OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 13, Nº. 1 (Maio-Outubro 2022)

JANUS.NET
e-journal of International Relations

O EQUILÍBRIO ENTRE PRIVACIDADE V. O ARGUMENTO DA VIGILÂNCIA: A PERSPECTIVA DO REINO UNIDO

VAIBHAV CHADHA
vchadha@jgu.edu.in
Professor Assistente de Direito na Jindal Global Law School, O.P. Jindal Global University (Índia). É mestre em Direito pela Queen Mary University of London e tem uma licenciatura em comércio, bem como em direito pela Universidade de Delhi. Autor de artigos internacionais sobre lei de fiança antecipada na Índia, lei de direitos de autor e liberdade de expressão. Antes de se tornar professor universitário, Vaibhav trabalhou nos Escritórios do Advogado Geral do Estado de Nagaland, Índia, e do Procurador Geral Adjunto da Índia. Os seus interesses incluem liberdade de expressão, direito da comunicação social e direito penal.

Resumo

Após as revelações feitas pelo ex-funcionário da Agência de Segurança Nacional (NSA) Edward Snowden sobre a violação da privacidade de indivíduos pelos estados em nome da vigilância, o direito à privacidade tornou-se um dos direitos mais debatidos. Não há dúvida que o Estado deve garantir a privacidade dos seus cidadãos, mas também tem a responsabilidade pela segurança dos mesmos. Existem diferentes visões relacionadas com privacidade e vigilância. Uma visão é que o Estado não tem o direito de examinar os assuntos privados de um indivíduo, enquanto a outra visão é que não há mal em colocar alguém suspeito sob vigilância, pois é dever do Estado impedir qualquer ato indevido na sociedade. Considerando as visões contrastantes sobre privacidade e vigilância, este artigo explora a posição existente no Reino Unido e visa responder a várias questões relativas ao debate Privacidade vs. Vigilância.

Palavras-chave

Privacidade; Vigilância; Lei de Poderes de Investigação; Regulamento Geral de Proteção de Dados e Proteção de Dados

Como citar este artigo

Chadha, Vaibhav (2022). O equillíbrio entre privacidade V. o argumento da vigilância: a perspectiva do Reino Unido. In Janus.net, e-journal of international relations. Vol. 13, Nº 1, Maio-Outubro 2022. Consultado [em linha] em data da última consulta, https://doi.org/10.26619/1647-7251.13.1.12

Artigo recebido em 15 Agosto 2021 e aceite para publicação em 27 Janeiro 2022

O EQUILÍBRIO ENTRE PRIVACIDADE V. O ARGUMENTO DA VIGILÂNCIA: A PERSPECTIVA DO REINO UNIDO[1]

VAIBHAV CHADHA

1. Introdução

O direito à privacidade continua a ser um dos bens primordiais dos seres humanos. Desde a sua criação, o direito à privacidade progrediu e tornou-se um direito estabelecido na maioria das democracias modernas[2]. O direito à privacidade é garantido pelo artigo 12 da Declaração Universal dos Direitos Humanos de 1948, que afirma que ninguém sofrerá "intromissões arbitrárias" na sua "vida privada, na sua família, no seu domicílio ou na sua correspondência" nem ataques à sua "honra e reputação". O artigo 17 da Convenção Internacional de Direitos Civis e Políticos de 1966 estabelece que a "privacidade, família, domicílio ou correspondência" não será sujeita a intrusão "arbitrária ou ilegal". A base legal da privacidade como um direito na Europa evolui a partir do artigo 8.º, n.º 1, da Convenção Europeia dos Direitos do Homem (CEDH), que prevê o direito ao respeito pela vida privada e familiar e do artigo 8.º, n.º 2, que estabelece que não haverá interferência neste direito por parte de autoridade pública, exceto em conformidade com a lei.

O direito à privacidade na Europa foi ainda mais reforçado com a aplicação do Regulamento Geral de Proteção de Dados (RGPD) em maio de 2018. O RGPD é uma das leis de privacidade e segurança mais rigorosas do mundo. Apesar de ter sido promulgada pela União Europeia (UE), a lei impõe um dever a todas as organizações situadas em qualquer lugar do mundo, na medida em que "encaminham ou compilam" dados de pessoas na região da UE. O RGPD também impõe multas pesadas contra aqueles que violam os padrões de privacidade e segurança por ele estabelecidos[3].

Existe uma relação intrínseca entre privacidade e segurança nacional porque há restrições relativamente ao quanto as pessoas estão dispostas a negociar a sua privacidade na procura da segurança nacional[4].

O artigo 23 do RGPD estabelece que o Direito da União ou dos Estados-Membros a que estejam sujeitos os responsáveis pelo tratamento ou o seu contratante pode limitar por

---

1 Artigo traduzido por Carolina Peralta.
2 Eric Caprioli, Ygal Saadoun e Isabelle Cantero, 'The Right to Digital Privacy: A European Survey' (2006) 3 Rutgers Journal of Law & Urban Policy 211.
3 'What is GDPR, the EU's new data protection law?' *GDPR.EU* disponível em https://gdpr.eu/what-is-gdpr/ acedido em 12 de maio de 2020
4 Fred H Cate, 'Government Data Mining: The Need for a Legal Framework' (2008) 43 Harvard Civil Rights-Civil Liberties Law Review 435, 484.

medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12 a 22 por motivo de segurança nacional, defesa, segurança pública e prevenção, investigação, deteção ou repressão de crimes.

No Reino Unido, o *Data Protection Act* 2018 (DPA, 2018) foi promulgado para implementar o RGPD. Antes da promulgação do DPA 2018, o *Data Protection Act* 1998 regulava o processamento nacional de dados pessoais pelas agências de inteligência. O DPA 2018 criou uma nova estrutura, que fornece um mecanismo distinto para supervisionar o processamento de dados pessoais pelas agências de inteligência. Este mecanismo baseia-se nas normas internacionais estabelecidas na "Convenção para a Proteção de Indivíduos em relação ao Processamento Automático de Dados Pessoais" do Conselho da Europa revista (a "Convenção 108 modernizada"; o Protocolo alterado foi adotado pelo Conselho da Europa em 18 de maio de 2018).

É pertinente notar que a segurança nacional não está no âmbito do direito da União Europeia. Como resultado, nem o RGPD nem a Diretiva de Aplicação da Lei (LED) abrangem o processamento de dados pessoais para fins de segurança nacional. Consequentemente, os termos do RGPD e do LED não se destinam a ser aplicáveis ao processamento de dados pessoais pelas agências de inteligência.[5] A Diretiva LED LED diz respeito ao tratamento de dados pessoais para efeitos de "prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais" pelas autoridades competentes[6].

A Parte 4 do DPA 2018 (processamento de serviços de inteligência) fornece um mecanismo específico às agências de inteligência. Garante que o tratamento de dados pessoais pelas agências de inteligência está sujeito a padrões adequados e correspondentes que reconheçam o papel sério das agências de inteligência ao lidar com ameaças atuais e potenciais à segurança nacional.[7] Além disso, a seção 110 do DPA 2018 isenta as agências de inteligência de certas disposições da Lei onde é essencial proteger a segurança nacional.

2. Antecedentes

A privacidade diz respeito a todos os indivíduos relativamente aos seus assuntos pessoais e privados. É um direito humano fundamental que permanece sob ameaça contínua devido aos avanços tecnológicos modernos[8].

A privacidade não deve ser considerada um direito individual em oposição ao bem social maior. As questões de privacidade exigem equilíbrio em ambos os extremos da escala, pois a privacidade implica proteção contra uma série de vários perigos ou problemas. O

[5] Home Office, Government of United Kingdom, *Data Protection Act 2018, Factsheet – Intelligence Services Processing,* p. 1, *disponível em* < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf > acedido em 19 de junho de 2020.

[6] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho (27 de abril de 2016), p. 1.

[7] Home Office, Government of United Kingdom, *Data Protection Act 2018, Factsheet – Intelligence Services Processing,* p. 2, disponível em < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf > acedido em 19 de junho de 2020.

[8] Ilina Georgieva, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Article 17 ICCPR and Article 8 ECHR' (2015) 31 Utrecht Journal of International and European Law 104.

valor da privacidade varia de acordo com o problema ou perigo específico que está a ser protegido. Os assuntos de privacidade não são todos iguais e alguns são mais perigosos que outros; assim, não é possível atribuir à privacidade um valor abstrato.[9] O conflito entre vigilância e privacidade é uma consequência dos nossos grandes problemas em ajustarmo-nos aos avanços da tecnologia[10].

A importância do direito à privacidade foi destacada quando o ex-funcionário da Agência de Segurança Nacional (NSA) Edward Snowden revelou que, por ordem secreta de um tribunal, registos de milhões de cidadãos norte-americanos estavam a ser reunidos pela NSA indiscriminadamente, independentemente do fato de esses indivíduos terem estado envolvidos em qualquer ato ilegal ou não[11]. Estas revelações provocaram um grande protesto entre a população e fortes objeções contra a tal vigilância do Estado. O público sentiu que representava uma intromissão nas suas vidas pessoais por parte do Estado e tornou-se mais consciente e cauteloso em questões relacionadas com a sua privacidade.

Na nossa sociedade, a tecnologia de vigilância é predominante e isso muitas vezes resulta num forte debate entre os defensores e opositores da tecnologia de vigilância. Especificamente, a vigilância do governo tem sido cada vez mais submetida ao escrutínio do público, com defensores afirmando que aumenta a segurança, enquanto os opositores a denunciam por infringir a privacidade[12]. Do ponto de vista de uma sociedade, é importante preservar o equilíbrio necessário entre as preocupações de segurança e privacidade e os direitos civis intrínsecos dos cidadãos[13].

3. Vigilância exercida por Entidades Estatais

A vigilância não é apenas para os governos. Uma grande parte é feita por empresas privadas que compilam, utilizam e vendem dados pessoais de pessoas[14]. Vigilância, em termos simples, significa "vigiar". Refere-se a "monitorização, rastreio, observação, análise, regulação, controlo, compilação de dados e invasão de privacidade". A palavra vigilância tem origem na palavra francesa "veiller" e na palavra latina "vigilare"[15].

O professor David Lyon define vigilância como "a atenção focada, sistemática e rotineira a detalhes pessoais para fins de influência, gestão, proteção ou direção". De acordo com este autor, a vigilância é "focada", pois presta atenção aos indivíduos.

A palavra "sistemática" indica que o escrutínio de detalhes pessoais é intencional e depende de alguns "protocolos e técnicas". Ao usar a palavra "rotina", o professor Lyon quer dizer que isso acontece em todas as sociedades modernas como uma parte 'normal'

9 Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 763.
10 H. Akin Ünver, 'Politics of Digital Surveillance, National Security and Privacy' (Centre for Economics and Foreign Policy Studies, 2018) 7.
11 Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (United Kingdom 6 de junho de 2013).
12 Michelle Cayford & Wolter Pieters, '*The effectiveness of surveillance technology: What intelligence officials are saying'* (2018) The Information Society 34(2), 88 DOI: 10.1080/01972243.2017.1414721.
13 Stefan Schuster, Melle Berg , Xabier Larrucea, Ton Slewe and Peter Ide-Kostic, 'Mass Surveillance and technological policy options: Improving security of private communications' (2017) 50 Computer Standards & Interfaces 76, 77.
14 Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1938.
15 Kelly Gates, 'Surveillance' in Laurie Ouellette and Jonathan Gray (eds), *Keywords for Media Studies* (NYU Press 2017) 186.

do dia a dia que depende da estrutura administrativa e de certas tecnologias da informação[16]. A vigilância, segundo ele, também está invariavelmente ligada a um determinado "objetivo"[17].

A vigilância não é apenas para os estados comunistas e ditatoriais. Após os ataques de 11 de setembro, os atentados de Londres em 2005 e vários outros crimes hediondos, até mesmo estados democráticos, fizeram grandes investimentos em tecnologias de vigilância.[18] Atualmente, a vigilância inclui tecnologias, formas, operações e um código de procedimento criado para replicar e escrutinar imagens, sons, *scripts* e transações[19]. A vigilância eletrónica é um instrumento vantajoso nas mãos das agências de aplicação da lei. Pode aumentar a segurança dos cidadãos, auxiliar nas investigações criminais e fornecer provas sólidas num processo judicial[20].

3.1. Lei de Poderes de Investigação 2016

Em 29 de novembro de 2016, a Lei de Poderes de Investigação (Investigatory Powers Act 2016 -IPA) entrou em vigor. Para regular o uso e a supervisão dos poderes de investigação pelas autoridades policiais e pelas agências de segurança e inteligência, a lei estabelece uma nova estrutura[21]. A IPA revoga a primeira parte da Lei de Regulamentação de Poderes de Investigação de 2000 (RIPA), que tinha 25 seções, substituindo-a por 272 seções sobre regulamentação de interceção. O objetivo principal da IPA é renovar o sistema sob o qual as agências de aplicação da lei e de inteligência do Reino Unido podem ser autorizadas a realizar "interceção, interferência de equipamentos ou aquisição de dados de comunicações em larga escala".[22]

O Secretário de Estado responsável pela "segurança e terrorismo" [23] emite o "mandado de interferência de equipamentos em larga escala" com base num pedido feito pelo chefe do serviço de inteligência[24]. No entanto, o Secretário de Estado toma pessoalmente a decisão de emitir um mandado de interferência de equipamentos em larga escala[25].

Essas disposições específicas e detalhadas tentam preencher a lacuna e procuram evitar o uso indevido, fornecendo a necessidade de autorização do Secretário de Estado antes de permitir qualquer interferência de equipamento em larga escala. Isso indica que a emissão de tais mandados está bem regulamentada e não pode ser usada indiscriminadamente por funcionários abaixo do Secretário de Estado sem a sua autorização para fins diferentes do especificado. A seção 176 até à seção 183 da Lei de

16 David Lyon, *Surveillance Studies: An Overview* (1ª ed., Polity 2007) 14.
17 David Lyon, *Surveillance Studies: An Overview* (1ª ed, Polity 2007) 15.
18 Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1938.
19 Kelly Gates, 'Surveillance' in Laurie Ouellette and Jonathan Gray (eds), *Keywords for Media Studies* (NYU Press, 2017) 187.
20 Edward Balkovich, Don Prosnitz, Anne Boustead e Steven C Isley, 'The Electronic Surveillance Challenge' In *Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law* (2015) RAND Corporation 1.
21 Investigatory Powers Act, *disponível em* https://www.gchq.gov.uk/information/investigatory-powers-act acedido em 15 de junho de 2020.
22 Thomson Reuters Practical Law, *Investigatory Powers Act 2016: Overview* by Practical Law Business Crime and Investigations, p. 1.
23 Secretary of State for the Home Department, Responsibilities https://www.gov.uk/government/ministers/secretary-of-state-for-the-home-department acedido em 3 de março de 2020.
24 Investigatory Powers Act 2016, s 178.
25 Investigatory Powers Act 2016, s 182.

Poderes de Investigação de 2016 trata de "mandados de interferência de equipamentos em larga escala". A "garantia de interferência de equipamentos em larga escala" autoriza a pessoa a quem se dirige a obter interferências em qualquer tipo de equipamento com o objetivo de obter "comunicações, dados de equipamentos e quaisquer outras informações"[26].

A partir de 27 de junho de 2018, ao abrigo da IPA, as operações de interceção de comunicações passaram a ser legitimadas. Somente o Secretário de Estado pode emitir mandados autorizando a interceção, e devem ser ratificados por um Comissário Judicial independente do Gabinete do Comissário de Poderes de Investigação. Antes da emissão de um mandado de interceção, o Secretário de Estado deve "acreditar" que um mandado é "necessário" por alguma razão e que a interceção corresponde ao objetivo que pretende alcançar. A interceção é considerada "necessária" por motivos de "segurança nacional", "bem-estar económico do Reino Unido" ou "prevenção ou deteção de crimes graves". Para restringir o uso de informações intercetadas e dados de comunicação associados, a IPA requer disposições de salvaguardas[27].

A IPA 2016 provocou uma mudança notável na forma como alguns poderes de investigação são aprovados e supervisionados. A introdução do que é informalmente chamado método de "bloqueio duplo" é a mudança mais notável trazida pela IPA 2016. O mecanismo "bloqueio duplo" implica que, após autorização do Secretário de Estado, um mandado IPA não pode ser emitido a menos que um Comissário de Justiça o autorize[28]. O uso do mecanismo de "bloqueio duplo" deu início a um novo recurso fundamental para a supervisão judicial das agências de inteligência e segurança do Reino Unido, dando a tarefa de analisar independentemente as aprovações solicitadas sob a IPA 2016 aos Comissários de Justiça[29].

Saudando a aprovação da IPA 2016, a secretária dos Assuntos Internos Amber Rudd declarou: "Este governo tem a certeza que, num momento de maior ameaça à segurança, é essencial que nossos serviços de aplicação da lei, segurança e inteligência tenham os poderes necessários para manter as pessoas seguras". Ela observou ainda: "A internet apresenta novas oportunidades para os terroristas e devemos garantir que temos a capacidade de enfrentar esse desafio. Mas também é certo que esses poderes estão sujeitos a salvaguardas estritas e supervisão rigorosa." Apontando para a transparência e proteção da privacidade estabelecidas na Lei, afirmou que "A Lei dos Poderes de Investigação é uma legislação líder mundial que fornece transparência sem precedentes e proteção substancial à privacidade"[30].

---

[26] Investigatory Powers Act 2016, s 176.

[27] Investigatory Powers Act, *disponível em* https://www.gchq.gov.uk/information/investigatory-powers-act acedido em 15 de junho de 2020.

[28] Government of UK, 'Annual Report of the Investigatory Powers Commissioner' (2018) p. 10, *disponível em:* https://ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf acedido em 16 de junho de 2020.

[29] Government of UK, 'Annual Report of the Investigatory Powers Commissioner' (2018) p. 9 [2.3], *disponível em:* https://ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf acedido em 26 de junho de 2020.

[30] Home Office (Government of UK), 'Investigatory Powers Bill receives Royal Assent' (28 de novembro de 2018) *disponível em:* https://www.gov.uk/government/news/investigatory-powers-bill-receives-royal-assent acedido em 15 de junho de 2020.

3.2. Operações das Agências Estatais

A interceção é um método em que uma pessoa que não seja o remetente ou destinatário dessa comunicação supervisiona a comunicação durante o curso da sua transmissão com o objetivo de tornar o seu conteúdo acessível[31]. O uso de tecnologias de mineração de dados na segurança nacional é um esforço para automatizar algum trabalho sistemático para permitir um exame mais preciso e oportuno dos conjuntos de dados predominantes. O objetivo é evitar atividades terroristas, reconhecendo e categorizando vários "*threads* e partes de informação", que podem já existir, mas são negligenciados devido ao uso de métodos de investigação tradicionais[32].

A era digital desencadeou uma transformação radical na vigilância conduzida pelo Estado, tanto em termos de como é realizada como nos tipos de *insights* que se pretende promover. A transformação da vigilância exercida pelo estado é representada pelo uso de "técnicas de dados de comunicação em larga escala" que compreendem a vasta compilação, armazenamento e análise sucessiva de dados de comunicação. Atualmente, essas técnicas constituem um aspeto integral da vigilância exercida pelo estado[33]. Ao contrário da recolha de dados direcionada, a vigilância de dados de comunicações em larga escala denota extensa "recolha" e "retenção" de dados de comunicações. Atualmente, é utilizada por agências de inteligência e de aplicação da lei[34].

A mineração de dados é o método que consiste em explorar novas informações nos dados já existentes[35]. A mineração de dados geralmente determina "padrões ou relacionamentos" nos itens de dados ou registos, que antes não eram reconhecidos, mas são divulgados apenas nos dados[36]. A mineração de dados oferece oportunidades favoráveis para superar a lacuna nos requisitos de informação do governo e os enormes conjuntos de dados de informações que lhe são disponibilizados. Os dados disponíveis podem ser convertidos em conhecimento através da mineração de dados[37]. O procedimento de mineração de dados exige essencialmente a revisão e avaliação automática de perfis contendo informações pessoais de várias pessoas[38].

---

31 Intelligence and Security Committee of Parliament: Privacy and Security: A modern and transparent legal framework (2015) 17 https://info.publicintelligence.net/UK-ISC-MassSurveillance.pdf acedido em 12 de junho de 2020.

32 KA Taipale, 'Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data', (2003-2004) 5 Columbia Science and Technology Law Review 1, 21.

33 Murray D e Fussey P, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31.

34 Daragh Murray e Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 36.

35 KA Taipale, 'Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data', (2003-2004) 5 Columbia Science and Technology Law Review 1, 22.

36 KA Taipale, 'Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data', (2003-2004) 5 Columbia Science and Technology Law Review 1, 22-23.

37 Tal Z Zarsky, 'Governmental Data Mining and its Alternatives' (2011) 116 Pennsylvania State Law Review 285, 294.

38 Tal Z Zarsky, 'Governmental Data Mining and its Alternatives' (2011) 116 Pennsylvania State Law Review 285, 295.

Programas como 'Mineração de Dados' constituem uma séria ameaça à vigilância. A mineração de dados apresenta instrumentos para analisar automaticamente os dados[39]. Enormes quantidades de dados são retidas pelos órgãos governamentais, que os examinam com a intenção de obter conhecimento para criação e armazenamento de informações importantes[40]. O interessante da mineração de dados é que visa prever as nossas ações futuras e as pessoas que correspondem a alguns perfis específicos são considerados envolvidos em "padrão semelhante de comportamento". Nessas circunstâncias, as ações que ainda não foram cometidas seriam difíceis de refutar e será mais oneroso para nós descartar as previsões de atividades futuras obtidas através da mineração de dados[41].

Muitos defensores da privacidade alertam que a recolha e retenção de 'metadados' ilimitados de atividades de comunicação de pessoas pelo governo é a forma mais intrusiva de vigilância[42]. Basicamente, metadados são dados sobre dados. Normalmente, as informações são compostas por *tags* semânticas aplicáveis aos dados. Os metadados contêm dados marcados semanticamente, que são utilizados para explicar os dados.[43] Os metadados também são conhecidos como 'dados de comunicação' e o Supremo Tribunal do Reino Unido em Davis e outros v Secretário de Estado do Departamento do Interior definiu 'dados de comunicação' da seguinte forma:

> *A frase "dados de comunicação" não inclui o conteúdo de uma comunicação. Esses dados podem ser usados para demonstrar quem estava a comunicar; quando; de onde; e com quem. Os dados podem incluir a hora e a duração de uma comunicação, o número ou endereço de e-mail do remetente e do destinatário e, às vezes, a localização do dispositivo a partir do qual a comunicação foi feita. Os dados não incluem o conteúdo de qualquer comunicação: por exemplo, o texto de um e-mail ou uma conversa telefónica*[44].

O tribunal afirmou ainda que, no curso das investigações sobre segurança nacional e crime organizado e grave, as organizações de inteligência e aplicação da lei usam dados de comunicação. Os dados ajudam as agências de investigação a identificar os associados de um nexo criminoso, colocando-os em locais específicos em horários predeterminados e, em alguns casos, a compreender a atividade criminosa em que estão envolvidos[45]. Quando "combinados" e "agregados" para produzir um registo detalhado da comunicação

[39] Stijn Vanderlooy, Joop Verbeek e Jaap van den Herik, 'Towards Privacy-Preserving Data Mining in Law Enforcement' (2007) 2(4) JICLT 202.
[40] Stijn Vanderlooy, Joop Verbeek e Jaap van den Herik, 'Towards Privacy-Preserving Data Mining in Law Enforcement' (2007) 2(4) JICLT 202.
[41] Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 764.
[42] Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' (*The Guardian,* 6 de junho de 2013) https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order acedido em 4 de março de 2018.
[43] Tony Hey and Anne Trefethen, 'The Data Deluge: An e-Science Perspective', disponível em https://eprints.soton.ac.uk/257648/1/The_Data_Deluge.pdf acedido em 25 de abril de 2020.
[44] Davis and Others v Secretary of State for the Home Department [2015] EWHC 2092 [13].
[45] Davis and Others v Secretary of State for the Home Department [2015] EWHC 2092 [14].

e atividade baseada na internet de um indivíduo, os dados de comunicação são considerados especificamente vantajosos para as agências de inteligência e segurança[46].

4. Avaliação do argumento Privacidade vs Segurança

Diz-se que a vigilância cria um efeito arrepiante quando as pessoas desistem de participar em atividades ao aperceber-se que isso terá algumas consequências se o fizerem[47]. A vigilância impede um indivíduo de desfrutar da sua liberdade, e liberdade de expressão. As pessoas não se podem movimentar ou falar livremente quando sabem que o estado os segue a cada passo e vê todos os seus atos. Isso conduz a uma sociedade que é bastante semelhante à descrita por George Orwell no famoso romance 'Mil novecentos e oitenta e quatro'. Na sociedade descrita por Orwell, todos viviam com o medo constante de serem vigiados pelo Estado e tinham que agir ou pensar da maneira que o Estado esperava e não da maneira que eles gostariam de pensar. Essa sociedade orwelliana restringe os movimentos, pensamentos, condutas dos cidadãos no seu cotidiano e torna-os robôs que deveriam seguir as instruções do Estado, o que pode ser muito prejudicial para a própria existência de uma sociedade livre.

Em 2013, Edward Snowden expôs a operação da Sede de Comunicação do Governo (GCHQ), designada 'Tempora', que ele denominou como "o maior programa de vigilância menos suspeita na história da humanidade"[48].

Sob a operação 'Tempora', grandes volumes de dados retirados de cabos de fibra ótica puderam ser armazenados durante 30 dias para análise pelo GCHQ. Os dados incluíam registos telefónicos, conteúdo de mensagens de e-mail, entradas no Facebook, histórico da internet e muitos outros detalhes, não apenas dos alvos suspeitos, mas também de pessoas inocentes[49]. Finalmente, a 6 de fevereiro de 2015, o Investigatory Powers Tribunal considerou que os regulamentos que permitiam o GCHQ aceder a e-mails e registos telefónicos intercetados pela NSA violavam o artigo 8 e o artigo 10 da Convenção Europeia dos Direitos do Homem (CEDH)[50].

As autoridades judiciárias intervieram e protegeram os direitos dos cidadãos ameaçados pelo Estado em questões relativas à sua privacidade. O Estado pode tentar justificar essa vigilância em larga escala e indiscriminada em nome da segurança e proteção dos cidadãos, mas não se deve esquecer que deve ser traçada uma linha para impedir que o Estado interfira nas atividades pessoais de cidadãos inocentes em nome da segurança e proteção. Programas como o 'Tempora' dão poderes às agências estatais para recolher

---

46 Daragh Murray e Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 34.

47 Daragh Murray e Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 43.

48 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies e James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian*, 21 de junho de 2013) https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa acedido em 13 de maio de 2020.

49 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies e James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian*, 21 de junho de 2013) https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa acedido em 13 de maio de 2020.

50 Owen Bowcott, 'UK-US surveillance regime was unlawful 'for seven years' *The Guardian* (6 de fevereiro de 2015) https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa acedido em 13 de junho de 2020.

dados em larga escala e fornecem acesso a detalhes pessoais. como mensagens de e-mail.

Nunca devemos esquecer que as agências governamentais não são compostas por um indivíduo, mas por muitos. Pode haver muitos funcionários que trabalham com integridade e seguem as diretrizes ou salvaguardas previstas nos estatutos quando usam dados pessoais para fins de vigilância. No entanto, permanece a probabilidade de que alguns funcionários com acesso a um volume tão alto de dados destinados a fins de segurança possam acabar com as salvaguardas fornecidas durante o período de "emergência ou crise" e fazer uso indevido desses dados[51]. O uso indevido de dados protegidos não constitui apenas uma invasão, mas também um ato ilegal. A parte mais lamentável da mineração de dados é que o indivíduo ou as pessoas que estão sob vigilância nem sequer sabem que estão sob vigilância e que seus atos, incluindo pesquisas no Google, dados bancários e outros detalhes, são observados pelo Estado. Se tais atos acontecerem em democracias vibrantes como o Reino Unido, então seria difícil imaginar as piores formas de vigilância que podem ser realizadas pelos regimes ditatoriais, onde tal intercetação em larga escala pode ser mal utilizada para amordaçar as vozes que se opõem ao governo.

O artigo 8º da CEDH é fundamental porque define o direito da pessoa de ter a sua privacidade respeitada por qualquer organização, ao mesmo tempo que indica as condições em que é permitido ao Estado, e às vezes autorizado, a "exercer certas prerrogativas". "A segurança nacional, a segurança pública [e] a prevenção da desordem ou do crime" estão entre as razões pelas quais um Estado pode intervir no direito à privacidade. Assim, pode-se sugerir que para aqueles que redigiram a CEDH, a segurança sobrepõe-se à privacidade[52].

As agências de inteligência e segurança estão comprometidas com uma missão. Garantir a segurança dos cidadãos é a principal razão do seu papel e afirmação sobre os recursos significativos e governamentais do país[53]. Isso sugere que as agências de inteligência precisam de ter acesso a informações privadas de um indivíduo para proteger a sociedade e não devem preocupar-se se estão a cometer um ato ilegal.

Há outro argumento que favorece a vigilância e sustenta que não pode haver invasão de privacidade através da mera recolha e organização automática de dados. Como os dados recolhidos são em larga escala, esses dados passam inicialmente pelos computadores que buscam números de telefone, nomes e outros detalhes de pessoas que constituem matéria para os serviços de inteligência governamentais. A "peneiração" automática de dados pelo computador impede a leitura de dados privados por um funcionário dos serviços e, portanto, não invade a privacidade[54]. Esse argumento fala a favor da vigilância e garante que certos protocolos sejam seguidos para fins de vigilância se forma a não invadir a privacidade.

---

51 Adam D. Moore, 'Privacy, Security and Government Surveillance: Wikileaks and the new Accountability' (2011) 25(2) Public Affairs Quarterly 141, 145.

52 Eric Caprioli, Ygal Saadoun e Isabelle Cantero, 'The Right to Digital Privacy: A European Survey' (2006) 3 Rutgers Journal of Law & Urban Policy 211, 213.

53 Charles D. Raab, 'Security, Privacy and Oversight' in Andrew W. Neal (ed) *Security in a Small Nation: Scotland, Democracy, Politics* (Open Book Publishers, 2017) 81.

54 Richard A. Posner, 'Our Domestic Intelligence Crisis' *Washington Post* (21 de dezembro de 2005) disponível em https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/ acedido em 14 de maio de 2020.

A capacidade de interceção em larga escala do GCHQ também tem causado muitas preocupações, e foi alegado que observa todas as comunicações na Internet. Mas, de acordo com a Comissão de Inteligência e Segurança do Parlamento, não é verdade porque a capacidade de interceção em larga escala do GCHQ é usada apenas para observar as pessoas que constituem ameaça ou com o objetivo de criar novas pistas de inteligência, como investigar qualquer ataque cibernético ou plano terrorista[55]. Outra questão que o relatório abordou foi uma acusação feita contra o GCHQ de que faz interceção "indiscriminadamente". Refutando essa alegação, a Comissão respondeu: o GCHQ primeiro escolhe os utilizadores aos quais quer ter acesso (uma pequena proporção daqueles aos quais podem ter acesso teoricamente) e depois usa seletores específicos, relacionados com alvos individuais, a fim de recolher dados sobre esses utilizadores[56]. Esclareceu que visava os indivíduos e não fazia vigilância em grande escala que possa ter incluído várias pessoas inocentes e, portanto, mantinha limites ao não invadir sua privacidade.

As vantagens da "interceção em larga escala" encontram-se no relatório apresentado pela Comissão de Inteligência e Segurança do Parlamento em 2015, que afirmou: "Ficamos surpresos ao descobrir que o principal valor para o GCHQ da interceção em larga escala não estava na leitura do conteúdo real da comunicação, mas nas informações associadas a essas comunicações"[57]. A vigilância de dados de comunicação permite, literalmente, ficar de olho em cada ação de todas as pessoas, descobrir e avaliar os seus relacionamentos com outros indivíduos e obter ter uma informação abrangente sobre a vida dessas pessoas[58].

Estas observações da comissão parlamentar tentam incutir uma sensação de segurança nas mentes dos cidadãos de que não estão sujeitos a interceções absolutas de larga escala e não controladas por agências de inteligência e que essas interceções são motivadas por suspeitos que representam uma ameaça para o Reino Unido.

É importante referir que a questão necessariamente não precisa ser sobre 'privacidade' ou 'segurança', pois um plano bem-sucedido, implementação consistente e supervisão meticulosa de extensas medidas de salvaguarda pelos legisladores podem aproveitar a vantagem da tecnologia para alcançar tanto a privacidade como a segurança[59].

Conclusão

Não seria correto dizer que tanto a privacidade como a vigilância estão uma contra a outra, ou que uma supera a outra. Nenhum estado pode negar a necessidade absoluta de uma ou outra. A menos que o estado tenha provas suficientes que alguém está

[55] Intelligence and Security Committee of Parliament: Privacy and Security: A modern and transparent legal framework (2015) 28, para F https://info.publicintelligence.net/UK-ISC-MassSurveillance.pdf acedido em 15 de maio de 2020.
[56] Intelligence and Security Committee of Parliament: Privacy and Security: A modern and transparent legal framework (2015) 28, para G https://info.publicintelligence.net/UK-ISC-MassSurveillance.pdf acedido em 15 de maio de 2020.
[57] Intelligence and Security Committee of Parliament, 'Privacy and Security: A modern and transparent legal framework' (2015) p. 32 [80].
[58] Murray D e Fussey P, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data" (2019) 52 Israel Law Review 31, 52.
[59] John P. Heekin, 'Leashing the Internet Watchdog: Legislative Restraints on Electronic Surveillance in the U.S. and U.K.' (2010) 28(1) American Intelligence Journal 40.

envolvido num crime, as agências de aplicação da lei devem abster-se de intercetar as comunicações desses indivíduos. A frase "os que não têm nada a esconder não têm nada a temer" não dá direito absoluto às agências de inteligência de intercetar todas as comunicações dos cidadãos indiscriminadamente, mas apenas com verificações e contrapesos.

Ao mesmo tempo, não devemos esquecer que a conspiração terrorista nos dias de hoje não se limita a locais físicos, tendo-se igualmente expandido às plataformas digitais, exigindo vigilância. Assim, o governo, antes de elaborar leis de vigilância mais eficientes e não intrusivas, deve fazer as devidas deliberações e consultas não apenas com as agências de aplicação da lei, mas também com organizações externas ao governo.

Referências

Balkovich, Edward; Prosnitz, Don; Boustead, Anne and Isley, Steven C. (2015). 'The Electronic Surveillance Challenge' In *Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law*. RAND Corporation 1.

Balkovich, Edward; Prosnitz, Don; Boustead, Anne; Isle, Steven C. (2015). Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law. RAND Corporation 1, https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR800/RAND_RR800.pdf

Berger, J.M. and Morgan, Jonathon (2015). 'The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter'. The Brookings Project on U.S. Relations with Islamic World (Analysis Paper) 2.

Bowcott, Owen (2015). 'UK-US surveillance regime was unlawful 'for seven years' In *The Guardian* (6 Fev 2015).

Caprioli, Eric; Saadoun, Ygal and Cantero, Isabelle (2006). 'The Right to Digital Privacy: A European Survey'. In *Rutgers Journal of Law & Urban Policy*, Vol 3:2: 211-218.

Cate, Fred H. (2008). 'Government Data Mining: The Need for a Legal Framework' (junho de 2008). In Harvard Civil Rights-Civil Liberties Law Review (CR-CL), Vol. 43, Nº. 2, 2008, Disponível em SSRN: https://ssrn.com/abstract=1151435

Cayford, Michelle & Pieters, Wolter (2018). '*The effectiveness of surveillance technology: What intelligence officials are saying'.* In The Information Society 34(2), 88 https://doi.org/10.1080/01972243.2017.1414721.

Davis and Others v Secretary of State for the Home Department (2015). EWHC 2092. https://vlex.co.uk/vid/david-davis-mp-and-793030889.

Dearden, Lizzie (2017). 'Khalid Masood: Suspected Isis supporter used WhatsApp two minutes before London attack'. In *The Independent* (24 de março de 2017).

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho (27 de abril de 2016), p. 1., http://data.europa.eu/eli/dir/2016/680/oj.

Feldstein, Steven (2019). *The Global Expansion of AI Surveillance*. Washington DC: Carnegie Endowment for International Peace. Working paper 11.

Gates, Kelly (2017). 'Surveillance'. In Laurie Ouellette and Jonathan Gray (eds), *Keywords for Media Studies*. NYU Press: 186.

Greenwald, Glenn (2013). 'NSA collecting phone records of millions of Verizon customers daily'. In *The Guardian* (6 de junho de 2013).

Hey, Tony e Trefethen, Anne (2020). 'The Data Deluge: An e-Science Perspective', disponível em https://eprints.soton.ac.uk/257648/1/The_Data_Deluge.pdf, acedido em 25 de abril de 2020.

Home Office, Department for Digital, Culture Media & Sport. (2018). *Data Protection Act 2018, Factsheet – Intelligence Services Processing.* Government of United Kingdom. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf.

Ilina Georgieva, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31(80) Utrecht Journal of International and European Law 104, DOI: http://dx.doi.org/10.5334/ujiel.cr

Intelligence and Security Committee of Parliament. (2015). *Privacy and Security: A modern and transparent legal framework.* Government of United Kingdom. https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

Investigatory Powers Commissioner's Office. (2018). *Annual Report of the Investigatory Powers Commissioner's Office*. Government of the United Kingdom. https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2018-final.pdf.

Moore, Adam D. (2011). 'Privacy, Security and Government Surveillance: Wikileaks and the new Accountability'. Public Affairs Quarterly, Vol 25, N2: 141-156.

Posner, Richard A. (2005). 'Our Domestic Intelligence Crisis'. In *The Washington Post* (21 de dezembro de 2005).

Raab, Charles D. (2017). 'Security, Privacy and Oversight' in Andrew W. Neal (ed) *Security in a Small Nation: Scotland, Democracy, Politics* (Open Book Publishers 2017), https://www.openbookpublishers.com/resources/9781783742684/Security-Small-Nation-ch3.pdf.

Investigatory Powers Act

GDPR.EU (2022). 'What is GDPR, the EU's new data protection law?', https://gdpr.eu/what-is-gdpr/

Heekin, J. P. (2010). Leashing the Internet Watchdog: Legislative Restraints on Electronic Surveillance in the U.S. and U.K. *American Intelligence Journal*, *28*(1), 40–58. http://www.jstor.org/stable/44327129.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity. University of Michigan: Wiley, 1st ed.

MacAskill, Ewen; Borger, Julian; Hopkins, Nick; Davies, Nick and Ball, James (2013). 'GCHQ taps fibre-optic cables for secret access to world's communications'. In *The Guardian* (21 de junho de 2013).

Murray, D., & Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review, 52*(1): 31-60. https://doi.org/10.1017/S0021223718000304.

Palmer, Danny (2019). 'What is GDPR? Everything you need to know about the new general data protection regulations' (*ZDNet*, 17 de maio de 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

R (Liberty) v. Secretary of State for the Home Department and another (National Union of Journalists intervening), EWHC 2057 (Admin). (2019).

Richards, Neil M. (2013). 'The Dangers of Surveillance'. In Harvard Law Review, Vol 126, N7: 1934.

Schuster, Stefan; Berg, Melle; Larrucea, Xabier; Slewe, Ton e Ide-Kostic, Peter (2017). 'Mass Surveillance and technological policy options: Improving security of private communications'. Computer, Standards & Interfaces, Vol. 50: 76-82, https://www.sciencedirect.com/science/article/pii/S0920548916300988.

Solove, Daniel J. (2007). 'I've Got Nothing to Hide" and Other Misunderstandings of Privacy'. In San Diego Law Review, 44: 745.

Szeghalmi, Veronika (2015). 'The Definition of the Right to Privacy in the United States of America and Europe'. In Hungarian Yearbook of International Law and European Law, 397.

Taipale KA (2003) Data mining and domestic security: connecting the dots to make sense of data. Columbia Sci Technol Law Rev 5(2): 83.

Thomson Reuters Practical Law, *Investigatory Powers Act 2016: Overview* by Practical Law Business Crime and Investigations: 1.

Ünver, H. Akin (2018). 'Politics of Digital Surveillance, National Security and Privacy'. Centre for Economics and Foreign Policy Studies, 2018/2: 17.

Vanderlooy, S., Verbeek, J. P. G. M., & van den Herik, H. J. (2007). Towards privacy-preserving data mining in law enforcement. *Journal of International Commercial Law and Technology*, *2*(4): 202-210.

Zarsky, Tal Z. (2011). 'Governmental Data Mining and its Alternatives', Pennsylvania State Law Review, Vol116: 2: 285-330.