmente alcançados. Caso ocorra a revisão judicial de conteúdo tornado indisponível, assegura em seu art. 11 que a rede social deverá substituir o conteúdo tornado indisponível pela ordem judicial que deu fundamento à correção. Destaca-se que a nova versão do PL veda a indisponibilização de conteúdos com fundamento na própria lei, exceto em casos de decisão judicial.

Interferindo nos serviços de mensagens privadas, o regulamento ainda tenta limitar o número de encaminhamentos de mensagens a usuários e grupos e o número de membros dos mesmos. Diante do art. 14, o Telegram, por exemplo, encontrará um problema no seu modelo de negócios, permitindo grupos com centenas de usuários. O usuário deverá sempre dar permissão
prévia antes de receber uma mensagem de serviço de comunicação em massa nos mensageiros, o que impõe também medidas técnicas por parte de inúmeros aplicativos.

Proíbe-se, no artigo 15, o uso e a comercialização de ferramentas externas aos provedores de aplicação de mensageria privada, voltadas ao disparo em massa de mensagens. Esta questão pode interferir em inúmeros negócios lícitos hoje existentes, macros, automatizadores, chatbots e outros recursos. Muitas ferramentas não tem como fim "o envio" de mensagens em massa, mas possuem a função, para usuários cadastrados e sem qualquer finalidade de espalhe de Fake News.

Percebe-se, por parte do legislador, igualmente, uma tentativa de se "descobrir à fórceps" quem começou uma corrente de possível "Fake News" nos serviços de mensageria privada, uma vez que o artigo 17 estabelece que o provedor de aplicação que apresenta funcionalidade e o reencaminhamento similar de conteúdos, deve guardar os registros da cadeia de
reencaminhamentos até sua origem, pelo prazo mínimo de 1 (um) ano, resguardada a privacidade do conteúdo das mensagens, podendo esses registros ser solicitados mediante ordem

judicial nos termos da Seção IV da Lei 12.965 de 2014. A norma, no entanto, não trata explicitamente da proibição de novos compartilhamentos de conteúdos indevidos, a partir da extração de metadados dos arquivos e seu cheksum, medidas aliás determinadas em alguns casos judiciais no país.

Em relação aos conteúdos impulsionados, os usuários passam a ter direitos, dentre os quais, o de saber quais as fontes de informação e quais os critérios utilizados para a definição de público alvo do conteúdo que teve contato. Basicamente, repisando parte do que já era disposto na Lei 12.965 de 2014, a Lei projetada destina sete artigos para tratar da atuação do Poder Público, que deverá incluir capacitação para o uso consciente da internet e deverá realizar campanhas sobre a importância do combate ao comportamento inautêntico na Internet.

As penalidades para o descumprimento estão previstas no artigo 29 do projeto e não excetuam sanções civis, criminais ou administrativas. As penalidades são advertência, multa e suspensão temporária das atividades. Nesta versão, não existe a penalidade de proibição das atividades.

Caberá, ainda, ao Comitê Gestor da Internet do Brasil, definir um grupo de trabalho multissetorial que deverá estabelecer proposta legislativa que conceitue "conteúdo desinformativo", bem como apresentar as formas de combate a desinformação a partir de boas práticas internacionais em estudo. Este grupo multissetorial teria 1 (um) ano, a partir da publicação da Lei, para apresentar a proposta.

Passa a ser considerada violação à Lei de Improbidade Administrativa o fornecimento de acesso às contas de redes sociais de órgãos públicos à administradores externos ou que não tenham relação contratual com a administração pública, e também o emprego de recursos públicos para condutas que violem a Lei Brasileira de Liberdade, Responsabilidade e Transparência na

Internet (Art. 11, XI e XII).

Do mesmo modo, a Lei das organizações criminosas (12.850) é alterada para também abranger às organizações formadas para a criação e ou operação de contas inautênticas, contas automatizadas não identificadas e ou redes de distribuição artificial não identificadas por meio do emprego de recursos financeiros e técnicos que praticam ilícitos.

Por fim, a norma exige que as redes sociais e mensageiros nomeiem mandatários judiciais no Brasil, aos quais serão dirigidos os atos processuais decorrentes desta Lei. Feito este resumo dos principais pontos do novo PL, ao qual está se impingindo um ritmo desproporcional à atenção que um projeto desta natureza merece, elencamos 10 (dez) pontos de atenção e consideração, antes de qualquer votação e que demandam esclarecimentos sob pena de consequências gravíssimas:

1) Existe grande risco a aplicativos que não usam contas automatizadas, mas utilizam tecnologias conectadas às redes sociais, uma vez que podem ser consideradas “rede de distribuição artificial”. Como se avaliará a finalidade destes aplicativos? Quem definirá o que realmente é conteúdo artificial? Como as redes farão este papel?

2) As medidas para a vedação de contas “automatizadas” previstas no artigo 5º da legislação são genéricas, não definidas, onerosas e podem implicar na exclusão de conteúdos e perfis legais, isto porque um perfil real ou serviço poderá automatizar alguma tarefa em redes sociais e sem finalidade de praticar desinformação, o que poderá gerar um falso positivo nos registros da rede social.

3) As medidas para a verificação de contas inautênticas já existem hoje em grande parte das redes sociais, porém, não existe o monitoramento prévio, o que é salutar, e somente quando provocado judicialmente os provedores agem em respeito às disposições do Marco Civil da Internet. O Twitter, por

exemplo, faz um questionário prévio antes liberar acesso à sua API. Medidas automatizadas poderão implicar em remoções de perfis legítimos, para pesquisas ou autorizados pelas pessoas reais e na limitação de direitos.

4) O relatório de dados que os provedores de aplicação deverão produzir a cada três meses possuem dados excessivos e desnecessários. Como as redes sociais poderão identificar "redes de distribuição artificial"? Qual critério? Qual metodologia e parâmetros para estas conclusões? Como aplicar na prática esta disposição legislativa?

5) Como uma rede social irá lidar com contestações e recursos de pessoas envolvidas em processos de notificação irregular? A rede social passará a julgar conteúdos? Quais as responsabilidades de um julgamento que exclua liberdade de expressão ou opinião? Não se está criando redes policialescas?

6) Como ficará a responsabilidade das redes sociais, a partir da inserção do art. 13 da Lei da Responsabilidade na Internet, quando algoritmos automaticamente reduzirem alcance de conteúdos ou removerem os mesmos? O artigo estabelece que é vedada a indisponibilização de conteúdo com fundamento nesta Lei, exceto por decisão judicial específica e fundamentada.

7) Ao proibir sistemas não oferecidos pelos mensageiros e que permitem o disparo de mensagens em massa, como lidar com serviços legais oferecidos por chatbots por exemplo, onde é possível enviar "broadcasts" aos usuários que optaram por receber os
referidos conteúdos? É possível considerar todos os serviços de disparo em massa como ilegais? E se o usuário concordou com o recebimento?

8) Como estender o conceito de "registros de acesso à aplicação" definidos no Marco Civil da Internet, para englobar também os tais "registros de cadeia de reencaminhamento" previstos na legislação projetada? O que seria este registro?

Quais campos o compõe? Estaríamos tratando de data, hora, ip, número telefônico e fuso horário em ordem crescente dos encaminhamentos, desde a primeira publicação no serviço ou mensageiro? Quais os riscos à privacidade dos usuários?

9) Como interpretar um conteúdo desinformativo, se o grupo multissetorial que irá definir seu conceito, terá um ano, após a edição da norma, para defini-lo? Como se produzirá a prova de improbidade administrativa para identificar que agentes públicos cederam a administração de redes sociais a terceiros sem contratos com a administração pública?

10) Como definir "desinformação" de forma clara e justa? Como não tratar usuários de internet como potenciais infratores?

Não há dúvidas que a estas primeiras questões, muitas outras são acrescentadas por associações, entidades de Direito Digital, peritos em informática, cientistas da informação, provedores de aplicações, pesquisadores e sociedade em geral.

Como se verifica, o Projeto de Lei retirado de pauta (2630/2020) trazia uma série de questões polêmicas e exigência de dados excessivos, como documentos de identidade para criação de perfis, além de enaltecer a responsabilização das plataformas, o que confrontava o Marco Civil da Internet e poderia estimular as redes a controlarem conteúdos das redes sociais e ampliar a censura.

Não obstante, a nova proposta, mais amena, também apresenta riscos e pontos que dependem de esclarecimentos e maior tempo de análise, e como concebida, ao obrigar as redes a classificarem e detectarem quem é bot e quem não é, pode gerar um ambiente perigoso e ainda mais nocivo a direitos e garantias fundamentais. Um projeto, com tantos pontos a serem esclarecidos, como o
presente, não pode, de forma alguma, tramitar à toque de caixa. Um amplo debate, que enfrente os quesitos aqui levantados, com dilatada participação da sociedade civil, é

fundamental. Trata-se, aqui, de um tema sensível a todos, como impactos diretos em direitos e garantias fundamentais. A pressa é inimiga, e poderá culminar em graves consequências à inovação, liberdade de expressão e informação e a outros direitos.

A Pandemia do Coronavírus [COVID-19] e questões relevantes envolvendo Proteção de Dados Pessoais

Durante a pandemia do Novo Coronavírus, é evidente que o tratamento de dados, incluindo pessoais, se torna relevante ao servir de suporte para a tomada de decisões que auxiliam na mitigação de outros riscos, redução dos danos e no combate a pandemia.

Na China, de acordo com o jornal chinês *South China Morning Post*, dados pessoais e sensíveis foram coletados de maneira massificada sem a conveniente autorização, acarretando assim, em uma preocupação global com a privacidade, em relação aos cuidados necessários e a manipulação adequada de dados nesta época.

Na

Itália e outros países da Europa, já se fala na cooperação das operadoras de telefonia móvel com o Governo, através do fornecimento de dados, aparentemente de forma “anonimizada”, capaz de identificar concentrações em zonas consideradas de risco. Quais dados a mais são coletados? Permanecerão por quanto tempo nas bases de dados? Qual a consciência do cidadão e titular de dados a respeito?

Inúmeros cientistas da informação, de dados, profissionais da saúde e da tecnologia da informação realizam o tratamento de dados pessoais com a finalidade de oferecer serviços à população e auxiliar as políticas na atuação do poder público no combate ao COVID-19.

O tratamento de dados pessoais sensíveis é descrito no art. 11 da LGPD, que prevê, salvo hipóteses legais, o consentimento do titular, de forma especifica e destacada. Contudo, a LGPD estabelece em seu artigo 4°, inciso III que a Lei não se aplica ao tratamento realizado para fins exclusivos da segurança pública, no entanto, esta temática deverá ser regulamentada, nos termos da Lei.

Vale salientar a Lei 13.979/2020, que foi criada para enfrentamento do Covid-19, prevendo o compartilhamento de dados de pessoas infectadas a órgãos públicos de

saúde, assim estabelecendo:

Art. 5º Toda pessoa colaborará com as autoridades sanitárias na comunicação imediata de:

I – possíveis contatos com agentes infecciosos do corona vírus;

II- circulação em áreas consideradas como regiões de contaminação pelo coronavírus.

Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.

§ 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.

§ 2º O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais.

A Legislação não serve para derrogar a LGPD que, embora se torne aplicável

somente em agosto de 2020 (caso não seja prorrogada), já tem seus princípios e premissas de tratamento conjeturadas por autoridades em inúmeros casos no país.

Neste sentido, o consentimento do titular (que pode ser um cliente, paciente ou empregado) para o tratamento de seus dados pessoais de saúde, poderá ceder espaço, em situações específicas, a outras premissas legais, dentre elas, a proteção à vida ou à incolumidade física do titular ou de terceiros. Do mesmo modo, poderá ocorrer o tratamento para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais da área, serviços de saúde ou autoridade sanitária, conforme previsão da Lei 13.853/2019.

O tratamento de dados pessoais de saúde, que pode ser realizado por meio de algoritmos, aplicações, cruzamento de dados e outras operações de tratamento, poderá se dar com base nas premissas legais acima identificadas, contudo, deverá ser realizado de forma responsável, limitando-se apenas aos dados necessários para o enfrentamento da crise, respeitando a finalidade, adotando princípios para a minimização dos referidos dados, sobretudo, com a adoção de práticas de *privacy by design* na construção destes sistemas de tratamento de dados.

Vale ressaltar que aquele tratamento de dados que não respeitar a finalidade

especificada, de combater o vírus, auxiliar o Estado no seu papel ou trazer avanços, prevenção e apoio aos cidadãos, poderá ser considerado irregular, passível de reparação, devendo-se cogitar, também, os casos envolvendo a discriminação de pacientes confirmados diante de falhas de segurança que expuserem os dados, compartilhamentos indevidos, diante de operações de tratamento não autorizadas, ou ainda os danos causados àqueles forem expostos à tomada de decisões a partir da exposição indevida de dados pessoais relativos à sua saúde.

Não se pode olvidar que o titular tem direito de conhecer as operações de tratamento realizadas a seu respeito e não deve ser exposto e sofrer discriminação. A exemplo, a Autoridad Nacional de Protección de Datos Personales do Perú estabeleceu recomendação, na qual adverte que a divulgação de dados pessoais de infectados pelo COVID-19 pode gerar multa de até 215.000 soles.

Já se tem relatos de uma plataforma digital chinesa capaz de identificar se há algum passageiro contaminado pelo Covid-19 em viagens urbanas, oferecendo aos usuários informações a respeito. Mais conhecido como Qihoo 360, o aplicativo tem como fonte a base de dados dos hospitais e informações das

companhias estatais de transporte, além do mais, a plataforma digital conta com algoritmos de inteligência artificial capaz de cruzar os dados e identificar os riscos de contaminação. Teríamos um rastreio de pessoas infectadas? Os dados são anonimizados? Outas pessoas poderiam apontar o celular para uma direção e identificar um suposto "contaminado"? Quais as consequências imprevistas destas tecnologias? Quais os impactos destas tecnologias que estão sendo construídas na urgência, considerando que apesar de estarem empenhadas em livrar pessoas da contaminação, tratam dados pessoais sensíveis.

A Presidente do Conselho Europeu de Proteção de Dados (EDPD), Andrea Jelinek, se pronunciou recentemente a respeito do tratamento dos dados pessoais diante deste cenário acarretado pelo covid-19, declarando que: *As regras de proteção de dados (como o GDPR) não impedem as medidas tomadas na luta contra a pandemia de coronavírus…".* Em seguida enfatiza: *…"o controlador de dados deve garantir a proteção dos dados pessoais dos titulares dos dados. Portanto, várias considerações devem ser levadas em consideração para garantir o processamento legal de dados pessoais. "*

Jelinek, faz considerações a respeito do processamento de dados de comunicação eletrônica, como dados de localização móvel, aos quais são

aplicadas regras adicionais. No caso da Europa, alguns regulamentos nacionais determinaram que os dados de localização só podem ser usados pelo controlador quando forem anônimos ou com o consentimento dos indivíduos, obtendo-se assim maior controle e transparência de acesso e compartilhamento desses dados.

Vale a compreensão do que o mundo está pensando no que tange às questões relativas a proteção de dados e o Novo Coronavírus. A *Global Privacy Assembly* reuniu em uma página um compilado das principais ações, regulamentos, manifestações e recomendações emanadas pelas autoridades de proteção de dados no mundo sobre o COVID-19: https://globalprivacyassembly.org/covid19/

É indisfarçável a necessidade de equilibrar a proteção de dados e o interesse público, lembrando que isso não habilita tratamentos inconsequentes de dados pessoais que possam ferir direitos e liberdades fundamentais, como aplicativos invasivos de classificação de pessoas, ao estilo *"Nosedive"…*

Posto isso, cabe indagar: Quais são os limites do mapeamento de infectados e os riscos à privacidade? Se os limites são desconhecidos, o que dizer dos impactos?

Como investigar e apurar judicialmente a autoria de crimes digitais e na internet

A apuração de crimes digitais importa na coleta de dados em provedores de conteúdo/serviços e provedores de acesso. Diante de um crime digital ou cibernético, como ofensa, difamação, calúnia ou outros crimes, praticados pela internet, a vitima é orientada a buscar apoio de um especialista para apurar a autoria do delito, quase sempre cometido por alguém que não se identifica.

E neste contexto, considerando que provedores de serviços, conteúdos e redes sociais, como Facebook, Google, Microsoft, dentre outros, só apresentam dados mediante ordem judicial, via de regra, faz-se necessário processar tais provedores para que eles apontem os dados de "conexão" relativos a alguém que utilizando seus serviços, praticou algum crime cibernético ou causou dano a outrem.

O grande problema é que na maioria das vezes os provedores de serviços fornecem apenas um número de endereço IP (internet protocol) relativo ao suposto usuário criminoso. E convenhamos: Ninguém vai ao Judiciário para descobrir um número IP! Por outro lado, busca apoio da Justiça para identificar a pessoa por trás da ofensa e que age amparada pela falsa sensação de anonimato. Busca-se a autoria do crime!

E é aí que entra o papel do Provedor de Acesso. Como base no número IP fornecido pelo provedor de serviços demandado judicialmente, pode-se ir ao registro.br e descobrir qual o Provedor de Acesso responsável e então, requerer nos autos a

expedição de ofício ao mesmo, para que aponte e forneça os dados cadastrais do usuário/seu cliente conectado na Internet, com o IP apurado, na exata data e hora da ofensa publicada ou do crime praticado.

E neste ponto surge outro problema, alguns Magistrados, sem muita intimidade com informática e tecnologia da informação, em casos dessa natureza, acabam por não consentirem com a determinação de ofício aos Provedores de Acesso identificados, sob a argumentação de que não são “partes no processo”, fazendo com o que o consumidor da justiça, além de não ter obtido sua pretensão, tenha de mover uma nova ação, desta vez em face dos Provedores de Acesso Identificados na ação anterior (Movida em face dos provedores de serviços onde o delito fora praticado).

Este é, apenas um exemplo de uma decisão desacertada:

Um desperdício em desprestígio da economia processual, e um risco, considerando que os dados (registros e logs) dos provedores de acesso a serem demandados podem vir a ser apagados. Neste sentido, é papel do advogado do Direito Digital também educar, conscientizar e apresentar ao julgador os riscos do encerramento prematuro de um processo de apuração de autoria.

Em um dos cursos que ministro sobre Direito Digital Avançado, onde tenho oportunidade de interagir com alunos que já atuam na área há mais de 10 (dez) anos e com profunda bagagem técnica e jurídica em Direito da Informática, representando grandes corporações e provedores, foi levantada esta questão, relativa a dificuldade de alguns julgadores em compreenderem que a efetiva tutela jurisdicional, nestes casos, só é alcançada com a apuração da autoria e não com o fornecimento de meros dados de conexão.

Neste cenário, é consenso que devemos desenvolver nossas

petições instruídas de documentos, gráficos, desenhos que ilustrem o procedimento de apuração da autoria de crimes e ilícitos virtuais, estabelecendo de forma clara as etapas e o papel dos provedores de serviços e de acesso. Ponderou-se no curso e até nas discussões via Facebook, sobre a necessidade da concepção de um gráfico, para que colegas da área pudessem instruir ou anexar em suas ações, cooperando para conscientização em relação aos procedimentos em casos envolvendo apuração de autoria em crimes e golpes na Internet.

Neste sentido, para auxiliar os colegas e advogados do direito da informática e digital, criei um gráfico ilustrativo e legendado, que denominei "Caminho básico para apuração judicial da autoria de um crime digital – 2013". O gráfico, que está na versão 1 e fica a disposição dos colegas, está disponível em formato JPG e PDF e pode ser baixado aqui. Pelo gráfico, advogados, promotores, acadêmicos, vitimas e membros do judiciário poderão rapidamente compreender de forma básica como um delito digital é praticado, via de regra, e como é possível apurar a autoria, na grande maioria dos casos.

Esperamos a contribuição dos colegas e especialistas para aprimoramento versões posteriores. O Documento é liberado para uso em requerimentos, petições e quaisquer outros pleitos judiciais envolvendo crimes informáticos. Uma contribuição modesta aos colegas que militam arduamente na área e que por vezes se frustram com decisões que asseguram impunidade em delitos de informática, cada vez mais comuns no Brasil. Compartilhem!

Acesse os gráficos (Versão PDF) (Versão JPG)

Referências
http://josemilagre.com.br/blog/sala-de-estudos/direito-tecnologico/documentos/grafico-para-apuracao-judicial-de-crimes-digitais/