ARTIGOS ACEITOS PARA PUBLICAÇÃO
DIREITO DIGITAL E SETOR PÚBLICO - 2020.2

ITS RIO

Pós-Graduação em Direito Digital

CEPED UERJ ITS

DESINFORMAÇÃO E DESAFIOS REGULATÓRIOS: REFLEXÕES À LUZ DA SEGURANÇA CIBERNÉTICA

Daniella Fernandes Ferrari

Desinformação e desafios regulatórios: reflexões à luz da segurança cibernética

Daniella Fernandes Ferrari

Dezembro 2020

> "A busca metódica pela verdade é, além disso, em si própria um produto daquelas épocas em que as convicções estavam em guerra umas com as outras."
>
> NIETZCHE, Friedrich. "Human, all too Human". United Kingdom: Cambridge University Press, 1996. P.201. (*tradução livre*)

O fatídico ano de 2020 ressaltou desafios sociais no combate a epidemias de diferentes tipos. Notadamente, a pandemia viral que assolou o globo veio acompanhada de uma "*infodemia*": o excesso de informação, muitas vezes falaciosa, disseminada por viralização virtual.[1] Ambas tiveram impactos na remodelação das relações humanas, mas a segunda já não era novidade. Popularizada pela alcunha de "*Fake News*", mas integrante do fenômeno mais amplo da desinformação, trata-se de um perigoso agravante da crise de confiança de nossos tempos.[2] A saúde pública é apenas um dos bens coletivos atingidos – processos eleitorais e a ordem democrática, crise climática e ambiental, e até mesmo as leis da física padecem da mesma vulnerabilidade quanto à manipulação maliciosa da informação, com consequências comprovadamente desastrosas.

A complexidade dos fatores e a multiplicidade de atores envolvidos lançam desafios a governos nacionais, entidades supranacionais e empresas de tecnologia, que se debruçam sobre o tema para desenvolver possíveis formas de regulação e contenção de danos do fenômeno. O componente tecnológico intrínseco à propagação desenfreada da desinformação por mídias virtuais faz com que a discussão necessariamente passe pelos moldes do ambiente cibernético, o qual também teve suas fragilidades expostas no último ano. Enquanto a internet acresce exponencialmente o alcance e potencial danoso da desinformação, o aumento da dependência

[1] "Excesso de informação sobre determinado tema, por vezes incorreta e produzida por fontes não verificadas ou pouco fiáveis." "infodemia", in Dicionário Priberam da Língua Portuguesa [em linha], 2008 2020, https://dicionario.priberam.org/infodemia [consultado em 01-11-2020].

[2] Utilizarei o termo "desinformação" para designar o fenômeno em questão, seguindo nomenclatura adotada pela COMISSÃO EUROPEIA, pelos motivos expostos no tópico (i) adiante.

nas redes informáticas trazido pela pandemia também viu crescer assombrosamente o número de cíber-ataques, sinalizando alertas urgentes quanto às deficiências no âmbito da segurança cibernética.[3]

Nesse contexto, há considerações importantes a serem desenvolvidas. Embora a desinformação não seja considerada um cíber-ataque em seu sentido mais técnico, por não se tratar diretamente de uma invasão cibernética que busca burlar camadas informáticas de segurança, é possível traçar interlocuções proveitosas entre ambos os institutos. A discussão sobre manipulação de conteúdo não é estranha ao campo da segurança cibernética, assim como os requisitos técnicos de segurança virtual não devem ser alheios à atividade reguladora. Considerando que a problemática da desinformação reside também na interseção entre o direito e a tecnologia, em espírito simbiótico, ambos os lados podem se beneficiar de contribuições interdisciplinares.

Nesse sentido, no presente artigo apresento argumentos de por que pensar a desinformação enquanto um componente de segurança cibernética pode ser vantajoso às discussões quanto à regulação do tema. Para isso, tratarei primeiro da desinformação em sua incompatibilidade com a liberdade de expressão e o Estado democrático de Direito, asseverando premissas básicas que abrem o campo para discussões sobre normatividade. Em segundo lugar, demonstrarei a desinformação inserida no contexto mais amplo da segurança cibernética, traçando relações entre conceitos técnicos e seus efeitos mais amplos. Por fim, apresentarei modelos de cíber-segurança aplicados à desinformação, considerados frente aos desafios regulatórios. Evidentemente, destaco que não há a pretensão de oferecer soluções contundentes, tampouco esgotar o assunto, mas ao menos instigar reflexões a partir da apresentação de abordagens multidisciplinares e criativas.

(i) Desinformação e liberdade de expressão – um breve panorama sobre fundamentos e incompatibilidades.

Preliminarmente, é necessário expor os motivos pelos quais a desinformação não pode e nem deve ser defensável sob o ponto de vista da liberdade de expressão, ressaltando as amarras democráticas que devem balizar ambos os institutos. Como restará claro, sociedades que se

[3] CONTRERAS, Belisario. "3 ways governments can address cybersecurity in the post-pandemic world". World Economic Forum. 29 de junho, 2020. Disponível em <https://www.weforum.org/agenda/2020/06/3-ways-governments-can-address-cyber-threats-cyberattacks-cybersecurity-crime-post-pandemic-covid-19-world/>. Último acesso em 20.11.2020.

pretendem liberais não apenas devem prezar pela livre circulação da informação como dependem desta, sendo implícito que tal informação seja verdadeira.[4] Extrai-se que a desinformação em todas suas acepções deliberadas, enquanto antítese a esta premissa, se demonstra intolerável, definindo-se também as condutas indevidas abarcadas pelo fenômeno.

É indiscutível que o direito à expressão livre, em todas as suas manifestações, é pilar sobre o qual o Estado democrático de direito se ergue, precipuamente por três motivos: (i) fomenta a livre circulação de ideias e difusão de conhecimento, possibilitando sociedades heterogêneas; (ii) permite e instiga a livre formação da subjetividade, base para a autonomia da vontade; e (iii) garante a legitimidade da soberania popular, alicerce da democracia. Nesta lógica, intimamente relacionados à liberdade de expressão estão a liberdade de imprensa (e dos meios de comunicação no geral) e a liberdade de informação.[5] Sem os dois últimos, a primeira padeceria, sobretudo ao enquadrarmos a dimensão social da livre manifestação e sua difusão através dos meios de comunicação em massa.

Para o contexto específico da desinformação, interessa particularmente tratar dos elementos próprios à liberdade de informação. Sem prejuízo da relação de dependência entre esta e a liberdade de expressão, é certo também que se trata de institutos distintos, especialmente no que toca ao critério da veracidade intrínseco à primeira – enquanto a livre expressão engloba ideias, opiniões, juízos de valor, ou essencialmente qualquer manifestação do pensamento humano, a livre informação se atém à disseminação de fatos.[6] Nas palavras de Luís Roberto Barroso:

> "É fora de dúvida que a liberdade de informação se insere na liberdade de expressão em sentido amplo, mas a distinção parece útil por conta de um inegável interesse prático, relacionado com os diferentes requisitos exigíveis de cada uma das modalidades e suas possíveis limitações. A informação não pode prescindir da verdade - ainda que uma verdade subjetiva e apenas possível (o ponto será desenvolvido adiante) - pela circunstância de que é isso que as pessoas legitimamente supõem estar conhecendo ao buscá-la."[7]

---

[4] BARROSO, Luís Roberto. "Colisão ente liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei da Imprensa." Revista de Direito Administrativo, Rio de Janeiro, n. 235, jan./mar. 2004.

[5] No caso brasileiro, os direitos fundamentais correlacionados às garantias de liberdade de expressão estão assegurados constitucionalmente no art. 5, IV, VI, IX, XVI e art. 220, enquanto o direito à informação vem expresso no art. 5 XIV e XXXIII. Além disso, ambos são previstos em tratados internacionais de direitos humanos, como o Pacto Internacional dos Direitos Civis e Políticos e a Declaração Universal dos Direitos do Homem adotados pelas Organizações das Nações Unidas, sendo nestes o direito à informação incluído no direito à liberdade de expressão.

[6] BARROSO, Luís Roberto. "Colisão ente liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei da Imprensa." Revista de Direito Administrativo, Rio de Janeiro, n. 235, jan./mar. 2004, p. 18.

[7] Id.

Em outras palavras, a liberdade de informação deve ter compromisso com a verdade, uma vez que isto é uma exigência da própria definição de informação. Indo além, a desinformação concebida enquanto a circulação descontrolada de informações errôneas ou falaciosas frustra o legítimo interesse do cidadão que busca se informar, o que por sua vez traz consequências nefastas para a coletividade como um todo. Somente é possível formar uma opinião, e a partir desta, tomar decisões conscientes e informadas, quando há informações acessíveis e confiáveis – sobretudo para finalidades eleitorais.[8] Sem informação verdadeira, não há real liberdade de escolha ou autonomia da vontade, o que pode ocasionar comportamentos temerários em nível individual e culminar ultimamente na deturpação da representatividade democrática.

Logo, partimos da premissa básica de que a desinformação, enquanto um instituto essencialmente antidemocrático e, desse modo, ilegítimo, não deve ser tolerada sob a égide do Estado democrático de direito. Isto, no entanto, não significa concluir imediatamente que o fenômeno deve ser regulado em termos estatais, e nem que a "mentira" *per se* deve ser coibida pelo Estado. Pelo contrário – o risco potencial de censura não deve ser considerado levianamente.

Com efeito, há determinadas manipulações da verdade que são tuteladas pelo poder público. A título de exemplo, o tipo penal da calúnia no ordenamento jurídico brasileiro traz repercussões jurídicas na esfera criminal, reprimindo a imputação falsa a outrem de um fato definido como crime.[9] Não obstante, para discernir a necessidade de intervenção regulatória, cumpre definir o que se entende por desinformação, visando distinguir quais comportamentos des-informativos importam à ordem democrática.

A bem da verdade, a desinformação enquanto uma prática desleal levada a cabo por adversários políticos para auferir vantagens competitivas é tão antiga quanto a própria mentira ou boato corriqueiro.[10] Todavia, tal artifício ganha contornos mais impactantes no contexto das sociedades da informação do século XXI, que tem como principal motor os grandes avanços das tecnologias de informação e comunicação (TICs), nas quais o uso, criação e distribuição da informação figuram como característica central.[11] Com efeito, o notório teórico da revolução

---

[8] ALVES, Giulia Ferrigno Poli Ide. "Reflexões sobre o fenômeno da desinformação: impactos democráticos e o papel do direito". Revista RED UnB – 16ª ed. (pp. 263-180).

[9] **"**Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime (...)." BRASIL. Código Penal Brasileiro - Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Art. 138, caput.

[10] WARDLE, Claire; DERAKHSHAN, Hossein. "Information Disorder: Toward an interdisciplinary framework for research and policy making". 2017: Council of Europe report DGI. p. 4

[11] Wikipedia. "Sociedade da informação". Disponível em <https://pt.wikipedia.org/wiki/Sociedade_da_informa%C3%A7%C3%A3o>. Último acesso em 10.12.2020.

informacional Manuel Castells é incisivo ao afirmar que, como a comunicação consciente é a principal característica que distingue os humanos, é evidente que foi nessa área que a sociedade sofreu sua mais profunda transformação.[12] Nesse sentido, o diferencial contemporâneo das estratégias de disputa pela verdade dos fatos é a difusão da "poluição informacional" em escala global e seu alcance em tempo real, tornados possíveis através das ferramentas da tecnologia da comunicação. [13]

Neste cenário caracterizado por alguns autores como a "nova desordem informacional", a problemática se aprofunda pela própria definição do que seria a desinformação.[14] Conquanto haja certo consenso que a expressão "*Fake News*" se demonstra inadequada para dar conta do fenômeno em todas as suas dimensões, devido tanto a sua vulgarização quanto por se tratar de práticas mais abrangentes do que a mera publicação de notícias com conteúdo falso, não há concordância doutrinária acerca da unicidade conceitual do termo. Além do prefixo "des-", na língua inglesa há ainda a possibilidade de combinação da palavra "informação" com os prefixos "mis-" e "mal-", cada qual com conotações ligeiramente diversas. Há ainda tentativas de adotar tipologias para as diferentes modalidades de manipulações desonestas englobadas pela desinformação, como, por exemplo, a classificação adotada por Claire Wardle:[15]

> "1. Sátira ou paródia (sem intenção de causar danos, mas com potencial enganoso).
> 2. Falsa conexão (quando as manchetes, elementos visuais ou legendas não conferem com o conteúdo).
> 3. Conteúdo enganoso (utilização enganosa da informação para enquadrar um assunto ou indivíduo).
> 4. Contexto falso (quando o conteúdo verdadeiro é compartilhado com informações contextuais falsas).
> 5. Conteúdo impostor (quando fontes verdadeiras são forjadas).
> 6. Conteúdo manipulado (quando o conteúdo ou imagens verdadeiras são manipuladas ou adulteradas com cunho enganoso).
> 7. Conteúdo fabricado (quando o conteúdo novo é 100% falso, projetado para enganar e causar danos)."

Em que pese ser um conceito fluido e ainda aberto, de acordo com a finalidade e escopo do presente artigo, utiliza-se a terminologia "desinformação" conforme a nomenclatura indicada pela Comissão Europeia em grupo especializado sobre o tema.[16] De acordo com o relatório final produzido em 2018, o termo "desinformação" surge enquanto mais apropriado para refletir a subversão da circulação da informação levada em curso, sendo certo que o termo

---

[12] CASTELLS, M. "A sociedade em rede. A era da informação: economia, sociedade e cultura". v. 1. 6. ed. São Paulo: Paz e Terra, 2011. p. IX.
[13] WARDLE, ibid.
[14] ALVES, Giulia Ferrigno Poli Ide. "Reflexões sobre o fenômeno da desinformação: impactos democráticos e o papel do direito". Revista RED UnB – 16ª ed. P. 264.
[15] WARDLE, Claire; DERAKHSHAN, Hossein. "Information Disorder: Toward an interdisciplinary framework for research and policy making". 2017: Council of Europe report DGI. p. 17
[16] COMISSÃO EUROPEIA. "Final report of the High Level Expert Group on Fake News and Online Disinformation". 2018. Disponível em <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>. Último acesso em 20.11.2020.

reflete a compreensão compartilhada de que a prática vai muito além do termo "notícias falsas". Desse modo, inclui todas as formas de informações falsas, imprecisas ou enganosas elaboradas, apresentadas e promovidas para causar dano público intencionalmente ou para lucro.[17] Desse modo, o termo não abrange questões decorrentes da criação e divulgação online de conteúdo ilegal (tais como a difamação, o discurso de ódio, e a incitação à violência), uma vez que estas estão sujeitas à regulamentação jurídica própria, e nem outras formas de distorções deliberadas dos fatos que não se pretendem enganosas, tais como a sátira e a paródia.

Desse modo, percebe-se que o objetivo não seria coibir erros honestos, devendo importar que seja um ato deliberadamente enganoso, o qual é frequentemente motivado por finalidades ideológicas e/ou financeiras.[18] Isto é, ainda que um indivíduo, por mera ignorância, possa repassar ou postar em rede social determinado conteúdo que venha a ser declarado falso, e mesmo que isto possa contribuir para a desinformação generalizada do público, não é este o comportamento chave a ser endereçado pelas instituições democráticas.

Além disso, agravando o problema, há em curso verdadeiras campanhas de desinformação.[19] Estas se caracterizam por operações em que tempo, inteligência e recursos financeiros são emplacados enquanto estratégias organizadas para manipular debates e distorcer a opinião das massas através da veiculação da desinformação. Tais campanhas se utilizam de artifícios tecnológicos lícitos disponibilizados pelas plataformas digitais quanto ao direcionamento e impulsionamento do conteúdo – justificando, desse modo, a condição indispensável de incluir nesse debate especialistas do campo da tecnologia da informação.

(ii) Desinformação e segurança cibernética: conexões através do elemento humano.

Superadas as premissas iniciais, passamos à temática mais técnica da segurança cibernética e sua interlocução com o campo da desinformação. A segurança cibernética vem sendo crescentemente alçada a uma condição *sine qua non* no contexto de hiperdigitalização da vida, fundamental para o desenvolvimento prudente do paradigma da indústria 4.0 e migração

[17] COMISSÃO EUROPEIA. "Final report of the High Level Expert Group on Fake News and Online Disinformation". 2018. Disponível em <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>. p. 5. Último acesso em 20.11.2020.
[18] WARDLE, Claire; DERAKHSHAN, Hossein. "Information Disorder: Toward an interdisciplinary framework for research and policy making". 2017: Council of Europe report DGI. p. 33-34.
[19] Ibid, p. 4.

segura das atividades cotidianas e seus respectivos dados para o ambiente cibernético.[20] De modo semelhante, a desinformação vem ganhando notoriedade enquanto uma grave ameaça manifestada no ambiente cibernético, visto que se utiliza de artifícios tecnológicos não apenas para forjar e adulterar fatos e imagens, como para direcionar, ampliar e propagar seus efeitos em plataformas sociais.

Curiosamente, apesar da aparente interseção entre os temas, a desinformação é frequentemente tratada de maneira isolada, concebida como um fenômeno à parte das estruturas e padrões de segurança – principalmente devido à sua dimensão material e à amplitude de suas causas, que transbordam os limites do mundo virtual. Visando aproximar ambos os institutos, trago motivos de porque a inserção da desinformação no contexto maior da segurança cibernética poderá trazer benefícios em prol de uma abordagem mais sistêmica. Para tanto, é necessário localizar a desinformação dentro da estrutura da segurança cibernética, compreendendo sua relação com segurança da informação e identificando suas particularidades.

Primeiramente, deve-se esclarecer em linhas breves o que significam segurança cibernética e segurança da informação (comumente apelidada de "InfoSec"). Estas guardam entre si relação umbilical e são frequentemente utilizadas de maneira intercambiável, embora detenham diferenciações técnicas. Sem aprofundar nos pormenores conceituais, até porque são um tanto nebulosos e não unânimes, podemos definir a segurança da informação como as práticas de proteção da informação e sua gestão de riscos, o que não necessariamente precisa se dar no meio virtual. Já a segurança cibernética engloba o conjunto de ferramentas, normas e práticas utilizadas para proteger o ambiente cibernético e os ativos dos usuários e organizações neste espaço, incluindo dispositivos, infraestrutura, aplicações, sistemas de telecomunicações e a totalidade da informação transmitida ou armazenada.[21]

Por conseguinte, é possível conceber a segurança cibernética como a segurança da informação aplicada ao ambiente cibernético – a primeira englobaria a segunda, se embasando nela e indo além.[22] Nesse sentido, a segurança da informação surge como o conceito-base,

---

[20] World Economic Forum Annual Meeting. "Why 2020 is a turning point for cybersecurity." 23 de janeiro, 2020. Disponível em < https://www.weforum.org/agenda/2020/01/what-are-the-cybersecurity-trends-for-2020/>. Último acesso em 23.11.2020.

[21] SOLMS, von Rossouw; NIEKERK, van Johan. "From information security to cyber security". Computer & Security, vol. 38 (pp97 -102). 2013: Elsevier. p. 97-98.

[22] "The term cyber security is often used interchangeably with the term information security. This paper argues that, although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous. Moreover, the paper posits that cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself. In information security, reference to the human factor usually relates to the role(s)

composta pela famosa tríade de atributos fundamentais da informação a serem resguardados: disponibilidade, integridade, confidencialidade, e, por vezes, também, a autenticidade (formando a sigla CIA em inglês ou DICA em português).[23] Do mesmo modo, a segurança cibernética está fortemente ancorada nos três pilares da "CIA" e seus respectivos quesitos de proteção da informação – esta deve se manter disponível para uso legítimo, confidencial (em relação a entidades não autorizadas) e íntegra, isto é, não-manipulada.

Em se tratando de práticas de desinformação, é justamente o atributo da integridade da informação que é comprometido. Em sua apresentação na Conferência RSA sobre cíber-segurança em 2018, Daniel Rogers, fundador da Global Disinformation Index (GDI), destaca que, dentre os três pilares consagrados, a comunidade de operadores da InfoSec se concentrou majoritariamente na disponibilidade e confidencialidade da informação, deixando de lado o atributo da integridade.[24] Rogers comenta que, embora a integridade não seja considerada como um elemento técnico, ela é tão relacionada à segurança da informação quanto os demais, representando uma ameaça verdadeiramente perniciosa.[25]

Há uma razão evidente para a integridade ser frequentemente desconsiderada: ela é mais difícil de definir e mais ainda de verificar. A Organização Internacional para Padronização - ISO define a integridade como "a propriedade de acurácia e completude" – em outras palavras, refere-se à qualidade daquilo que é verdadeiro.[26] Isto é, enquanto a disponibilidade e a confidencialidade são facilmente compreensíveis e verificáveis a partir de padrões binários – os dados estão disponíveis ou não, são privados ou públicos – a integridade é recheada de nuances por tratar diretamente do conteúdo em si, em seu aspecto material.[27]

---

of humans in the security process. In cyber security this factor has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility." SOLMS, von Rossouw; NIEKERK, van Johan. "From information security to cyber security". Computer & Security, vol. 38 (pp97 -102). 2013: Elsevier. p. 97.

[23] O padrão uniformizado do ISO/IEC 27000 – International Organization for Standardization traz no item 3.28 e seguintes a definição de segurança da informação e seus atributos. Observo que há outras propriedades eventualmente incluídas para além da tríade CIA, como a não-repudiação, o que não nos interessa esmiuçar para os fins propostos neste artigo. ISO/IEC 27000:2018(en). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Disponível em <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.48>. Último acesso em 27.11.2020.

[24] ROGERS, Daniel. "#FakeNews as an Information Security Problem." RSA Conference, 2018. Disponível em <https://www.youtube.com/watch?v=zAibdueUxkg>. Último acesso em 27.11.2020.

[25] Id.

[26] Tradução livre de "Property of accuracy and completeness". ISO/IEC 27000:2018(en). Information technology — Security techniques — Information security management systems — Overview and vocabulary. "3.36. Integrity". Disponível em <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.48>.

[27] ROGERS, Daniel. "#FakeNews as an Information Security Problem." RSA Conference, 2018. Disponível em <https://www.youtube.com/watch?v=zAibdueUxkg>. Último acesso em 27.11.2020.

Para Rogers, as emblemáticas campanhas de desinformação lançadas a partir das eleições presidenciais norte-americanas em 2016 são um caso paradigmático de violação da integridade da informação – assim como o caso de vazamento de dados sensíveis da empresa de crédito norte-americana Equifax está para o atributo da confidencialidade (ou, mais recentemente, o escândalo envolvendo a Cambridge Analytica), e os ataques DDOS sofridos pela DynDNS, popular provedora de serviços DNS, está para o quesito da disponibilidade. Nesse sentido, se trataria de uma referência exemplificadora de violação à integridade da informação e suas graves consequências, no qual haveria a convergência entre fraude, segurança da informação e desinformação, motivada por questões político-ideológicas e/ou financeiras.

Corroborando esse entendimento, operadores dessa área já afirmam a sobreposição crescente entre a desinformação e a cíber-segurança.[28] A questão passa a ser como a comunidade de especialistas em tecnologia da informação poderá se agregar para endereçar questões dos riscos relacionados ao uso humano dos sistemas informáticos – que naturalmente traz consigo toda a falibilidade e criatividade inerente aos humanos, empregadas tanto para fins legítimos quanto ardilosos. Não à toa, a Conferência RSA de 2020 designou como seu tema central a dimensão humana no bojo da segurança cibernética, que permanece sendo o calcanhar de Aquiles de sistemas de segurança da informação.[29] Um notório exemplo disso é a engenharia social: operantes da área de InfoSec citam a engenharia social como a principal vulnerabilidade dos sistemas informáticos, mais do que as brechas técnicas por si só.[30] De modo análogo, podemos dizer que o relacionamento entre humanos, máquinas e redes virtuais está na raiz da problemática da desinformação.

---

[28] "“For people who think disinformation and cybersecurity aren’t related, things are going to change very quickly for you. The issue of disinformation is increasingly becoming something that security teams are expected to address,” Melanie Ensign, security, privacy, and engineering communications lead at Uber, said in a discussion of disinformation at the Enigma conference here Wednesday.”. FISHER, Dennis. “The growing overlap of disinformation and security”. Decipher: 23 de janeiro, 2020. Disponível em <https://duo.com/decipher/the-growing-overlap-of-disinformation-and-security>. Último acesso em 27.11.2020.

[29] RSA Conference. “The Power of the Human Element”, RSAC 2020. Disponível em <https://www.rsaconference.com/industry-topics/video/2020-the-power-of-the-human element#:~:text=The%20theme%20of%20RSA%20Conference,key%20to%20creating%20a%20more>. Último acesso em 27.11.2020.

[30] A engenharia social, no contexto de ataques cibernéticos e segurança da informação, refere-se à manipulação psicológica de usuários, através de artifícios fraudulentos e/ou indução ao erro, para que inadvertidamente divulguem informações confidenciais ou executem ações para burlar procedimentos de segurança. GROSSMANN, Luís Osvaldo; LOBO, Ana Paula. “Engenharia social é principal backdoor de segurança, sem patch que resolva”. Convergência Digital. Disponível em <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=55429&sid=18.> Último acesso em 27.11.2020.

(iii) Desafios regulatórios da desinformação: interlocuções entre direito e tecnologia.

No que tange aos desafios regulatórios voltados para a contenção de danos, afirmar que a desinformação é um problema de segurança cibernética permite começar a aplicar o *know-how* metodológico já adquirido por especialistas desse campo também a esta faceta das redes virtuais, compelindo-os a voltarem sua atenção ao conteúdo da informação. Este é um dos desafios encabeçados pelo grupo de estudos em andamento intitulado "MisinfoSec" (uma junção em inglês de "misinformation" com "Infosec"), da *Credibility Coalition*, que tem como missão aplicar os paradigmas da segurança da informação às campanhas de desinformação.[31] Mais especificamente, o objetivo do grupo é o desenvolvimento de uma estrutura teórica baseada em táticas, técnicas e procedimentos que possa fornecer aos pesquisadores da desinformação uma linguagem comum para discutir e interromper incidentes de desinformação.

Conforme alertado pelo próprio MisinfoSec, trata-se de uma missão ambiciosa – enquanto os ataques à segurança da informação estão firmemente enraizados no campo quantitativo da ciência da computação, as campanhas de influência estão, em sua essência, arraigadas nos campos qualitativos da sociologia e psicologia. [32] Ressaltam, com razão, que a vinculação dos campos quantitativos e qualitativos da ciência sempre foi precária em termos epistemológicos. De todo modo, considerando que a desinformação opera dentro de um ecossistema sócio-técnico complexo, a abordagem necessariamente deverá ser multidisciplinar, havendo benefícios nas abordagens mais holísticas.[33]

Nesse sentido, uma das metodologias já conhecidas aos profissionais da InfoSec se refere à modelagem de ameaças, aplicada normalmente a sistemas, aplicativos e redes. Esta envolve o mapeamento sistemático e estruturado de potenciais ameaças, bem como de vulnerabilidades estruturais ou ausência de salvaguardas adequadas, as quais, uma vez identificadas e enumeradas, tem as ações de mitigação correspondentes ordenadas de acordo com sua prioridade. Para Rogers, há um método na forma como campanhas de desinformação são projetadas e implementadas, de modo que seria possível formular uma modelagem de

[31] GRAY, John; TERP, Sarah-Jane."The MisinfoSec Framework Takes Shape: Misinformation, Stages, Techniques and Responses". Medium, 19 de junho, 2019. Disponível em https://medium.com/@credibilitycoalition/misinfosec-framework-99e3bff5935d. Último acesso em 13.12.2020.
[32] WALKER, Christopher. Et al. "Misinfosec - Applying Information Security Paradigms to Misinformation Campaigns". WWW '19: The Web Conference (WWW '19), May 13, 2019. p. 6.
[33] Ibid, p.2.

ameaças voltada para a integridade da informação.[34] Da mesma forma, o grupo MisinfoSec estuda a aplicação de exercícios de mapeamento relativo ao espectro de atores, alvos e táticas envolvidas nas campanhas de desinformação, classificando-as como "ameaças avançadas persistentes".[35]

Seguindo esta lógica, haveria valor em analisar as fraquezas não-técnicas de determinada plataforma digital visando encontrar pontos cegos e vieses que possam eventualmente ser explorados por adversários mal-intencionados para influenciar comportamentos.[36] Tal entendimento poderia dialogar com a análise de Wardle, por exemplo, que enfatiza a necessidade de separar as três fases distintas da desordem informacional: criação, produção e distribuição. Essa classificação alerta que o "agente" criador de uma mensagem fabricada poderá ser diferente do agente que produz a mensagem, que poderá também se distinguir daquele que a distribui.[37] Dissecar os componentes envolvidos em operações complexas como campanhas de desinformação poderia ser útil para identificar lacunas a serem preenchidas, eliminar vulnerabilidades mais superficiais ou, ao menos, dirimir onde os maiores esforços devem ser concentrados.

Tais considerações importam tanto para questões técnicas de desenho e concepção original das plataformas e serviços digitais quanto para fins regulatórios, uma vez que possibilitam o (re)direcionamento da atividade normativa para ameaças mais delimitadas, onde ações estatais possam surtir mais efeito, inclusive em termos preventivos. Abordagens regulatórias sobre-inclusivas ou que se pretendem enquanto panaceia, sobretudo frente a problemáticas complexas, sujeitam-se ao imenso risco de adentrar na famigerada ladeira escorregadia da censura, em última grau gerando consequências tão ou mais indesejadas quanto o problema original. Nesse sentido, a intervenção direta do Estado sobre controle de conteúdo deve ser vista com cautela, devido aos riscos de ingerência estatal exacerbada sobre a liberdade de expressão, liberdade de imprensa e informação.[38]

---

[34] ROGERS, Daniel. "#FakeNews as an Information Security Problem." RSA Conference, 2018. Disponível em <https://www.youtube.com/watch?v=zAibdueUxkg>. Último acesso em 27.11.2020.
[35] WALKER, Christopher. Et al. "Misinfosec - Applying Information Security Paradigms to Misinformation Campaigns". WWW '19: The Web Conference (WWW '19), May 13, 2019. p. 6.
[36] FISHER, Dennis. "The growing overlap of disinformation and security". Decipher: 23 de janeiro, 2020. Disponível em <https://duo.com/decipher/the-growing-overlap-of-disinformation-and-security>. Último acesso em 27.11.2020.
[37] WARDLE, Claire; DERAKHSHAN, Hossein. "Information Disorder: Toward an interdisciplinary framework for research and policy making". 2017: Council of Europe report DGI. p. 22-23.
[38] BARROSO, Luís Roberto. "Colisão ente liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei da Imprensa." Revista de Direito Administrativo, Rio de Janeiro, n. 235, jan./mar. 2004. p. 33-34.

Nesse contexto, a identificação da desinformação enquanto uma variante das ameaças enfrentadas pela segurança cibernética é um atestado de que a primeira é permeada pelas mesmas características do tema mais amplo: trata-se de uma problemática transversal, sem solução única, imbricada em um ecossistema informático de mídias e serviços em que os princípios de governança e transparência devem ser maximizados. Na sociedade da informação, manter a integridade dos fatos torna-se um desafio conjunto – a elevação dos níveis de cíber-segurança devem ser uma responsabilidade compartilhada entre o poder público, setor privado e os próprios cidadãos, devendo ser levada em consideração a educação digital dos usuários enquanto medida preventiva.[39]

Dito isto, não é razoável que se exija um compartilhamento de responsabilidades equilibrado entre as três pontas – atores do setor privado, como empresas de tecnologia, assim como órgãos dotados de poder público parecem possuir maiores condições de ingerência sobre o tema, como também maiores deveres de cuidado. Talvez o melhor exemplo recente de iniciativa que reflita tal compartilhamento seja a proposta corregulatória adotada pela Comissão Europeia, em que um código de práticas direcionado às plataformas digitais foi elaborado, criando um espaço para a necessidade de diálogo entre os agentes responsáveis.[40] Tal iniciativa poderia ser ampliada ou reforçada às plataformas digitais com base em estudos de modelagem de ameaças e mapeamento de vulnerabilidades pertinentes à segurança cibernética, além de considerar a necessidade de exigir a implementação de mecanismos de checagem de fatos desde a concepção dos serviços digitais, por exemplo.

Por óbvio, qualquer abordagem meramente mecânica enfrentará as mesmas dificuldades que tipicamente desafiam o campo da segurança cibernética em detrimento da proteção de seus usuários. Todavia, a proposta de considerar elementos mais técnicos vai ao encontro do ideal de aproveitarmos todos os recursos que nos estão disponíveis, além de estimular que utilizemos nossa criatividade. De acordo com os diretores do Berkman Klein Center, centro de pesquisa da Universidade de Harvard na vanguarda de temas envolvendo direito e tecnologia, é preciso que sejamos mais criativos quanto à segurança cibernética.[41] No mesmo diálogo citado, Zittrain e Mickens refletem que a desinformação se localizaria no domínio da cíber-segurança, apesar

[39]ORGANIZATION OF AMERICAN STATES – OAS. "2020 Cybersecurity Report: Risks, Progress and the way forward in Latin America and the Caribbean". 2020: Inter-American Development Bank. p. 29.

[40] VALENTE, Jonas. C. L. "Regulando desinformação e *fake news*: um panorama internacional das respostas ao problema". Comunicação pública. VOL.14 Nº 27, 2019. Disponível em <https://journals.openedition.org/cp/5262>. Último acesso em 13.12.2020.

[41] MILANO, Brett. "We need to be more imaginative about cybersecurity than we are right now". Harvard Law Today, 7 de outubro, 2020. Disponível em <https://today.law.harvard.edu/we-need-to-be-more-imaginative-about-cybersecurity-than-we-are-right-now/>. Último acesso em 28.11.2020.

de sua atipicidade, o que por si só justificaria a necessidade de soluções mais criativas. Pois enquanto a tecnologia se torna mais omnipresente, questões de segurança se tornam mais complexas – sobretudo aquelas que envolvem nossos atributos humanos em sua essência.

(iv) Considerações Finais

Em conclusão, se é certo que os fundamentos democráticos que norteiam a liberdade de expressão visam garantir uma arena de livre debate, no qual dissensos e antagonismos não apenas são permissíveis como desejáveis, nem todos os discursos estão protegidos sob o manto da livre expressão. Um desses limites é a distorção da informação e sua propagação desimpedida, nomeada hoje de desinformação. A informação maliciosamente manipulada deturpa a própria noção da liberdade na medida em que não serve aos propósitos democráticos das sociedades liberais, gerando graves deformações da autonomia da vontade e dos processos participativos inerentes à democracia.

Todavia, diante do iminente risco de censura que circunda a regulação estatal da liberdade de informação, é válido que outros modelos de mitigação de riscos sejam apreciados. Considerando que a desinformação se insere também na seara cibernética, a identificação da desinformação no contexto maior da segurança cibernética poderá trazer benefícios em prol de uma abordagem mais sistêmica e, ultimamente, contribuir para soluções mais criativas em relação a desafios regulatórios. Frente à interseção mais do que evidente entre o direito e a tecnologia, o diálogo entre ambos os campos de estudo deve ser encorajado, visando ultimamente minimizar os riscos da desinformação.

Referências Bibliográficas

ALVES, Giulia Ferrigno Poli Ide. “Reflexões sobre o fenômeno da desinformação: impactos democráticos e o papel do direito”. Revista RED UnB – 16ª ed. (pp. 263-180).

BARROSO, Luís Roberto. “Colisão ente liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei da Imprensa.” Revista de Direito Administrativo, Rio de Janeiro, n. 235, jan./mar. 2004

BRASIL. Código Penal Brasileiro - Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Art. 138, caput.

CASTELLS, M. “A sociedade em rede. A era da informação: economia, sociedade e cultura”. v. 1. 6. ed. São Paulo: Paz e Terra, 2011

COMISSÃO EUROPEIA. “Final report of the High Level Expert Group on Fake News and Online Disinformation”. 2018. Disponível em <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>. Último acesso em 20.11.2020

CONTRERAS, Belisario. “3 ways governments can address cybersecurity in the post-pandemic world”. World Economic Forum. 29 de junho, 2020. Disponível em <https://www.weforum.org/agenda/2020/06/3-ways-governments-can-address-cyber-threats-cyberattacks-cybersecurity-crime-post-pandemic-covid-19-world/>. Último acesso em 20.11.2020.

Dicionário Priberam da Língua Portuguesa [em linha], 2008 2020, https://dicionario.priberam.org/infodemia. Consultado em 01-11-2020.

FISHER, Dennis. “The growing overlap of disinformation and security”. Decipher: 23 de janeiro, 2020. Disponível em <https://duo.com/decipher/the-growing-overlap-of-disinformation-and-security>. Último acesso em 27.11.2020.

GRAY, John; TERP, Sarah-Jane.“The MisinfoSec Framework Takes Shape: Misinformation, Stages, Techniques and Responses”. Medium, 19 de junho, 2019. Disponível em https://medium.com/@credibilitycoalition/misinfosec-framework-99e3bff5935d. Último acesso em 13.12.2020.

GROSSMANN, Luís Osvaldo; LOBO, Ana Paula. “Engenharia social é principal backdoor de segurança, sem patch que resolva”. Convergência Digital. Disponível em <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=55429&sid=18.>

ISO/IEC 27000:2018(en). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Disponível em <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.48>. Último acesso em 27.11.2020.

MILANO, Brett. “We need to be more imaginative about cybersecurity than we are right now”. Harvard Law Today, 7 de outubro, 2020. Disponível em <https://today.law.harvard.edu/we-need-to-be-more-imaginative-about-cybersecurity-than-we-are-right-now/>.

NIETZCHE, Friedrich. “Human, all too Human”. United Kingdom: Cambridge University Press, 1996.

ORGANIZATION OF AMERICAN STATES – OAS. “2020 Cybersecurity Report: Risks, Progress and the way forward in Latin America and the Caribbean”. 2020: Inter-American Development Bank. p. 29.

ROGERS, Daniel. “#FakeNews as an Information Security Problem.” RSA Conference, 2018. Disponível em <https://www.youtube.com/watch?v=zAibdueUxkg>. Último acesso em 27.11.2020.

RSA Conference. “The Power of the Human Element”, RSAC 2020. Disponível em <https://www.rsaconference.com/industry-topics/video/2020-the-power-of-the-human element#:~:text=The%20theme%20of%20RSA%20Conference,key%20to%20creating%20a %20more>. Último acesso em 27.11.2020.

SOLMS, von Rossouw; NIEKERK, van Johan. “From information security to cyber security”. Computer & Security, vol. 38 (pp97 -102). 2013: Elsevier.

VALENTE, Jonas. C. L. “Regulando desinformação e *fake news*: um panorama internacional das respostas ao problema”. Comunicação pública. VOL.14 Nº 27, 2019. Disponível em <https://journals.openedition.org/cp/5262>. Último acesso em 13.12.2020.

WALKER, Christopher. Et al. “Misinfosec - Applying Information Security Paradigms to Misinformation Campaigns”. WWW '19: The Web Conference (WWW '19), May 13, 2019.

WARDLE, Claire; DERAKHSHAN, Hossein. “Information Disorder: Toward an interdisciplinary framework for research and policy making”. 2017: Council of Europe report DGI.

Wikipedia. “Sociedade da informação”. Disponível em < https://pt.wikipedia.org/wiki/Sociedade_da_informa%C3%A7%C3%A3o>. Último acesso em 10.12.2020.

World Economic Forum Annual Meeting. “Why 2020 is a turning point for cybersecurity.” 23 de janeiro, 2020. Disponível em <https://www.weforum.org/agenda/2020/01/what-are-the-cybersecurity-trends-for-2020/>. Último acesso em 23.11.2020.