

# A era digital e suas implicações sociais: Desafios e contribuições

## O TRÁFICO DE ARMAS DE FOGO NA DARK WEB: DESAFIOS PARA A SEGURANÇA PÚBLICA

**Felipe Alves Trindade, Frediano José Momesso Teodoro.**

Universidade do Vale do Paraíba/Instituto de Pesquisa e Desenvolvimento, Avenida Shishima Hifumi,  
2911, Urbanova - 12244-000 - São José dos Campos-SP, Brasil, felipetrindadesjc@gmail.com,  
frediano@univap.br.

### Resumo

Este artigo pretende analisar o impacto das recentes mudanças tecnológicas no tráfico de armas presente no ambiente digital e seu efeito na segurança pública. A manipulação criminosa de tecnologias que garantem anonimato na internet deu origem a uma nova camada da *internet*, a *Dark Web*, onde crimes de ódio, terrorismo, exploração sexual infanto-juvenil, violações de direitos autorais e tráfico de drogas e armas são frequentes. O estudo destaca a existência de mercados negros digitais nesta camada obscura que disponibilizam armas e munições sem fiscalização por parte das agências reguladoras, representando uma séria ameaça à segurança pública. Dessa forma, destaca-se a necessidade de investimentos em tecnologia, cooperações internacionais entre nações e aprimoramento da capacitação em cibersegurança, visando fortalecer as competências investigativas das autoridades policiais na busca pela redução dos danos ocasionados pelo tráfico de armas de fogo no ciberespaço e na prevenção dessas atividades ilícitas.

**Palavras-chave:** Tráfico de armas de fogo. Segurança Pública. Anonimato. *Dark web*.

**Área do Conhecimento:** Ciências Jurídicas. Direito Público.

### Introdução

As recentes inovações tecnológicas têm proporcionado novas vantagens e oportunidades para os entusiastas do mundo digital, desempenhando um papel catalisador nas transformações da interação social no ambiente cibernético. Com o advento da era digital, o progresso eletrônico atingiu proporções globais, estando intimamente relacionado ao aumento significativo das transgressões criminais no ciberespaço, tais como crimes de ódio, terrorismo, abuso e exploração sexual infanto-juvenil, violações de direitos autorais e comércio ilegal de drogas, armas e munições (BARRETO, SANTOS, 2019).

Sob a ótica dos criminosos, este novo ambiente revelou-se altamente favorável para a execução de práticas escusas, visto que a rede fornecera um relativo grau de anonimato e privacidade. A sensação de impunidade gerada pela anonimidade digital atraiu transgressores de diversas partes do globo, capazes de operar com relativa liberdade no submundo digital.

Conforme essa solução se mostrou vantajosa para os criminosos, revelou-se um desafio para as autoridades policiais. A contenção e repressão de condutas, como o tráfico internacional de armas de fogo no meio digital, são simplificadas em camadas superficiais da *internet*, onde a identificação dos perpetradores se torna factível pela presença de registros de histórico de conteúdos acessados e ao rastreamento de endereços do usuário. Além disso, nesta camada superficial, há a colaboração entre entidades de segurança e grandes empresas de tecnologia, bem como a cooperação internacional entre nações. Essas ações colaborativas têm o potencial de fortalecer a capacidade de rastrear e combater atividades criminosas no mundo virtual, contribuindo para a segurança digital em escala global.

O expansionismo tecnológico recente forneceu uma nova ferramenta aos usuários da rede: a *internet* profunda, conhecida como *deep web*. Segundo Silva (2019), essa nova camada do ciberespaço se destaca pela sua habilidade em contornar a censura digital por meio da descentralização, codificação aberta e mascaramento de seus endereços virtuais, permitindo maior privacidade e anonimato para os usuários. No entanto, este recurso deturpou-se nas mãos de criminosos que, aproveitando-se das tecnologias que garantem anonimato, transformaram o ambiente digital em um local propício para a comunicação e coordenação de atividades ilícitas. Assim, fóruns e mercados

# A era digital e suas implicações sociais: Desafios e contribuições

dedicados ao comércio ilegal de armas de fogo, munições e outros produtos ilícitos encontraram maneira de se expandir (BARRETO, SANTOS, 2019, p. 8).

O impacto à segurança pública com o advento do tráfico de armas de fogo na era digital se revela como um desafio adicional para as autoridades policiais, pois a intervenção policial em camadas profundas torna-se complexa e exige estratégias específicas de identificação e combate. Frente a essa realidade, o presente artigo tem por objetivo analisar as implicações decorrentes do comércio ilegal de armas de fogo presentes no submundo virtual.

## Metodologia

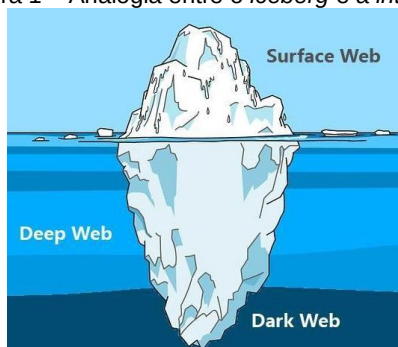
Este estudo baseia-se principalmente no método dedutivo de abordagem, com ênfase nas técnicas de pesquisa documental e bibliográfica, não tendo envolvido qualquer pesquisa com seres humanos como parte do processo de investigação.

## Resultados

O conceito de "camadas" na *internet* se refere à divisão da rede em diferentes níveis com características próprias. Essa estrutura é comumente ilustrada pela analogia a um *iceberg*. Considerando isso, a rede digital é dividida em três camadas: a *surface web*, que representa a camada superficial, seguida pelos segmentos inferiores, *deep web* e *dark web*.

Assim como o bloco de gelo, a *surface web* revela apenas cerca de 10% de sua massa total acima da superfície, representando, assim, somente uma pequena fração visível aos usuários de uma rede maior. Logo, a maior parte do conteúdo existente na *internet* encontra-se nas diversas redes profundas e obscuras que compõem o vasto ciberespaço (BARRETO, SANTOS, 2019, p. 11).

Figura 1 – Analogia entre o iceberg e a internet.



Fonte: BGA Cyber Security (2019).

Conforme a análise de Bergman (2000), a *deep web*, ou rede profunda, é a região da *internet* que não pode ser acessada por meio dos mecanismos de busca convencionais. Neste ambiente encontram-se sites e conteúdos criptografados, o que assegura a privacidade, segurança e anonimato dos usuários. A *dark web*, por outro lado, é definida como o submundo do ciberespaço ou como a deturpação do uso das tecnologias da *deep web*. Essa rede obscura representa uma porção ainda mais restrita e oculta, onde atividades ilegais são frequentemente realizadas com o auxílio de tecnologias que garantem anonimato e sigilo de seus usuários (SERASA, 2022). Através desta, crimes de ódio, terrorismo, abuso e exploração sexual infanto-juvenil, violações de direitos autorais e comércio ilegal de drogas e armas tornaram-se cada vez mais frequentes (BARRETO, SANTOS, 2019).

Nas profundezas obscuras, onde a luz da persecução policial não alcança, fóruns e plataformas permitem a disseminação global do comércio digital ilícito, ultrapassando barreiras geográficas que antes limitavam compradores e vendedores no mercado negro convencional.

Analisando a proposta do mercado negro digital na *dark web*, identificaram-se duas maneiras pelas quais armas de fogo e munições são ofertadas livremente: os criptomercados e as lojas de vendedores.

Criptomercados são essencialmente espaços virtuais que abrigam diversos vendedores e uma variedade de mercadorias ilícitas. Neles, os usuários desfrutam de um ambiente de anonimato, com intermediação entre as vendas para reduzir golpes e possibilidade de avaliar publicamente a qualidade

## A era digital e suas implicações sociais: Desafios e contribuições

dos itens adquiridos (BARRATT, ALDRIDGE, 2016). A seu turno, as lojas de vendedores são administradas por um único fornecedor e costumam ser especializadas em categorias específicas de mercadorias. Neste mercado, compradores que preferem adquirir produtos sem a intervenção de intermediários podem estabelecer contato direto com o vendedor, porém, correm o risco de cair nos diversos golpes presentes na rede obscura (CHAINALYSIS, 2023).

Nestes mercados, utiliza-se com frequência criptoativos para transacionar financeiramente, aproveitando-se do pseudoanonimato proporcionado. Essa tática possibilita evitar parcialmente a investigação contábil e, conseqüentemente, a persecução judicial (AXUR, 2018). Concluída a transação, a entrega do produto adquirido se dá por via aérea, marítima ou terrestre, sendo empregadas técnicas de envio especializadas para minimizar o risco de detecção. No comércio ilegal de armas de fogo no ciberespaço, as práticas de envio incluem a desmontagem das armas e o transporte de suas distintas partes em pacotes separados, visando reduzir a detecção (PAOLI et al., 2017, p. 100).

Em 2017, através de um estudo realizado por Paoli e colaboradores, em parceria com o Escritório das Nações Unidas sobre Drogas e Crimes (UNODC), foram identificados 18 mercados digitais em plena atividade relacionados à compra e venda de armas de fogo e munições na *dark web*. Destes, 15 apresentavam regras explícitas que permitiam ou não proibiam explicitamente a comercialização de armamentos. Além disso, observou-se que 9 dessas plataformas possuíam uma categoria específica dedicada exclusivamente às armas de fogo (*Ibid.*, p. 46, tradução nossa<sup>1</sup>).

Dentre os anúncios identificados, encontravam-se marcas amplamente reconhecidas no mercado internacional de armas, como Glock, Potro, SIG Sauer, Beretta, Ruger, e outras (*Ibid.*, p. 55). Além disso, a maioria esmagadora das armas de fogo disponíveis nos criptomercados consistiam-se em rifles, submetralhadoras, espingardas e pistolas, que, em sua grande parte, eram autênticas, exceto pelas submetralhadoras, onde as réplicas predominavam (*Ibid.*, p. 101).

O estado das armas, seja novo ou usado, não é frequentemente mencionado como uma característica relevante, visto que grande parte das listagens identificadas não fornecem informações nesse sentido (*Ibid.*, p. 16). Listagens de pacotes que incluem o armamento, suas munições e até mesmo acessórios são recorrentes, o que indica que os vendedores possuem amplo acesso a essa categoria de produtos (*Ibid.*, p. 52).

Segundo a pesquisa de Paoli et al. (2017, p. 101–102, tradução nossa<sup>2</sup>) “as transações envolvendo armas de fogo, peças, componentes, munições e acessórios atingiram 136 vendas mensais, gerando uma receita bruta estimada em 392 mil reais<sup>3</sup>”. Fora do contexto cibernético, de acordo com estimativas realizadas pelo Escritório das Nações Unidas sobre Drogas e Crimes (2012), “o crime organizado transnacional movimenta 870 bilhões de dólares ao ano”, equivalente a 4,35 trilhões de reais em receitas.

Entretanto, comparar o comércio ilícito de armas de fogo e produtos relacionados entre os mercados clandestinos tradicionais e digitais é um desafio devido à falta de dados precisos, dificultando a mensuração total de ambos e sua repressão. As informações disponíveis muitas vezes são baseadas em dados secundários após eventos como ataques terroristas ou operações policiais bem-sucedidas.

### Discussão

O potencial impacto na segurança pública representa uma preocupação constante para os formuladores de políticas e para agências aplicadoras da lei, dado que o acesso facilitado a armas em

<sup>1</sup> No original: “Of the 18 accessed markets, 15 (83 per cent) had rules explicitly allowing, or not explicitly prohibiting, arms sales. Nine markets (50 per cent) provided vendors with a dedicated ‘firearms’ category into which vendors could place listings.”

<sup>2</sup> No original: “Concerning sales, based on the estimates generated by this study, firearms (including their parts, components, ammunition and accessories), explosives and digital products generate 136 sales per month, with an estimated monthly gross revenue in the region of US\$80,000”.

<sup>3</sup> Em sua publicação original, Paoli e demais autores (2017) empregam valores expressos em moeda americana Dólar (US\$). Para efeitos de conversão, utilizou-se a taxa de câmbio da presente data (08/08/2023) de R\$4,90 para cada US\$1,00.

## A era digital e suas implicações sociais: Desafios e contribuições

mercados online ilícitos sem qualquer regulamentação pode aumentar significativamente o risco de atividades criminosas violentas na sociedade. Essa ameaça abrange uma ampla gama de cenários, desde o apoio a organizações criminosas até o incentivo a atos de terrorismo e violência armada em comunidades locais e internacionais.

Acontecimentos notáveis exemplificam o impacto social do comércio ilegal de armas na *dark web*.

Liam Lyburd, em 2015, foi condenado à prisão perpétua por planejar um ataque em sua antiga faculdade em Newcastle, Reino Unido. Lyburd adquiriu uma pistola e munição na *dark web*, e, para um amigo próximo, descreveu a compra da pistola como "comprar uma barra de chocolate" (BBC, 2015).

Por complemento, o caso de David Ali Sonboly em 2016 na Alemanha ilustra ainda mais essa situação. No episódio do massacre em Munique, nove indivíduos foram vitimados e outras 27 pessoas, incluindo crianças, ficaram feridas. Após sua captura, as autoridades alemãs realizaram perícias técnicas em seus dispositivos eletrônicos, corroborando a tese de aquisição do armamento via mercados da *dark web* e obtendo sucesso ao localizar e apreender seu fornecedor, bem como outras armas em seu esconderijo (THE TELEGRAPH, 2016).

A pronta denúncia em Newcastle e a ágil ação das autoridades resultaram na preservação de vidas, impedindo que o atentado se concretizasse, ao contrário do ocorrido em Munique. Essas situações demonstram como a facilidade de acesso a armas através da *dark web* pode colocar em risco a segurança pública, resultando em efeitos devastadores.

No contexto brasileiro, o Poder Legislativo promulgou a Lei n.º 10.826 em 2003, com a intenção de reduzir a violência armada e regular o acesso às armas de fogo no país. Essa legislação estabelece sanções severas que variam de 6 a 12 anos para indivíduos envolvidos no comércio ilícito de armas de fogo no país, e penas de 8 a 16 anos para aqueles envolvidos no tráfico internacional de armas (BRASIL, 2003). No entanto, na presente conjuntura, os responsáveis por esse crime no Brasil não estão sendo integralmente abrangidos por esse instituto.

Considerando isso, é importante observar que essa lei fora estabelecida em um período em que o progresso tecnológico não havia atingido as proporções atuais e o comércio ilegal de armas de fogo ainda não havia se infiltrado no mundo digital. A *internet* sempre se mantém à frente da legislação através dos contínuos e ininterruptos avanços tecnológicos, tornando o regulamento incapaz de acompanhar todas as inovações tecnológicas em constante evolução (TECNOBLOG, 2017).

A deficiência na atualização tecnológica adequada das forças policiais diante das sofisticadas táticas empregadas por criminosos destaca a importância de investir na capacidade técnica policial, abrangendo áreas como cibersegurança e conhecimentos sobre o ciberespaço. Além disso, é crucial fomentar esforços colaborativos entre os Estados para a prévia identificação desses indivíduos, visto que possam estar situados em país adverso ao qual se iniciou a investigação.

De acordo com Barreto e Santos (2019, p. 81), as dificuldades da prévia identificação de criminosos em camadas inferiores são evidenciadas:

“Atribuir autoria delitiva é um desafio para os integrantes da polícia judiciária, em razão da oferta de inúmeros serviços garantidores de privacidade, notadamente na *deep web*. Inúmeras dificuldades são apontadas, desde a inexistência de leis para dar suporte a essas novas tecnologias até a falta de expertise investigativa no cenário cibernético.”

Demais disposições como a Lei Federal n.º 12.737/2012 obtiveram êxito ao criminalizar atividades informáticas relacionadas à invasão de dispositivos, interrupção de serviços telegráficos, telefônicos, informáticos ou telemáticos, bem como falsificação de documentos e cartões. No entanto, este marco regulatório não abordou a questão do comércio de produtos ilícitos por meio da *internet* e suas tecnologias emergentes.

Destacando uma alternativa plausível, acordos como a Convenção de Budapeste, elaborada em consenso entre os Estados-membros do Conselho da Europa (COE) e Estados signatários em 2001, e recebida no Brasil por meio do Decreto n.º 11.491/2023, obtiveram um papel fundamental para as



# A era digital e suas implicações sociais: Desafios e contribuições

autoridades brasileiras ao disponibilizar recursos adicionais para as investigações cibernéticas (BRASIL, 2023). Compreendendo que os criminosos buscam constantemente se reinventar para continuar suas práticas delituosas e esquivar-se da persecução judicial, surge a necessidade de fomentar a cooperação entre os Estados. Essa colaboração almeja proteger a sociedade contra os crimes no ciberespaço e salvaguardar os interesses legítimos relacionados ao uso e desenvolvimento das tecnologias da informação (BUDAPESTE, 2001).

Nesse sentido, a fim de combater essa atividade criminosa, é fundamental implementar ações que incluam uma abordagem punitiva, por meio da cooperação entre Estados e da melhoria das leis e regras vigentes. Ademais, a tarefa de identificar os responsáveis na *dark web* requer uma ampla capacidade técnica investigativa das agências aplicadoras da lei, devido aos desafios do anonimato e à relativa dificuldade de rastreamento nesse ambiente.

Consequentemente, é de suma importância que as autoridades policiais se especializem em cibersegurança, ampliem o contingente de agentes capacitados e desenvolvam técnicas periciais adequadas para a preservação de evidências digitais. Essa abordagem coordenada e especializada será fundamental para enfrentar o desafio crescente do crime cibernético e garantir a segurança pública diante do comércio ilícito de armas de fogo.

## Conclusão

Diante dessa realidade, o presente estudo tem como seu ponto focal a apresentação à sociedade das consequências sociais decorrentes do tráfico de armas de fogo no contexto tecnológico atual. Destaca-se, de forma enfática, a urgência de abordar e enfrentar esse desafio crescente no ciberespaço. Somente através de investimentos públicos no setor tecnológico e no aprimoramento da capacitação das autoridades policiais em disciplinas de cibersegurança que se poderá amenizar os efeitos prejudiciais do tráfico de armas de fogo na *dark web*. Além disso, a busca pela segurança digital em âmbito global, por meio da colaboração coordenada entre Estados, assume uma importância fundamental. Assim, torna-se imperativo avançar tecnologicamente, mas com um enfoque claro na preservação tanto da segurança pública quanto do mundo digital. Essa visão tem como objetivo contestar a ressoante frase do poeta norte-americano Richard Buckminster Fuller, que observa que "A humanidade está adquirindo a tecnologia correta para as razões erradas".

## Referências

- BARRAT, M. J.; ALDRIDGE, J. **Everything you always wanted to know about drug cryptomarkets**. ScienceDirect, 2016. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0955395916302274?via%3Dihub>. Acesso em: 7 mar. 2023.
- BARRETO, A. G.; SANTOS, H. **Deep Web: Investigação no submundo da internet**. Rio de Janeiro: Brasport, 2019.
- BERGMAN, M. K. **The Deep web: surfacing hidden value**. BrightPlanet, 2000. Disponível em: [https://resources.mpi-inf.mpg.de/d5/teaching/ws01\\_02/proseminarliteratur/deepwebwhitepaper.pdf](https://resources.mpi-inf.mpg.de/d5/teaching/ws01_02/proseminarliteratur/deepwebwhitepaper.pdf). Acesso em: 13 mai. 2023.
- BRASIL. **Decreto n.º 11.491, de 12 de abril de 2023**. Brasília, DF: Diário Oficial da União, 2023. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_Ato2023-2026/2023/Decreto/D11491.htm](https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm). Acesso em: 23 abr. 2023.
- BRASIL. **Lei Federal nº 10.826, de 22 de dezembro de 2003**. Dispõe sobre o registro, posse e comercialização de armas de fogo e munição, sobre o Sistema Nacional de Armas – SINARM, define

# A era digital e suas implicações sociais: Desafios e contribuições

crimes e dá outras providências. Brasília, DF: Diário Oficial da União, 2003. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/2003/l10.826.htm](https://www.planalto.gov.br/ccivil_03/leis/2003/l10.826.htm). Acesso em: 04 abr. 2023.

BRASIL. **Lei Federal nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação de delitos informáticos; altera o Decreto-Lei n.º 2.848, de 7 de setembro de 1940 – Código Penal; e dá providências. Brasília, DF: Diário Oficial da União, 2003. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm). Acesso em: 04 abr. 2023.

CONVENÇÃO de Budapeste sobre cibercrimes. **Budapeste**, 2001. Disponível em: <https://rm.coe.int/16802fa428>. Acesso em: 02 jun. 2023.

GEOGRAPHIC Distinctions in Crypto Darknet Market Activity. **Chainalysis**, 2021. Disponível em: <https://blog.chainalysis.com/reports/crypto-darknet-markets-2021-geographic-breakdown/>. Acesso em: 3 jun. 2023

HOW Darknet Markets and Fraud Shops Fought for Users In the Wake of Hydra's Collapse. **Chainalysis**, 2023. Disponível em: <https://blog.chainalysis.com/reports/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/>. Acesso em: 3 jun. 2023.

LIAM Lyburd mass murder plot: Teen sentenced to life. **BBC**, 2015. Disponível em: <https://www.bbc.com/news/uk-england-tyne-34359392>. Acesso em: 20 jun. 2023.

LUCHI, D. Deep Web e Monero: A moeda dos criminosos. **Axur**, 2018. Disponível em: <https://blog.axur.com/pt/deep-web-e-monero-a-moeda-dos-criminosos>. Acesso em: 7 jun. 2023.

NOVA campanha do UNODC aponta que Crime Organizado Transnacional movimenta 870 bilhões de dólares ao ano. **UNODC**, 2012. Disponível em: <https://www.unodc.org/lpo-brazil/pt/frontpage/2012/07/16-unodc-lanca-campanha-global-sobre-crime-organizado-transnacional.html>. Acesso em: 23 jul. 2023.

ORTIZ, E. O que é *dark web*? Como se proteger?. **Serasa**, 2022. Disponível em: <https://www.serasa.com.br/premium/blog/o-que-e-dark-web-como-se-proteger/>. Acesso em: 7 jun. 2023.

PAOLI, P. G.; ALDRIDGE, J.; RYAN, N.; WARNES, R., **Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web**. Santa Monica, CA: RAND Corporation, 2017. Disponível em: [https://www.rand.org/pubs/research\\_reports/RR2091.html](https://www.rand.org/pubs/research_reports/RR2091.html). Acesso em: 2 mar. 2023.

ROTHWELL, J.; HUGGLER, J.; FINNIGAN, L. Ali Sonboly: Everything we know about the Munich gunman. **The Telegraph**, 2016. Disponível em: <https://www.telegraph.co.uk/news/2016/07/23/munich-shooting-everything-we-know-about-the-shopping-centre-gun/>. Acesso em: 10 jul. 2023.

SILVA, G. K. P. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep web e Dark web**. Anhanguera, 2019. Disponível em: <http://repositorio.anhanguera.edu.br:8080/jspui/handle/123456789/227>. Acesso em: 7 jun. 2023.

SURFACE, Deep ve Dark Web Nedir? **BGA Security**, 2019. Disponível em: <https://www.bgasecurity.com/2019/08/surface-deep-ve-dark-web-nedir/>. Acesso em: 15 jul. 2023.

VENTURA, F. FBI usa vídeo infectado para revelar a identidade de suspeito na rede anônima Tor. **Tecnoblog**, 2017. Disponível em: <https://tecnoblog.net/noticias/2017/08/11/fbi-nit-tor-anonimato/>. Acesso em: 01 jun. 2023.