ANONIMATO: RESISTÊNCIA TECNOPOLÍTICA NA REDE

Anonymity: Technopolitical Resistance in the Network

Samuel Medeiros Andreatta
PUCRS
ORCID: https://orcid.org/0000-0003-2862-1776
E-mail: samuelandreatta@hotmail.com

Jesus Sabariego
Universidade de Sevilha
ORCID: https://orcid.org/0000-0002-4500-8589
E-mail: bitnik77@gmail.com

Trabalho enviado em 24 de maio de 2024 e aceito em 22 de setembro de 2024

RESUMO

O anonimato assume um caráter utópico diante das matrizes da Sociedade de Controle. Partindo do estudo de modelos de controle tecnológico, ou expressões da Sociedade de Controle, percebe-se que o fluxo de dados tem circuitos que escapam à tentativa de se fazer concretizar as proteções conferidas pela Lei. A problemática contemporânea deste fenômeno é abordada a partir de um olhar Criminológico Crítico estruturado pela exploração bibliográfica e análise transversal de legislação. O objetivo do presente trabalho é mostrar os entrecruzamentos teóricos na conceituação do anonimato e resistência política no espaço da web. Como o anonimato e as táticas de anonimização funcionam como formas de resistência política em contextos tecnológicos? Os limites legais da criptografia são claros e objetivos no controle das populações? A hipótese central do trabalho , que foi confirmada ao longo da pesquisa, é que o anonimato desempenha um importante papel no cenário de política criminal em espaços digitais e pode atuar como forma de resistência política. Diante da rápida e exponencial incorporação das novas tecnologias em diversas áreas do saber, torna-se evidente a importância de um olhar que abdique do maniqueísmo que usualmente vem atrelado às potencialidades tecnológicas, especialmente no que diz respeito às práticas punitivas.

Palavras-chave: Anonimato. Resistência Política. Criminologia Crítica. Novas tecnologias.

ABSTRACT

Anonymity takes on a utopian character in the face of the frameworks of the Control Society. Starting from the study of models of technological control, or expressions of the Control Society, it's noticeable that the flow of data has circuits that elude attempts to concretize the protections conferred by the law. The current problematic of this phenomenon is approached through Critical Criminology and structured by bibliographical exploration as well as transversal legislation analysis. The objective of this work is to exhibit the points of contact in the contextualization of anonymity and political resistance on the web. How does anonymity and anonymization tactics work as ways of political resistance in technological contexts? Are the legal limits of cryptography objectively clear in the control of populations? The central hypothesis, that was verified along the research, is that anonymity can act to bolster political resistance. Given the rapid and exponential integration of new technologies in various areas of knowledge, the importance of a perspective that abstains from the dualism that is usually attached to technological potentials becomes evident, especially concerning punitive practices.

Keywords: Anonymity. Political Resistance. Critical Criminology. New Technologies.

1. INTRODUÇÃO

Trata-se de pesquisa teórica de caráter indutivo que propõe indagações respondidas por avaliação crítica e reunião de trabalhos teóricos. O objetivo do presente trabalho é exibir os entrecruzamentos teóricos na conceituação do anonimato e resistência política no espaço da web e apontar para as práticas de criminalização primária desse fenômeno na legislação brasileira. De maneira geral, objetiva-se demarcar as reações sociais às práticas de anonimato nas redes que exibem uma função de resistência política. Adota-se como teoria base a ideia de "tomada de posição" defendida por Amaral (2020, p. 17) e que se expressa ao abdicar das posições de "filósofo legislador e filósofo pedagogo" na linha de Foucault (2006). A técnica utilizada é a pesquisa bibliográfica centrada em levantamento de obras e notícias sobre o tema e análise transversal de legislação. A hipótese de trabalho central é a de que o anonimato performa um importante papel no cenário de política criminal em espaços digitais e pode atuar como forma de resistência política.

Em termos criminológicos, adotamos a posição fragmentária, conforme Sozzo (2006) postulada pelas Criminologias Críticas. Entendendo a inexistência ontológica do delito, através do combate à proposição de independência entre ato e a reação, nos aliamos à posição de Becker (2009, p.32), 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 Foucault[1]. 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.

Na presente pesquisa, partimos da ideia de Deleuze (1992) das Sociedade de Controle como teoria base para tensionar o cenário tecnopolítico frente ao anonimato caracterizando a passagem da sociedade disciplinar para a sociedade de controle. A nova razão algorítmica pode ser vista pelo prisma, como indicado em Sabariego (2020), dos "*algoritarismos"*, o termo designa a imposição que os novos dispositivos tecnológicos projetam na vida cotidiana, e atenta para as mudanças nas táticas de gerenciamento; o controle passa a ser materializado por vetores biopolíticos que

[1] A explicação pormenorizada do termo pode ser encontrada no curso ministrado por Foucault (2020, p. 275) na Collége de france em 1971. O termo também foi objeto de entrevista, em discussão com Roger Pol-Droit (2008).

estabelecem "clusters" informacionais; o vetor de controle biopolítico dos corpos é superposto às técnicas disciplinares e é instrumentalizado por uma razão algorítmica.

A difusão algorítmica dos controles populacionais nos leva a perceber a construção de novos regimes de veridição, em um contexto de pós verdade, que postulam eficiência de maneira dúplice: enquanto característica central da definição teórica do próprio conceito[2], e como discurso político-jurídico que propaga a expansão de ingerência de ferramentas tecnológicas, por exemplo, na aplicação da pena[3]; é um conjunto de proposições centradas, como nos esclarece Morozov(2020) em um "solucionismo tecnológico". Para se alcançar a eficiência é preciso haver desperdício, são etapas indissociáveis, como aponta Klossowski (2017). O desperdício, em termos de avanço tecnológico, é uma etapa para se alcançar a eficiência, e é materializado pela repetição de atos de construção e destruição que continuam indefinidamente; basta prestar atenção nas técnicas de obsolescência programada, no avanço vertiginoso das tecnologias e no fetichismo do consumo que leva a substituição constante de ferramentas tecnológicas e traz consequências ambientais devastadoras, assim como as mega fazendas de mineração de ativos da *blockchain* que produzem um desperdício de poder computacional, conforme Truschtel (2017) e um desperdício material pelo alto consumo de energia e sobre uso das placas de GPU. Em termos de práticas punitivas o desperdício é dos corpos humanos, a eficiência tecnológica possui um circuito de velocidade muito mais rápido do que o tempo processual, fragilizando a presunção de inocência sob o mote de eficiência, afinal em uma lógica punitivista mais prisões significam uma política criminal mais eficiente. Dentro desse panorama tecnopolítico buscamos exibir o relacionamento entre anonimato e táticas de controle social. Como o anonimato e as "táticas"[4] de anonimização funcionam como formas de resistência política em contextos tecnológicos? Os limites legais da criptografia são claros e objetivos no controle das populações?

No que concerne à resistência política, utilizamos a acepção que parte de uma perspectiva foucaultiana que, por sua vez, define a resistência política como a insuportabilidade de certo

[2] Algoritmo, segundo a definição computacional presente em llis (2004), é o método utilizado pelo computador para solução de um problema composto pelas seguintes características: 1) input 2) output 3) definitividade (instruções não ambíguas) 4) Finito (algoritmo termina depois de certo número de passos 5) O algoritmo é eficiente. Cabe também destacar aqui a mudança denotada por Galloway (2004, p. 108) entre a programação procedural e a programação orientada a objetos. Enquanto a primeira atua a partir de uma linearidade de encadeamentos, a segunda trata cada um dos códigos como entidades munidas de características próprias.

[3] A utilização de sistemas estatísticos para verificação de reincidência traz problemas de algoritmos enviesados e aplicações desproporcionais de pena, como delimita O'Neil (2016). O sistema COMPAS vem despertando críticas por ter características enviesadas quando se trata de minorias, como descrito por Simon Maybin (2016). Ainda nessa linha, uma douta pormenorização dos avanços tecnológicos em termos de processo penal pode ser encontrada em artigo realizado por Giacomolli (2023).

[4] Tática aqui é entendida como flutuação do jogo posicional da dinâmica de poder, que exibe a fragilidade e "desfetichiza" um cenário assentado. Nesse sentido a delimitação do termo encontra-se em Dardot (2021, p. 40).

exercício de poder (Foucault, 2006, p. 49). Ainda nessa linha, o anonimato pode conferir uma coerência tática a formas de resistência, mas por si só não caracteriza a resistência política. O anonimato aqui encarado se relaciona com as práticas -posteriormente descritas - de autodefesa, práticas essas que implicam em uma relação na qual a oposição de resistência é feita por um sujeito pertencente a uma minoria não legitimada pela atuação estatal.

Os resultados alcançados proporcionam uma sistematização do conceito de anonimato. O conceito de anonimato se caracteriza inicialmente nos dois graus estratégicos postulados por Bordeleau (2018), o primeiro é centrado na utilização do anonimato para alcançar maior projeção política e escapar da criminalização secundária, o segundo trata de um modo de vida que abdica de metas culturais. O anonimato é também caracterizado pela crítica ao reducionismo dos conceitos de Privacidade e Autodeterminação Informativa e, seguindo o exemplo dos nu pieds, na coerência da tática de contrapoder exibida pela força do anonimato enquanto fator de união.

As táticas de anonimização empíricas trabalhadas aqui são a utilização das chamadas VPNs como maneira de blindar o número de IP, especificamente durante a Primavera árabe, e a emergência da plataforma Darkfi, circuito econômico especulativo que se propõe a construir algoritmos anônimos que conferem a materialização da liberdade na rede.

Os limites legais às práticas criptográficas não são objetivos, tampouco se preocupam com a defesa da manifestação política em torno do anonimato. Verificou-se que a legislação pátria parte da criminalização do anonimato de maneira reflexa no que diz respeito a majorantes específicas e de maneira direta quando tratamos do novo Projeto de Lei das Fake News.

2. ENTRECRUZAMENTOS TEÓRICOS

Para definir o anonimato é preciso manejar alguns vetores. O primeiro é derivado de um autor que constituiu a pista inicial da presente pesquisa, Erik Bordeleau. O autor trabalha no campo da estética, e procura traçar atravessamentos da obra foucaultiana na relação entre anonimato e resistência política. Manejando exemplos históricos de performances políticas de anonimato, como a figura do subcomandante Marcos do Movimento Zapatista, as ações cibernéticas do grupo *Anonymous*, e a amálgama de movimentos do *occupy wall street*, Bordeleau (2018, p. 5) constituiu uma maneira de perceber a potência de escapar das molduras depositadas pelos processos de identificação.

O autor propõe uma esquematização dos atravessamentos entre resistência política e anonimato em dois graus. O primeiro grau é chamado de grau estratégico e figura na teatralidade das táticas. Sua intenção é dissimular a identidade a fim de maximizar a intervenção. A função do anonimato

aqui é, por um lado, manifestar um descontentamento político sem precisar soluções e, por outro, obviamente, evitar os processos de criminalização secundária. Trata-se enfim de estabelecer "zonas de opacidade, onde pessoas podem circular e experimentar livremente sem trazer o fluxo de informações do Império" (TIQUUN, 2020, p. 80).

Estar visível na internet é estar sujeito a todo tipo de controle. Controle exercido de maneira geral pela multiplicidade de agenciamentos, nesse sentido: "Cada um de nós é envolvido num tal agenciamento, reproduz o enunciado quando acredita falar em seu nome, ou antes fala em seu nome quando produz o enunciado". (DELEUZE; GUATARRI, 2000, p. 48)

O funcionamento desses agenciamentos pode ser exibido em diversas instâncias da rede, pelo circuito de extração de dados (ZUBOFF, 2019), por táticas de contra insurgência internalizada (HARCOURT, 2021) e desejo de exposição (HARCOURT, 2015) assim como pelo autocontrole sinóptico (MATHIESEN, 2013) e afetivo (DUNKER, 2020). Opor resistência política através do anonimato é expor o problema da visibilidade. A força do anonimato é evidenciada, por óbvio, diante da impossibilidade de criminalização secundária, mas ao mesmo tempo, por ser uma barricada a essas formas de agenciamento, ele impede o fluxo normal do circuito de velocidade (VIRILIO, 1998), visto que o anonimato na rede impossibilita a "ubiquidade, a instantaneidade e a imediatez" (VIRILIO, 1998, p. 48) do controle. Em um jogo de cartas marcadas, o mínimo que se pode fazer é não revelar sua mão; se colocar anônimo na rede não equivale apenas a escapar da redução do sujeito a um produto ou à matéria bruta[5] , mas a criar uma outra forma de existência.

O segundo grau do anonimato em Bordeleau (2018, p. 13) conjuga formas de ação política e de modo de vida. Para ele, no nível da ação política prática, é preciso converter o anonimato em uma função ofensiva e não passiva ou reativa. Como modo de vida, é preciso aceitar o anonimato enquanto categoria política de resistência, contribuir para a negação dos lugares comuns que configuram a hegemonia cultural do capitalismo, abdicar do que significa ser alguém: "basta ver a cara de quem é alguém na sociedade para compreender a alegria de não ser nada" (BORDELEAU, 2018, p. 16). Trata-se, em suma, de uma negação experiencial, que se constitui como modo de vida crítico ao marco cognitivo hegemônico e que, antes de tudo, visualiza a tensão normativa entre liberdade e liberdade (Egaliberté) que define o Estado de Direito contemporâneo segundo Etienne Balibar (2010).

Ao mesmo tempo, ao expor a insuportabilidade de determinada relação de poder em um regime de visibilidade, ou seja, ao abdicar do anonimato, tem de se ter em mente que o discurso não demora a ser capturado pela lógica neoliberal. Basta ver os efeitos que alcançaram as políticas identitárias

[5] O entendimento do sujeito enquanto matéria bruta no regime do Capitalismo de vigilância é a perspectiva defendida por Zuboff (2019).

não transversais, sua expressão de suposta garantia pelo Direito Penal levou ao que Rubio (2021) chamou de reversibilidade dos Direitos Humanos: um instrumento reconhecido por suas violações é chamado para acudir as minorias. No Brasil, o fenômeno da expansão do âmbito punitivo como proteção às minorias pode ser visto pela criminalização da homofobia pelo STF[6] e pela recente tipificação da injúria racial como crime mais grave, de racismo[7].Através da constitucionalização do Direito privado à propriedade como Direito Fundamental e sua proteção como bem individual, o resto de direitos se submetem à interpretação hierárquica na qual a propriedade privada individual e sua proteção supõem o maior bem a ser protegido na sociedade. A propagação do discurso de necessidade de representação individualizante acaba por culminar em um tokenismo acrítico e uma amputação da dimensão do comum, que logo são capturados pelo nexo neoliberal em forma de "identidades estratificadas autointoxicantes" (BORDELEAU, 2023, p. 95).

Dentro da perspectiva das resistências atuais entende-se que essa posição tenha íntima relação com a proposição de Safatle no seu enfrentamento de um identitarismo não transversal, aquele que pode ser facilmente capturado por pautas neoliberais. Assim, o anonimato é relacionado à força da categoria proletariado como princípio de "desindentidade" e desdiferenciação. Nas palavras do autor: "De certa forma, há em Marx uma espécie de "condição proletária" presente como horizonte regulador de seu igualitarismo radical. Essa condição mereceria ser recuperada na reflexão política contemporânea" (SAFATLE, 2015, p. 4).

A presente crítica, fundada em um ceticismo próprio da desconfiança foucaultiana, não pretende descrever o anonimato a partir de um maniqueísmo tacanho. Assim como a tecnologia, o anonimato não é intrinsecamente bom ou mau. Nos importa traçar os vetores que estabelecem o conceito, apontar formas de resistência que se estruturam pelo anonimato e enumerar instâncias de criminalização primária através da tipificação indireta do anonimato, já que a própria assunção do anonimato como opção política mostra a desintegração dos limites entre o público e o privado constituintes do Estado de Direito questionando sua artificialidade hoje.

Como anteriormente postulado, não é a intenção do trabalho atuar como "filósofo legislador", ou seja, não se tenta por via criminológica reformar o dispositivo constitucional que veda o anonimato quando atrelado à manifestação política, mas demonstrar que ambos são inexoravelmente ligados. A história da nossa tênue democracia, vista pelas lentes do jogo de poder das práticas de cabresto, é prova da importância política conferida ao anonimato através da aprovação do voto secreto. Em termos do panorama global da Sociedade de Controle a conexão

[6] A expansão do direito penal como forma de proteção que exibe qualidade simbólica é incorporada na decisão da Ação Direta de Inconstitucionalidade por Omissão nº 26.
[7] Uma análise sobre as nuances da nova legislação foi feita pelo MPPR (2023).

entre ambos é explícita, basta prestar atenção nos casos em que o anonimato é condição de possibilidade da atuação política como nas manifestações realizadas durante a Primavera árabe.

Enfrentando um regime autoritário que possuía extenso controle da rede, os manifestantes de diversos países árabes passaram a fazer uso das chamadas VPNS, ferramentas que anonimizam o local de envio de pacotes permitindo um acesso menos restrito da internet. Novamente a armadilha se apresenta: não se defende que tal ferramenta seja a panaceia, tampouco entende-se que essas ferramentas por si só proporcionariam um anonimato absoluto. Apesar de opor barreiras às técnicas de controle[8] estatal, os VPNS[9] permitem a captura de dados pelas empresas privadas que fornecem essas ferramentas. Aqui é exibida uma das características concretas do anonimato das redes: não há a possibilidade de anonimato absoluto. Especialistas como Sparc (2021) indicam que mesmo que sejam utilizadas todas as técnicas de anonimização, se uma agência de Inteligência se empenhar na busca de um indivíduo específico não há escapatória. A estruturação física da rede da internet, visto que para se comunicar à rede internacional é preciso de um servidor local, permite que a vigilância seja depositada no ponto de entrada de conexão, possibilitando a materialização da ubiquidade das técnicas de controle exibidas, por exemplo, pela interação entre o setor privado e público dos programas de inteligência americana, como indicou Assange (2013, p. 111), que demonstram um aspecto totalizador da vigilância.

O anonimato aqui encarado não é um desdobramento da privacidade. É uma posição ofensiva, ao contrário da privacidade reativa. A privacidade na rede assume um caráter individual. Como apontam Neto e Demoliner (2018, p. 25), a privacidade, por se tratar de um conceito multifatorial, comporta diversas definições: "privacidade como não intrusão; privacidade como possibilidade de exclusão; privacidade como limitação; privacidade como controle; privacidade centrada no binômio acesso restrito e controle limitado; privacidade a partir do direito de manter o controle sobre as próprias informações". Paralelamente, o desenvolvimento do âmbito de proteção necessária frente aos avanços tecnológicos foi aventada a necessidade do estabelecimento do conceito de autodeterminação informativa. A autodeterminação informativa pode ser classificada, na sua dimensão individual como: "o direito de cada indivíduo poder controlar e determinar o acesso e o uso de seus dados pessoais" (CANOTILHO, 2003, p. 233). Já a dimensão coletiva elege a autodeterminação informativa, como garantidora de uma "ordem comunicacional livre" nos termos de Sarlet (2021).

[8] A primavera árabe demonstrou a potência dessas ferramentas, como indicado pela BBC (2013) e em Johsnton (2013). Ademais, recente mudança legislativa realizada pela Lei 175 de 2018 do Egito passou a proibir a utilização de VPNS para o acesso de sites proibidos como explicitado em Chawki (2020)

[9] Para compreender a questão do mercado de ferramentas de privacidade, sugere-se o estudo de Elvy (2017).

Todas essas definições sofrem de um problema: pressupõem a existência dos dados em um vácuo. Não há uma sequência lógica onde os dados são criados de forma livre, e depois os mecanismos do Direito incidem para impedir os abusos dos agenciamentos virtuais, eles já nascem atrelados às técnicas de gerenciamento, como prática de "assujeitamento"[10] que reduz o titular aos dados que a própria empresa ou Estado produziram. Quando se encaram os dados a partir de uma perspectiva mercadológica, como bens que o titular consegue dispor, mesmo que se admita a constitucionalidade da autodeterminação informativa como Direito fundamental, olvida-se a relação de poder intrínseca à criação desses dados. Ao mesmo tempo, ao aceitar essas definições, presume-se que as empresas atuariam de acordo com a legislação, o que não é verossímil, seja numa perspectiva de violação da Lei, como indicam diversos escândalos de vazamento de dados[11], seja a partir de um *lawfare* corporativo que postula novas teses jurídicas para legitimar a atuação das empresas de tecnologia. Como comprova Zuboff[12] em sua análise dos problemas jurídicos atinentes ao Google Street View, o Google propagou diversas teses jurídicas quanto a ausência de expectativa de privacidade em espaços públicos para driblar as proteções anteriormente concedidas.

Esses pontos de vista pressupõem um nascimento livre e soberano dos dados, manejam os dados desde uma perspectiva contratual, e os encaram ou como bem passível de ser transacionado, ou como extensão de direitos da personalidade que seriam tutelados pelas normas do Direito. Entretanto, depositar confiança no Direito como barreira ao retrocesso é, no mínimo, ingênuo[13].

Ao contrário, em uma perspectiva crítica, é preciso perceber que o titular não cria os dados sozinho, a relação de poder que implica a criação de dados na sociedade de controle constitui uma condição de possibilidade limitante do discurso, o que pode ser postado na rede é muito mais amplo do que um adequado tratamento e uma clara finalidade do objetivo dos dados[14], e passa por circuitos muito mais amplos do que a adequação jurídica estatal. O olhar que vê os indivíduos como portadores de dados é essencialmente uma prática de "assujeitamento" que exibe a intimidade própria do gerenciamento do individual e a naturalização acrítica desse tipo de discurso, que descontextualiza ou por melhor dizer, "desterritorializa" a própria soberania e o estatuto cidadão dos sujeitos portadores de dados. Ao depositar o olhar sobre o anonimato, ao invés da identificação

[10] O termo se refere a análise foucaultiana encontrada em Foucault (1995, p. 231).
[11] Basta lembrar do exemplo da Cambridge Analytica, como elabora Confessore (2018). No Brasil, o governo Bolsonaro foi palco de outro escândalo de vazamento de dados, como se pode observar em matéria do G1 (2021).
[12] Um enfrentamento pormenorizado do tema pode ser encontrado em Zuboff (2019, p. 96). Para uma análise sob lentes do ordenamento jurídico pátrio, a problemática do fluxo de informações é abordada sob uma visão constitucional em Assis (2023).
[13] Os Direitos fundamentais amparados em Cláusulas pétreas não constituíram qualquer barreira para o retrocesso advindo das reformas trabalhistas e previdenciárias vivenciadas pelo Brasil desde a primeira Gestão do governo Lula em 2002. Como se pode observar em matéria vinculada pelo portal Terra (2003).
[14] Como explicitado na LGPD Lei Geral de Proteção de Dados em seu art. 6º, inc. I e II.

que é própria do gerenciamento de dados, do titular identificável dos dados, invertemos o olhar criminológico para as posições de fricção, para as reações sociais de contrapoder às práticas de controle, no caso o anonimato.

Para nós, a resistência política é sintetizada como "a luta contra a insuportabilidade de uma relação de poder" (FOUCAULT, 2006, p. 46). Entendemos ser mais rico, diante das críticas tecidas às noções de privacidade e autodeterminação informativa, relacionar anonimato e resistência política a partir da fricção entre a noção jurídica de Legítima Defesa e a noção teórica, defendida por Elsa Dorlin 2020) de autodefesa. A legítima defesa, na prática, é atrelada aos verdadeiros sujeitos de direito, ou seja, o reconhecimento da legítima defesa, como a autora demonstra no caso de Rodney King, é inerente ao sujeito que a pratica, às técnicas punitivas de criminalização secundária e ao circuito de ilegalismos que é próprio da Lei penal. A legítima defesa proporciona uma moldura jurídica para a violência policial, e tende à expansão que é própria da seara punitiva, como demonstra o absurdo projeto de tentativa de exculpação de mortes exercidas por policiais de governos autoritários, e usualmente na difusão devastadora dos autos de resistência (ZACCONE, 2011). Já a autodefesa é aquela exercida por minorias, não positivada pela legislação, justamente daqueles sujeitos cujo Estado não reconhece o direito de legítima defesa. A autodefesa, ao contrário da legítima defesa, não pressupõe um sujeito preexistente consubstanciado pela ficção jurídica do sujeito de direitos, mas surge no próprio movimento de resistência, quando é preciso se defender de determinada prática punitiva. Segundo Butler (2020), trata-se de "uma forma de cuidado – não a ética do *care* contemporâneo – mas aquele cuidado das práticas feministas que se dá coletivamente, no contexto de um movimento de resistência".

Assim, equaciona-se a autodefesa como expressão de resistência política que tratamos aqui. Para precisar o que consideramos como práticas de resistência política é interessante traçar um paralelo pouco usual, o de uma revolta da Normandia no século XVII, a revolta dos Nu-pieds, e o recente movimento QANON. Foucault aborda a revolta dos Nu-pieds em seu curso "Teorias e Instituições penais", ainda quando entendia o sistema penal enquanto medida de prevenção antisediciosa, a partir de uma matriz de contrapoder. Tomando por base o recém traduzido livro de Porshnev sobre o assunto, as nuances das críticas de Mousnier e o trabalho de Thompson, Foucault encara os Nu-pieds como acontecimento expresso de contrapoder[15].

A relação entre anonimato e resistência política pode ser encontrada no exemplo histórico de "Jean Nu-Pieds" (FOUCAULT, 2020, p. 28). Jean Nu-Pieds era uma figura anônima, líder da revolução dos Nu-pieds que ocorreu na Normandia por conta da insustentabilidade da tributação

[15] A pormenorização dessa relação pode ser encontrada em Andreatta (2022).

régia na produção de sal. Foucault localiza, neste momento, atrelada à subversão de categorias do direito germânico, o nascimento de toda uma nova malha de práticas punitivas. Jean Nu-Pieds assinava todas as ações sediciosas dando a elas um caráter político, assim como o Rei assinava seus atos de poder. Diante de uma larga "malha de poder", para utilizar a terminologia de Foucault (1981), assim como o Rei estava distante de seus súditos, e a maioria das pessoas só havia visto no máximo sua assinatura, a aceitabilidade de uma figura não corporificada permitiu conceder unidade e legitimidade ao movimento sedicioso, caracterizando-se como um contrapoder por mimetizar atos que seriam privativos do Estado, como alistamento, cobrança de tributos e aplicação de penas.

Mais tarde, descobre-se que, de fato, essa figura existia apenas como um recurso prático e discursivo. Ou seja, o anonimato funcionou aqui como uma despersonalização que atribuiu um caráter político a determinadas ações e não necessitava nem da efetiva existência do sujeito. É nesse sentido de contrapoder que Foucault trabalha uma das expressões do anonimato enquanto ordenadora de uma tática que confere coerência política. Mas não é só essa característica que confere a condição de resistência política aqui trabalhada. As ações performadas por esse movimento, que se caracterizava expressamente como descalços para demonstrar que nada possuíam, muito embora a revolução tenha sido apoiada também por parte da burguesia e senhores feudais, visava à insuportabilidade da tributação indireta, que necessariamente atinge de maneira mais robusta os mais pobres. Assim, diante desse devir minoritário, podemos aproximar tal revolução às práticas de autodefesa e um aspecto de contrapoder. As ações políticas dos descalços de ataques às diligências não eram meros saques, mas confiscos; a morte de seus inimigos políticos não eram apenas homicídios, mas execuções. A tentativa de deslegitimar o nascente estado monárquico por uma invenção de outra Lei era muito mais perigosa do que o mero desvio da Lei.

Feitas as considerações sobre os Nu-pieds, passemos para o movimento Qanon. O Qanon[16] foi um movimento de extrema direita americana que nasceu durante a gestão Trump. O movimento nasce a partir de posts no site de subforums 4chan que afirmavam haver uma conspiração da "esquerda global satânica" contra Donald Trump, os posts são assinados por um autor que se autointitula Q, talvez ecoando o romance de autoria coletiva sob o pseudônimo Luther Blisset do movimento Wu Ming publicado na Itália em 1999[17]. O que nos importa destacar aqui é que o fato desse autor ter postado anonimamente trouxe legitimidade política ao que ele dizia e conferiu uma coerência ao movimento. Os seguidores de Q divergem sobre sua identidade, e exatamente por isso diferentes perspectivas sobre o direcionamento político do movimento podem conviver na coerência de uma tática. A força mítica do anonimato, e a ideia de Q enquanto o salvador da pátria, aglutinou

[16] Essas informações foram coletadas do documentário: "Q into the storm".
[17] Informações quanto ao movimento podem ser encontradas no site do projeto que leva o mesmo nome.

diversas pessoas em torno do movimento exatamente por se blindar da fragilidade do nome. Fragilidade do nome no sentido de que fazendo uso do anonimato Q permite que diferentes perspectivas convivam sobre sua verdadeira identidade e, ao mesmo tempo, impede que se possam apontar as contradições entre sua vida pessoal e suas ideias.

Se o anonimato nesse caso conferiu coerência a uma tática porque não pode ser interpretado como resistência política? Como explicitamos, não é apenas nessa função de ordenação do anonimato que se caracteriza a resistência política, antes é preciso verificar qual é o jogo de fricção próprio dessas relações de poder. O movimento Qanon não se contrapõe às práticas abusivas do Estado; pelo contrário, legitima-as a partir de um fetichismo próprio de pulsões fascistas pela exacerbação da figura do Lider supremo que deve salvar as pessoas, no caso do Qanon, Donald Trump. O movimento Qanon não é construído por minorias, ele postula a defesa de valores tradicionais numa guerra cultural constante lutada com armas tecnopolíticas contra um inimigo invisível, designado de maneira geral como comunismo, que pode a qualquer momento tolher sua liberdade. O comunismo, como indica Adorno (2020, p. 60) na classificação dos aspectos do radicalismo de direita, se tornou uma palavra que causa, através da propaganda, um temor irracional. Nessa linha, os movimentos de Extrema-Direita se caracterizam por uma "constelação de meios racionais e fins irracionais" (ADORNO, 2020, p. 54). O slogan de Trump, "Make America Great Again" simboliza o caráter reacionário dos objetivos perseguidos.

E, por fim, o movimento Qanon, diferente dos nu pieds, não parte de uma posição dos despossuídos, mas de um discurso fictício que se centra na ideia de políticas de extermínio de "homens de bem" propagadas por uma guerra cultural travada por uma suposta conspiração global satânica. Porém, o que vemos na prática é justamente o contrário, não só não houve perda de direitos e práticas de violência exercidas contra os defensores do movimento, mas se permitiu que o Capitólio fosse invadido. Como se pode falar de insuportabilidade de relação de poder, se o Estado permitiu que os golpistas entrassem sem qualquer resistência nas casas legislativas americanas? Então, é preciso ter cuidado ao filtrar movimentos políticos, pois muito embora o anonimato exercido pelo Qanon confira coerência como tática política, a ele não atribuímos o rótulo de resistência, tampouco de autodefesa.

Continuando na nossa caracterização teórica, afirmamos que o anonimato implica no que Bordeleau vai chamar da "intimidade compartilhada da encriptação mútua" (BORDELEAU, 2023, p. 95), afinal organizar-se não significa necessariamente se filiar a um partido, mas atuar de acordo com uma percepção comum. O anonimato na rede tem íntima relação com a criptografia, mas obviamente há uma miríade de exemplos que demonstram a possibilidade de um anonimato formal

sem maiores táticas criptográficas, como a utilização de chatrooms[18], assim como a opção por determinada plataforma cujos servidores estejam localizados fora do território do usuário e que não possuam acordo de cooperação de dados ou possuam legislações díspares.

No entanto, o foco aqui é depositado em práticas que manejam técnicas criptográficas para atingir um grau de anonimato mais sofisticado e ofensivo do que apenas tentar se esconder, e que tentam limitar a possibilidade de violações exercidas, que como vimos, não podem ser combatidas pelo arcabouço jurídico. E é nessa esteira, de estabelecer padrões técnicos que dificultam o circuito de extração de dados que o DARKFI nasceu. Essa nova tecnologia é centrada em uma nova técnica criptográfica chamada de Zero Knowledge proof.

A criptografia é parte integral da internet, não é apenas uma técnica de anonimização de dados, mas um regime de veridição, pois estabelece a verdade de proposições algorítmicas vinculadas a identidades específicas. Como indica o especialista Rosen (2019), trata-se de uma forma de estabelecer a verdade. A novidade dessa forma de criptografia é o fato de que é desnecessário revelar todos os fatores algorítmicos para haver a comprovação de identidade. Vejamos o exemplo clássico - envolvendo daltonismo - utilizado para exemplificar a Zero Knowledge proof: temos dois polos, o sujeito que está tentando provar que conhece a "verdade", chamaremos, por conveniência, esse polo de (P); e o sujeito que precisa verificar a veracidade dessa informação, designaremos esse polo como (V). (V), que é daltônico, está próximo de nós com duas bolas de cores diferentes, e (P) está tentando convencer (V) que ele consegue distinguir essas duas bolas. Para (V) ambas as bolas são cinzas; para (P), uma é vermelha e a outra verde, e ele afirma que consegue diferenciar as duas. O protocolo prossegue em duas mensagens, ida e volta. Então (V), randomicamente, decide se inverte a posição das duas bolas. Digamos que ele tenha invertido, em seguida ele "mostra" as bolas à (P) perguntando se inverteu ou não. (P), como consegue ver a cor das bolas, confirma a inversão. Esse processo pode ocorrer diversas vezes, podem ser feitas diversas inversões para confirmar a confiabilidade de (P). Assim, (V) por não conseguir verificar a cor das bolas, detém informações sobre a interação, mas não sobre as bolas em si. Ele só consegue confirmar se (P) acertou ou não se as bolas foram trocadas, e não precisa da informação da cor das bolas. Por sua vez, (P) não precisa da informação sobre a ocorrência da inversão, pois consegue ver as cores. O ponto central é que (P) foi capaz de provar que conhecia "a verdade" sem ter que revelá-la a (V). Resumidamente, sem entrar nas nuances matemáticas, o ZK proof funciona dessa maneira.

Mas como ele atua dentro do DARKFI? Esse movimento pressupõe que a forma contemporânea da internet: "encoraja docilidade e consumismo ao invés de uso individuado ativo, é uma arquitetura

[18] Tal fenômeno e observável no caso do vazamento de informações do pentágono feitas através de uma chatroom do jogo infantil Minecraft como abordado por Clark (2023).

de opressão estruturada no controle de usuários"[19]. Como contraposição, o DARKFI propõe um deslocamento do lugar de produção de valor, a partir de uma arquitetura fundada nos chamados DAOS (Descentralized Autonomous Networks), trata-se de um circuito econômico centrado em cripto ativos, utilizando a especulação como forma de defesa, focada na saúde da comunidade ao invés de captura de mais valia. Nesse sistema não há distinção entre os criadores dos aplicativos e a comunidade em si. E é sobre esse circuito econômico de contrapoder que a ZK proof pode funcionar como um escudo, justamente por constituir uma estrutura social que se pretende, presumidamente, resistente ao controle estatal e totalitarismo. A plataforma pretende construir espaços que se contrapõem à atomização social e "promovem conexões comunitárias voluntárias que valorizam a liberdade"[20]. Então há a produção de valor a partir do regime de verificabilidade fundado na ZKProof, regime esse que, por incorporar o anonimato como característica intrínseca, impede a captura de dados pelos grandes monopólios tecnológicos. De fato, o uso das ZK proofs, viabiliza a verificação da veracidade de dados sem que esses sejam explicitamente informados, mas, assim como toda ferramenta tecnológica, não constitui um elixir milagroso ou solução absoluta.

3. ANONIMATO E PRÁTICAS PUNITIVAS

As nuances entre o anonimato, resistência política e as práticas de criminalização não são novas. Zaffaroni (2013, p. 51) narra que uma das emergências da crítica do Direito Penal foi a obra "Caution Criminalis", de Friederich Spee. Nessa obra, Spee tece uma crítica aos procedimentos inquisitórios vigentes de seu tempo (século XVII). O livro é uma contraposição ao manual dos inquisidores Malleus Malleficarum, e defende que há uma arbitrariedade flagrante no procedimento de reconhecimento de Bruxaria. Aqui nos importa destacar que o livro foi publicado anonimamente, justamente para maximizar a intervenção política e escapar das instâncias punitivas, encaixando-se no primeiro grau do anonimato que tratamos aqui.

Em termos históricos jurídicos a Constituição Brasileira trouxe a vedação do anonimato quando relacionado à manifestação política. Na constituição de 1891, o sigilo da fonte, resguardado pela constituição atual, era proibido. Na época, ao invés de sigilo, o termo utilizado era anonimato; muito embora o intuito do trabalho não seja o de perscrutar as relações entre a importância política do sigilo da fonte e suas nuances jurídicas, há de se reconhecer o papel central que a proteção da fonte traz dentro de um jogo de forças. O que nos importa destacar, não é exatamente a proibição do anonimato do artigo 72 parágrafo 12, mas sim as críticas tecidas contra o artigo, como indicam

[19] A citação foi retirada do manifesto do Darkfi.
[20] Citação retirada do manifesto do Darkfi.

documentos da Assembleia Nacional Constituinte. Francisco Veiga[21], em 1891, percebera, notadamente em uma perspectiva liberal, a estreita relação entre anonimato e resistência política, postulando 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 para defender sem poder ser suplantado".

Atualmente, o termo anonimato aparece expressamente no Código Penal como majorante do crime de denunciação Caluniosa, no artigo 339 parágrafo primeiro. A tipificação mais gravosa do sujeito que pratica o crime de denunciação caluniosa por meio do anonimato demonstra que o Direito Penal entende que as práticas que tentam blindar o reconhecimento da autoria devem ser punidas de maneira mais severa.

Todavia, o anonimato que tratamos aqui, como resistência política na rede, é verificável na criminalização reflexa na majorante do furto qualificado (art. 155, par 4-c, Inc I) e de maneira direta no PL 2630, de 2020, popularmente conhecido como PL das Fake News. A majorante do furto qualificado narra que o furto mediante fraude cometido por meio de dispositivo eletrônico pode ter a pena aumentada de 1/3 à 2/3 se o crime for praticado mediante utilização de servidor mantido fora do território nacional. Aqui vemos que o legislador optou por estabelecer moldura mais gravosa para aqueles que possuem maior conhecimento técnico. Ignorando o problema flagrante de que diversos servidores de plataformas de redes sociais se localizam no exterior, até 2018 pelo menos[22], e logo, a prática de crimes por meio dessas redes se enquadraria erroneamente nesse tipo por equívoco do legislador, o anonimato aparece tipificado de maneira tácita. O sujeito que pratica o crime de furto mediante fraude por meio de dispositivo eletrônico se conecta a um servidor externo justamente para se manter anônimo, para que seu número de IP seja vinculado a um local fictício. Então o anonimato aparece criminalizado aqui, por exemplo, quando se pune mais severamente um hackerativista que pratica o furto de dados. Frustrando a vigilância da vítima para que possa fazer a subtração[23], o sujeito toma medidas para assegurar seu anonimato e o faz por meio da conexão com um servidor fora do país.

Feitas as considerações sobre a nova tipificação penal atinente ao crime de furto qualificado, cabe abordar as nuances do anonimato e o PL das Fake News. O trâmite de tal projeto tem sido palco de uma disputa entre o poder público e as empresas de tecnologia. A proposição do PL trouxe

[21] O acesso ao texto original manuscrito das emendas constituintes e comentários foi disponibilizado pelo arquivo nacional e está disponibilizada sob a designação Item: AC1891-DISC-2-40-538.
[22] Nesse sentido, o Ministério Público Federal se posiciona favorável a aplicação da lei brasileira quanto às especificidades dos conflitos de jurisdição.
[23] Tal definição do crime de Furto mediante Fraude surge também problemática nos crimes da internet, pois não há de fato uma subtração, é preciso haver uma conexão, adequando-se a conduta à prática do crime de Estelionato

um novo campo de batalha, como indica a pesquisa do Internet LAB da UFRJ[24]. Com a tramitação do projeto, as empresas de tecnologia se empenharam em construir, a partir do direcionamento realizado pela hierarquização de resultados nos buscadores, uma contraposição à legislação, vinculando artigos que postulam que a introdução da nova legislação levará a diversos riscos de segurança. O argumento central é que ao explicitar as formas que os algoritmos proprietários se comportam, esses buscadores estariam se abrindo a ataques, diminuindo a suposta segurança sob a qual atuam (LACERDA, 2023). A preocupação de ocasião pela segurança dessas empresas demonstra a necessidade de encarar seriamente o anonimato.

O anonimato é classificado nessa legislação como "contas inautênticas". O artigo 5º do inc. II do PL narra que:

> Para os efeitos desta Lei, considera-se: II – conta inautêntica: conta criada ou usada com o propósito de assumir ou simular identidade de terceiros para enganar o público, ressalvados o direito ao uso de nome social e à pseudonímia nos termos desta Lei, bem como o explícito ânimo humorístico ou de paródia.

Em seu artigo 6º há a estipulação de obrigação para os provedores de redes sociais e serviços de mensageria privada de vedar o funcionamento de contas inautênticas. Todavia, no parágrafo primeiro do artigo, encontra-se uma ressalva:

> As vedações do caput não implicarão restrição à manifestação artística, intelectual ou de conteúdo satírico, religioso, político, ficcional ou literário, ou a qualquer outra forma de manifestação cultural, nos termos dos arts. 5º, inciso IX, e 220 da Constituição Federal.

Aparentemente, tal ressalva protegeria a manifestação política através do uso de contas inautênticas ou, nos termos que tratamos aqui, a resistência política através do anonimato. Muito embora tal proteção seja importante, ao determinar esse pressuposto de não aplicação da Lei, há um deslocamento do que pode vir a ser entendido como manifestação política para a seara Judiciária. Na prática, o que pode vir a ser considerado como ato político dependerá da discricionariedade do Juiz.

Ao mesmo tempo, o projeto de lei, em seu artigo 7 confere uma margem de atuação inédita para empresas de tecnologia. Nesse artigo, é positivada a possibilidade de empresas de tecnologia para requererem o documento físico de identidade em caso de denúncia por desrespeito à Lei no caso de indícios de contas inautênticas. Então, além do controle do manejo dos dados, essas empresas poderão realizar um controle ainda mais minucioso de seus usuários pela confirmação (ou não) de

[24] O grupo de pesquisa "internet lab" da UFRJ vem fazendo um trabalho crítico de diversas tecnopolíticas atinentes ao espaço brasileiro.

sua identidade física. Ampliar a ingerência dessas plataformas, no que diz respeito ao controle da identidade dos usuários, amplia as possibilidades de mercantilização dos dados, e consequentemente, as possibilidades de violação.

A legislação delimita também que na vedação de contas inautênticas, as plataformas devem atuar nos limites técnicos do seu serviço. Ora, como vimos, por exemplo, no movimento DARKFI, fundado na chamada ZKPROOF, há um próprio limite técnico autoimposto para garantir a anonimização e o fornecimento mínimo de informações. Assim, se o sujeito utiliza uma plataforma que faz uso desse tipo de criptografia, as obrigações constantes na lei seriam impossíveis de serem cumpridas. Apesar de conter essa limitação, a legislação esbarra nas obrigações postuladas pelo Marco Civil no que tange à guarda e registro de dados.

Esse espaço cinza, ainda não delimitado pelo ordenamento jurídico brasileiro, traz uma situação de insegurança jurídica que não será sanada apenas pelo Direito. Barrar a utilização de ferramentas de anonimização criptográfica por se considerar que não realizam uma adequada manutenção e guarda de registros pode ter consequências desastrosas. O anonimato da fonte, que pode ser garantido por esses serviços, será indubitavelmente fragilizado. A legislação que também confere tratamento especial para autoridades públicas em seu artigo 18, pode vir a coibir a manifestação política anônima na internet, visto que na incestuosa relação entre Estado e sujeitos privados expressa pelo fenômeno do "coronelismo eletrônico"[25], determinado agente político poderia fazer uso do requerimento de dados de conta inautêntica para controlar seus desafetos políticos.

4. CONSIDERAÇÕES FINAIS

Expostas as considerações, culminamos em um ponto de chegada que se situa na formalização teórica do conceito de anonimato e sua relação com a resistência política, na exemplificação empírica das formas de resistência política realizadas através do anonimato e pela maneira com a qual a legislação penal vem tratando esse fenômeno.

Primeiro, vimos que o anonimato pode se situar teoricamente em dois graus. O primeiro diz respeito à maximização do efeito político, e como forma de escapar à criminalização secundária. O segundo consiste em uma nova forma de vida que abdica dos lugares comuns da hegemonia cultural no capitalismo cognitivo, opondo-se ao que significa ser alguém na vida, em uma tentativa de

[25] Uma análise pormenorizada do coronelismo eletrônico pode ser encontrada em Melo e Feitosa (2021), assim como em Santos (2006).

recuperar, nos termos de Safatle, um princípio de "desindentidade", ou em outros termos, de anonimização.

O anonimato não pode ser inserido no mesmo patamar dos Direitos à Privacidade e autodeterminação informativa, em um contexto de reorganização dos direitos sob a égide da constitucionalização do direito à propriedade como direito fundamental, pois o olhar depositado sobre os dados desse patamar pressupõe uma captura mercadológica que se olvida da relação de poder e a desterritorialização soberana do próprio fundamento de cidadania no momento de criação de dados, é pressuposta uma vacuidade na criação, como se houvesse um momento puro de não controle na criação dos dados. Entende-se mais preciso caracterizar o anonimato como prática minoritária de contrapoder a partir da fricção entre as noções de Legítima defesa e Autodefesa, o anonimato como autodefesa é uma tática de defesa não reconhecida pela legislação, praticada por grupos minoritários nas redes, exercida frente a insuportabilidade de determinada relação de poder.

Como exemplos empíricos dessas formas de autodefesa relacionada ao anonimato trabalhamos a utilização das ferramentas de VPN na Primavera Árabe, e concluímos pela impossibilidade de materialização de um anonimato absoluto diante da extensão do controle das agências de inteligência. A partir da diferenciação entre os Nu-pieds e o movimento Qanon, estabelecemos os padrões que determinam que o anonimato, por si só, mesmo que confira coerência a uma tática, não representa a resistência política aqui trabalhada, já que não representa uma verdadeira insuportabilidade do exercício do poder. Por fim, nos concentramos no movimento DARKFI para apontar novas ferramentas tecnológicas que possam, pelo seu funcionamento real, materializar uma forma de anonimato como resistência política na rede.

Em termos de criminalização, foi oportuno, para destacarmos a relação entre anonimato e resistência política na seara penal, narrar a crítica anônima de Spee ao Malleus Maleficarum. Em seguida, descrevemos como a vedação do anonimato na constituição vem produzindo embates desde sua concepção inicial. Em um terceiro momento, tratamos de como o termo vem expresso na legislação, e como o Direito Penal entende ser mais grave sua utilização na prática de ilícitos penais.

Foi possível verificar que os limites legais para as práticas de criptografia de maneira a assegurar uma anonimização de viés mais robusto esbarram em legislações que as proíbem e carecem de regulamentação específica. Com a evolução de técnicas criptográficas é preciso um trabalho interdisciplinar, entre autoridades legais, especialistas e sociedade civil, para redigir legislação adequada que garanta os direitos dos titulares de dados e que esteja em consonância com os pressupostos de um Estado democrático de Direito. No entanto, não se espera que apenas esforços legislativos possam barrar cenários de retrocessos.

Por fim, verificamos como a criminalização do anonimato surge de maneira reflexa no aumento de pena consubstanciado pela utilização de servidor no exterior no crime de furto mediante fraude, e como surge de maneira direta na Lei das Fake News, ao impor a vedação de contas inautênticas, ao atrelar a verificação do fator político de determinada ação à discricionariedade judiciária e ao estender as possibilidades de ingerência das empresas de tecnologia na verificação da identidade.

5. REFERÊNCIAS

ADORNO, Theodor. **Aspectos do Novo Radicalismo de Direita**. Editora Unesp: São Paulo, 2020

ANDREATTA, Samuel. **A Construção da Sociedade Punitiva em Michel Foucault**. Dissertação de Mestrado (2022). Pontifícia Universidade Católica do Rio Grande do Sul. Curso: Ciências Criminais.

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

ASSANGE, Julian. **Cypherpunks**. Boitempo editorial: Rio de janeiro, 2013.

ASSIS, Christiane. **O paradoxo da esfera pública digital**. Cadernos de Dereito Actual, nº 21, pp. 101–129, 2023.

BALIBAR, Etienne**. La proposition de l'égaliberté: Essais politiques 1989-2009**. Presses Universitaires de France: França, 2010.

BBC. **Turkish people turn to VPNs as Istanbul protests spread**. Publicado em: 06/06/2013. Disponível em: <https://www.bbc.com/news/technology-22799768> Acesso em: 17/05/2023

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

BORDELEAU, Erik. **Bellonging in Becoming: partes anárquicas y Comunes Cripto escalables**. Dissenso: Revista de pensamento político, Ano 4, nº V, pp. 91-105, 2023, p. 95.

BORDELEAU, Erik. **Foucault Anonimato**. Buenos Aires: Cactus, 2018.

BRASIL. STF. **Ação Direta de Inconstitucionalidade por Omissão nº 26**. Tribunal Pleno do Supremo Tribunal Federal. Relator Min: Celso de Mello. Julgamento em: 13/06/2019.Disponível em:<https://portal.stf.jus.br/processos/detalhe.asp?incidente=4515053> Acesso em: 18/06/2023

BRASIL. **PL 2630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.** Brasília, DF: Diário Oficial da União, 2020.

BRASIL. **Lei Geral de Proteção de Dados.** Capítulo I, Disposições Preliminares, Art. 6º, inc. I e II. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>

BRASIL. [Constituição 1891]. **Constituição Da República dos Estados Unidos do Brasi**l. Rio de Janeiro, RJ: Congresso Nacional Constituinte, 1891.

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-constituinte-de-1890-1891.pdf> Acesso em: 06/03/2023

BRASIL. PRSP. **Nota Técnica referente à ADC 51 2018**. Disponível em: <https://www.mpf.mp.br/pgr/documentos/2CCR_NotaTecnicaADC51.pdf.>

BUTLER, Judith. **Introdução**. In: DORLIN, Elsa. **AutoDefesa: Uma filosofia da Violência.** UBU: São Paulo, 2020.

CANOTILHO, José Gomes. **Direito Constitucional e Teoria da Constituição**. Ed. Almedina: Coimbra. 2003.

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.

CLARK, Emily. **The Pentagon leak that landed on a chat forum about Minecraft exposes an unavoidable weakness in US national security**. Publicado em: 13/04/2023. Disponível

em:<https://www.abc.net.au/news/2023-04-14/pentagon-leak-human-vulnerability-in-us-national-security/102211120>. Acesso em: 10/05/2023.

CONFESSORE, Nichole. **Cambridge Analytica and Facebook: The Scandal and the Fallout So Far**. Publicado: 04/04/2018. Disponível em: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.> Acesso em: 18/07/2023.

DARDOT, Pierre. et Al. **A escolha da guerra civil.** Elefante: São Paulo, 2021.

DELEUZE, Gilles. **Conversaciones. Post Scriptum das Sociedades de controle. Conversações: 1972-1990.** Ed. 34: Rio de Janeiro, 1992.

DELEUZE, Gilles; GUATARRI, Felix. **Mil platôs: capitalismo e esquizofrenia. VOL I**. Editora 34: São Paulo, 2000.

DORLIN, Elsa. **Autodefesa: Uma filosofia da Violência**. UBU: São Paulo, 2020.

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

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

ELLIS, Horowitz. **Fundamentals of Computer Algorithms.** Galgotia Publications Pvt Ltd: EUA, 2004.

ELVY, Stacy-Ann**. Paying for privacy and the personal data Economy**. Columbia Law Review, nº 6, pp. 1369-1459, 2017.

FOUCAULT, Michel. **As malhas do poder**. Barbárie, nº 4, p. 23- 27, 1981.

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

FOUCAULT, Michel. **O Sujeito e o Poder**. In RABINOW, Paul; DREYFUS, Hubert. **Foucault uma trajetória filosófica.** Forense Universitária: Rio de Janeiro, 1995.

GALLOWAY, Alexander. **Protocol: how control exists after decentralization**. The MIT Press: Massachussets, 2004.

GIACOMOLLI, Nereu. **Conhecimento e Saber na era digital: Riscos, desafios e limites**. Cadernos de Dereito Actual. Espanha. nº 20. Núm. Extraordinário (2023) pp. 8–22. Disponível em: https://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/issue/view/20. Acesso em: 18/07/2023.

G1. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**. Publicado: 25/01/2021. Disponível em:<https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml > Acesso em: 11/09/2022

HARCOURT, Bernard. **A contrarevolução: 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.

HOBACK, Clark; MCKAY, Adam. **Q into the storm**. Washington: HBO, 2021.

JOHNSTON, Susan. **Making Freedom Part of the Business Model: How a Young Trep Helped Fuel the Arab Spring**. Disponível em:<https://www.entrepreneur.com/business-news/making-freedom-part-of-the-business-model-how-a-young-trep/225403>. Publicado: 09/01/2023. Acesso: 18/07/2023

KLOSSOWSKI, Pierre. **The living currency**. Bloomsbury Academic: Nova York, 2017.

LACERDA, Marcelo. **PL das Fake News pode aumentar a confusão sobre o que é verdade ou mentira**. Publicado: 27/05/2023. Disponível em: <https://blog.google/intl/pt-br/novidades/iniciativas/pl2630-2>. Acesso em: 15/05/2023.

MATHIESEN, Thomas. **Towards a Surveillant Society: The Rise of Surveillance Systems in Europe**. Waterside Press: Londres, 2013.

MPPR. **Entenda Direito: Injúria racial é equiparada ao racismo**. Publicação: 09/02/2023. Disponível em: <https://mppr.mp.br/Noticia/Entenda-Direito-Injuria-racial-e-equiparada-ao-racismo >.Acesso em: 30/07/2023.

MAYBIN, Simon. **Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA**. Disponível em:<https://www.bbc.com/portuguese/brasil-37677421>. Acesso em: 18/04/2023.

MELO, Vinicius.; FEITOSA, Gustavo. **Coronelismo e a propriedade dos meios de comunicação: a influência da mídia no poder político**. Revista Vindere, vol. 13, n. 28, pp.386-412, 2021.

MOROZOV, Eygeny. **Solucionismo, nova aposta das elites globais**. Disponível em:< https://outraspalavras.net/tecnologiaemdisputa/solucionismo-nova-aposta-das-elites-globais/>. Acesso em 30/07/2023

NETO, Eugênio. **Direito à Privacidade e Novas Tecnologias: Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa.** Revista Internacional Consinter de Direito, nº VII, pp- 19-40, 2018, p. 25.

O'NEIL, Cathy. **Weapons of Math Destruction**. Crown: Nova York, 2006.

ROSEN, Alon. **Introduction to Zero Knowledge**. The 9th BIU School on Cryptography, 2019. Disponível em: <https://www.youtube.com/watch?v=6uGimDYZPMw> Acesso em: 12/03/2023

RUBIO, David. **Reversibilidade do direito: os Direitos Humanos na tensão entre o mercado, os seres humanos e a natureza**. Revista de Estudos Criminais, v.6, nº 22, p.21-32, 2021.

SABARIEGO, Jesus. et al (org.) **Algoritarismos.** Tirant Lo Blanche: São Paulo 2020.

SANTOS, Suzy. **E-Sucupira: o Coronelismo Eletrônico como herança do Coronelismo nas comunicações brasileiras**. Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação. Vol. 7, pp. 1-27, 2006.

SAFATLE, Vladmir. **Por um conceito "antipredicativo" de reconhecimento**. Revista Lua Nova, Nº 94, pp. 1- 20, 2015.

SARLET, Ingo. **Fundamentos Constitucionais: O Direito Fundamental à proteção de dados**. In BIONI, Bruno. (coordenador Executivo). **Tratado de proteção de dados Pessoais.** Forense: Rio de Janeiro, 2021, Ebook.

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

SPARC, Flow. **How to Hack like a ghost.** No starch press: São Francisco, 2021.

TERRA. **Reforma da Previdência é a primeira grande vitória de Lula.** Disponível em: https://www.terra.com.br/economia/reforma-da-previdencia-e-a-primeira-grande-vitoria-de-lula,caf9bb6b4572d3bc5d8bb41926e163fflr91owco.html. Publicado em: 11/12/2003. Acesso em: 18/08/2023.

TIQQUN. **The Cybernetic Hypothesis.** Semiotext(e) / Intervention Series: França, 2020.

TRUTSCHEL, Thomas**. Bitcoin: what a waste of resources: The cryptocurrency's insistence on meaningless computer tasks is outdated, profligate and holds the technology back**. Publicado: 01/11/2017. Disponível em: https://www.newscientist.com/article/mg23631503-300-bitcoin-what-a-waste-of-resources/ Acesso em: 31/06/2023.

"The DarkFi Manifesto". Disponível em: https://dark.fi/manifesto.html. Acesso em 12/04/2024.

VIRILIO, Paul. **Lá Maquina de Vision**. Ediciones Catedra: Madrid, 1998.

ZACCONE, Orlando. **Indignos de Vida. A forma Jurídica da Política de Extermínio de Inimigos na Cidade do Rio de janeiro**. Tese de Doutorado. Curso: Ciência Política. Universidade Federal Fluminense, 2011.

ZAFFARONI, Eugênio. **A questão criminal**. Revan: Rio de Janeiro, 2013.

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

Sobre os autores:

Samuel Medeiros Andreatta
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.
PUCRS
ORCID: https://orcid.org/0000-0003-2862-1776
E-mail: samuelandreatta@hotmail.com

Jesus Sabariego
Bacharel em Humanidades, PhD em Direitos Humanos. Professor Convidado do Programa de pós-graduação em Ciências Criminais da PUCRS. Professor da Faculdade de Comunicação da Universidade de Sevilha, que desenvolve o trabalho na sede do projeto MSCA Technopolitics – The Challenge of Digital Media to Democracy in Europe: an engaged approach (Grant Agreement ID: 897796. DOI 10.3030/897796)
Universidade de Sevilha
ORCID: https://orcid.org/0000-0002-4500-8589
E-mail: bitnik77@gmail.com