


Direito da pessoa imputada ao anonimato digital


*The accused person's right
to digital anonymity*

Jamilla Monteiro Sarkis¹

Pontifícia Universidade Católica do Rio Grande do Sul – Porto Alegre, RS, Brasil

jamilla.sarkis@gmail.com

 <http://lattes.cnpq.br/5715311540839235>

 <https://orcid.org/0000-0002-2730-5950>

RESUMO: Partindo da necessidade de se ampliar, na era virtual, o rol de direitos fundamentais disponíveis à pessoa imputada na mesma proporção em que se estendem, em seu desfavor, as práticas processuais que se valem de recursos tecnológicos, o artigo propõe responder a seguinte pergunta: teria a pessoa imputada o direito ao anonimato digital? Sem desconsiderar a necessidade de intervenção estatal quando utilizado na prática de ilícitos penais, o trabalho propõe, metodologicamente, uma revisão bibliográfica interdisciplinar para conceituar as técnicas antiforenses como importantes ferramentas para proteger o direito da pessoa imputada de não produzir provas digitais em seu desfavor, destacando o anonimato como uma de suas mais eficazes ferramentas e defendendo a relevância de sua tutela jurídica na era *cyber*.

PALAVRAS-CHAVE: Anonimato; Provas Digitais; Antiforense.

ABSTRACT: *Based on the need to expand, in the virtual age, the list of fundamental rights available to the accused person in the same proportion that procedural practices that use technological resources are extended to their disadvantage, the article proposes to answer the following question: would the accused person*

¹ Doutora em Direito pela Pontifícia Universidade Católica de Minas Gerais, em Estágio Pós-Doutoral na Pontifícia Universidade Católica do Rio Grande do Sul. Mestre em Direito pela Universidade Federal de Minas Gerais. Advogada.

have the right to digital anonymity? Without disregarding the need for state intervention when used in the practice of criminal offences, the paper methodologically proposes an interdisciplinary bibliographical review to conceptualize anti-forensic techniques as important tools for protecting the right of the accused person not to produce digital evidence against them, highlighting anonymity as one of its most effective tools and defending the relevance of its legal protection in the cyber age.

KEYWORDS: *Anonymity; Digital evidence; Antiforensics.*

SUMÁRIO: Introdução; 1. As ferramentas antiforenses: novo conceito para um conceito novo; 2. Anonimato das provas digitais: a técnica antiforense na prática; 3. Anonimato como direito da pessoa imputada na era *cyber*; Considerações Finais; Referências.

INTRODUÇÃO

A frase “tudo que você disser poderá e será usado contra você nos Tribunais” faz parte do roteiro de todo filme ou seriado policial desde meados da década de 1960 e é dita sempre que alguém é preso ou acusado da prática de crime. O brocardo surgiu no julgamento, realizado pela Suprema Corte dos Estados Unidos da América, do caso *Miranda v. Arizona*, ocasião na qual se fixou o entendimento de que as pessoas imputadas devem ser cientificadas acerca do direito de não produzirem provas em seu desfavor – o *nemo tenetur se detegere*.

Esse direito fundamental – consagrado, no Brasil, como a não autoincriminação² - passou a ser insuficiente quando não apenas “o que disser”, mas tudo que postar, digitar, conversar, fotografar, arquivar, gravar, filmar, curtir, *printar* ou pesquisar poderá e será usado contra a pessoa imputada.

² Sobre a não autoincriminação e a importância de sua adequação à tecnologia, veja-se: Sarkis (2024).

Em tempos de constante incremento da *surveillance*³ no ambiente *cyber*⁴, os métodos ocultos de investigação criminal⁵ – aqueles que têm como elemento principal o desconhecimento da pessoa afetada - evoluem constantemente e a passos largos. As novidades tecnológicas os tornam, cada vez mais, onipotentes, onipresentes e onisciente, úteis a identificar padrões de comportamento, a traçar perfis psicológicos, a localizar pessoas de interesse e acessar a integralidade de seus dados.

Todas essas interações entre tecnologia e processo acabam por criar conflitos e viabilizar novas formas de interação entre os sujeitos e instituições. Afinal, com a criminalidade se voltando aos espaços virtuais e com o incremento da *cyber-surveillance* nos ambientes digitais, parece natural que as atividades de persecução penal também sofram os reflexos da virada tecnológica.

Ilustra bem essa nova realidade um caso ocorrido na cidade de Swansea, no País de Gales, no qual um homem foi condenado pelo homicídio de sua esposa após a Polícia ter extraído da assistente virtual

³ Utiliza-se o termo em inglês *surveillance* diante da insuficiência, na Modernidade, do termo “vigilância”. Conforme esclarece Elias Jacob Menezes Neto (2016, p. 89), enquanto as práticas de vigilância são tão antigas quanto a própria civilização ocidental, o fenômeno da *surveillance* apenas ocorre com o surgimento de novas tecnologias, com consequências próprias – “especialmente a fluidez, a descentralização e a desterritorialização” – que possibilitam a superação da singela ideia de vigiar.

⁴ Expõe Mariah Brochado que teria sido André Marie Ampère o primeiro a adotar a expressão *cyber*, em 1834, quando designou a inauguração de “um novo rol de saberes que se ocupam do estudo do pensamento e dos meios pelos quais os homens, por intermédio da comunicação, vivem e se governam” (Brochado, 2023, p. 162). Etimologicamente, *cyber* é uma palavra inspirada no prefixo grego *kyber*, que remetia “à condução de embarcações, e vindo pelo latim a expressar também comando, governo” (Brochado, 2023, 162).

⁵ Conforme as lições de Manuel Valente (2017, p. 473), os métodos ocultos de obtenção da prova se baseiam na interseção entre dois importantes pilares sociais: primeiro, o clamor dos cidadãos – que se encontram em estado paranoico e de medo esquizofrênico – pela celeridade e “eficiência” da justiça perante fenômenos como o terrorismo, o tráfico de drogas e a criminalidade organizada. Em segundo lugar, a opção dos decisores políticos por implementar políticas criminais populares, capazes de angariar votos, mas insuficientes para solucionar o problema da criminalidade na perspectiva do Estado de Direito.

Alexa⁶, desenvolvida pela Amazon, áudios que comprovavam seu envolvimento no crime.

Exatamente por isso, pode-se afirmar que, hoje, significativa parcela das evidências produzidas contra as pessoas envolvidas nos fatos penais consistem em provas digitais. Estas são descritas por Burkhard Schafer e Stephen Mason (2017, p. 19)⁷ como aquelas que transitam pelo *cyberespaço*, ainda que naturalmente digitais ou digitalizadas.

No caso das provas físicas – como um documento impresso em papel, por exemplo – a não autoincriminação poderia ser exercida de diferentes maneiras: o papel poderia ser rasgado, descartado, queimado, rasurado. Mas, no âmbito das provas digitais, o exercício desse direito fundamental exige práticas próprias, denominadas antiforenses, e se realiza a partir da exclusão, da alteração e do anonimato de elementos digitais.

Diante desse contexto, surge a necessidade de se ampliar o rol de direitos fundamentais disponíveis às pessoas envolvidas nos fatos penais, na mesma proporção em que se estendem, em seu desfavor, as práticas processuais que se valem de recursos tecnológicos. Para os fins deste trabalho, especificamente, a pergunta para a qual se busca resposta é a seguinte: teria a pessoa imputada o direito ao anonimato digital?

Para tanto, o trabalho está dividido em três partes: (a) uma primeira, que introduz as técnicas antiforenses como importantes ferramentas para proteger o direito da pessoa imputada de não produzir provas digitais em seu desfavor; (b) uma segunda, que analisa o anonimato das provas digitais; e (c) uma terceira, que busca caracterizar o anonimato digital como um direito das pessoas imputadas que pode coexistir com o dever no Estado de investigar, processar e julgar os ilícitos penais praticados no ambiente *cyber*.

⁶ A reportagem está disponível em: <https://bit.ly/3HgfNpy>. Acesso em: 11 jun. 2024.

⁷ Conceituam os autores como provas digitais os “dados (incluindo a saída de dispositivos analógicos ou dados em formato digital) que sejam manipulados, armazenados ou comunicados por qualquer dispositivo fabricado, computador ou sistema de computador ou transmitidos por um sistema de comunicação, que tenham o potencial de tornar o relato factual de qualquer uma das partes mais provável ou menos provável do que seria sem a evidência” (Schafer; Mason, 2017, p. 19).

Metodologicamente, a pesquisa será desenvolvida a partir de revisão bibliográfica interdisciplinar, que conjuga obras jurídicas que, por si, já são dotadas de interdisciplinaridade, com textos elaborados no âmbito das Ciências da Computação e da Engenharia.

Ao final, evidencia-se que, assim como o Estado tem, diuturnamente, investido em tecnologias auxiliares às investigações em ambiente eletrônico, as pessoas usuárias de dispositivos eletrônicos têm a seu dispor diversas ferramentas que permitem a potencialização da tutela dos seus direitos no “mundo virtual”.

1. AS FERRAMENTAS ANTIFORENSES: NOVO CONCEITO PARA UM CONCEITO NOVO

Por tratar-se de tema relativamente novo, a literatura especializada nas provas digitais não desenvolveu, até então, um conceito uníssono em torno do que seria uma prática antiforense. Em trabalho conduzido por membros do Cyber Forensics Research & Education Group (Conlan; Baggili; Breitinger, 2016), foram catalogadas quatorze definições diferentes para o termo, adotadas em pesquisas publicadas entre os anos de 2002 e 2012. Em comum, todas as conceituações apresentam desvalores sobre a aplicação das técnicas antiforenses, atribuindo uma conotação negativa com tons de reprovabilidade.

Alguns exemplos seriam: “tentativa de limitar a identificação, coleta, agrupamento e validação de provas digitais” (Peron e Legary, 2005); “quaisquer tentativas de comprometer a disponibilidade ou a utilidade de provas digitais para o processo forense” (Harris, 2006); “prática de impedir uma investigação forense adequada” (Sremack e Antonov, 2007); “métodos utilizados para impedir o processo de investigação digital conduzido por investigadores forenses legítimos” (Albano, Castiglione, Cattaneo e De Santtis, 2011).

Outras definições, promovidas em trabalhos posteriores àqueles coletados por Conlan, Baggili e Breitinger também atribuem à ideia de antiforense um sentido nocivo. Para Anu Jain e Gурpal Chhabra (2014, p. 413), por exemplo, o termo consistiria em uma série de contramedidas adotadas para frustrar ou se esquivar de investigações forenses.

Já de acordo com Stephen Mason, Andrew Sheldon e Hein Dries (2017, p. 325), seria antiforense qualquer técnica, ferramenta de *hardware* ou *software* capaz de impedir, frustrar ou retardar a análise forense de um portador de dados e afetar, negativamente, a existência, a quantidade, a autenticidade ou a qualidade das provas digitais disponíveis em um dispositivo.

“Invalidar”, “comprometer”, “dificultar”, “frustrar”, “impossibilitar”, “impedir”, “disfarçar”, “falsificar”, “esquivar” e “retardar” são alguns dos verbos que, de acordo com autores e autoras da área, atribuem significado às ações antiforenses. Seu papel, nesse sentido, seria de antagonismo em relação às investigações que envolvem provas digitais.

A própria etimologia do termo “antiforense” não parece dar margem a conceitos diversos. O prefixo “anti” deriva do idioma grego antigo e denota a ideia de oposição ou contrariedade. A expressão “forense”, por sua vez, se refere à ciência aplicada pelas agências de segurança pública na solução de crimes e está, intrinsecamente, relacionada aos termos “foro” e “justiça”.

O fato de serem, à unanimidade, compreendidas como prejudiciais às investigações ou contrárias aos interesses da justiça, acaba por problematizar a utilização das práticas antiforenses. É como se qualquer mácula à obtenção de provas digitais por parte das agências de investigação devesse, necessariamente, ser vilanizada e, em última instância, combatida.

Tais conceituações, todavia, não se coadunam com o ideal democrático de que os fins da investigação criminal não devem prevalecer sobre os direitos fundamentais, inclusive o direito à não autoincriminação – em especial, no âmbito de não produzir provas em desfavor da pessoa.

Propõe-se, nessa linha, que as técnicas antiforenses sejam conceituadas como aquelas que garantem, às pessoas usuárias do ambiente *cyber*, o exercício afirmativo do direito de não produzirem contra si provas digitais. Essa definição incorpora, ao mesmo tempo, a ideia de oposição representada pelo prefixo “anti” – aqui lido como a oposição da pessoa envolvida no fato penal à produção de provas em desfavor – e o objeto da expressão “forense” – notadamente as provas digitais.

O conceito aqui proposto também se adequa à perspectiva de soberania digital (Floridi, 2020, p. 369). Trata-se de ideia multidimensional

(Belli, 2021, *e-book*) que se refere à capacidade de Estados, pessoas jurídicas e físicas⁸ de exercerem - com autonomia estratégica - controle e poder sobre as infraestruturas digitais que acessa e seus dados.

Nesse aspecto, é imperioso que usuários e usuárias do ambiente *cyber* conheçam e estejam aptos a compreender os efeitos positivos e negativos que cada escolha tecnológica determina, sendo essencial uma “visão sistêmica para entender como os diferentes elementos dos ecossistemas digitais se inter-relacionam e como desenvolver, usar e regular a tecnologia ao invés de ser regulado por ela” (Belli *et al*, 2023, p. 54).

Para os fins deste artigo, entende-se que as pessoas envolvidas em fatos penais podem exercer sua soberania digital a partir de técnicas antiforenses, as quais afirmam o direito de não produzir provas digitais desfavoráveis aos seus interesses defensivos.

São diversas as categorias antiforenses e, a esse respeito, também inexistente consenso na literatura especializada. Os professores da National Defense University Murat Gül e Emin Kugu (2017) promoveram uma pesquisa qualitativa a respeito das diferentes formas a partir das quais os autores e autoras que escreveram sobre o tema categorizaram as técnicas antiforenses, demonstrando que apesar das diferentes categorias estabelecidas por cada autor e autora no tocante às técnicas antiforenses, existem elementos que são comuns à maioria: a exclusão (ou destruição e eliminação), a alteração (ou ocultação, codificação, reorganização e substituição) e o anonimato (ou ofuscação, contracepção, codificação, codificação, criptografia e prevenção) de provas digitais.

Como três grandes categorias, a exclusão, a alteração e o anonimato agregam, em si, muitas práticas diferentes. A seguir, tendo o anonimato como foco do trabalho, serão estudadas as principais ferramentas para o emprego dessa técnica antiforense.

⁸ Válido destacar, conforme Belli *et al* (2023, p. 51) que “A soberania digital deve, portanto, ser vista como a capacidade de uma nação, de um grupo ou de uma pessoa – física ou jurídica – de entender o funcionamento da tecnologia digital e ter um controle efetivo sobre as infraestruturas e dados digitais”.

2. ANONIMATO DAS PROVAS DIGITAIS: A TÉCNICA ANTIFORENSE NA PRÁTICA

Ao introduzir o tema das técnicas antiforenses na obra que dedicaram às provas digitais, Mason, Sheldon e Dries (2017, p. 324) comentam que, assim como o desenvolvimento da papiloscopia levou os criminosos a usarem luvas durante a prática de crimes, o incremento das perícias digitais tem incentivado ações preventivas que evitem a identificação das pessoas envolvidas no fato penal.

No ambiente eletrônico, o anonimato é o principal método de proteção de informações e comunicações cujo conteúdo deseja-se proteger. Sua compreensão, porém, não pode ser confundida com outra técnica: a anonimização de dados.

De acordo com a Lei Geral de Proteção de Dados (LGPD)⁹, consideram-se anonimizados aqueles dados relativos à pessoa titular que não possa ser identificada, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (artigo 5º, inciso III).

Trata-se, na definição de Jordan Oliveira e Marília Cunha (2021, p. 161), de um esforço adotado pelo agente de tratamento de dados em fase posterior à sua criação e ao seu compartilhamento por quem detém sua titularidade e cuja reversão, ainda que difícil, é possível¹⁰.

Os autores exemplificam a ideia de anonimização a partir de um caso concreto envolvendo a empresa Netflix, que lançou um concurso para potencializar seu algoritmo de sugestão de conteúdo. Para tanto, os candidatos tiveram acesso a uma versão anonimizada da base de dados da

⁹ Válida a ressalva no sentido de que a LGPD que está em vigor no Brasil não tem aplicação aos dados relacionados à segurança pública ou à persecução penal.

¹⁰ Para o Grupo de Trabalho 29, constituído pela União Europeia para lidar com as questões relacionadas à proteção da privacidade e dos dados pessoais e que atuou até 25 de maio de 2018, com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados: “A anonimização constitui um tratamento posterior de dados pessoais; como tal, deve satisfazer o requisito de compatibilidade em função dos fundamentos jurídicos e circunstâncias do tratamento posterior. Além disso, os dados anônimos são, de facto, abrangidos pelo âmbito de aplicação da legislação relativa à proteção de dados, mas os titulares dos dados podem ainda ter direito à proteção ao abrigo de outras disposições (tais como as relativas à proteção da confidencialidade das comunicações)”. Disponível em: <http://bit.ly/48szaHJ>. Acesso em: 11 jun. 2024.

plataforma de *streaming*, que contava com a avaliação de filmes e séries entre o período de 1998 a 2005 (Oliveira; Cunha, 2021, p. 162).

Nessa versão anonimizada dos dados da Netflix, os candidatos tinham acesso apenas ao título do conteúdo avaliado (nome do filme ou série), à data em que foi feita a avaliação pelo usuário ou usuária da plataforma de *streaming* e a nota que foi conferida¹¹.

A anonimização, porém, não impediu que os dados fornecidos pela Netflix fossem cruzados com informações disponíveis em outra base – a do *website* Internet Movie Database – na qual usuários e usuárias se cadastram e identificam com a finalidade de avaliarem filmes e séries.

Bastou uma interface entre os dados anonimizados pela Netflix e aqueles disponíveis abertamente no *website* Internet Movie Database para que usuários e usuárias da plataforma de *streaming* que avaliaram determinados filmes em certas datas fossem identificados (Narayanan; Shmatikov, 2008).

Eis a principal diferença entre anonimização e anonimato: enquanto a anonimização é resultado de um tratamento realizado sobre os dados já criados e disponíveis e, portanto, pode ser reversível¹², o anonimato consiste em um esforço do usuário ou da usuária em relação aos seus próprios dados que se realiza antes mesmo de sua criação ou disponibilização, viabilizado por instrumentos como VPN e The Onion Routing (Tor), duas ferramentas que têm o mesmo modelo de comunicação

¹¹ A técnica de anonimização empregada, nesse caso, é a da generalização, a partir da qual “busca-se modificar as escalas ou magnitudes de um dado pessoal” (Oliveira; Cunha, 2021, p. 162). A generalização, na definição do Grupo de Trabalho 29 da União Europeia, consiste em “em generalizar, ou diluir, os atributos dos titulares dos dados através da alteração da respetiva escala ou ordem de grandeza (isto é, uma região em vez de uma cidade, um mês em vez de uma semana). Embora a generalização possa ser eficaz para impedir a identificação, não permite a anonimização efetiva em todos os casos; requer, em particular, abordagens quantitativas específicas e sofisticadas para evitar a possibilidade de ligação e inferência”. Disponível em: <http://bit.ly/48szaHJ>. Acesso em: 11 jun. 2024.

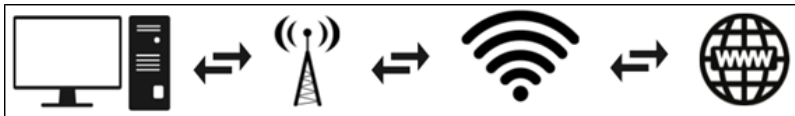
¹² Nesse sentido, escreve Bruno Bioni (2020, p. 191) que a representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados constitui um mito, sendo “cada vez mais recorrente a publicação de estudos que demonstram ser o processo de anonimização algo falível”.

por tunelamento¹³ e usam a tecnologia de criptografia para garantir a integridade dos dados (Ramadhani, 2018).

O acesso à internet é intermediado, em regra, pela operadora contratada pela pessoa usuária, que atribui um endereço de IP ao dispositivo e, conseqüentemente, é capaz de monitorar todas as atividades realizadas *online*.

A Figura 1 ilustra o acesso regular à internet, que se dá mediante a conexão direta entre o dispositivo da pessoa usuária (representado pelo computador), a empresa provedora (representada pela torre de transmissão), a internet (representada pelo símbolo próprio, também associado à conexão *wi-fi*) e o *website* que se quer acessar (representado pela sigla WWW, ou World Wide Web). As setas em sentido duplo indicam que, tão logo a pessoa usuária faça a requisição de acesso a determinado *website*, as informações solicitadas lhe serão transmitidas:

FIGURA 1. Conexão de internet regular



Fonte: Elaborado pela autora.

Por outro lado, quando a pessoa usuária se vale do acesso à internet com VPN, a requisição junto ao *website* que se pretende visitar é precedida por um servidor particular.

A Figura 2 ilustra o acesso à internet com a utilização de VPN, que se dá mediante a conexão inicial entre o dispositivo da pessoa usuária (representada pelo computador), a empresa provedora (representada pela torre de transmissão) e a internet (representada pelo símbolo próprio).

Mas, antes que a requisição de acesso seja encaminhada pela pessoa usuária ao *website* que pretende visitar, seus dados passam pelo servidor particular VPN (representado pela imagem de um servidor),

¹³ Técnica de interligação de diferentes redes que possibilita a comunicação entre *hosts* de protocolos diferentes (Tanenbaum, 2003, p. 328).

que pode, inclusive, criptografar as informações antes de enviá-las ao *website*. As setas em sentido duplo indicam que, tão logo a pessoa usuária faça a requisição de acesso a um determinado *website*, as informações solicitadas lhe são transmitidas:

FIGURA 2. Conexão de internet com VPN



Fonte: Elaborado da autora.

Efetivamente, ainda que seja promovida com o uso de VPN, a conexão de internet passa pela operadora contratada. A diferença é que, como todos os dados passam, inicialmente, pelo servidor VPN, o provedor não tem acesso às ações que foram praticadas pela pessoa usuária durante o uso do serviço e, com isso, desconhece informações como quantos e quais *websites* foram visitados, em qual horário e por quanto tempo, a partir de qual local etc.

Da mesma forma, o provedor do *website* visitado desconhecerá as informações (como, por exemplo, o IP e os *cookies*¹⁴) da pessoa usuária.

São diversas as opções de VPN que podem ser utilizadas por quem pretende manter anônimos seus acessos à internet. Alguns dos principais *softwares* são o ExpressVPN¹⁵, o CyberGhost¹⁶ e o TunnelBear¹⁷. A Figura 5 demonstra o funcionamento deste último aplicativo.

¹⁴ Segundo Park e Sandhu (2000), servidores e navegadores da WWW usam *cookies* para capturar informações, a fim de otimizar comunicações subsequentes. Essas informações são capazes de identificar características e preferências dos usuários, motivo pelo qual possuem elevado valor de mercado.

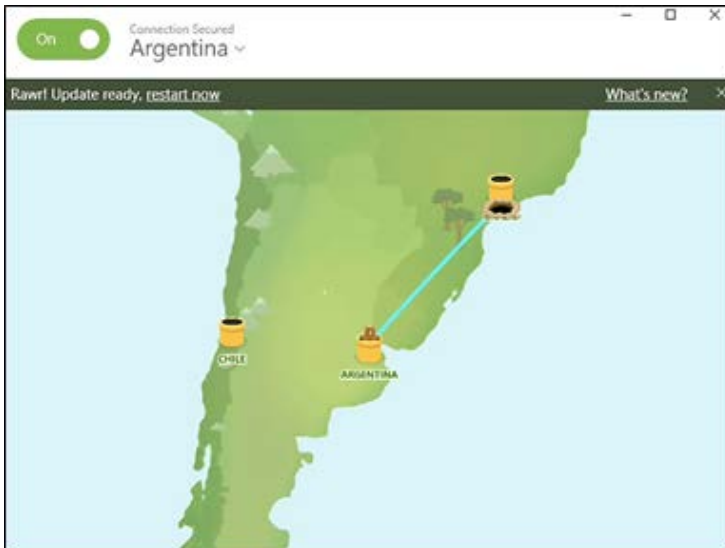
¹⁵ O ExpressVPN oferece, como funcionalidades básicas servidores em 94 países, mascaramento de endereços de IP e compatibilidade com múltiplos sistemas operacionais.

¹⁶ O CyberGhost “criptografa seu tráfego on-line e oculta seu endereço IP real, quer você esteja fazendo transmissões, baixando torrents, jogando, comprando, usando seu banco ou simplesmente navegando”.

¹⁷ O TunnelBear “criptografa sua conexão de internet para manter sua atividade online privada em qualquer rede” (Tradução nossa).

De forma lúdica, o aplicativo identifica a localização da pessoa usuária (no exemplo, o Brasil) pelo ícone de um urso. Demarcada sua posição geográfica, a pessoa usuária seleciona a qual país deseja conectar sua rede (no exemplo, a Argentina). Em seguida, o ícone do urso se movimenta até o país escolhido e ali se instala.

FIGURA 3. Conexão de internet com VPN pelo aplicativo TunnelBear



Fonte: TunnelBear (c2023).

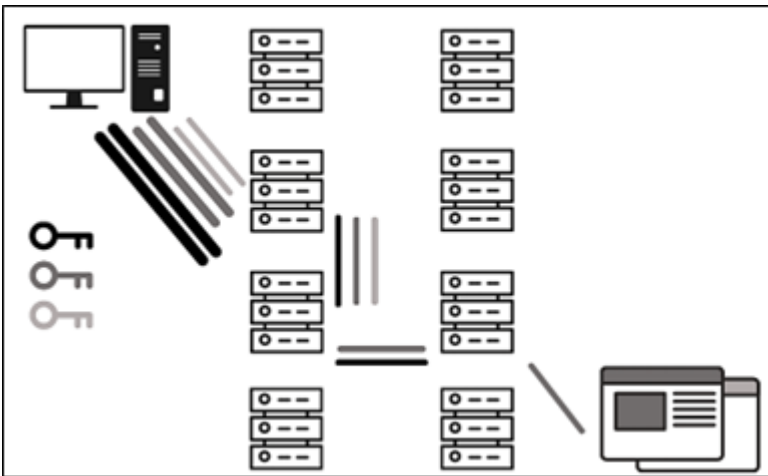
A partir do momento em que a conexão é feita a uma rede estrangeira, os dados da pessoa usuária tornam-se anônimos. Assim, quando ingressar em qualquer *website*, as informações enviadas para o provedor darão conta de que o dispositivo (que, na verdade, está no Brasil) está em outro país (Argentina). Além do anonimato, a pessoa usuária consegue, utilizando-se da VPN, visitar *sites* que não estão disponíveis em sua localidade.

A segurança da conexão pode, ainda, ser incrementada pelo Tor, tecnologia que consiste no processo de roteamento por diversas camadas (por isso, a referência à cebola, ou *onion* em inglês), nas quais os dados são criptografados em três etapas.

Com isso, o Tor é capaz de isolar cada *website* visitado e impedir rastreamentos, apagando automaticamente todos os *cookies* e registros do histórico de navegação. Além disso, ele mascara o número IP de seus usuários e obsta sua identificação e localização.

A Figura 4 ilustra o acesso à internet com a utilização do Tor. O dispositivo da pessoa usuária (representado pelo computador) trafega por meio de três servidores aleatórios (chamados nós ou relés – representados pelos diferentes servidores). O último relé do circuito é o que vai enviar os dados para a internet, já submetidos a três fases de criptografia (representadas pelas cores das três chaves) para, finalmente, conseguir acessar suas camadas (representadas pelas páginas) mais profundas:

FIGURA 4. Conexão de internet com Tor



Fonte: Elaborado pela autora, adaptado de The Tor Project¹⁸.

¹⁸ Organização sem fins lucrativos fundada em 2006 para manter o desenvolvimento da rede Tor e enfrentar a censura governamental. O *website* oficial do projeto coteja suas atividades com importantes eventos da história recente: “O Tor começou a ganhar popularidade entre ativistas e usuários aficionados por tecnologia interessados em privacidade, mas seu uso ainda era difícil por pessoas com menos intimidade com os meandros tecnológicos. Assim, em 2005, deu-se início ao desenvolvimento de ferramentas que transcendessem o proxy Tor. O desenvolvimento do Navegador Tor começou em 2008. Com o Navegador Tor, a rede Tor tornou-se mais acessível a pessoas comuns na internet e a

É exatamente pela conexão do dispositivo a diferentes nós, conforme demonstrado pela Figura 4, que as pessoas usuárias do Tor conseguem garantir seu anonimato.

O Tor, originalmente, foi desenvolvido pelo Laboratório de Pesquisa Naval dos Estados Unidos com a finalidade de acessar conteúdo bloqueado, contornar a censura e manter a privacidade de comunicações confidenciais. Hoje, consiste na principal ferramenta de acesso à *deep web* e à *dark web*.

Explicam Nazah *et al.* (2020, p. 171.797) que, enquanto a internet normalmente utilizada pode ser acessada por meio de mecanismos de busca padrão, como Google e Yahoo, existem grandes seções – chamadas de *deep web* – que não são indexadas e estão ocultadas dos mecanismos de busca padrões e correspondem a mais de noventa por cento de toda a informação disponível na internet.

A *dark web*, por sua vez, consiste em um subconjunto que representa, aproximadamente, 57% do total páginas da *deep web* e no qual se verifica, inclusive, a prática de inúmeros ilícitos penais.

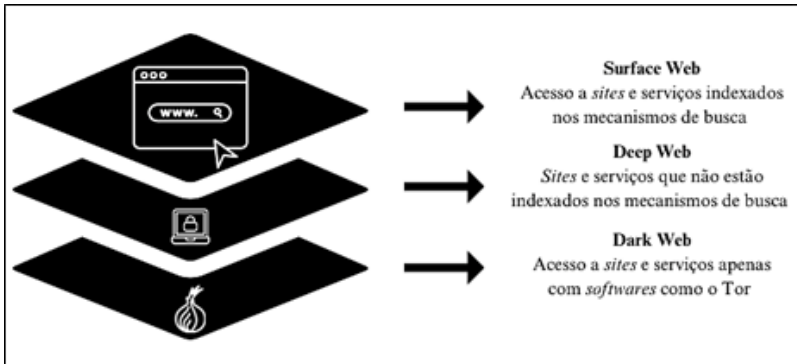
A Figura 5 representa a divisão da internet nessas três camadas. A primeira (quadro superior) ilustra a *surface web*, composta pelas páginas que são indexadas e podem ser localizadas pelos mecanismos de busca tradicionais (representados pela imagem de um buscador).

A segunda camada (quadro do meio), por sua vez, corresponde à *deep web*, capaz de acessar sites que não estão indexados (representados pela imagem de uma tela com um cadeado ao meio). Por fim, a terceira camada (quadro inferior) estampa a *dark web*, cujo acesso

ativistas, o que fez do Tor uma ferramenta fundamental durante a Primavera Árabe no final de 2010. Ele não somente protegia a identidade das pessoas on-line como possibilitava o acesso a recursos fundamentais, a mídias sociais e a websites bloqueados. A necessidade de ferramentas de proteção contra a vigilância em massa se tornou uma preocupação principal graças às revelações de Snowden em 2013. O Tor não somente operacionalizou as atividades de denúncia de Snowden, mas o conteúdo dos documentos revelados também assegurava que, naquela época, o Tor não podia ser quebrado. A consciência do público sobre rastreamento, vigilância e censura pode ter aumentado, porém, também aumentou a prevalência desses freios à liberdade na internet. Hoje, a rede dispõe de milhares de relés operados por voluntários com milhões de usuários ao redor do mundo. É essa diversidade que mantém seguros os usuários Tor”.

depende de *softwares* próprios, como o Tor (representado pelo símbolo do programa – uma cebola):

FIGURA 5. Divisão da internet em camadas



Fonte: Elaborado pela autora.

Nazah *et al.* (2020) elencam como oito principais atividades ilícitas disponíveis na *dark web* as seguintes: tráfico de pessoas e exploração sexual, indústria pornográfica, *marketing* de homicidas mercenários, compra e venda de entorpecentes, pornografia infantil, terrorismo, compra e venda de dados pessoais e ocultação de valores por meio de criptoativos¹⁹.

Ressaltam, igualmente, as dificuldades encontradas pelas autoridades durante as investigações que envolvem essas camadas mais profundas da internet, mencionando algumas das ferramentas disponíveis

¹⁹ Esclarecedora a definição cunhada por Ahamad, Nair e Varghese (2013, p. 43, tradução nossa): “As criptomoedas são arquivos físicos pré-computados que utilizam uma chave pública/pares de chaves privadas gerados com base em um algoritmo de criptografia específico. A chave atribui a propriedade de cada par de chaves, ou “moeda”, à pessoa que está de posse da chave privada. Esses pares de chaves são armazenados em um arquivo chamado ‘wallet.dat’, que reside em um diretório oculto padrão no disco rígido do proprietário. As chaves privadas são enviadas aos usuários usando endereços de carteira dinâmicos gerados pelos usuários envolvidos nas transações. O endereço de pagamento de destino é a chave pública do par de chaves de criptomoeda. Há uma quantidade finita de cada criptomoeda disponível na rede, e o valor de cada unidade é atribuído com base na oferta e na demanda, bem como nos níveis de dificuldade flutuantes exigidos para a mineração de cada moeda”.

para mitigar as consequências do anonimato: o rastreamento de contas em redes sociais que são potencialmente utilizadas por usuários da *dark web* e a análise do fluxo de criptomoedas (Nazah *et al.*, 2020, p. 171.804).

Válido registrar, porém, que nem toda utilização da *dark web* está relacionada à prática de condutas delituosas. Thais Sardá, Simone Natale e John Downey (2022) pesquisam o tema da *dark web* e, após a realização de trabalho empírico que analisou mais de 830 artigos publicados nos seis principais periódicos do Reino Unido, concluíram que essa tecnologia é, comumente, associada ao cometimento de crimes ou atos imorais; enquanto seus aspectos positivos, relacionados à proteção da privacidade e da liberdade de expressão são pouco mencionados.

Essa repercussão será objeto de análise no próximo item, que buscará discutir e enfrentar as principais críticas atreladas ao exercício do anonimato como técnica antiforense, com enfoque na tutela da privacidade e da intimidade, diante das práticas de *cyber-surveillance*, a ser exercida por meio do anonimato digital.

3. ANONIMATO COMO DIREITO DA PESSOA IMPUTADA NA ERA CYBER

Na era *cyber* o anonimato não pode ser visto apenas como uma técnica antiforense, empregada pela pessoa envolvida em fatos penais para evitar a produção de provas em seu desfavor. Deve, concretamente, ser percebido como um direito que demanda proteção e deriva da garantia à não autoincriminação porquanto busca assegurar, à pessoa imputada, o direito de não produzir provas digitais em seu desfavor.

Em suas primeiras expressões (Coleman, 2019, p. 568), o anonimato esteve relacionado, precipuamente, às liberdades civis – como o direito à livre associação defendido pela National Association for the Advancement of Colored People (NAACP) em meados da década de 1950, após ser obrigada, pela Suprema Corte do Alabama, a informar os dados pessoais de seus membros.

No âmbito virtual, conforme salientam Diego Machado e Danilo Doneda (2020), até o início dos anos 2000, na então era Web 1.0²⁰, os

²⁰ Os marcos Web 1.0 e Web 2.0 estão na obra de Lawrence Lessig (2009).

protocolos de internet acabaram por estabelecer o anonimato das pessoas usuárias como regra, de modo que apenas a empresa provedora dos serviços de conexão conhecia a identidade por trás da máquina.

Porém, com o advento da Web 2.0, criou-se uma gama de serviços em rede, especialmente direcionada às interações sociais, a partir das quais a ideia de “ser anônimo” deu lugar às de “ser conhecido”, “ser identificado”, “ser conectado”²¹.

Toda essa exposição (Lanier, 2018), entretanto, passou a constituir verdadeiro obstáculo ao desenvolvimento dos direitos da personalidade – inclusive, a privacidade – quando se tornou ferramenta da *cyber-surveillance*.

A literatura especializada, nesse aspecto, é uníssona ao atribuir a um evento certo o “despertar da consciência” das pessoas usuárias para essa realidade: as denúncias feitas por Edward Snowden²², que expuseram o acesso irrestrito das agências de segurança estadunidense ao tráfego de comunicações a nível mundial.

²¹ Os autores mencionam que, a partir de 2012, a principal rede social do mundo – o Facebook – passou a adotar como diretriz a *real-name policy*, ou política do nome real, que exigia de seus usuários uma identificação verdadeira como condicionante à criação do perfil.

²² O analista de sistemas da Central Intelligence Agency (CIA) atuava na National Security Agency (NSA) quando trouxe a público informações sobre a estrutura de *cyber-surveillance* estabelecida pela Agência, capaz de acessar as comunicações eletrônicas mantidas por milhões de pessoas e de coletar dados pessoais mediante a utilização de programas de espionagem. Em sua biografia, narra Snowden (2019, *e-book*, tradução nossa): “Nas profundezas de um túnel sob uma plantação de abacaxis - uma antiga fábrica de aviões subterrânea da época de Pearl Harbor - eu estava sentado em um terminal a partir do qual eu tinha acesso praticamente ilimitado às comunicações de quase todos os homens, mulheres e crianças do mundo que já haviam discado um telefone ou tocado em um computador. Entre essas pessoas estavam cerca de 320 milhões de meus concidadãos americanos, que, na condução regular de suas vidas cotidianas, estavam sendo vigiados em flagrante violação não apenas da Constituição dos Estados Unidos, mas dos valores básicos de qualquer sociedade livre. A razão pela qual você está lendo este [livro] é que eu fiz uma coisa perigosa para um homem em minha posição: Decidi contar a verdade. Coletei documentos internos do IC que evidenciavam a violação da lei pelo governo dos EUA e os entreguei a jornalistas, que os examinaram e publicaram para um mundo escandalizado”.

A partir do caso Snowden, vários outros exemplos de *cyber-surveillance* vieram à tona: Machado e Doneda (2020) citam que, em 2016, a Electronic Frontier Foundation (EFF) divulgou a existência do programa Hemisphere, operado pela operadora de telefonia AT&T e que preservava trilhões de registros de ligações; no mesmo ano, se tornou pública a existência do monitoramento, realizado pela empresa Yahoo e por ordem da Foreign Intelligence Surveillance Court (FISC), de milhares de contas de *e-mails*.

É nessa perspectiva que o anonimato passa a demandar uma tutela própria, com um modelo jurídico de proteção alicerçado na privacidade, mas com conceitos e técnicas específicos. Entende-se, portanto, como anonimato digital o direito das pessoas de se comunicarem sem serem identificadas ou rastreadas, assim como de terem o conteúdo de suas mensagens e os dados relacionados ao envio/recebimento protegidos.

Comentam Machado e Doneda (2020) que, em alguns países, o reconhecimento do anonimato digital já foi objeto de decisões pelos Tribunais Superiores, como Israel, Estados Unidos, Alemanha e Canadá. A pesquisa mais intensa realizada sobre o tema do anonimato *online*, no âmbito do Direito comparado, foi desenvolvida por Giorgio Resta (2014), cujas principais contribuições – apesar de, expressamente, não serem destinadas a fins penais²³ – estão na proposta de dois modelos regulatórios que, mesmo não sendo ideais, poderiam contribuir com a tutela jurídica desse direito.

Um primeiro, baseado na licitude do anonimato como instrumento do exercício da liberdade de expressão e voltado a “incentivar uma troca de ideias e informações o mais autônoma, livre e descentralizada possível e permitir a construção de relações sociais de forma voluntária e até mesmo definida artificialmente” (Resta, 2014, p. 173, tradução nossa).

O segundo, considerando o anonimato como uma projeção do direito à proteção de dados pessoais, de modo a contemplar “o anonimato como um critério capaz de circunscrever o escopo objetivo de aplicação do regulamento ou como um princípio geral com o qual o processamento

²³ “Além disso, o foco será exclusivamente nos problemas subjacentes à proteção civil dos direitos, enquanto a proteção criminal não será abordada” (Resta, 2014, p. 172, tradução nossa).

de dados pessoais deve estar em conformidade” (Resta, 2014, p. 178-179, tradução nossa).

No Direito brasileiro, todavia, os modelos propostos por Giorgio Resta (2014) encontram obstáculos.

Isto porque, apesar de a Lei Geral de Proteção de Dados prever a anonimização de dados pessoais como técnica de tratamento de informações sensíveis (conforme discutido no item 6.3.2), a Constituição de 1988 veda, expressamente, o anonimato (artigo 5º, inciso IV). Tal restrição, conforme preleciona Virgílio Afonso da Silva (2021, p. 170), se fundamenta na ideia de que a liberdade de expressão não é absoluta e quem a excede está sujeito a punições, sendo o anonimato uma barreira da qual resultaria impunidade.

Nada obstante à vedação constitucional, necessário situar o debate do anonimato digital na era *cyber*. Afinal, no contexto da virada tecnológica²⁴, os modelos jurídicos, hoje, precisam ser pensados a partir de um paradigma tecnológico que reconhece, especialmente, as diferenças entre os espaços de expressão existentes à época em que foi elaborada a Constituição de 1988 e os que passaram a existir, de forma legítima, com o advento da internet²⁵.

No ambiente *cyber*, portanto, a vedação constitucional ao anonimato deve ser concebida de forma restrita, sem recair sobre as pessoas usuárias da internet que não desejam ser digitalmente identificadas.

Para a categoria do anonimato digital, é necessário que se assegure o anonimato em todas as etapas da comunicação virtual (Hildebrandt, 2014, p. 33), a saber: (a) em relação à pessoa responsável pelo envio,

²⁴ Os impactos do movimento conhecido como virada tecnológica, conforme identifica Dierle Nunes (2020, p. 15-17), transcendem sua mera aplicação instrumental. Afetam, de maneira concreta, o campo processual, seja pela mudança dos institutos jurídicos, seja pelo dimensionamento de uma nova racionalidade para sua implementação, seja pela criação de novos institutos.

²⁵ Queiroz (2021, p. 256-257) comenta caso concreto em que uma empresa buscava a remoção de conteúdos negativos a respeito de seu ambiente de trabalho que foram postados no portal de recursos humanos Catho Online. Um dos comentários dizia “só aceite [trabalhar nessa empresa] se estiver muito desesperado!” Na ocasião, a empresa argumentos que embora os comentários não fossem ilícitos, o mero fato de terem sido realizados de forma anônima já caracterizavam violação constitucional.

deve ser assegurado o direito de se comunicar livremente; (b) em relação à pessoa que recebeu a comunicação, deve ser assegurado o direito de se informar livremente; (c) em relação ao conteúdo da mensagem, deve ser assegurado o direito de não ser acessado indevidamente; (d) em relação aos locais de onde foi enviada e onde foi recebida, deve ser assegurado o direito de não serem conhecidos.

Esses aspectos, para além de detalharem o papel desempenhado pelo anonimato digital em cada uma das quatro fases da comunicação (Floridi, 2014), também são relevantes na medida em que refutam o ditado popular “quem não deve, não teme”.

Evidenciam, na verdade, que qualquer troca de dados, por mais trivial que seja, tem um enorme potencial de exposição, a ponto de que quem afirma “não se importar com o anonimato porque não tem nada a esconder” se equipara a quem “não se importa com a liberdade de expressão porque nada tem a dizer” (Coleman, 2019, p. 572).

Importante salientar que, apesar de serem comumente atreladas a práticas criminosas (Sardá *et al.*, 2019, p. 588), as ferramentas como VPN ou Tor têm múltiplas funcionalidades: desde mitigar o impacto das tecnologias *online* de armazenamento de dados pessoais (por exemplo, os *cookies*) e impor um limite à lógica da *cyber-surveillance*, até possibilitar a livre manifestação por parte de dissidentes de regimes políticos autoritários.

Nesse ponto, relevante o esclarecimento de Eric Jardine, após pesquisa empírica relacionada às motivações políticas de usuários do Tor:

Dados sobre o uso da rede Tor de 2011 a 2013 sugerem que a repressão política realmente impulsiona o uso de tecnologias de concessão de anonimato. Os resultados indicam que tanto os níveis muito altos quanto os muito baixos de repressão política tendem a impulsionar mais o uso do Tor. Em outras palavras, a relação entre o nível de repressão de um país e a taxa de uso individual de tecnologias de concessão de anonimato é em forma de U (Jardine, 2018, p. 436, tradução nossa).

Obviamente, não se pretende comparar, a nível de relevância social, a prática de anonimato por uma pessoa que deseja adquirir entorpecentes com o anonimato de dados promovida por alguém que teme ser compreendido por motivos raciais, sexuais, religiosos ou políticos.

Além disso, não se nega o potencial que o anonimato agrega às práticas ilícitas. Foi pela rede Tor, por exemplo, que o Silk Road – maior mercado *online* de mercadorias ilícitas, principalmente drogas, já desoberto – operou entre 2011 e 2013²⁶.

A ideia do anonimato digital, porém, não deve ser confundida com uma tentativa de esvaziar a legitimidade investigativa do Estado. Como direito das pessoas inseridas no ambiente *cyber*, anonimato digital pode ser permitido sem deixar de reclamar a intervenção estatal quando vinculado à prática de ilícitos penais.

Ainda que represente obstáculos à atuação do Estado na persecução penal – assim como o são as luvas em relação à identificação papiloscópica ou a rasura sobre documentos físicos – o anonimato digital não anula a possibilidade de identificação e repressão a ilícitos penais.

Pelo contrário: o anonimato digital, inclusive, pode servir à função secundária de incrementar a expertise informática das Autoridades:

Iniciativas como as do *Tor Project* e outras redes anônimas (*anonymity networks*) visam atender os dois requisitos citados para promover a irrastreabilidade de seus usuários. Pode haver dificuldades para a responsabilização do sujeito que lança mão das ferramentas técnicas para atingir esse tipo de anonimato na internet e cometer atos que implicam lesão a direitos e liberdades fundamentais de outrem ou infrações penais, na medida em que identificar as pessoas imputáveis é tarefa que depende da expertise informática das autoridades de investigação, principalmente, e da observância das decisões judiciais e regras legais pelos provedores de serviço de internet. Nesses casos em que o recurso a programas de computador e outros meios técnicos ocorre de modo abusivo, é legítima a intervenção de entidades estatais, nacionais ou supranacionais, para combater e reprimir as condutas de cibercriminosos nas redes digitais (Machado; Doneda, 2020).

²⁶ O caso é objeto do documentário “Deep Web”, lançado em 2015 e dirigido por Alex Winter, que mostra os detalhes da operação policial que desmantelou o Silk Road, bem como do julgamento que condenou o administrador da plataforma, Ross William Ulbricht, à prisão perpétua.

Desse modo, o anonimato digital, por si, não seria vedado e nem consistiria uma prática ilícita; além disso, os ilícitos cuja responsabilidade se pretendesse esconder poderiam ser objeto de investigações forenses por parte das agências de Segurança Pública – desde que, repita-se, o anonimato em si não fosse impedido²⁷.

Efetivamente, o anonimato digital deve ser um direito garantido às pessoas usuárias de tecnologias como forma de proteção e antes de criarem e compartilharem os dados pessoais. Caso esse anonimato seja utilizado para fins ilícitos – e apenas depois que o forem, é legítima a busca do Estado pela identificação e atribuição de responsabilidades.

Até porque, apesar de ser frequente a associação do anonimato “exclusivamente à covardia e à evasão de responsabilização”, é falaciosa a atribuição de falta de responsabilização pessoal e aumento da criminalidade ao anonimato digital (Queiroz, 2021, p. 243).

O tema da responsabilidade no ambiente digital está em voga há pelo menos três décadas e faz lembrar a frase que diz que “na internet, ninguém sabe que você é um cachorro” (*on the internet, nobody knows you're a dog*), que acompanhou a charge publicada por Peter Steiner na revista norte-americana *The New Yorker*, em julho de 1993.

A ideia de poder ser quem quiser, sem estar atrelada a um nome, uma imagem e uma localização é uma das maiores seduções proporcionadas pelo meio *online* às pessoas usuárias da internet.

Ainda em 1996 e inspirada pela charge de Steiner, a socióloga Sherry Turkle definiu a noção de “ser quem você quiser ser” como uma

²⁷ Nesse sentido: “A interpretação da vedação constitucional ao anonimato deve preferir uma concepção restrita desse conceito, que exclua situações de anonimato meramente superficial, fraco ou aparente. Além disso, a resposta jurídica a situações de ausência de identificação do autor de uma manifestação expressiva deve privilegiar a intervenção mínima (intervenção de baixa intensidade): qualquer esforço de identificação do autor de uma manifestação pressupõe a existência de ilicitude no ato expressivo, e sua responsabilização demanda a identificação de seu autor. Tal ilicitude não se confunde com a própria ausência de identificação (ilicitude pela forma), mas se limita aos casos em que o teor da manifestação seja substantivamente ilícito, como ocorre nas calúnias, ameaças, manifestações racistas e discriminatórias em geral” (Queiroz, 2021, p. 261).

poderosa fantasia, na qual ninguém estaria limitado à própria história, que poderia ser recriada no mundo virtual com poucos cliques:

A noção de que “você é quem você finge ser” tem uma ressonância mítica. A história de Pigmalião perdura porque desperta uma fantasia poderosa: a de que não estamos limitados por nossas histórias, que podemos ser recriados ou que podemos recriar a nós mesmos. No mundo real, ficamos entusiasmados com histórias de autotransformação dramática. [...] Mas, é claro, para a maioria das pessoas, essas recriações do eu são difíceis. No [mundo virtual], entretanto, você pode escrever a autodescrição do seu personagem da maneira que desejar. Os mundos virtuais podem proporcionar ambientes para experiências que são difíceis de se obter no mundo real (Turkle, 1996, p. 162, tradução nossa).

Essa despersonalização da pessoa usuária, por sua vez, teria o potencial de diminuir o sentimento de responsabilidade pessoal. É como se, protegida por uma ficção, a pessoa se sentisse confortável para agir – no “mundo virtual” – de modo diferente em relação aos seus hábitos no “mundo real”.

De acordo com Tim Jordan (2019), contudo, esse não seria um problema a ser atribuído ao anonimato, mas sim à capacidade do “mundo virtual” de conectar uma quantidade de pessoas infinitamente maior que o “mundo real”.

O autor, com razão, comenta que a natureza do anonimato pode ser expressa em duas perguntas: “O anonimato permitirá que eu seja responsável porque garante que eu possa distribuir informações?” e “O anonimato permitirá que eu negue a responsabilidade por minhas ações e declarações?” (Jordan, 2019, p. 575, tradução nossa).

Conforme pondera Jordan, esses questionamentos não são, exatamente, uma novidade decorrente da internet – o anonimato já existia antes da WWW. Com o advento virtual, porém, passaram a cruzar a mente de mais pessoas que, a todo momento, se questionam “o que eu faria se minhas ações online pudessem ser atreladas a mim?”. Com isso, Jordan conclui que os princípios do anonimato não se alteraram no ambiente virtual, mas tão somente fizeram-se expandir.

Acerca dos argumentos que buscam relacionar o anonimato ao aumento da criminalidade *online*, explica Judith Aldridge (2019, p. 578) que, de fato, as atividades ilegais promovidas no ambiente virtual são, constantemente, incrementadas, em especial pela circulação de criptomoedas.

Pondera a autora, porém, ser uma mera presunção – que não se sustenta em dados concretos extraídos da realidade – a premissa de que a virtualização da criminalidade é negativa ou socialmente ruim.

Sendo assim, Aldridge (2019, p. 579) propõe uma nova perspectiva, a partir da qual encara o crescimento o mercado eletrônico ilícito como um benefício capaz de reduzir os danos às pessoas que consomem os produtos ilegais comercializados, assim como de diminuir a violência dessas atividades criminosas no “mundo real”.

Segundo pesquisa capitaneada pela autora (Aldridge; Stevens; Barrat, 2018), os mercados que movimentam valores em criptomoeda incentivam a avaliação (*feedback*) sobre os produtos adquiridos, na medida em que retêm os pagamentos até que a transação seja finalizada pelo consumidor, que confirma ter comprado exatamente aquilo que lhe fora anunciado (*as advertised*).

Com isso, há um substancial aumento na qualidade das mercadorias, fator que implica a redução de danos àqueles que irão consumi-las – aqui, válido o destaque especial à categoria das pessoas usuárias de substâncias entorpecentes.

Além disso, os pagamentos são normalmente mantidos em “custódia” pelo *marketplace* e liberados para os vendedores somente quando os clientes recebem suas compras. Os compradores insatisfeitos com a qualidade do produto têm o recurso de deixar um *feedback* negativo. Juntos, esses fatores podem tornar os vendedores mais responsáveis, com os compradores, por sua vez, mais propensos a obter produtos “conforme anunciado” e de melhor qualidade do que aqueles que compram off-line.

Estão surgindo evidências de pesquisas em apoio a essa possibilidade. O *feedback* dos clientes pode ser manipulado pelos vendedores, mas como a maioria dos vendedores tem pontuações de *feedback* perfeitas (5/5), parece que os medicamentos comprados no mercado de criptomoedas atendem ou excedem as expectativas da maioria dos compradores. Entrevistas com clientes de

criptomercados destacam a qualidade do produto como um dos principais motivos para o acesso a medicamentos dessa forma (Aldridge; Stevens; Barrat, 2018, p. 790, tradução nossa).

Essa mesma pesquisa (Aldridge; Stevens; Barrat, 2018) considera outro importante fator que corrobora a ideia de redução de danos pela qualidade superior dos produtos transacionados ilegalmente no mercado virtual: além das avaliações dos consumidores, exames periciais feitos na Espanha concluíram que noventa por cento das amostras de entorpecentes adquiridas no comércio virtual correspondiam ao idêntico grau de pureza anunciado.

A Figura 6 apresenta a imagem de uma tela extraída em 2022 de página da *dark web* que comercializa outros produtos ilícitos – em vez de substâncias entorpecentes, são cartões de crédito roubados.

Veja-se que, ao lado dos preços cobrados por cada produto, existe uma avaliação que é promovida pelos compradores sobre os vendedores, com os requisitos de discrição, qualidade e comunicação:

FIGURA 6. Página da *dark web* que comercializa cartões de créditos obtidos ilicitamente



Fonte: Rufio e Zoltan (2022).

Da mesma forma, para Aldridge (2019, p. 581), a migração dos mercados ilícitos para o ambiente virtual resultaria em potencial diminuição dos atos de violência. As evidências coletadas sobre o tema (Martin, 2014; 2017) sugerem que o fato de não manterem qualquer contato e de não serem capazes de se identificar entre si tornam as relações entre quem compra e quem vende mais seguras.

Desmistificadas, portanto, as noções de que o anonimato digital deslegitimaria as ações investigativas do Estado, incentivaria a falta de responsabilização criminal ou potencializaria a violência, pesa um último argumento a favor da revisão da cláusula constitucional que o veda: os riscos gerados a usuários e usuárias a partir da obrigatoriedade de identificação no ambiente *cyber*.

A compreensão desse problema, que já é objeto de debate na União Europeia (Masseno, 2023), parte da crescente “biometrização”²⁸ de espaços virtuais públicos e privados, cujo acesso somente é possível mediante a cessão, por usuários e usuárias, de elementos da sua identidade visual.

Apesar de constituírem dados pessoais sensíveis por excelência, como reconhece o artigo 5º, inciso II da LGPD, os dados biométricos têm se popularizado a ponto de serem solicitados para atividades cotidianas simples, desde o ingresso a prédios monitorados por “portarias virtuais” até o desbloqueio de *smartphones* ou acesso a serviços públicos por meio do aplicativo estatal oficial Gov.br.

Essa identificação biométrica, para além de compreender uma ferramenta de grande potencial para a *cyber-surveillance* (conforme discutido no capítulo 3 deste trabalho), também é potencialmente lesiva a usuários e usuárias na medida em que os torna vulneráveis a situações como a *deepfake*, tecnologias capazes de mesclar, combinar, substituir e sobrepor vozes, imagens e vídeo para criar registros falsos hiper-realistas (Maras; Alexandrou, 2019).

Veja-se, nesse sentido, que pesquisa conduzida pela provedora de segurança McAfee em 2023 concluiu que uma a cada quatro pessoas já foi

²⁸ A biometria proporciona o reconhecimento de pessoas com base em suas características de comportamento ou biológicas. Sistemas construídos a partir da biometria se popularizaram a partir dos anos 2000 com o uso de impressões digitais para autorizar operações bancárias ou permitir o ingresso em imóveis. Nesse sentido: Li, Jain, 2015.

vítima de algum tipo de crime, tentado ou consumado, por meio da utilização de tecnologias de *deepfake*, sendo que 77% delas afirmou ter perdido dinheiro como resultado da fraude (Artificial Intelligence [...], 2023).

Nessas circunstâncias, a vedação ao anonimato não apenas é imprestável para mitigar a criminalidade, mas acaba por fornecer elementos que lhe são úteis e dão origem a uma vasta gama de novos delitos.

CONSIDERAÇÕES FINAIS

A cada desenvolvimento tecnológico, uma nova plataforma de investigação oculta será estabelecida e nem sempre existirá uma tutela adequada de direitos individuais em contrapartida. Exatamente por isso, surge a necessidade de se ampliar o rol de direitos fundamentais disponíveis às pessoas envolvidas nos fatos penais, na mesma proporção em que se estendem, em seu desfavor, as práticas processuais.

A demanda pela extensão do catálogo de direitos fundamentais foi analisada, no presente artigo, a partir do direito ao anonimato digital, que não se confunde com a ideia de anonimização contida na LGDP e se caracteriza como ferramenta antiforense de grande potencial para que as pessoas envolvidas em fatos penais possam deixar de produzir provas digitais em seu desfavor.

Para a pergunta “teria a pessoa imputada o direito ao anonimato digital?”, portanto, a resposta deve ser positiva. Apesar da vedação constitucional, o anonimato digital precisa ser tutelado, em especial diante da necessidade de se reconhecer que os impactos da tecnologia sobre o Direito diferenciam os espaços de expressão que existiam à época da Constituição de 1988 daqueles em que, hoje, se desenvolvem a maior parte das interações humanas.

Além disso, a consagração do anonimato digital como direito da pessoa imputada não isentaria de responsabilidades sempre que utilizado para fins ilícitos – porém, apenas depois de o serem.

REFERÊNCIAS

AHAMAD, Shaikshakeel; NAIR, Madhusoodhnan; VARGHESE, Biju. A survey on crypto currencies. *4th International Conference on Advances in Computer Science*, Nova Delhi, p. 42-48, 2013.

ALBANO, Pietro; CASTIGLIONE, Aniello; CATTANEO; Giuseppe; DE SANTTIS, Alfredo. A novel anti-forensics technique for the android OS. *International Conference on Broadband and Wireless Computing, Communication and Applications – IEEE*, Barcelona, p. 380-385, 2011. <https://doi.org/10.1109/BWCCA.2011.62>

ALDRIDGE, Judith. Does online anonymity boost illegal market trading? *Media, Culture & Society*, v. 41, n. 4, p. 578-583, 2019. <https://doi.org/10.1177/0163443719842075>

ALDRIDGE, Judith; STEVENS, Alex; BARRATT, Monica J. Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction*, v. 113, n. 5, p. 789-796, 2018. <https://doi.org/10.1111/add.13899>

ARTIFICIAL Intelligence Voice Scams on the Rise with 1 in 4 Adults Impacted. Disponível em: <<https://bit.ly/3vrDsk1>>. Acesso em: 11 jun. 2024.

BELLI, Lucas. CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS. In: BELLI, Lucas (ed.). *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham: Springer International Publishing, 2021. p. 15-46.

BELLI, Lucas; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia, CHANG, Sofia; DA HORA, Nina; GASPAS, Walter B. *Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano*. Rio de Janeiro: FGV Direito Rio, 2023.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *In: Cadernos Jurídicos*, v. 21, p. 191-201. 2020.

BROCHADO, Mariah. *Inteligência Artificial no horizonte da Filosofia da Tecnologia: técnica, ética e direito na era cibernética*. São Paulo: Dialética, 2023.

CONLAN, Kevin; BAGGILI, Ibrahim; BREITINGER, Frank. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation*, v. 18, p. 66-75, 2016. <https://doi.org/10.1016/j.diin.2016.04.006>

COLEMAN, Gabriella. How has the fight for anonymity and privacy advanced since Snowden's whistle-blowing? *Media, Culture & Society*, v. 41, n. 4, p. 565-571, 2019. <https://doi.org/10.1177/0163443719843867>

FLORIDI, Luciano. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, v. 33, n. 3, p. 369–378, 2020. <https://doi.org/10.1007/s13347-020-00423-6>

FLORIDI, Luciano. *The fourth revolution: how the infosphere is reshaping human reality*. Oxford: Oxford University Press, 2014.

GÜL, Murat; KUGU, Emin. A survey on anti-forensics techniques. *International Artificial Intelligence and Data Processing Symposium*. Malatya, p. 1-6, 2017. <https://doi.org/10.1109/IDAP.2017.8090341>

HARRIS, Ryan. Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem. *Digital Investigation*, v. 3, n. 1, p. 44-49, 2006. <https://doi.org/10.1016/j.diin.2006.06.005>

HILDEBRANDT, Mireille. Location Data, Purpose Binding and Contextual Integrity: What's the Message? In: FLORIDI, Luciano (ed.). *Protection of information and the right to privacy-a new equilibrium?* Cham: Springer, 2014. p. 31-62.

JAIN, Anu; CHHABRA, Gurpal Singh. Anti-forensics techniques: An analytical review. *Seventh International Conference on Contemporary Computing*, Noida, p. 412-418, <https://doi.org/2014.10.1109/IC3.2014.6897209>

JARDINE, Eric. Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society*, v. 20, n. 2, p. 435-452, 2018. <https://doi.org/10.1177/1461444816639976>

JORDAN, Tim. Does online anonymity undermine the sense of personal responsibility? *Media, Culture & Society*, v. 41, n. 4, p. 572-577, 2019. <https://doi.org/10.1177/0163443719842073>

LANIER, Jaron. *Dez argumentos para você deletar agora suas redes sociais*. Rio de Janeiro: Intrínseca, 2018.

LESSIG, Lawrence. *Code: version 2.0*. Nova Iorque: Basic Books, 2009.

LI, Stan Z.; JAIN, Anil K. (Eds.). *Encyclopedia of Biometrics*. 2. ed. Nova Iorque: Springer, 2015.

MACHADO, Diego; DONEDA, Danilo. Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no direito brasileiro. *Revista de Direito Civil Contemporâneo*, v. 7, n. 23, p. 95-140, 2020.

MARAS, Marie-Helen; ALEXANDROU, Alex. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos.

The International Journal of Evidence & Proof, v. 23, n. 3, p. 255-262, 2019. <https://doi.org/10.1177/1365712718807226>

MARTIN, James. *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Londres: Palgrave Macmillan, 2014.

MASON, Stephen; SHELDON, Andrew; DRIES, Hein. Proof: the technical collection and examination of electronic evidence. In: MASON, Stephen; SENG, Daniel (eds.). *Electronic Evidence*. 4. ed. Londres: Institute of Advanced Legal Studies, 2017. p. 285-338.

MASSENO, Manuel David. Da vigilância biométrica no Ordenamento da União Europeia (para fins de segurança em espaços acessíveis ao público): Uma perspetiva portuguesa especialmente destinada ao Brasil. *Revista do CEJUR/TJSC: Prestação Jurisdicional*, v. 11, p. 1-19, 2023. <https://doi.org/10.37497/revistacejur.v11i00.402>

MENEZES NETO, Elias Jacob de. *Surveillance, democracia e direitos humanos: os limites do Estado na era do big data*. 2016. Tese (Doutorado em Direito) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2016.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust de-anonymization of large sparse datasets. In: *2008 IEEE Symposium on Security and Privacy*, Oakland, p. 111-125, 2008. <https://doi.org/10.1109/SP.2008.33>

NAZAH, Saiba; HUDA, Shamsul; ABAWAJY, Jemal; HASSAN, Mohammad Mehedi. Evolution of dark web threat analysis and detection: A systematic approach. *IEEE Access*, v. 8, p. 171.796-171.819, 2020. <https://doi.org/10.1109/ACCESS.2020.3024198>

NUNES, Dierle. Virada tecnológica no direito processual (da automação à transformação): seria possível adaptar o procedimento pela tecnologia? In: NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro (orgs.). *Inteligência artificial e direito processual: os impactos da virada tecnológica no direito processual*. Salvador: Editora Juspodivm, 2020. p. 15-40.

OLIVEIRA, Jordan Vinícius; LOPES, Marília Carneiro da Cunha. Considerações sobre anonimato, pseudoanonimato e criptomoedas. *Revista Eletrônica Direito e Sociedade*, Canoas, v. 9, n. 1, p. 159-176, 2021. <https://doi.org/10.18316/redes.v9i1.6749>

PARK, Joon S.; SANDHU, Ravi. Secure cookies on the Web. *IEEE Internet Computing*, v. 4, n. 4, p. 36-44, 2000. <https://doi.org/10.1109/4236.865085>

PERON, Christian; LEGARY, Michael. Digital anti-forensics: emerging trends in data transformation techniques. *Center for Education and Research in Information Assurance and Security*, West Lafayette, 2005

QUEIROZ, Rafael Mafei Rabelo. Liberdade de expressão na internet: a concepção restrita de anonimato e a opção pela intervenção de menor intensidade. *Suprema: Revista de Estudos Constitucionais*, Brasília, v. 1, n. 1, p. 241-266, 2021. <https://doi.org/10.53798/suprema.2021.v1.n1.a24>

RAMADHANI, Erika. Anonymity communication VPN and Tor: a comparative study. *Journal of Physics*, v. 983, 2018. <https://doi.org/10.1088/1742-6596/983/1/012060>

RESTA, Giorgio. Anonimato, responsabilità, identificazione: prospettive di diritto comparato. *Diritto dell'informazione e dell'informatica*, Milano, v. 30, n. 2, p. 171-205, 2014.

SARDÁ, Thais; NATALE, Simone; DOWNEY, John. Inventing the dark Web: Criminalization of privacy and the apocalyptic turn in the imaginary of the Web. *First Monday*, v. 27, n. 11, 2022. <https://doi.org/10.5210/fm.v27i11.12691>

SARDÁ, Thais; NATALE, Simone; SOTIRAKOPOULUS, Nikos; MONAGHAN, Mark. Understanding online anonymity. *Media, Culture & Society*, v. 41, n. 4, p. 557-564, 2019. <https://doi.org/10.1177/0163443719842074>

SARKIS, Jamilla Monteiro. *Não autoincriminação: uma (re)leitura constitucional na era tecnológica da cyber-surveillance*. São Paulo: Tirant lo Blanch, 2024.

SCHAFER, Burkhard; MASON, Stephen. The characteristics of electronic evidence. In: MASON, Stephen; SENG, Daniel (eds.). *Electronic Evidence*. 4^a ed. Londres: University of London Press - Institute of Advanced Legal Studies, 2017. p. 18-35.

SILVA, Virgílio Afonso da. *Direito constitucional brasileiro*. São Paulo: Edusp, 2021.

SNOWDEN, Edward. *Permanent Record*. Londres: Pan Macmillan, 2019. *E-book*.

SREMACK, Joseph; ANTONOV, Alexandre. Taxonomy of anti-computer forensics threats. *It-Incident Management & It-Forensics*, Bonn, p. 103-112, 2007.

TANENBAUM, Andrew. *Redes de Computadores*. 4. ed. Rio de Janeiro: Elsevier, 2003.

TURKLE, Sherry. Parallel Lives: Working on Identity in Virtual Space. In: GRODIN, Debra; LINDLOF, Thomas (eds.). *Constructing the self in a mediated world*. Thousand Oaks: Sage Publications, 1996. p. 156-177.

VALENTE, Manuel Monteiro Guedes. Editorial dossiê “Investigação preliminar, meios ocultos e novas tecnologias”. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 3, n. 2, p. 473-482, maio/ago. 2017. <https://doi.org/10.22197/rbdpp.v3i2.82>

Authorship information

Jamilla Monteiro Sarkis. Doutora em Direito pela Pontifícia Universidade Católica de Minas Gerais, em Estágio Pós-Doutoral na Pontifícia Universidade Católica do Rio Grande do Sul. Mestre em Direito pela Universidade Federal de Minas Gerais. Advogada. jamilla.sarkis@gmail.com

Additional information and author's declarations (scientific integrity)

Acknowledgement: O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Conflict of interest declaration: the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

Declaration of originality: the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; she also attests that there is no third party plagiarism or self-plagiarism.

Editorial process dates

(<https://revista.ibraspp.com.br/RBDPP/about>)

- Submission: 14/06/2024
- Desk review and plagiarism check: 15/07/2024
- Review 1: 08/08/2024
- Review 2: 14/08/2024
- Review 3: 15/08/2024
- Preliminary editorial decision: 06/09/2024
- Correction round return: 08/09/2024
- Final editorial decision: 29/09/2024

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 3

HOW TO CITE (ABNT BRAZIL):

SARKIS, Jamilla M. Direito da pessoa imputada ao anonimato digital. *Revista Brasileira de Direito Processual Penal*, vol. 10, n. 3, e1044, set./dez. 2024. <https://doi.org/10.22197/rbdpp.v10i3.1044>



License Creative Commons Attribution 4.0 International.



Disponível em:

<https://www.redalyc.org/articulo.oa?id=673982337001>

Como citar este artigo

Número completo

Mais informações do artigo

Site da revista em redalyc.org

Sistema de Informação Científica Redalyc
Rede de Revistas Científicas da América Latina e do Caribe,
Espanha e Portugal
Sem fins lucrativos acadêmica projeto, desenvolvido no
âmbito da iniciativa acesso aberto

Jamilla Monteiro Sarkis

**Direito da pessoa imputada ao anonimato digital
The accused person's right to digital anonymity**

Revista Brasileira de Direito Processual Penal
vol. 10, núm. 3, e1044, 2024
Instituto Brasileiro de Direito Processual Penal,
ISSN-E: 2525-510X

DOI: <https://doi.org/10.22197/rbdpp.v10i3.1044>