



CYPHER PUNKS: PERSPECTIVAS HACKERS

CYPHER PUNKS: HACKER PERSPECTIVES

Por: Samuel Medeiros Andreatta¹

RESUMO

A presente pesquisa busca recuperar os discursos de resistência cypherpunk à limitação de práticas criptográficas na rede. É realizada uma contextualização geral do campo da criptografia para ilustrar a presença desse tipo de agenciamento na sociedade contemporânea. Em seguida, textos do movimento cypherpunk são analisados desde a chave filosófica da Classe Hacker. O hacker é aquele que cria rupturas ou fissuras, consegue enxergar possibilidades de fazer emergir novas maneiras de mundo. Defende-se que, dentro da emergência de mecanismos criptográficos, que são restringidos pela moldura de propriedade. A pesquisa atenta para a tensão proporcionada entre o surgimento do Hack e as formas de gerenciamento que pretendem limitá-lo, ou subordiná-lo à classe vetorial. Diante do caráter material e imaterial da informação a escassez artificial escancarada pelo Hack legal da propriedade intelectual se torna um paradigma. O desequilíbrio da relação de poder trazido pelas novas práticas criptográficas, ou com este Hack, além de gerar uma reformulação no modo de produção específico de verdades, trouxe à tona novas possibilidades de mundo diante do caráter solidário da difusão e adoção de protocolos criptográficos, para além da forma proprietária. O Hack exibido pelos mecanismos criptográficos e outras técnicas de anonimização na rede, assim, não assumem uma mera isenção por possibilitar a inovação, mas nos recordam da potência constante da virtualização que pode ameaçar a estabilidade das relações de poder vigentes.

Palavras-chave: Criptografia- Criminologia Crítica - Cypherpunks

ABSTRACT

The present research aims to recover the Cypherpunk discourses of resistance to the limitation of cryptographic practices on the network. A general contextualization of the field of cryptography is carried out to illustrate the presence of this kind of agency in contemporary society. Subsequently, Cypherpunk texts are analyzed through the philosophical lens of the Hacker Class. The hacker is the one who creates ruptures or fissures, able to envision possibilities for new ways of bringing worlds into being. It is argued that within the emergence of cryptographic mechanisms, these are restricted by the framework of property. The research focuses on the tension between the rise of the Hack and the management strategies that aim to limit or subordinate it to the vector class. Given the material and immaterial nature of information, artificial scarcity, as exposed by legal hacks, becomes evident. The imbalance of power relations brought about by new cryptographic practices, or by this Hack, not only leads to a reformulation of the specific mode of truth production but also brings forth new possibilities for the world, due to the solidarity character of both the diffusion and adoption of cryptographic protocols beyond proprietary forms. The Hack revealed by cryptographic mechanisms and other anonymization techniques on the network, therefore, does not merely take on a neutral stance by enabling innovation but serves as a reminder of the ongoing potential of virtualization, which can threaten the stability of existing power relations.

Keywords: Critical Criminology- Cypherpunks - Cryptography

¹ Bacharel em Ciências Jurídicas, Mestre em Ciências Criminais, Doutorando em Ciências Criminais. Advogado Criminalista. Membro do Grupo de Pesquisa “ Cultura Punitiva e Crítica Filosófica” do programa de pós-graduação em Ciências Criminais da PUCRS. O presente trabalho foi realizado com auxílio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.



BREVE SÍNTESE CRÍTICA E METODOLOGIA

A criptologia é a ciência que estuda a criptoanálise e a criptografia: o ato de decifrar mensagens e a criação de escrita codificada. Cartas para amores impossíveis², utilização de línguas próprias como encriptação social mútua³, sociedades secretas antimônárquicas⁴ até códigos específicos para o tráfico de rum⁵ durante o proibicionismo americano dos anos 20; o uso de cifras e métodos para quebrá-las possuem uma rica história. A necessidade de sigilo nas comunicações humanas é algo que pode expressar uma contrariedade. Para Maurits de Vries⁶, a antítese da comunicação é o sigilo, e a criptografia combina esses pontos divergentes numa única operação, trata-se de uma “comunicação não-comunicante”. A criptografia é um dos instrumentos que materializa um certo tipo de anonimato. Certamente é um mecanismo de anonimização do conteúdo da mensagem, podendo atuar, não em via de regra, até para mascarar a identidade do receptor e emissor da mensagem. Este ensaio busca situar os mecanismos de anonimização na economia punitiva.

A criptografia convive conosco. Ela assegura que a URL digitada na barra da pesquisa leve para o endereço certo, e torna essa mensagem indecifrável até chegar ao destino através de protocolos específicos. Segundo Galloway⁷, a expressão contemporânea das “Sociedades de Controle” é justamente o protocolo. Um modelo de agenciamento de condutas, de algoritmização da vida, de dividação deleuziana e com inspiração no biopoder foucaultiano⁸. O “protocolo” é uma tática que mira atingir uma autorregulação voluntária dentro de um ambiente contingente. Ele atua como fenômeno despersonalizado, apartado de seu local de emergência, e com intenção homogeneizadora na sua atuação. O protocolo pode ser exemplificado pelo fluxo de trânsito: o sujeito opta por aderir ao código de trânsito e aos protocolos específicos daquele espaço, como parar em sinais vermelhos ou até optar por uma rota mais direta.

Para Galloway o protocolo na rede de computadores é baseado em duas máquinas opostas: uma máquina que distribui radicalmente controle em locais autônomos (TCP/IP) e

² KAHN, David. **Codebreakers: The Story of Secret Writing**. Nova Iorque: Macmilan Company, 1968, p. 96.

³ STORIG, Hans Joachim. **A Aventura das Línguas: Uma História dos Idiomas do Mundo**. São Paulo: Editora Melhoramentos, p. 69.

⁴ KAHN, David. **Codebreakers: The Story of Secret Writing**. Nova Iorque: Macmilan Company, 1968, p.797

⁵ Ibid, p. 803

⁶ Ibid, p.780.

⁷ GALLOWAY, Alexander. **Protocol Society: How Control Exists after Decentralization**. Cambridge: The MIT Press, p. 9.

⁸ Ibid.p 13.



outra que se foca no controle de hierarquias rígidas(DNS). Ambos os protocolos se realizam concretamente através de ferramentas criptográficas⁹. Em 1977, houve a emergência da criptografia de RSA¹⁰, modelo que vigora -com alterações- até hoje e que utiliza uma chave pública e uma chave privada. A segurança desse modelo criptográfico está ancorada no problema da fatoração de primitivos, ou no fato de que encontrar os valores originais de uma função a partir de um grande valor demanda um poder computacional que torna a operação impraticável, é o que Goldreich¹¹ indica como a possibilidade prática, mas não matematicamente possível, da existência de “funções unidirecionais”.

A criptografia é uma relação tripartida. É formada pelo emissor, receptor e o adversário, chamado por vezes de observador. Com a realização da amplitude da vigilância denunciada por Snowden, a sedimentação dos efeitos “expositivos”¹², digitalmente narcísicos¹³ e espetaculares, em um meio geral de “insatisfação apática que caracteriza a experiência social”¹⁴, houve uma alteração total de nossa relação com a privacidade, e a ingerência quanto à forma de se expor na rede, gerando novas práticas de assujeitamento.

O potencial de órgãos de inteligência americana¹⁵ exposto pelos diversos vazamentos da Wiki Leaks é o que poderíamos chamar de adversário global. Como nos lembra Michael Hayden¹⁶, ex-chefe da NSA, o governo americano considera que os metadados (dados sobre quem se comunica com quem, quando e aonde) são suficientes para justificar a morte de pessoas. Esses tipos de metadados não são necessariamente escondidos ao criptografar as mensagens¹⁷. A criptografia, embora proteja o conteúdo da mensagem, não confere, à princípio, anonimato ao receptor e emissor.

O adversário é também próprio da logística militar. A guerra catalisou a expansão da

⁹ Como indicado em: <https://www.ibm.com/docs/en/i/7.3?topic=security-elements-in-tcpip-network> Acesso em: 20/08/2024.

¹⁰ Como indicado em : RIVEST, R.L; SHAMIR, A.; ADLEMAN, L."A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" . **Communications of the ACM**. 21 (2): 120–126. Disponível em: CiteSeerX 10.1.1.607.2677. doi:10.1145/359340.359342. S2CID 2873616. Archived from the original (PDF) on 2023-01-27. Acesso em: 16/11/2024

¹¹ GOLDREICH, Oded. **Foundations of Cryptography: Basic Techniques**.Cambridge: Cambridge University press. 2004, p. 44.

¹² HARCOURT, Bernard. **Exposed: Desire and disobedience in the digital age**. Harvard University Press: Cambridge, 2015.

¹³ DUNKER, Christian. **Narcisismo Digital e seus Algoritmos**. In: SABARIEGO, Jesus. et al (org.) Algoritmos. Tirant Lo Blanche: São Paulo, 2020.

¹⁴ PLANT, Sadie. **The most radical gesture: The Situationist International in a postmodern age**. Routledge: Londres, 2000, p. 9.

¹⁵ Disponível em: <https://wikileaks.org/-Leaks-.html> Acesso em: 20/10/2024.

¹⁶ FERRAN, Lee. **Ex-NSA chief: we kill people based on metadata**. ABCNEWS. Publicado em: 12/05/2014. Disponível em: <http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/>. Acesso em 20/09/2024.

¹⁷ JAKOBSEN, Sune . **Cryptogenography: Anonymity without trust**. Tese de Doutorado no departamento de Filosofia. Londres. Queen Mary University of London, 2016.



criptografia e a internet foi criada com a guerra total em mente. Paul Baran, um dos inventores da internet, segundo Galloway¹⁸, após a publicação de sua estrutura de rede pela Rand Corporation, se interessou na sobrevivência das comunicações diante de um ataque nuclear. Para “sobreviver” a um ataque nuclear uma rede descentralizada é realmente uma ótima solução.

Existem diversos outros exemplos, como a utilização de línguas nativas durante contexto de guerra¹⁹, a interceptação de sinais de rádio²⁰ e o circuito de comunicação das embaixadas. O envio de documentos e comunicações secretas, como aquelas das torturas relatadas pela CIA na ditadura brasileira²¹, ou na ditadura chilena²² ou na ditadura Nicarágua²³ ou das práticas na baía de Guantánamo ou Abu Ghreib²⁴ gerou a institucionalização de departamentos voltados para a criptoanálise, e posterior legitimação jurídica²⁵ para as práticas de tortura, vinculada a decisões administrativas quanto ao acesso de documentos sigilosos. A revelação de documentos sigilosos pode até ser derivada de um imperativo contido no discurso geral transparência, mas os efeitos dessa revelação geram uma sensação de ubiquidade ou onipresença dos vetores da globalização manejados por grandes potências, estabilizando um desequilíbrio de poder. A decisão de revelar determinada informação contém em si mesma a decisão de não revelar outras.

A necessidade de realizar e de desvendar comunicações secretas em escala industrial, em concorrência com as tensões de um discurso centrado no imperativo da “transparência”²⁶, funcionou para criar um regime de verificação específico. Por um lado, atuou para delimitar os objetos passíveis de proteção criptográfica, notadamente o sistema financeiro e a segurança nacional, e para manejar os ilegalismos que são próprios a esse circuito. Por outro, a reciclagem de dados dentro de uma lógica da plataformização da vida,

¹⁸ GALLOWAY, Alexander. **Protocol Society: How Control Exists after Decentralization**. Cambridge: The MIT Press, p. 4.

¹⁹ DOOLEY, John. **History of Cryptography and Cryptanalysis Codes, Ciphers, and Their Algorithms**. Galesburg: Springer.

²⁰ KAHN, David. **Codebreakers: The Story of Secret Writing**. Nova Iorque: Macmillan Company, 1968, p. 752.

²¹ EUA. ARQUIVO DA NSA. KORNBLUH, Peter. Publicado em: 8/07/2014. Disponível em: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB478/>

²² EUA. ARQUIVO DA NSA. KORNBLUH, Peter. Disponível em: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB8/nsaebb8i.htm>

²³ EUA. ARQUIVO DA CIA. Atrocities in the nicaraguan civil war. Publicado em: 12/01/2012. Disponível em: <https://www.cia.gov/readingroom/document/cia-rdp85t01058r000100170001-7>

²⁴ HERSH, Seymour. **Torture at Abu Ghraib**. New Yorker. Publicado em: 04/05/2004. Disponível em: <https://www.newyorker.com/magazine/2004/05/10/torture-at-abu-ghraib>

²⁵ HARCOURT, Bernard. **A contrarrevolução: como o governo entrou em guerra contra os próprios cidadãos**. Glac Edições: São Paulo, 2021

²⁶ BIRCHALL, Claire. Introduction to ‘Secrecy and Transparency’: The Politics of Opacity and Openness. **Theory, Culture & Society**. 2011 (SAGE). Vol. 28(7- 8): 7^25 DOI: 10.1177/0263276411427744



a transformação do sujeito em matéria bruta²⁷, ocorreu pois os padrões criptográficos são quebrados pelos trackers²⁸. Ou seja, há uma tolerância quanto a vulnerabilidade de certas comunicações enquanto outras são protegidas. Quando grandes empresas violam os padrões criptográficos desanonimizando usuários, há um circuito distinto de relações de poder. Um indivíduo que pratique essa conduta tem uma resposta estatal distinta em relação à prática da mesma conduta por uma empresa. Enquanto os ilegalismos praticados por empresas são submetidos a uma razão comercial, que pode até gerar penas pecuniárias, o indivíduo é submetido a uma razão penal. Enquanto, por exemplo, o site que vendia dados roubados de usuários “*Raid Forum*”²⁹ é rotulado como um espaço de prática criminosa, toda a economia das empresas de “*data brokering*”, ou especulação de dados, é legitimada sob uma razão comercial. Obviamente há uma distinção no modo de obtenção de dados, no entanto a mera autorização para *cookies*, por exemplo, que veda o acesso a determinado site e é superada pelo mero clique não implica em uma possibilidade de fragilização absoluta de direitos fundamentais pelas empresas. Se o panóptico é um cartaz com os dizeres “você está sendo filmado”, a sociedade de controle é um ícone clicável que afirma que você não é um robô. Ao clicar nesse ícone, aparentemente inofensivo, você permite que o programa vasculhe seu histórico da internet para determinar se as suas buscas são compatíveis com as de um humano³⁰, a vigilância não é flagrante como no panóptico, é concreta, contínua e velada.

A construção desse atrito posicional passa pelo acesso/limitação do sujeito a determinadas informações, desde segredos industriais e *Insider trading*, até a diferenciação dos processos de subjetivação e exatidão pelo nível de acesso que o sujeito tem à informação e seu potencial interpretativo. A individuação de cada sujeito também depende da maneira que é exposto e se expõe na rede e pelo valor unitário atribuído a determinado usuário diante da inserção de seu potencial de compra nos algoritmos de direcionamento, frente aos interesses que exhibe repetidamente. Lembra-se que a criptografia não invisibiliza, via de regra, os metadados, ou seja, o emissor e receptor da mensagem podem ser vistos.

O caso clássico que evoca as comunicações secretas em tempos de guerra é o

²⁷ ZUBOFF, Shoshana. *The age of surveillance capitalism*. Public Affairs: Nova York, 2019.

²⁸ DEUBER, C. ; PASSMAN, S. ; STRUFE, T. "Browsing Unicity: On the Limits of Anonymizing Web Tracking Data," *2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2020, pp. 777-790, doi: 10.1109/SP40000.2020.00018.

²⁹ DONN, Natasha. Portugal Resident. "21-year-old Portuguese 'hacker' arrested in UK". Disponível em: <https://www.portugalresident.com/21-year-old-portuguese-hacker-arrested-in-uk/>. Acesso em: 24/11/2024.

³⁰ O funcionamento do modelo de captcha é pormenorizado em: WILLIAMS, Owen. Google Promises reCAPTCHA Isn't Exploiting Users. Should You Trust It? Onezero, 2019. Disponível em: <https://onezero.medium.com/google-promisesrecaptcha-isn-t-exploiting-users-should-you-trust-it-ed99f1543f28>. Acesso em: 28/11/2021.



enigma³¹. A máquina de criptoanálise desenvolvida pelo time de Turing decifrou os criptogramas alemães a partir da redundância dos termos “Heil hitler” no envio de mensagens das tropas nazistas³². Esse acontecimento demonstra a intrínseca violabilidade das comunicações e o fato de que repetições de padrões, sejam eles geográficos ou linguísticos, tornam mais fácil o rastreamento. Não existe fórmula mágica indecifrável. A força do adversário está intrinsecamente ligada à manutenção da integridade das mensagens.

Ao mesmo tempo, há um limite pragmático da criptoanálise: durante a segunda guerra mundial, como indica Kahn³³, diversas mensagens interceptadas seguiam sem análise, justamente porque se dava preferência às mensagens protegidas por criptografia mais avançada. Nesse sentido, a tentativa de obtenção de anonimato pode gerar o efeito contrário, o que é verdade no geral. A utilização de ferramentas para garantir a anonimidade pode servir para expor ainda mais o sujeito, como indica Goodin³⁴, a NSA armazena os dados daqueles que utilizam a rede Tor, justificando que como os números de IP não podem ser atribuídos ao território americano, as proteções legais do País não são aplicáveis.

Durante a operação que derrubou a Silkroad³⁵ (maior mercado de venda de drogas da deepweb³⁶) houve uma suspeita confirmada em relação a um agente infiltrado do DEA. O agente conseguira realizar diversas transferências em ativos de bitcoin, e justificara, antes de qualquer mobilização de criminalização secundária, a utilização de protocolos de encriptação da rede TOR como forma de garantia da privacidade. Tal fato levantou suspeitas dos agentes que investigavam o mercado de drogas e levou à descoberta do desvio de fundos em bitcoin.

A analogia de Zimmerman³⁷ com cartões postais é adequada. Imagine que todos enviassem suas correspondências sem um envelope; o primeiro que utilizasse um envelope para a correspondência estaria mais exposto. A adoção “protocolar” de diversos tipos de mecanismos de anonimização já é realidade, mas é preciso lembrar que todo tipo de relação

³¹ Disponível em: <https://www.cryptomuseum.com/crypto/enigma/> Acesso em: 19/10/2024.

³² KERRIGAN, Michael. **Enigma: A verdadeira história do código secreto da segunda guerra mundial**. EUA: M.Books, 1989.

³³ KAHN, David. **Codebreakers: The Story of Secret Writing**. Nova Iorque: Macmilan Company, 1968, p 120.

³⁴ [chnica.com/techpolicy/2013/06/use-of-tor-and-e-mail-crypto-could-increase-chances-that-nsa-keeps-your-da](https://www.chnica.com/techpolicy/2013/06/use-of-tor-and-e-mail-crypto-could-increase-chances-that-nsa-keeps-your-da)

³⁵ GREENBERG, Andy. **Lords of Crypto Crime: The Race to Bring Down the World’s Invisible Kingpins**. EUA: Monoray, 2024.

³⁶ Aqui utilizamos o termo “deepweb” ao invés de por exemplo darknet, que indicaria a parte não indexada por buscadores e reservada a prática de crimes. No entanto tal diferenciação é equivocada, seria o mesmo que dizer que determinado espaço concreto só se caracteriza pela prática de crimes, reforçando a ontologia do delito.

³⁷ ZIMMERMAN, Philip R. **Por que eu escrevi o PGP?** In: **Manifestos Cypherpunks**. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.17.



de poder é passível de ser fragilizada. E a exposição das capacidades tecnológicas do complexo industrial militar³⁸ americano demonstram que a dimensão da coleta de informações é, no mínimo, preocupante.

Esse é um ensaio embrionário que deriva de pesquisa de doutorado. A intenção de apresentação deste trabalho no congresso foi expandir e somar novas perspectivas à pesquisa em andamento. A metodologia de pesquisa é de caráter indutivo que propõe indagações respondidas por avaliação crítica e reunião de trabalhos teóricos. O problema de pesquisa é a punição de práticas de anonimização. A pesquisa busca entender como os mecanismos criptográficos gerenciam e são gerenciados pelo circuito de práticas punitivas. O objetivo geral deste ensaio é verificar a utilidade dos discursos cypherpunk para o “trabalho crítico”³⁹. A pesquisa tem como objetivo específico realizar uma reinterpretação da atividade criptográfica dos cypherpunks dentro do termo Hack, na linha de Mckenzie Wark⁴⁰.

Os resultados obtidos ainda estão em andamento, mas inicialmente conclui-se que o conceito de Hack se relaciona com a possibilidade de virtualização e capacidade de diferenciação frente ao avanço informacional. Apesar de ser aplicado nessa pesquisa para o campo digital, o termo hacker é mais amplo. O processo de virtualização, de percepção de um porvir, tende a ser subordinado à forma da propriedade. A classe hacker emergiu com a alocação da informação dentro da moldura da propriedade intelectual. Diante do caráter material e imaterial da informação, a artificialidade da escassez (inerente ao modo de produção capitalista) escancarada pelo Hack legal da propriedade intelectual aumenta também a necessidade de mecanismos de proteção criptográfica, e de limitações específicas deste mecanismo moduladas por práticas punitivas. O desequilíbrio da relação de poder trazido pelas novas práticas criptográficas, ou com este Hack, além de gerar uma reformulação no modo de produção específico de verdades, trouxe à tona possibilidades de mundo de caráter solidário na difusão e adoção de protocolos criptográficos, para além da forma proprietária.

Adota-se como teoria base a ideia de “tomada de posição”⁴¹ defendida por Augusto Jobim do Amaral, e que se expressa ao abdicar das posições de “filósofo legislador e filósofo

³⁸ As revelações de Snowden estão disponíveis em: <https://theintercept.com/series/snowden-archive/>. Acesso em: 20/08/2024.

³⁹ HARCOURT, Bernard. On Critical Genealogy. *Contemporary Political Theory*. Coletânea de artigos open Access”. Agosto, 2024. Disponível em: <https://doi.org/10.1057/s41296-024-00715-y>. Acesso em: 19/10/2024.

⁴⁰ WARK, Mckenzie. *A hacker manifesto*. Cambridge: Harvard university press, 2004.

⁴¹ AMARAL, Augusto. *Política da Criminologia*. Tirant Lo Blanch: São Paulo, 2020, p. 17.



pedagogo”⁴². A técnica utilizada é a pesquisa bibliográfica centrada em levantamento de obras e notícias sobre o tema e análise transversal de decisões judiciais.

Em termos criminológicos, adota-se a posição fragmentária postulada pelas Criminologias Críticas⁴³. Entendendo a inexistência ontológica do delito, através do combate à proposição de independência entre ato e a reação, nos aliamos à posição de Becker⁴⁴, que entende que tal argumento parte de uma relutância na aceitação do caráter contingente das regras.

No presente estudo, opta-se pela linha demarcada por alguns dos pressupostos da Labelling approach. No entanto, não se adota a teoria por completo, visto que a categoria desvio é revisitada a partir da reformulação do conceito de “ilegalismo” como estruturado por Foucault⁴⁵. Isto posto, incorporando as críticas foucaultianas, entende-se que o “desvio” não seria de fato um desvio, pois funcionaria em uma lógica de sustentação recíproca. Todavia, é importante apontar que, mesmo que não se utilize dessa categoria, a criminalização primária e a secundária podem ser entendidas como resultado de um processo de rotulação, como atribuição de determinadas características a um grupo social, abdicando da ideia de neutralidade da Lei.

2. CYPHERPUNKS E O HACK

A criptografia foi a bandeira levantada pelos cypherpunks como forma de resistência às tentativas do governo americano de diminuir a privacidade nos espaços da rede. Historicamente, a proteção do anonimato tem um caráter de resistência política latente. Francisco Veiga, membro da assembleia constituinte, já em 1891, percebera, notadamente em uma perspectiva liberal, a estreita relação entre anonimato e resistência política, visto que defendia que “ O anonimato não protege só o fraco e oprimido contra os fortes e opressores, muita gente honesta, independente e digna, por isso mesmo que se serve dele

⁴² FOUCAULT, Michel. *Filosofia analítica da política*. In: FOUCAULT, Michel. Ética, sexualidade, política. Ditos e Escritos V. Org Manoel Barros da Motta; tradução Elisa Monteiro. Forense Universitária: Rio de Janeiro, 2006, p. 37-55.

⁴³ SOZZO, Maximo. *Reconstruyendo las criminologias Críticas*. Ad Hoc: Buenos Aires, 2006.

⁴⁴ BECKER, Howard. *Outsiders*. Zahar: Rio de Janeiro, 2009, p. 32

⁴⁵ A explicação pormenorizada do termo pode ser encontrada em: FOUCAULT, Michel. *Teorias e instituições Penais*. São Paulo: WMF. Martins fontes, 2020, p. 275. Tradução Rosemary Costhek Abílio; E em DROIT, Roger Paul. *Entrevistas com Michel Foucault*. Paidós: Buenos Aires, 2008.



para defender sem poder ser suplantado”⁴⁶. Zimmerman⁴⁷ argumenta que escreveu o PGP (*pretty good privacy*) para garantir o direito à privacidade, materializando no mundo digital a proteção presente na constituição americana.

A privacidade depende de instrumentos anônimos de transação, que viabilizem a liberdade do sujeito, pois ele deve ter a opção de se revelar seletivamente. Para os cypherpunks, a privacidade é “o poder de se revelar seletivamente ao mundo.”⁴⁸ Privacidade, autodeterminação informativa, segredo, opacidade, são problematizações que não são mutuamente excludentes, há intersecções entre todos esses tensionamentos no grande campo do anonimato.

Longe de ser um empreendimento individualista, o anonimato alcançado por determinadas técnicas criptográficas é uma forma de “solidariedade”⁴⁹. Essa característica é ecoada por Roger Dingledine⁵⁰, o criador do sistema de anonimização “Tor” que, a sua vez, afirma que o anonimato se torna mais robusto quanto maior o número de usuários; a integridade dos chamados mixers, serviços que aglutinam as mensagens antes de seu destino final para nublar o emissor se tornam mais seguras com mais pessoas⁵¹, esse tipo de anonimato, desaparecer na multidão, é também categorizado como “anonimato horizontal”⁵².

Zimmerman⁵³ demonstra a tensão inerente entre técnicas que possibilitam uma camada de anonimização dos usuários e as práticas punitivas, citando diversas medidas legislativas. A benevolência do governo americano é objeto de ceticismo do autor. Citando dissidentes políticos que foram objeto de espionagem, como Martin Luther King, o autor reforça que não é absurdo concluir que esses dispositivos são utilizados como uma forma de vigilância contra a resistência política. A inversão de técnicas de espionagem e guerras

⁴⁶ BRASIL. Arquivo Nacional. Congresso Nacional Constituinte. Item: AC1891-DISC-2-40-538. “Emenda do constituinte Francisco Veiga ao parágrafo 12, artigo 71 do Projeto de Constituição, que dispõe sobre anonimato na manifestação de opiniões”, p. 439. Disponível em: “<https://arquivohistorico.camara.gov.br/downloads/congresso-nacional-constituente-de-1890-1891.pdf>” Acesso em: 06/03/2023

⁴⁷ ZIMMERMAN, Philip R. *Por que eu escrevi o PGP?* In: *Manifestos Cypherpunks*. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.17.

⁴⁸ HUGHES, Eric. *Manifesto Cypherpunk*. In: *Manifestos Cypherpunks*. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.29.

⁴⁹ ZIMMERMAN, Philip R. *Por que eu escrevi o PGP?* In: *Manifestos Cypherpunks*. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.19.

⁵⁰ DINGLEDINE, Roger. Conferência Black Hat, 2002. *Black Hat USA 2002 - Why is Anonymity So Hard?* Disponível em: https://www.youtube.com/watch?v=RDcXXslH48I&list=PLg_vgvhrkFa6whQn7cy4tRE9UD52i38Ke . Acesso em 20/08/2024.

⁵¹ JAKOBSEN, Sune K. *Cryptogenography: Anonymity without trust*. Tese de Doutorado no departamento de Filosofia. Londres. Queen Mary University of London, 2016.

⁵² Anon Collective. *Book of Anonymity*. Alemanha: Punctum Books, 2021.

⁵³ ZIMMERMAN, Philip R. *Por que eu escrevi o PGP?* In: *Manifestos Cypherpunks*. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.19.



externas para o campo nacional é uma tendência percebida por Harcourt⁵⁴. Para o autor, os americanos internalizaram técnicas de guerra civil aprendidas em guerras externas, e as voltaram contra movimentos sociais, como os panteras negras. A repercussão de ferramentas criptográficas no Direito brasileiro é esperada frente às lacunas que a tecnologia gera. Recentemente, o ministro Alexandre de Moraes determinou que empresas de VPN inserissem obstáculos tecnológicos que impossibilitassem a utilização do X , muito embora tenha voltado atrás⁵⁵. Já começa a se perceber uma desconfiança dos mecanismos punitivos quanto a plataformas que expandem a criptografia, visto que a mera utilização de VPN gerou uma presunção de culpabilidade. Legislações mais explicitamente autoritárias, como a do Egito, já proibem a utilização de VPN em si⁵⁶.

Em outro julgado, não tão recente, na ADPF 407 e ADI N° 5527⁵⁷, o Min. Edson Fachin fez referência ao sistema bancário para reforçar a viabilidade do cumprimento de ordens judiciais pelo Facebook. O ministro acredita que serviços bancários, apesar de usarem a criptografia, cumprem regularmente ordens judiciais. Tal opinião poderia demonstrar a adequação legal de práticas criptográficas nesse espaço, mas o que demonstra em verdade é o circuito de tolerância de ilegalismos praticados por determinados sujeitos. O discurso atua de maneira dúplice, invisibilizando a cifra oculta (dos crimes que ocorrem nesses espaços), e convenientemente se olvidando do fato de que instituições financeiras não são transparentes quanto às condutas lá praticadas, visto que a necessidade de fornecimento de informações depende de ordem judicial, a miríade de escândalos bancários, e o monitoramento de transações atípicas demanda uma confiança no compliance descolada da realidade. O ministro também destaca o fato de que:

Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais

⁵⁴ HARCOURT, Bernard. **A contrarrevolução: como o governo entrou em guerra contra os próprios cidadãos**. Glac Edições: São Paulo, 2021

⁵⁵ CONJUR. Alexandre de Moraes volta atrás. Publicado em: 30 de agosto de 2024. Disponível em: <https://www.conjur.com.br/2024-ago-30/alexandre-volta-atras-sobre-exclusao-de-vpns-mas-mantem-multa/>. Acesso em: 20/09/2024.

⁵⁶ CHAWKI, Mohamed. **Anti-Cyber and Information Technology Crimes Law “EGYPT” Law No. 175 of 2018 “Unofficial Translation”**. Disponível em: <<https://cybercrime-fr.org/wp-content/uploads/2020/04/Egyptian-cybercrime-law-.pdf>> Acesso em 31/08/2023.

⁵⁷ BRASIL. Supremo Tribunal Federal. Arguição de descumprimento de preceito fundamental nº 403, Sergipe. Requerente: Partido Popular Socialista (PPS). Rel: Min. Edson Fachin. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf> .



para a vida pública⁵⁸.

O voto reproduz muito do relatório elaborado por David Kanye⁵⁹ na ONU, e ambos destacaram a necessidade de garantia de ferramentas criptográficas em cenários autoritários. No STF a questão ainda não foi decidida, e os debates permanecem ocorrendo. Mas o que esse processo revela é que novos mecanismos criptográficos são submetidos ao crivo de uma razão punitiva. Esse discurso, como é perceptível pelo caso debatido pelo tribunal, trata de problemática de obtenção de informações durante investigação de tráfico de drogas. O questionamento geral que pode ser inferido desse discurso que modula o desenvolvimento criptográfico é “ Se existisse uma impossibilidade técnica de fornecimento de informações, como poderia o Estado obter informações específicas para punir o sujeito ? ”. Logo, a validação de um dispositivo de anonimização dependeria, paradoxalmente, de sua capacidade de ser quebrado. Ao mesmo tempo, o Estado atua para que as limitações de obtenção de informações permaneçam restritas a determinados atores do jogo de poder estabelecido.

As revelações de Snowden, os vazamentos da Wikileaks, e as ações americanas após o 11 de setembro, a “ABIN paralela de Bolsonaro”⁶⁰, e diversos outros acontecimentos reforçam a ideia de que o ceticismo quanto às ações do complexo privado-estatal de vigilância é fundamentado. Não há chave (pública ou privada) mágica, a criptografia perfeita não existe. Mesmo ferramentas que ainda se dizem totalmente anônimas, como o TOR, podem ser fragilizadas. Em um dos vazamentos da WIKI LEAKS que divulgava a comunicação interna do “Hacking Team”⁶¹, uma empresa de venda de malwares italiana, circulava um e-mail com a explicação de como se aproveitar de Nodos de saída para a identificação de usuários na rede TOR. Novamente, é preciso se ater a um dos paradigmas da criptografia, o nível de proteção criptográfico é inversamente proporcional ao poder do adversário. E quando limitamos a ingerência dos governos através de restrição de coleta de dados a partir da legislação não basta mais pensar a partir da velha noção de soberania, já que com a globalização, localização externa de servidores e cabos submarinos internacionais, a questão

⁵⁸ BRASIL. Supremo Tribunal Federal. Arguição de descumprimento de preceito fundamental nº 403, Sergipe. Requerente: Partido Popular Socialista (PPS). Rel: Min. Edson Fachin. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf> .

⁵⁹ KANYE, David. ONU. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Disponível em: <https://documents.un.org/doc/undoc/gen/g15/095/85/pdf/g1509585.pdf> Acesso em: 19/07/2024.

⁶⁰ CNN. “ Abin Paralela: veja quem foi monitorado pelo esquema ilegal”. Publicado em: 12/07/2024. Disponível em: <https://www.cnnbrasil.com.br/politica/abin-paralela-veja-quem-foi-monitorado-pelo-esquema-ilegal/> Acesso em: 20/08/2024.

⁶¹ Disponível em: <https://wikileaks.org/hackingteam/emails/> Acesso em: 20/10/2023.



se torna geopolítica, redesenhando as fronteiras de outrora. Para os cypherpunks, como indica Hughes⁶², as legislações são frágeis frente a criptografia, o que é certamente aplicável aos outros padrões neoliberais algorítmicos.

2.1 Captura e propriedade intelectual

É com uma referência ao manifesto comunista que Timothy May⁶³ dá início ao seu manifesto criptoanarquista. O autor traça um paralelo entre a invenção da impressão, que trouxe um desequilíbrio das relações de poder entre setores da sociedade medieval, e os protocolos criptográficos, que fizeram emergir uma nova relação de poder entre agentes da sociedade presente.

A criptografia é uma ferramenta de resistência altamente ingovernável, pois pode escapar às legislações e gerar uma impossibilidade de vigilância. Esse tipo de resistência tecnopolítica também problematiza os contornos de um novo tipo de propriedade explorado na rede, diz o autor:

E assim, como uma invenção aparentemente insignificante, como o arame farpado tornou possível o cercamento de vastas fazendas e territórios, alterando para sempre os conceitos de terra e direitos de propriedade na fronteira ocidental, também, a descoberta aparentemente menor de um ramo arcano da matemática se tornará o alicate que cortará o arame farpado em torno da propriedade intelectual⁶⁴.

A esquemática proposta por Wark, pode nos auxiliar a potencializar a resistência proposta pelos cypherpunks⁶⁵. As classes produtivas, formadas por fazendeiros, trabalhadores e hackers, estão em embate com as classes expropriadoras, pastoralistas, capitalistas e vetoralistas, que também estão em embate entre si. Os capitalistas tentam dilapidar o monopólio da classe pastoral sobre a terra, e subordiná-la à produção industrial. Os vetoralistas tentam quebrar o monopólio do capital nos processos de produção, e intencionam subordinar a produção de bens à circulação de informação.

A propriedade intelectual é a forma de mercantilização da vida da qual provém a

⁶² HUGHES, Eric. *Manifesto Cypherpunk*. In: *Manifestos Cypherpunks*. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.31.

⁶³ MAY, Timothy. *Manifesto Criptoanarquista*. In: *Manifestos Cypherpunks*. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.25.

⁶⁴ MAY, Timothy. *Manifesto Criptoanarquista*. In: *Manifestos Cypherpunks*. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.27.

⁶⁵ Ibid, p. 196.



limitação à imaginação das possibilidades de virtualização, segundo Wark⁶⁶, da classe Hacker. A classe hacker é uma classe possibilitadora, que formula abstrações. Os hackers criam a oportunidade para que novas rupturas possam se lançar no mundo. A classe hacker não é composta só do mundo eletrônico, muito pelo contrário, há hackers nas artes, nas ciências exatas, na política, no direito, etc...

Ao reconhecer a propriedade intelectual, o Estado cria um plano no qual a classe vetorial consegue se desenvolver, atingir uma vitória no jogo posicional do poder, pois tem a posse do plano mais abstrato no qual objetos podem ser produzidos. Para a autora, a potência inesgotável da informação consegue produzir tanto a repetição, quanto a diferenciação: “A informação é representação, no qual a diferenciação é o limite da repetição. Mas informação também é expressão, no qual a diferenciação excede o limite da repetição. A propriedade transforma a diferenciação em repetição, congelando a produção livre e distribuindo-a como representação⁶⁷”.

A propriedade intelectual demonstra o jogo de poder inerente às abstrações de novos mundos, é fruto da possibilitação de novas formas de gerar valor a partir da diferenciação hacker, mas é o que também codifica a transformação da informação em propriedade. É o que a autora chama de “Hack legal”⁶⁸, o Hack é o que possibilita a abertura de virtualização, a invenção da impressão, assim como a criptografia, também é um Hack, e a moldura da propriedade intelectual torna o Hack um modo de produção próprio, e logo gera o surgimento de uma nova classe: a classe hacker.

Com deslocamento da riqueza, como Foucault⁶⁹ havia demonstrado na passagem do sistema monárquico para o capitalismo nascente, com a concentração da riqueza nos portos, é instaurado um novo circuito punitivo. E o mesmo ocorre com a propriedade intelectual, para os mecanismos de produção de valor no circuito de dados, intensificam a segurança e a vigilância dessa economia de dados através de técnicas criptográficas, dispositivos de vigilância, uma proteção espacial e jurídico-penal. O acesso a esses dados é comercializado, ao mesmo tempo que a própria privacidade, ou a expansão dos mecanismos de anonimização e de ferramentas de criptoanálise, gera outro mercado, que vai do nível estatal(notadamente o mercado de spywares) ao individual(como empresas de VPN).

⁶⁶ WARK, Mckenzie. **A hacker manifesto**. Cambridge: Harvard university press, 2004.

⁶⁷ WARK, Mckenzie. **A hacker manifesto**. Cambridge: Harvard university press, 2004, p. 127.

⁶⁸ Ibid, p. 27.

⁶⁹ FOUCAULT, Michel. **Teorias e instituições Penais**. São Paulo: WMF. Martins fontes,2020, p. 91. Tradução Rosemary Costhek Abílio.



A autora defende uma redefinição do termo hacker. Trata-se, em verdade, de um esforço de recuperação do termo, de denúncia daqueles que o subvertem e se aliam com o que ela chama de classe vetorial, reduzindo o termo à mera prática de crime, ou na divisão binária entre White hat ou black hat, precisamente por temer seu potencial de abstração, seu potencial de organizar-se como classe. A limitação desse potencial faz parte também do discurso californiano tecnocrata, que conseguiu tomar para si também o termo “ruptura” ou *disruption*, utilizado hoje em dia com forte vinculação às startups americanas.

A autora propõe uma nova esquemática da luta de classes. Expressando uma das perspectivas sob a qual Foucault sempre insistiu, a fragilidade de um contexto situacional e a potência de uma classe subjugada, que nada tem de dominada- como explicita Foucault⁷⁰, tal divisão, entre classes dominadas e dominantes, deve mais a Gobineau do que a Marx. É a abstração da forma “propriedade” que clama por transformações, criando suas próprias subjetividades, e não a representação que se ancora na “falta” ou opressão de determinado bem, que marcaria determinado grupo social, sujeitando-o a uma “identidade negativa”⁷¹. Como a inversão foucaultiana procura encarar o modo de produção em relação recíproca e não subordinadora à disciplina, defende-se que o escopo das propostas críticas de Wark não é uma mera democratização dos produtos gerados pelo capitalismo, mas a desestabilização desses fenômenos sob um novo horizonte de possibilidades para além do parco “produto”.

Com as mudanças proporcionadas por uma nova razão neoliberal de mundo⁷² e pela inserção do novo animal zoopolítico que serpenteia⁷³, não é absurdo estar de acordo com o fato de que a classe vetorial substitui os capitalistas como classe dominante exploradora, e isso é próprio da forma que essas empresas assumem. As empresas desinvestem de sua capacidade produtiva, conferindo uma importância nova à massa de terceirizados que competem pela manufatura dos produtos. O seu poder está no monopólio da propriedade intelectual e dos meios de reprodução de valor, o que ela chama de “vetores da comunicação”⁷⁴.

A pobreza do “realismo capitalista”⁷⁵ é também de imaginação. Tudo é subsumido à abstração da propriedade. O que protege os negócios vetorialistas é sua capacidade de

⁷⁰ FOUCAULT, Michel. *Ditos e Escritos IV- Estratégia poder Saber*. Rio de Janeiro: Forense universitária. 2006, p. 223.

⁷¹ WARK, Mckenzie. *A hacker manifesto*. Cambridge: Harvard university press, 2004, p. 107.

⁷² DARDOT, Pierre; LAVAL, Christian. *The new way of the world : on neoliberal Society*. EUA: French Voices, 2014.

⁷³ CHIGNOLA, Sandro. A toupeira e a serpente. *R. Dir. Gar. Fund.*, Vitória, v. 19, n. 3, p. 239-270, set./dez. 2018.

⁷⁴ WARK, Mckenzie. *A hacker manifesto*. Cambridge: Harvard university press, 2004, p. 148.

⁷⁵ FISHER, Mark. *Realismo Capitalista*. São Paulo: Autonomia Literária, 2016.



qualitativamente transformar a informação que possui e extrair novo valor dela. É esse fenômeno que Zuboff⁷⁶ descreve no ciclo de reciclagem de dados mantidos por empresas. O hacker, assim, torna-se indispensável para uma economia pouco produtiva, uma economia em que a flagrante artificialidade da escassez torna-se ainda mais evidente com a reprodutibilidade da informação. A criptoanálise e a criptografia fazem parte desse jogo, pois os mecanismos de anonimização que opõe barreiras na obtenção de informação atuam na manutenção da escassez, blindando a artificialidade do que é em verdade inesgotável, e a possibilidade de quebra dessas cadeias atua para exhibir justamente a artificialidade e possibilidade de multiplicação da informação.

Os mecanismos de produção de escassez se tornam mais óbvios, e demonstram uma indignação, percebida de maneira mais ativa, geralmente, pela classe Hacker. Para o hacker, sempre há um excedente de possibilidade, uma mais valia do virtual ainda não capturada. A representação do Hack na abstração de direitos de propriedade limita sua capacidade, pois toda a forma de propriedade não expressa a multiplicidade, mas repetição, algo passível de ser submetido aos mecanismos de valoração vigentes. A propriedade é incapaz de capturar a virtualidade da qual o Hack deriva sua potência.

Pela sua própria natureza, o Hack supera os limites impostos pela propriedade. Pensemos na criptografia. A sucessão de virtualizações possibilitadoras da segurança da informação se desenvolveu no mesmo campo dos softwares livres, e como vimos, a adoção de determinado padrão criptográfico por mais pessoas é desejável, pois a criptografia se torna mais forte. Não é possível conter o Hack da criptografia, justamente pela sua inesgotável renovação. Muito embora a autora admita que a classe hacker tem um “interesse tático” na propriedade intelectual, os limites impostos por esses mecanismos submetem as capacidades criptográficas à economia de tolerância do circuito capitalista.

Os cypherpunks arriscavam novas possibilidades de mundo. Com a bandeira da privacidade ou da criptografia eles conseguiram viabilizar uma ruptura, uma abstração a qual permitiu que novos embates na fricção do poder pudessem ocorrer. A defesa irrestrita da privacidade e da liberdade de expressão e previsões de vigilância total que se materializaram, nada mais são do que hacks que trouxeram à superfície novos jogos de poder.

Existe uma tensão na criação de hacks, visto que as bifurcações da forma “propriedade” o movimentam para a classe vetorialista. Mas o potencial de resistência da criação permanente, permite que diferentes assuntos ou problematizações, diferentes

⁷⁶ ZUBOFF, Shoshana. *The age of surveillance capitalism*. Public Affairs: Nova York, 2019.



genealogias⁷⁷, trazidas por essa abertura de mundo, possam multiplicar a posição crítica.

Para a autora “ a história é a produção de abstração e a abstração da produção”⁷⁸. A sociedade produz rupturas possibilitadoras que geram discursos e modelos de inteligibilidade, e o capitalismo abarca essas abstrações, esses hacks, e os incorpora ao seu modo de produção. A propriedade intelectual assumiu seus contornos a partir da vampirização da classe hacker, de sua capacidade de abstração explorada por uma classe que é dona dos meios de produção, a classe vetorialista. A classe vetorialista é dona das patentes desses produtos e monopoliza a possibilidade de aferir o valor dessas abstrações.

Essas abstrações têm a capacidade abrir as possibilidades informacionais para além de sua mercantilização, tornar possível novas formas de vida. O pessimismo compreensível do realismo capitalista, pode ser fragilizado. Novas abstrações sustentam o palco de novas disputas, especialmente no campo informacional. Os defensores da criptografia, ou da ampliação de mecanismos de anonimização na rede, não têm o poder de mudar o mundo sozinhos. Essa classe que oferece seus serviços para a classe vetorialista, também pode se expressar como um presente, levando a abertura de possibilidade de virtualização de mecanismos de anonimização para além de um mero produto.

CONCLUSÕES INICIAIS

Neste tópico é apropriado asseverar que essa pesquisa trata de um trabalho em andamento. Todavia, algumas conclusões incipientes devem ser destacadas. Inicialmente, demonstra-se tanto pela estruturação adversarial, quanto por uma necessidade histórico-logística fundamentada nos exemplos suscitados, que a criptografia é catalisada a partir de sua relação com a guerra e com uma razão militar. O circuito criptográfico é baseado numa série de protocolos que são aceitos de forma não impositiva, na linha de um gerenciamento centrado no controle.

A materialização do Hack criptográfico na rede funcionou para criar um regime de verificação específico. Os discursos vigentes realizam uma clivagem entre fenômenos cuja proteção criptográfica é indiscutível, com os ilegalismos próprios que são manejados por um crivo punitivo. Enquanto outros fenômenos, justamente por subverterem os limites da relação de produção da propriedade informacional traduzida pelo Hack legal da propriedade

⁷⁷ HARCOURT, Bernard. On Critical Genealogy. *Contemporary Political Theory*. Coletânea de artigos open Access”. Agosto, 2024. Disponível em: <https://doi.org/10.1057/s41296-024-00715-y> Acesso em: 19/10/2024.

⁷⁸ WARK, Mckenzie. *A hacker manifesto*. Cambridge: Harvard university press, 2004, p. 148.



intelectual, não seriam passíveis do mesmo nível de proteção criptográfica. A construção desse atrito posicional passa pelo acesso/limitação do sujeito a determinadas informações, e aos tipos de circuito determinada informações são submetidas, desde segredos industriais e Insider trading, até a diferenciação dos processos de subjetivação e exaustão pelo nível de acesso que o sujeito tem à informação.

A pesquisa intencionou demonstrar como o anonimato ou privacidade proporcionada por técnicas criptográficas pode, à contrário sensu, gerar o efeito de maior exposição, e logo maior criminalização. Isso também se relaciona com o caráter solidário das técnicas criptográficas, visto que a força de um sistema de anonimização depende tecnicamente da quantidade de usuários.

O complexo estatal privado age para garantir que as restrições no acesso à informação sejam limitadas a certos grupos envolvidos no jogo de poder vigente. Assim, a legalidade de um dispositivo de anonimização estaria, de maneira paradoxal, ligada à sua possibilidade de ser vulnerabilizado frente a uma razão punitiva. Ao mesmo tempo, o Estado assegura que as barreiras no acesso a informações fiquem concentradas em determinados atores desse jogo de poder.

O movimento cypherpunk demonstra não só a necessidade de defesa irrestrita de direitos da privacidade ou de mecanismos de anonimização, mas a intrínseca fragilidade do jogo posicional de poder. Sempre há retrocessos e avanços que naturalizam determinados tipos de vigilância, a adoção de protocolos específicos, linhas de fuga para além da forma que o valor é aferido hoje em dia, fazem emergir um regime de verificação que legitima ou deslegitima o uso de comunicações anonimizadas.

Foi possível verificar como a noção de Hack, e classe hacker, trazida por Mckenzie Wark, pôde servir como modelo de inteligibilidade e eco propagador, dos discursos aventados pelos Cypherpunks. Vimos que a certidão de nascimento da classe hacker é vinculada à propriedade intelectual, que gera seu próprio modo de produção. Com o deslocamento da riqueza para a produção de dados, para a forma da propriedade intelectual, foi necessário gerenciar esse circuito sob novas pulsões punitivas.

A mercantilização da informação, por seu caráter material e imaterial, escancara a artificialidade dos mecanismos de escassez. O compartilhamento livre de informações já demonstra um modo de vida para além da mercantilização. E mesmo que a virtualização hacker abra novas possibilidades produtivas, isso não significa que a classe hacker está necessariamente vinculada à confecção de produtos. A classe hacker é uma classe possibilitadora, que ao visualizar abstrações, consegue manejar o virtual para desestabilizar

o momento atual.

Os mecanismos de criptografia são Hacks, ou pertencem à virtualização da classe hacker, pois criam novas formas de mundo a partir da diferenciação do que já existe. E muito embora a classe hacker se subordine à classe vetorialista, ao pensarmos em termos criptográficos, a virtualidade libertada pela produção de novas informações nesse campo tem um potencial inesgotável. Um potencial que fragiliza a mercantilização da vida e as relações de poder vigentes.

REFERÊNCIAS

AMARAL, Augusto Jobim . **Política da Criminologia**. Tirant Lo Blanch: São Paulo, 2020.

BECKER, Howard. **Outsiders**. Zahar: Rio de Janeiro, 2009.

BIRCHALL, Claire. Introduction to ‘Secrecy and Transparency’: The Politics of Opacity and Openness. *Theory, Culture & Society*. 2011 (SAGE). Vol. 28(7- 8): 7[^]25
DOI: 10.1177/0263276411427744

BRASIL. Arquivo Nacional. Congresso Nacional Constituinte. Item: AC1891-DISC-2-40-538. **“Emenda do constituinte Francisco Veiga ao parágrafo 12, artigo 71 do Projeto de Constituição, que dispõe sobre**

BRASIL. Supremo Tribunal Federal. Arguição de descumprimento de preceito fundamental nº 403. Sergipe. Requerente: Partido Socialista Brasileiro. Relator: Min.Edson Fachin. Disponível em:
<https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf> .

DEUBER,C. ; PASSMAN, S. ; STRUFE, T. "Browsing Unicity: On the Limits of Anonymizing Web Tracking Data," **2020 IEEE Symposium on Security and Privacy (SP)**, San Francisco, CA, USA, 2020, pp. 777-790, doi: 10.1109/SP40000.2020.00018.

DOOLEY, John F. **History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms**. Galesburg: Springer, 2018.

DINGLEDINE, Roger. “Conferência Black Hat, 2002. Black Hat USA 2002 - Why is Anonymity So Hard?” Disponível em:
https://www.youtube.com/watch?v=RDcXXSIH48I&list=PLg_vgvhrkFa6whQn7cy4tRE9UD52i38Ke . Acesso em: 20/08/2024.

DROIT, Roger Paul. **Entrevistas com Michel Foucault**. Paidós: Buenos Aires, 2008.

DUNKER, Christian. Narcisismo Digital e seus Algoritmos. In: SABARIEGO, Jesus. et al (org.) **Algoritmos**. Tirant Lo Blanche: São Paulo, 2020.



EUA. Arquivo NSA. KORNBLUH, Peter. “Brazil: Torture Techniques revealed in declassified US documents” Publicado em: 8/07/2014. Disponível em: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB478>

EUA. Arquivo NSA. KORNBLUH, Peter. “Chile and the United States: Declassified Documents Relating to the Military Coup, September 11, 1973,” Disponível em: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB8/nsaebb8i.htm>. Acesso em: 21/07/2024.

EUA. Arquivo CIA. Relatório de campo[sem autoria]. “Atrocities in the nicaraguan civil war”. Publicado em: 12/01/2012. Disponível em: <https://www.cia.gov/readingroom/document/cia-rdp85t01058r000100170001-7>

FERRAN, Lee. “Ex-NSA chief: we kill people based on metadata”. ABCNEWS. Publicado em: 12/05/2014. Disponível em: <http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/>. Acesso em 20/09/2024.

FOUCAULT, Michel. Filosofia analítica da política. In: FOUCAULT, Michel. **Ética, sexualidade, política**. Ditos e Escritos V. Org Manoel Barros da Motta; tradução Elisa Monteiro. Forense Universitária: Rio de Janeiro, 2006.

FOUCAULT, Michel. **Teorias e instituições Penais**. São Paulo: WMF. Martins fontes, 2020. Tradução Rosemary Costhek Abílio

GALLOWAY, Alexander. **Protocol Society: How Control Exists after Decentralization**. Cambridge: The MIT Press, 2014.

GREENBERG, Andy. **Lords of Crypto Crime: The Race to Bring Down the World’s Invisible Kingpins**. EUA: Monoray, 2024.

GOLDREICH, Oded. **Foundations of Cryptography: Basic Techniques**. Cambridge: Cambridge University press. 2004

HARCOURT, Bernard. **A contrarrevolução: como o governo entrou em guerra contra os próprios cidadãos**. Glac Edições: São Paulo, 2021

HARCOURT, Bernard. **Exposed: Desire and disobedience in the digital age**. Harvard University Press: Cambridge, 2015.

HARCOURT, Bernard. On Critical Genealogy. **Contemporary Political Theory**. Coletânea de artigos open Access”. Agosto, 2024. Disponível em: <https://doi.org/10.1057/s41296-024-00715-y> Acesso em: 19/10/2024.

HERSH, Seymour. “Torture at Abu Ghraib”. New Yorker. Publicado em: 04/05/2004. Disponível em: <https://www.newyorker.com/magazine/2004/05/10/torture-at-abu-ghraib>



HUGHES, Eric. Manifesto Cypherpunk. In: **Manifestos Cypherpunks**. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021.

JAKOBSEN, Sune K. **Cryptogenography: Anonymity without trust**. Tese de doutoramento no Departamento de Filosofia. Londres. Queen Mary University of London, 2016. Disponível em: <https://qmro.qmul.ac.uk/xmlui/handle/123456789/23264> Acesso em: 21/10/2024.

KAHN, David. **Codebreakers: The Story of Secret Writing**. Nova Iorque: Macmillan Company, 1968.

KANYE, David. ONU. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.". Disponível em: <https://documents.un.org/doc/undoc/gen/g15/095/85/pdf/g1509585.pdf> Acesso em: 19/07/2024.

KERRIGAN, Michael. **Enigma: A verdadeira história do código secreto da segunda guerra mundial**. EUA: M.Books, 1989

MAY, Timothy. Manifesto Criptoanarquista. In: **Manifestos Cypherpunks**. Org. FOLLETO, Eduardo. São Paulo: Baixa Cultura, 2021, p.25.

PLANT, Sadie. **The most radical gesture: The Situationist International in a postmodern age**. Routledge: Londres.

RIVEST, R.L; SHAMIR, A.; ADLEMAN, L."A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). **Communications of the ACM**. Fevereiro de 1978. 21 (2): 120-126. CiteSeerX 10.1.1.607.2677. doi:10.1145/359340.359342. S2CID 2873616. Archived from the original (PDF) on 2023-01-27. Acesso em: 16/11/2024

SOZZO, Maximo. **Reconstruyendo las criminologias Críticas**. Ad Hoc: Buenos Aires, 2006.

STORIG, Hans Joachim. **A Aventura das Línguas: Uma História dos Idiomas do Mundo**. São Paulo: Editora Melhoramentos, 1995 .

WARK, Mckenzie. **A hacker manifesto**. Cambridge: Harvard University Press, 2004.

WILLIAMS, Owen. Google Promises reCAPTCHA Isn't Exploiting Users. Should You Trust It? Onezero, 2019. Disponível em: <https://onezero.medium.com/google-promisesrecaptcha-isn-t-exploiting-users-should-you-trust-it-ed99f1543f28> Acesso em: 28/11/2021.

ZUBOFF, Shoshana. **The age of surveillance capitalism**. Nova York: Public Affairs: 2019.