A luta pelas garantias processuais e a mudança de paradigma em matéria de prova: do liberalismo à *mass surveillance* no processo penal europeu

The fight for fair trial rights and the paradigm shift in evidence: from liberalism to mass surveillance in criminal proceedings in Europe

Lorena Bachmaier Winter[1]

Universidad Complutense Madrid, Madri, Espanha

l.bachmaier@der.ucm.es

https://orcid.org/0000-0002-9212-3336

Resumo: As informações de fontes abertas disponíveis de cada um de nós permitem, por meio do processamento adequado, criar um perfil detalhado de praticamente todos os aspectos de nossa vida privada. De acordo com o algoritmo utilizado, isso pode levar a identificar um indivíduo como uma "pessoa de interesse" e, no logo em seguida, esses mesmos dados podem ser usados para caracterizar a justa causa e iniciar um processo criminal. Se o caso for a julgamento, esses dados podem ser apresentados como prova. Este artigo discute como o acesso a plataformas de mensagens criptografadas (como no caso Encrochat) e o processamento massivo de dados por meio de algoritmos e inteligência artificial exigem repensar toda a estrutura do processo penal. Defende-se que é necessário revisar as garantias processuais desenvolvidas nos últimos dois séculos para poder enfrentar os riscos

[1] Professora Catedrática de Direito Processual da Universidade Complutense de Madrid, Madri, Espanha. Doutora em Direito.

Este trabalho insere-se no projeto de investigação de I+D+i «*Prueba penal y nuevos retos en el proceso penal transnacional*» (ref. PID2023-148413NB-100), financiado pelo Ministerio de Ciencia, Innovación y Universidades.

Tradução do espanhol ao português por Fernanda Vilares e Luiz Eduardo Cani.

da era digital. Conclui-se que há uma nova mudança na obtenção de provas, o que exige o fortalecimento das garantias do devido processo na fase de investigação.

Palavras-Chave: processo penal; prova; devido processo; algoritmos; investigação transnacional; prova eletrônica; interceptação de comunicações; buscas digitais; vigilância em massa; justa causa; Tribunal de Justiça da União Europeia.

Abstract: *Only with the open source information available of each any person it is possible through the adequate processing to create a detailed profile of practically all aspects of our private life. According to the algorithm used, this can lead to identify an individual as a "person of interest", and this it is only one step away from that same data being used to establish probable cause to open a criminal case, and if the case ends up in a trial, to present such data as evidence. This article discusses how the access to encrypted messaging platforms (as in the Encrochat case) and the massive processing of data through algorithms and artificial intelligence requires to rethink the whole structure of the criminal procedure. It advocates that there is a need to revisit the procedural safeguards developed during the past two centuries to be able to face the risks of the digital era. It concludes that there is a new shift in the gathering of evidence, which calls for strengthening the fair trial rights at the pre-trial stage.*

Keywords: *criminal procedure; evidence; fair trial rights; algorithms; transnational investigation; electronic evidence; interception of communications; digital searches; mass surveillance; probable cause; European Court of Justice.*

Introdução

As democracias liberais do denominado mundo ocidental estão submetidas a crescentes tensões que se traduzem, entre outras coisas, em perda de confiança na representação parlamentar, maior polarização política, aparecimento de crescentes focos de corrupção, manipulação massiva da informação, aumento de movimentos políticos radicais e ataques ou tentativas de neutralização do Poder Judiciário. Se este diagnóstico parece indubitável, entretanto, é mais complexo determinar quais são as causas desses fatores de risco para nossas democracias.

Um elemento que claramente atua como motor de mudança da sociedade atual e opera de forma transversal em todas as áreas de nossa vida, também na esfera política, é a digitalização de todos os âmbitos de nossas vidas. Naturalmente, estudar de maneira integral em que medida a transformação digital contribuiu para criar ou agravar os problemas das democracias ocidentais excede o objetivo e os limites deste trabalho. Aqui nos interessa indagar em que medida essas mudanças – e especificamente a digitalização – são «digeridos» de forma adequada: não tanto por cada um dos indivíduos, senão pelos sistemas jurídicos e, em particular, a partir da perspectiva da resposta dos sistemas de justiça frente ao delito.

Nesse contexto, se observa um progressivo distanciamento dos princípios que até agora se havia considerado fundamentais tanto do direito como do processo penal; princípios que provêm do Iluminismo e estavam fortemente consolidados na segunda metade do século XX no movimento de reconhecimento internacional e constitucional dos direitos humanos, os quais frequentemente identificamos com o liberalismo jurídico. É certo que o próprio conceito de liberalismo foi entendido de muitas maneiras[2]; porém, sem pretensões de fazer uma

[2] Vid. ALCALÁ ZAMORA, Niceto. Liberalismo y autoritarismo en el proceso. *Boletin Mexicano de Derecho Comparado*, v. 1, n. 2-3, pp. 559-600, 1968, no qual destaca que um sistema processual se caracteriza como liberal ou autoritário levando «em consideração as características intrínsecas e os princípios em que seu funcionamento se inspira », p. 572. Apesar de sua análise centrar-se no processo civil, muitas de suas afirmações são aplicáveis igualmente ao processo penal, em particular quando sublinha a

análise completa, bastará explicar que aqui o utilizo como o oposto do autoritarismo: um modelo jurídico em que a dignidade humana e os direitos fundamentais constituem o eixo sobre o qual gira todo o sistema normativo. Se nos referíssemos especificamente ao processo penal «liberal», estaríamos falando do «processo justo ou devido», cuja função e características essenciais poderiam ser sintetizados nos seguintes elementos: respeito à presunção de inocência do imputado; compreensão da função do direito processual penal consistente em proteger os direitos fundamentais daqueles que se veem submetidos ao poder público a fim de permitir-lhes defender-se da melhor maneira possível; e tudo isso com a convicção de que quando se comete o fato criminoso o sujeito débito é a vítima, porém no momento do processo o sujeito débil é o imputado[3].

Nas seguintes páginas serão analisados alguns dos problemas ou tensões aos quais se vê submetido o processo penal atual e que obrigam a repensar seu futuro em nosso mundo «digitalizado» para que possa seguir constituindo um marco de garantias do indivíduo frente ao poder cada vez mais abrangente do Estado. Isso se torna ainda mais urgente porque somos testemunhas de como democracias que críamos imunes aos excessos se veem assaltadas por governos com tendências autocráticas que se prolongam naturalmente em respostas de idêntica tendência frente a determinados fenômenos delitivos. Neste cenário, meu objetivo é advertir como as tecnologias da informação e da comunicação, junto com a capacidade de *mass surveillance* por parte dos Estados, já está gerando uma mudança tanto na estrutura como nas funções do processo penal, fundamentalmente no âmbito do direito probatório, com um claro impacto – não necessariamente positivo – no direito de

observação do devido processo como critério que caracteriza como liberal a fase judicial. Vid. p. 592 e ss.

[3] Diante da reconhecível tendência populista – e de clara tendência autocrática –, efetivista e «eficientista» da justiça penal, não é de estranhar que algumas vozes se levantem a favor da defesa dos chamados princípios jurídico-liberais. Um exemplo é o denominado «Manifesto del diritto penale liberale e del giusto processo», publicado em 2019, elaborado pela *Unione delle Camere Penali Italiane*. Disponível em: https://www.camerepenali.it/public/file/Riservato/Luglio_2019_Manifesto%20del%20diritto%20penale%20liberale%20e%20del%20giusto%20processo.pdf.

defesa. Junto a isso não se pode perder de vista as grandes corporações de prestação de serviços de internet, não só pela capacidade de intrusão que têm em nosso direito à privacidade, senão também porque se estão erigindo como "*partners*" necessários na investigação penal através da gestão de nossos dados[4].

1. O processo penal liberal frente ao paradigma digital e a prevenção do delito

Coletar informação e processá-la para fins de segurança (o que entendemos normalmente por inteligência) não só é uma tarefa necessária e útil, senão também indispensável para atuar eficazmente contra os fenômenos da delinquência em geral, e em particular contra a delinquência organizada, o terrorismo e, ligado a esses, a lavagem de dinheiro[5]. Sem embargo, tendo em vista as dimensões que adquiriu a coleta de informação e as possibilidades tecnológicas da *mass surveillance*, é natural que nos perguntemos se não se está introduzindo de forma sub-reptícia um sistema alternativo ou adicional de prevenção – e inclusive de punição – do delito, permeando as estruturas processuais sem um marco jurídico adequado e transparente. A solução simplista de advogar pela proibição dos sistemas de *mass surveillance* e de análise de *big data*, sendo realistas, não é viável e quiçá tampouco sensata: não se podem ignorar as possibilidades que oferecem os sistemas de vigilância em massa das

---

[4] Vid. RATNER, Steven R. Corporations and Human Rights: A Theory of Legal Responsibility. *Yale Law Journal*, v. 111, n. 3, pp. 443-545, 2001, p. 496 e ss; BILCHITZ, David. The Right to Privacy, Surveillance and the Global Obligations of Corporations. *In*: COLE, David D.; FABBRINI, Federico; SCHULHOFER, Stephen. (Eds.) *Surveillance, Privacy and Trans-Atlantic Relations*: Hart Studies in Security and Justice. Dublin: Bloomsbury Publishing, 2017, p. 113-138.

[5] Sobre a necessidade da informação de inteligência no âmbito da prevenção penal e da segurança nacional, vid., entre outros: DERENCINOVIC, Devor, GETOS, Anna-Maria. Cooperation of law enforcement and intelligence agencies in prevention and suppression of terrorism. European perspective. *Revue internationale de droit pénal*, v. 78, pp. 79-112, 2007, p. 86; BACHMAIER WINTER, Lorena. Información de inteligencia y proceso penal. *In*: BACHMAIER WINTER, Lorena. (Coord.). *Terrorismo, proceso penal y derechos fundamentales*. Madri: Marcial Pons, 2012.

comunicações, nem tampouco a necessidade que tem a sociedade de se proteger frente a ameaças graves à sua segurança e à convivência pacífica. Porém, como expressou o Parlamento Europeu, «a vigilância em massa é incompatível com as pedras angulares da democracia»[6] se dita vigilância em massa não se limita a casos excepcionais e não se realiza em conformidade com a lei[7]. Portanto, a necessidade de prevenir e perseguir fenômenos de delinquência grave e o uso de ferramentas de *mass surveillance* devem ser feitos garantindo a plena tutela dos direitos fundamentais[8]. Naturalmente, o problema gira novamente em torno dos limites, dos controles e sobretudo da proporcionalidade dessas medidas.

O debate acerca do papel do direito penal na prevenção do delito, desde a lavagem de dinheiro até o terrorismo ou em matéria de proteção do meio ambiente e sobre as medidas adotadas pelos Estados além dos clássicos limites do direito penal e do processo penal, não é completamente novo[9].

---

6 Resolução do Parlamento Europeu de 12 de março de 2014 sobre o programa de vigilância em massa da NSA estadunidense e seu impacto sobre os direitos fundamentais dos cidadãos da União Europeia e sobre a cooperação transatlântica em matéria de assuntos de Justiça e Interior. Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

7 Vid. também a Recomendação CM/Rec(2014)6 do Comitê de Ministros do Conselho da Europa aos Estados membros sobre um «Guide to Human Rights for Internet Users» (adotado em 16 de abril de 2014): «4. Você não deve ser submetido a vigilância geral ou medidas de interceptação. Em circunstâncias excepcionais, previstas em lei, sua privacidade em relação a seus dados pessoais pode sofrer interferência, como no caso de uma investigação criminal. Informações acessíveis, claras e precisas sobre as leis ou a políticas relevantes e seus direitos a esse respeito devem ser disponibilizadas para você».

8 Vid. também Conferência Mundial de Direitos Humanos da ONU, Declaração de Vienna de 1993, parágrafo 17; e a Recomendação R(96)8 do Comitê de Ministros do Conselho da Europa aos Estados membros sobre «Crime Policy in Europe in a Time of Change» (adotada em 5 de setembro de 1996). Disponível em: https://rm.coe.int/16804f836b.

9 A bibliografia sobre esse tema é abundante. Vid., entre outros: SIEBER, Ulrich. Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt: eine Analyse der Vorfeldtatbestände im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten". *Neue Zeitschrift für Strafrecht*, v. 29, n. 7, pp. 353-364, 2009; e também SIEBER, Ulrich. Risk prevention by means of criminal law – On

Em muitos âmbitos, a fronteira entre prevenção e repressão tende a se confundir, já que, por um lado, o direito penal passou da repressão à prevenção; e, por outro, as medidas do direito administrativo tendem a ter um caráter punitivo[10]. Sem dúvida, isso tem impacto sobre os direitos fundamentais e também sobre a concepção mesma do processo penal. Embora esse tipo de processo tenha sido concebido tradicionalmente como um marco de garantias para proteger ao indivíduo de intrusões indevidas por parte do Estado e para impedir o uso abusivo do *ius puniendi*, podemos observar hoje medidas igualmente intrusivas fora do âmbito do direito penal e, portanto, fora das garantias previstas pelo processo penal[11]. Pode-se dizer que na atualidade o direito administrativo se «criminaliza» através de um eficaz sistema sancionatório, ao mesmo tempo que o processo penal se «administrativiza», não só com âmbitos

---

the legitimacy of anticipatory offenses in Germany's recently enacted counter-terrorism law. *In*: GALLI, Francesca; WEYEMBERGH, Anne. (Eds.), *EU counter-terrorism offences: What impact on national legislation and case-law?*. Bruxelas: Editions de l'Université de Bruxelles, Bruselas, 2012, p. 251-279; HIRSCH, Marianne F. H. Terrorism Causing a Shifting Responsibility in Criminal Pre-Trial Investigation: from Repression to Prevention. *In*: HIRSCH, Marianne F. H. et al. (Ed.). *Shifting Responsibilities in Criminal Justice*. Haia: Eleven International Publishing, 2012, p. 21 e ss; ASHWORTH, Andrew; ZEDNER, Lucia. *Preventive Justice*. Oxford: Oxford University Press, 2014, p. 13-26 e 179 e ss.

[10] Vid. por exemplo: OJANEN, Tuomas. Administrative counter-terrorism measures – a strategy to circumvent human rights in the fight against terrorism?. *In*: COLE, David; FABBRINI, Federico; VEDASCHI, Arianna. (Ed.). *Secrecy, National Security and the Vindication of Constitutional Law*. Cheltenham: Edward Elgar Publishing Limited, 2013, p. 251 e 254; GALLI, Francesca. The freezing of terrorists' assets: preventive purpose with a punitive effect. *In*: GALLI, Francesca; WEYEMBERGH, Anne. (Ed.). *Do labels still matter*? Blurring boundaries between administrative and criminal law. The influence of the EU. Bruxelas: Editions de l'Université de Bruxelles, 2014, p. 51 e ss.; MITSILEGAS, Valsamis. The Security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law. *In*: CARRERA, Sergio; MITSILEGAS, Valsamis. (Ed.). *Constitutionalising the Security Union*. Effectiveness, Rule of Law and Rights in Countering Terrorism. Bruxelas: CEPS, 2017, pp. 5-21.

[11] ASHWORTH, Andrew; ZEDNER, Lucia. *Preventive Justice*. Oxford: Oxford University Press, 2014, p. 181-190, embora a respeito das medidas preventivas adotadas no Reino Unido em matéria de terrorismo e alheias ao processo penal.

de responsabilidade penal objetiva, senão especialmente através da busca de soluções de conformidade ou justiça negociada.

O recurso a amplas medidas preventivas também provocou o aparecimento de uma nova categoria de pessoas – as chamadas «pessoas de interesse» - que não chegam a serem consideradas como suspeitas para o processo penal, mas se compreende que devam permanecer sob um «radar de controle»[12]. Naturalmente, isso leva a perguntar-se como se convertem certos sujeitos nessa esfera da «justiça preventiva», dirigida para fins de segurança. A situação atual na luta contra certos tipos de delinquência mostra que determinadas pessoas apresentam um potencial risco de vincular-se a atividades delitivas e que os sistemas de *mass surveillance* baseados em algoritmos os identificam como pessoas de interesse ou «pré-suspeitas». Uma vez classificadas pelo algoritmo nessa categoria, podem estar sujeitos a vigilância permanente, precisamente para coletar dados destinados à atividade de inteligência e fazer uma análise mais específica dos possíveis riscos. A «pessoa de interesse» passa assim a ficar sob a esfera de vigilância policial ou dos serviços de inteligência; porém, enquanto não houver indícios ou suspeitas fundadas da prática de um delito, não é, a rigor, suspeita desde a perspectiva processual tradicional. Daí que a máquina do sistema de justiça penal não pode ser ativada contra esse sujeito, porém também não lhe serão aplicáveis os direitos reconhecidos na esfera processual penal aos suspeitos em sentido próprio. É o que se denominou «princípio constitucional de intervenção indiciária»[13], que, como veremos mais adiante, se conecta com o conceito de causa provável da quarta emenda da Constituição estadunidense[14].

---

[12] Analisei esse tema anteriormente em: BACHMAIER WINTER, Lorena. Countering Terrorism: Suspects without suspicion and (Pre-)Suspects under surveillance. *In*: SIEBER, Ulrich; MITSILEGAS, Valsamis; MYLONOPOLUS, Christos; KNUST, Nandor. (Eds.). *Alternative systems of Crime Control*. Berlim: Duncker & Humblot, 2018, p. 171-191.

[13] A esse respeito, vid. MARTÍN MORALES, Ricardo. El principio constitucional de intervención indiciaria. *Revista de la Facultad de Derecho de la Universidad de Granada*, n. 2, pp. 341-506, 1999.

[14] Vid. BACHMAIER WINTER, Lorena. Probable cause y la Cuarta Enmienda de la Constitución estadounidense: una garantía tan imprecisa como necesaria. *Quaestio Facti*, v. 4, n. 1, pp. 191-220, 2023.

E é aqui que podemos identificar os fatos que obrigam a repensar as garantias do sistema de justiça penal e do processo penal. Por um lado, existe uma invasão no âmbito dos direitos fundamentais das pessoas sem que exista uma suspeita prévia sobre elas. E, por outro lado, a utilização da vigilância em massa ou *mass surveillance* abre as portas para a possibilidade de elaborar indícios racionais ou suspeitas fundadas que, por sua vez, permitirão o início do processo penal.

Com relação ao primeiro desses fatos, as «pessoas de interesse» estão sujeitas a certas medidas de vigilância que podem afetar seu direito à privacidade[15] e seu direito à proteção de dados. Na maioria dos casos não saberão que estão ou estiveram sob vigilância ou acompanhamento. Apenas se forem objeto de medidas administrativas que suponham uma restrição importante a seus direitos fundamentais – por exemplo, como a proibição de atravessar as fronteiras estatais ou de entrar em um determinado país, ou o congelamento de seus ativos – tomarão consciência de sua condição de «pessoas de interesse» ou «pré-suspeitas». E justamente em relação a isso convém considerar o tipo de garantias que se deve conceder a esses «suspeitos preventivos», àqueles que foram identificados como sujeitos de risco. Dado que essas pessoas não são suspeitas em uma investigação criminal e que o processo penal não foi iniciado formalmente, as garantias correspondentes não são aplicáveis. Porém, parece claro que sua situação não é comparável a de um cidadão comum, alheio à atenção dos sistemas de segurança.

Os critérios que devem ser seguidos nesses casos não estão claros porque não estão definidos legalmente e nem são públicos, de modo que as agências de segurança ou serviços de inteligência dispõem de uma ampla margem de apreciação para decidir se uma pessoa deve entrar ou não na categoria de «pessoa de interesse», baseando-se na informação coletada com ou sem o uso de *software* baseado no uso de algoritmos

[15] Não é fácil definir o direito à *privacy*, já que é composto por uma multiplicidade de direitos. Sem abordar essa questão, devo explicar que, para os efeitos deste estudo, nos referimos à privacidade como o controle da informação pessoal e o direito dos cidadãos a se autodeterminarem quando, como e em que medida a informação sobre eles se comunica aos demais. Assim o define: WESTIN, Alan. *Privacy and Freedom*. Nova Iorque: Atheneum, 1967, p. 7 e ss.

que identificam riscos[16]. Sem dúvida, não é fácil encontrar o adequado equilíbrio que permita manter a proteção das garantias do indivíduo frente ao Estado e ao mesmo tempo a elaboração de perfis que podem ter importantes repercussões no âmbito da liberdade e da privacidade dos cidadãos (embora devamos aceitar que a segurança passa por algum tipo de invasão na privacidade dos cidadãos)[17].

Esta realidade, sem ser nova, tem atualmente algumas características muito diferentes daquelas da época pré-digital. Em primeiro lugar, as gigantescas possibilidades que oferecem as ferramentas tecnológicas e, cada vez mais, o uso da inteligência artificial. E, em segundo lugar, a evanescente divisão entre a prevenção e a repressão, assim como a possibilidade – nem sempre regulada – de que os dados compilados acedam ao processo penal e se convertam em prova penal.

Os direitos dos suspeitos no processo penal estão definidos nos códigos processuais penais de âmbito nacional com a mínima harmonização que se produziu no âmbito da União Europeia por meio das distintas diretivas adotadas na matéria. Porém quais são os direitos reconhecidos aos pré-suspeitos ou «suspeitos preventivos»? Desde o ponto de vista da prevenção e da segurança nacional – e inclusive da segurança pública em geral – pode-se afirmar que sempre existiram mecanismos de vigilância para identificar riscos.

Porém convém reiterar que, devido à enorme expansão das possibilidades de vigilância através das tecnologias digitais e a sofisticados programas informáticos, o alcance da vigilância preventiva oferece hoje um panorama muito diferente em comparação com a informação

---

[16] Sobre as diferenças entre o *predictive policing* baseado em algoritmos e os sistemas tradicionais de avaliação dos riscos por parte dos agentes de polícia, vid. RADEMACHER, Timo. Predictive Policing im deutschen Polizeirecht. *Archiv des öffentlichen Rechts*, v. 142, n. 3, pp. 366–416, 2017, p. 391-393.

[17] No mesmo sentido: GALISON, Peter; MINOW, Martha. Our Privacy, Ourselves in the Age of Technological Intrusions. *In*: ASHBY WILSON, Richard. (Ed.). *Human Rights in the 'War on Terror'*. Cambridge: Cambridge University Press, 2005, p. 260, destacando que o conflito entre a segurança e a privacidade é inevitável. Não obstante, a meu juízo, ambos os interesses jurídicos devem andar de mãos dadas e é necessário que se busque o necessário equilíbrio entre eles, de tal maneira que as restrições e limites de um e do outro não necessariamente devem ser entendidos como conflitos.

coletada no passado através de informantes, de vigilância policial ou de interceptação de comunicações por parte dos serviços de inteligência. Como é sabido, os sistemas informáticos complexos utilizam uma série de algoritmos para elaborar uma vigilância policial preditiva, o qual possibilita a detecção de riscos através de mecanismos computacionais capazes de cruzar enormes quantidades de dados de pessoas físicas[18]. A consequência lógica é o maior número de pessoas que podem cair dentro da categoria de «pessoas de interesse». E também aumenta a capacidade de submetê-las a acompanhamento eletrônico intrusivo, o que acarreta maiores riscos para sua privacidade.

Especialmente em matéria de crime organizado e terrorismo – porém não só –, a tendência atual é centrar esforços a nível preventivo para enfrentar as ameaças e atuar muito antes do início formal do processo penal. E, como a tecnologia oferece a possibilidade de identificar – com maior ou menor margem de erro – os sujeitos que representam um risco potencial e submetê-los à vigilância eletrônica ou aplicar-lhes medidas administrativas de prevenção, parece que também deve ser redefinida a proteção dos cidadãos nessa etapa preventiva, ou bem estabelecer claras fronteiras com o processo penal. Assim, é necessário regular os direitos daquelas que foram consideradas «pessoas de interesse», as quais podem ser objeto de um conjunto de medidas encaminhadas a prevenir delitos graves ou ataques terroristas.

[18] A esse respeito, vid. BRAYNE, Sarah. *Predict and Surveil*: Data Discretion and the Future of Policing. Oxford: Oxford University Press, 2020, em especial o capítulo 7, «Algorithmic Suspicion and Big Data Searches: The Inadequacy of Law in the Digital Age», p. 118 e ss;; Vid. também RICH, Michael. Machine learning, automated suspicion, algorithms and the Fourth Amendment. *University of Pennsylvania Law Review*, v. 164, pp. 870-929, 2016.

2. Inteligência, prevenção e interceptação de comunicações: do caso *Big Brother Watch* ao *EncroChat*

2.1 Inteligência, prevenção e interceptação de comunicações na jurisprudência do TEDH

2.1.1 Segurança e interceptação de comunicações

A jurisprudência do TEDH estabeleceu os padrões mínimos de direitos que devem ser garantidos às pessoas nas ações de proteção da segurança nacional na conhecida sentença *Big Brother Watch e outros v. Reino Unido*, mais conhecida como caso *Big Brother Watch*[19], bem como em muitas sentenças anteriores[20].

O TEDH deixa uma ampla margem de apreciação aos Estados membros, tanto para valorar a existência e a qualificação de riscos para a segurança nacional quanto para eleger os instrumentos ou mecanismos para abordá-los[21]. Não obstante, o art. 3º da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais (CEDH) indica o limite intransponível. Desde *Klass e outros v. Alemanha*[22], o TEDH

---

[19] *Big Brother Watch e outros v. Reino Unido*, 13 de setembro de 2018, Appl. nos. 58170/13, 62322/14 e 24960/15; e posteriormente a sentença da Grand Chamber de 25 de maio de 2021. Sobre essa sentença, vid. e posteriormente a sentença da Grande Câmara de 25 de maio de 2021. Sobre essa sentença, vid. BACHMAIER WINTER, Lorena. Proportionality, surveillance and criminal investigation: Strasbourg Court facing Big Brother. *In*: BILLIS, Emmanouil; KNUST, Nandor; RUI, Jon Petter. (Ed.). *The Principle of Proportionality in Crime Control and Criminal Justice*. Oxford: Hart Publising, 2021, p. 317-335.

[20] *Szabó* e *Vissy v. Hungria*, Appl. nº. 37138/14, de 12 de janeiro de 2016; *Weber e Saravia v. Alemanha*, decisão de inadmissibilidade, Appl. nº. 54934/00, de 29 de junho de 2006; *Liberty e outros v. Reino Unido*, Appl. nº. 58243/00, de 1º de julho de 2008; *Roman Zakharov v. Rússia*, Appl. nº. 47143/06, de 4 de dezembro de 2015; *Centrum för Rättvisa v. Suécia*, Appl. nº. 35252/08, de 19 de junho de 2018.

[21] *Leander v. Suécia*, Appl. nº. 9248/8, de 26 de março de 1987. Em geral, vid. CAMERON, Iain. *National Security and the European Convention on Human Rights*. Haia: Kluwer Law, 2000, p. 74 e ss.

[22] *Klass e outros v. Alemanha*, Appl. nº. 5029/71, de 6 de setembro de 1978: em conformidade com a lei (que deverá cumprir com os requisitos de acessibilidade e previsibilidade), e a medida deverá estar justificada por um fim legítimo e ser necessária em uma sociedade democrática. Vid. também *Malone*

focou no destaque da importância das garantias que devem acompanhar os métodos de vigilância encoberta (*covered surveillance*), assim como a forma de registrar cada uma dessas atuações.

Porém, o Tribunal valorou apenas uma situação relacionada à segurança nacional, embora tenha destacado que o interesse na proteção da segurança nacional sempre deve ser ponderado com a gravidade da intromissão no direito à privacidade[23]. Na prática, isso significa que não se valora de forma independente o requisito de «estrita necessidade», pois a análise do Tribunal tem como ponto central a existência de garantias adequadas e efetivas contra intromissões abusivas em conjunto com a presença de adequados mecanismos de supervisão[24]. Por outro lado, apesar de inicialmente o TEDH ter considerado que o termo «necessário» para legitimar a intromissão no direito protegido no art. 8º da CEDH não equivalia a «indispensável», sua jurisprudência evoluiu até exigir que a *secret surveillance* esteja justificada por uma «estrita necessidade» de proteger as instituições democráticas.

Nesse contexto, a sentença *Szabó e Vissy v. Hungria*[25] estabeleceu os principais requisitos para as medidas de vigilância secreta através da interceptação de comunicações eletrônicas com a finalidade de proteger os interesses da segurança nacional. Segundo o art. 7/E 3 da lei antiterrorista da Hungria (versão de 2011), a polícia estava autorizada a levar a

---

v. Reino Unido, Appl. nº. 8691/79, de 2 de agosto de 1984; *Kruslin v. França*, Appl. nº. 11801/85, de 24 de abril de 1990, e *Huvig v. França*, Appl. nº. 11105/84, de 24 de abril de 1990. Posteriormente, vid. também, *Liberty e outros v. Reino Unido*, Appl. nº. 58243/00, de 1 de julho de 2008; *Roman Zakharov v. Rússia*, Appl. nº. 47143/06, de 4 de dezembro de 2015; *Ekimdzhiev e outros v. Bulgária*, Appl. nº. 70078/12, de 11 de janeiro de 2022; *Hašťák v. Eslováquia*, Appl. nº. 58359/12 et al., de 23 de junho de 2022; *Zoltán Varga v. Eslováquia*, Appl. nº. 58361/12 de 20 de julho de 2021.

[23] *Leander v. Suécia*, já citada, parágrafo 59.

[24] *Kennedy v. Reino Unido*, Appl. nº. 26839/05, de 18 de maio de 2010, parágrafo 153; *Weber e Saravia v. Alemanha*, decisão de inadmissibilidade, Appl. nº. 54934/00, de 29 de junho de 2006. Sobre o requisito de «estrita necessidade», vid. também as sentenças do TJUE caso C-293/12 y C-594/12 Digital Ireland v. Minister for Communications e outros, de 8 de abril de 2014; TJUE, caso C-473/12 Institut professionnel des agents immobiliers (IPI), de 7 de novembro de 2013.

[25] *Szabó* e *Vissy v. Hungria*, Appl. nº. 37138/14, de 12 de janeiro de 2016.

cabo operações de vigilância, inclusive a interceptação de comunicações eletrônicas em virtude da Lei de Segurança Nacional, se essa informação não pudesse ser obtida de outra maneira, sem a necessidade de haver suspeita da prática de algum delito grave[26]. Essa Lei tampouco exigia uma prévia autorização judicial para adotar a medida de vigilância secreta das comunicações, sendo suficiente uma autorização do Ministério correspondente.

Ademais, a Lei em questão só previa a destruição dos dados obtidos se não fosse necessário conservá-lo para os fins de inteligência. Os membros de uma organização não governamental (ONG) crítica a essas medidas recorreram ao TEDH alegando que referida Lei infringia seu direito constitucional à privacidade[27]. A análise efetuada pelo Tribunal é particularmente interessante, já que não se centrou na valoração de uma infração concreta, mas em examinar tanto se a Lei se ajustava aos requisitos de acessibilidade e previsibilidade, quanto se garantia que as medidas de vigilância secreta só se aplicariam quando fosse estritamente «necessário em uma sociedade democrática», proporcionando salvaguardas e garantias efetivas contra possíveis fins arbitrários ou abusos.

O Tribunal entendeu que nesse caso se havia produzido uma violação do art. 8º da CEDH com base nos cinco argumentos seguintes: 1) A legislação nacional não descrevia as categorias de pessoas que na prática poderiam ter suas comunicações interceptadas (parágrafo 66) e não existia nenhum tipo de requisito para que as autoridades demonstrassem a relação real ou presumida entre as «pessoas de interesse» e a prevenção de qualquer ameaça terrorista 2) O TEDH reconheceu que é lícito que os governos recorram a medidas de *mass surveillance* das comunicações e que utilizem as últimas tecnologias para prevenir ataques

---

[26] *Ibid*., parágrafo 12.

[27] Seguindo a jurisprudência do TEDH que outorga o *status* de vítima e, portanto, permite recorrer ao TEDH, a todo cidadão que poderia ter-se visto submetido a medidas de vigilância secreta em qualquer momento e sem notificação alguma, o Tribunal nesse caso também aceitou considerar o recorrente como vítima de uma violação pela mera existência de uma legislação que permite medidas secretas, sem ter que alegar que foi alvo dessas medidas. Nesse sentido, vid. *Klass e outros v. Alemanha*, e *Weber e Saravia v. Alemanha*, já citadas, além do caso *Association for European Integration and Human Rights Ekimdhiev v. Bulgária*, Appl. nº. 62540/00, de 28 de junho de 2007.

terroristas, porém, nesse caso, a lei não exigia da autoridade solicitante que apresentasse elementos que sustentassem o pedido, «em particular, uma base fática suficiente para a adoção de medidas secretas de inteligência que permitam valorar a necessidade da medida proposta»; e, segundo a sentença, isso não garantia que se levasse a cabo uma valoração sobre a «estrita necessidade» da medida de vigilância (parágrafo 71). 3) A lei não indicava se o prazo de noventa dias de duração da medida de vigilância podia ser prorrogado reiteradamente ou não. 4) A ausência de controle da concorrência do pressuposto de «estrita necessidade» por parte do Poder Judiciário ou de qualquer outro órgão independente. Para o Tribunal, a ausência de controle judicial não pode ser ignorada «tendo em vista a magnitude do conjunto de informações que podem obter as autoridades que aplicam sistemas de coleta de dados altamente eficientes e processam grandes quantidades de dados» (parágrafo 79). Embora esse controle judicial não possa ser feito sempre *ex ante* – por exemplo, em situações excepcionais de emergência –, como regra geral a lei deve contemplar uma revisão judicial *ex post factum* (parágrafo 81), já que não é considerado suficiente o controle parlamentar por parte de um comitê específico duas vezes ao ano. 5) Por último, a lei húngara não previa a notificação das medidas de vigilância para as «pessoas de interesse» uma vez concluídas as medidas (parágrafo 86). Tendo em vista todos esses argumentos, o Tribunal considerou que referida legislação não parecia oferecer garantias suficientes contra as medidas de vigilância em massa previstas para prevenir ataques terroristas.

2.1.2 O caso *Big Brother Watch* e a vigilância em massa

Posteriormente, foi julgado outro caso chave em matéria de *mass surveillance* e direito à privacidade, o caso *Big Brother Watch e outros v. Reino Unido*, no qual um grupo de organizações não governamentais de defesa do direito à privacidade recorreram ao TEDH por considerar que o sistema de interceptações previsto na legislação britânica em matéria de interceptação de comunicações violava os arts. 8º e 10 da CEDH. Especificamente, argumentavam que o art. 8º da RIPA (*Regulation of Investigatory Powers*) de 2000, que permite a vigilância de interceptações em massa (por meio de programas como KARMA POLICE, Black Hole

ou TEMPORA), não cumpria com os padrões estabelecidos pelo TEDH em sua própria jurisprudência nos casos *Weber e Saravia v. Alemanha*, *Zakharov v. Rússia*, e *Szabó e Vissy v. Hungria*. Essas ONGs, lideradas pelo caso *Big Brother Watch*, sustentavam que, para aplicar as medidas de vigilância em massa, deveriam ser cumpridos pelo menos os seguintes pressupostos e garantias: indícios objetivos que permitissem estabelecer uma suspeita razoável da prática de um delito grave ou de uma conduta que representasse uma ameaça específica à segurança nacional pelas pessoas a respeito de quem se pretende obter os dados; autorização judicial prévia emitida por uma autoridade independente; e, finalmente, a medida, uma vez concluída, devia ser comunicada aos afetados para que pudessem exercer seu direito de impugnação à interceptação de suas comunicações e ao armazenamento de seus dados.

Da análise da jurisprudência do TEDH nessa matéria, portanto, conclui-se que as leis nacionais devem prever salvaguardas mínimas nas atividades de inteligência para coleta de informações e na aplicação de medidas preventivas contra as ameaças à segurança nacional. O primeiro e mais importante requisito para a legalidade de tal sistema de vigilância que opera fora do processo penal é que essas medidas estejam respaldadas por suficientes elementos que constituam uma base fática suficiente para supor que, se não houver um delito, pelo menos exista um risco certo e que dito risco justifica as medidas de monitoramento. Em segundo lugar, é necessário um marco legal que estabeleça esses requisitos, as autoridades que podem ordenar tais medidas e os prazos e condições máximos para sua extensão. A lei também deveria prever a possibilidade de comunicar à pessoa *ex post*, desde que a notificação não tenha um impacto negativo na segurança. Por último, haveria que se estabelecer um controle judicial por parte de um órgão independente, ainda que fossem permitidas restrições à publicidade das audiências e também fosse aceitável a possibilidade de contar com defensores com autorização de segurança. Quanto ao controle judicial, enquanto no caso *Big Brother Watch* os demandantes exigiam que as medidas de vigilância em massa estivessem sujeitas a uma ordem judicial prévia quando envolvessem jornalistas e outros atores relevantes da sociedade civil, esse requisito não foi mencionado explicitamente no caso *Szabó*.

Em sua análise do caso *Big Brother Watch*, o Tribunal começou reiterando o enfoque já adotado em sua jurisprudência, especificamente no caso *Weber*, afirmando que «a licitude da ingerência está estreitamente relacionada com a questão de se foi cumprido o teste de "necessidade" pelo que convém que o Tribunal aborde conjuntamente os requisitos de "conformidade com a lei" e de "necessidade". A "qualidade da lei", nesse sentido, implica que o direito interno não só deve ser acessível e previsível em sua aplicação, mas também deve assegurar que as medidas de vigilância secretas só se aplicam quando "for necessário em uma sociedade democrática", em particular, proporcionando salvaguardas e garantias adequadas e efetivas contra o abuso» (parágrafo 334).

Porém, longe de se limitar a invocar a jurisprudência em matéria de interceptações em massa, no caso *Big Brother Watch*, o Tribunal analisou-se essa jurisprudência de dez anos antes continuava aplicável ao presente contexto digital e chegou à conclusão de que o alcance possível das interceptações e o volume de dados que pode ser analisado e armazenado atualmente exigem a reconsideração de algumas das premissas anteriores, estabelecidas para interceptações muito mais limitadas (parágrafos 341 e 342).

A sentença indica também que nem todas as salvaguardas previstas para as interceptações dirigidas a sujeitos concretos são aplicáveis no caso das interceptações em massa. Especificamente, não teria sentido exigir uma prévia delimitação legal das categorias de pessoas objeto da medida, nem tampouco o requisito prévio de «suspeita razoável» que se exige para as interceptações seletivas (parágrafo 348). As demais cautelas, sim, seriam aplicáveis. Nas palavras da sentença:

> Em particular, a legislação nacional deve estabelecer com suficiente clareza os motivos pelos quais a interceptação em massa pode ser autorizada e as circunstâncias nas quais as comunicações de um indivíduo podem ser interceptadas. As quatro salvaguardas mínimas restantes, definidas pelo Tribunal em suas sentenças anteriores – vale dizer, que o direito interno deve estabelecer um limite para a duração da interceptação, o procedimento a seguir para examinar, utilizar e armazenar os dados obtidos, as precauções que devem ser tomadas ao comunicar os dados a terceiros e as circunstâncias nas quais os dados interceptados podem ou devem ser apagados

> ou destruídos – são igualmente pertinentes para a interceptação em massa (parágrafo 348).

Antes de analisar as salvaguardas específicas que devem ser adotadas na interceptação em massa de comunicações, o Tribunal destaca quais as diferentes fases nas quais pode ser dividida essa medida: 1) busca inicial de informação, que se produz em sua maior parte de forma automatizada; 2) aplicação de critérios de seleção na busca para afinar os objetivos ou detecção de riscos; 3) exame do material pela primeira vez por parte do analista dos resultados obtidos na busca com o uso dos critérios de seleção; e 4) fase na qual se utiliza o material interceptado. A partir daí, o Tribunal insiste que em cada fase devem estar presentes mecanismos de controle e garantias efetivas.

Nas palavras do Tribunal, «o processo deve estar sujeito a "salvaguardas de extremo a extremo", o que significa que, a nível interno, deve ser feita uma avaliação em cada etapa do processo acerca da necessidade e proporcionalidade das medidas tomadas». E a isso deve adicionar-se a existência de uma autorização prévia por parte de uma autoridade independente – que não necessariamente precisa ser uma autoridade judicial – «quando o objeto e o alcance da operação ainda estão sendo definidos»[28]; «uma supervisão e revisão independente *ex post factum*» (parágrafo 350); e a existência de um recurso efetivo contra a medida adotada, que possa ser interposto inclusive pelos sujeitos que não sabem se foram objeto da medida, por não ter sido notificados.

O Tribunal dedica especial atenção à fase 2 de «aplicação dos critérios de seleção», a qual é especialmente sensível, pois através da escolha desses critérios se pode direcionar a interceptação para sujeitos determinados. A questão a elucidar é se esses critérios devem estar definidos previamente na decisão que autoriza a busca ou não. Embora

---

[28] Conforme sustenta o Tribunal: «Ademais, a fim de proporcionar uma salvaguarda eficaz contra o abuso, o órgão independente que conceda a autorização deve ser informado tanto do fim da interceptação como das operadoras ou rotas de comunicação que serão interceptados. Isso permitirá a referido órgão avaliar a necessidade e a proporcionalidade da operação de interceptação em massa e também avaliar se a seleção de operadoras é necessária e proporcional em relação aos fins para os quais se realiza a interceptação» (parágrafo 352).

alguns Estados assim o prevejam, o TEDH entende que isso nem sempre é factível e que reduzir esses critérios em muitas ocasiões «restringiria gravemente a efetividade da interceptação em massa» (parágrafo 353). Depois de reconhecer que na aplicação dos critérios pode aceitar-se certa flexibilidade, exige que a autorização pelo menos identifique «os tipos ou categorias de critérios que serão utilizados» (parágrafo 354), justificando a seleção dos critérios e registrando-os.

A sentença, portanto, confirma a possibilidade de que os Estados utilizem medidas de interceptação em massa das comunicações e que o âmbito de aplicação – segurança nacional – deve ser delimitado por cada um dos Estados membros. A conformidade com a CEDH depende do nível de salvaguardas existente. O Tribunal não definiu nada acerca do uso do material obtido por meio de interceptações em massa como prova em um processo penal, pois o art. 17 da RIPA, então aplicável especificamente, destacava que as comunicações interceptadas não poderiam ser apresentadas como provas. Não obstante, o argumento de que as informações obtidas por meio de interceptação em massa não seriam aproveitadas como provas não era convincente para todos os juízes do Tribunal. Em um dos votos[29], os juízes divergentes – ou parcialmente convergentes – sustentavam que, ao fim e ao cabo, com base na informação obtida por meio da vigilância em massa podem ser decretadas outras medidas de investigação ou a prisão, pois lhes serviriam de elementos probatórios[30].

2.1.3 Vigilância e prevenção sem *mass surveillance*

São vários os casos posteriores nos quais o TEDH teve a oportunidade de pronunciar-se sobre até que ponto os sistemas de interceptação

---

[29] Vid. os votos conjuntos parcialmente concorrentes dos juízes Lemmens, Vehabović e Bošnjak.

[30] *Ibid*. parágrafo 29: «A explicação do Governo demandado de que a informação obtida mediante interceptação em massa não podia ser utilizada em um processo penal é, em nossa opinião, pouco convincente. Parece que, com base na informação assim obtida, os órgãos encarregados de fazer cumprir a lei podiam atuar, por exemplo, procedendo para levar a cabo medidas de investigação ou até mesmo prisões, o que, por sua vez, produziria provas com a finalidade de ajuizar o caso».

de comunicações, seja com caráter preventivo, seja por parte dos serviços de inteligência, são compatíveis com a Convenção, especificamente com o direito à privacidade reconhecido no art. 8º da CEDH. Embora se trate de casos de vigilância dirigida a sujeitos concretos, e não de sistemas de *bulk surveillance*, interessa recordar brevemente aqui esses casos, na medida em que incidem no tema que estamos abordando, que em definitivo não é apenas a legitimidade de sistemas de vigilância sem prévia suspeita, mas também a questão de como essa informação de inteligência afeta o processo penal.

Na sentença *Ekimdzhiev e outros v. Bulgária*[31], de 11 de janeiro de 2022, os demandantes alegaram que as normas de vigilância secreta das comunicações previstas no Código de Processo Penal da Bulgária permitiam interceptar as comunicações de qualquer pessoa e que, ademais, as normas sobre preservação e acesso às comunicações, por sua vez, possibilitavam que as autoridades policiais tivessem conhecimento dessas comunicações. Também afirmavam que esse marco legal não oferecia suficientes garantias para prevenir abusos ou arbítrios no acesso ou uso da medida de vigilância por parte das autoridades. Essa medida estava prevista, na Bulgária, no marco da proteção dos interesses de segurança nacional, assim como para a prevenção de delitos graves (para os quais a pena máxima supera 5 anos de prisão).

Neste caso, o TEDH estimou que se havia produzido uma violação do art. 8º da CEDH por falta de adequada previsão legal para garantir que a vigilância secreta – e o posterior sistema de preservação e acesso às comunicações interceptadas – se limitaria ao estritamente necessário. O Tribunal também enfatizou a força vinculante das sentenças do TEDH e no dever de executá-las que pesa sobre os Estados membros, tal como prevê o art. 46 da CEDH, pois o Tribunal já havia condenado a Bulgária em uma sentença anterior pelos mesmos motivos. Por isso, o Tribunal recordava que a Bulgária devia fazer as mudanças necessárias em seu direito interno para pôr fim à referida violação e reestabelecer a situação na medida do possível, e insistia na obrigação do país de zelar para que suas leis fossem compatíveis com a Convenção.

---

[31] *Ekimdzhiev e outros v. Bulgária,* Appl. nº. 70078/12, de 11 de janeiro 2022.

Posteriormente, o caso *Haščák v. Eslováquia*[32], de 23 de junho de 2022, trata de interceptação de comunicações por parte dos serviços de inteligência no âmbito de uma operação complexa contra a delinquência. O demandante teve suas comunicações interceptadas ao comunicar-se com um dos sujeitos que estava sendo vigiado e alegou que a legislação não contemplava suficientes instrumentos para a proteção das pessoas afetadas aleatoriamente por esse tipo de medidas, acrescentando que as normas internas aplicáveis à retenção de material de inteligência eram inadequadas. Assim como no caso *Zoltán Varga v. Eslováquia*[33], e com referência expressa a essa sentença, o Tribunal apreciou de novo uma violação do art. 8º da CEDH. Embora reconhecesse a existência de uma base jurídica para a intercepção de comunicações, concluiu que, na execução das ordens judiciais que autorizavam a vigilância no âmbito de uma operação contra outros sujeitos, os serviços de inteligência gozavam, na prática, de uma discricionariedade quase equivalente a um poder ilimitado. A falta de salvaguardas contra ingerências arbitrárias, como exigem os princípios do Estado de Direito, e o fato de que a preservação das comunicações interceptadas não foi submetida a um controle externo, supunham uma violação à Convenção[34].

---

[32] *Haščák v. Eslováquia*, Appl. nº. 58359/12 *et al.*, de 23 de junho 2022.

[33] *Zoltán Varga v. Eslováquia,* Appl. nº. 58361/12 de 20 de julho 2021. Este caso está relacionado com o de *Haščák*, pois as comunicações desse último foram acessadas no âmbito da operação dirigida contra Zoltán, seu amigo e sócio. É por isso que o TEDH faz referência à sentença do caso Zoltán, pois tem relação com os mesmos fatos/interceptações, com a agravante de que no caso de *Haščák*, ele não era o alvo da vigilância, senão um terceiro que foi afetado pela operação.

[34] No momento da escrita deste trabalho, se encontram pendentes de decisão várias demandas relacionadas à interceptação de comunicações por parte de serviços de inteligência, embora não especificamente sobre *mass surveillance*. Entre as quais, *Association confraternelle de la presse judiciaire v. França*, Appl. nos. 49526/15 e mais 11, demanda apresentada por uma série de advogados e jornalistas, assim como pessoas jurídicas relacionadas a essas profissões, contra a Lei francesas de 24 de julho de 2005, que regulamenta os serviços de inteligência e a interceptação de comunicações. Em sentido similar, estão pendentes de decisão as demandas nos casos *Follorou v. França*, Appl. nº. 30635/17; *Johannes v. França*, Appl. nº. 30636/17.

Recentemente, na sentença nos casos *Pietrzak v. Polônia* e *Bychawska-Siniarska e outros v. Polônia*[35], de 28 de maio de 2024, o TEDH teve novamente a oportunidade de pronunciar-se acerca das medidas de vigilância adotadas com caráter preventivo com fundamento na normativa antiterrorista da Polônia. Nesse caso, o TEDH concluiu que houve uma violação ao art. 8º da CEDH por falta de adequada supervisão do monitoramento das comunicações realizado com fundamento na legislação antiterrorismo. Reiterava o TEDH que, devido à natureza das ameaças terroristas contemporâneas, poderia haver situações de emergência nas quais não seria possível exigir uma prévia autorização judicial para medidas de vigilância secreta e, inclusive, poderia ser contraproducente por falta de conhecimentos específicos, com a possibilidade de causar uma perda de tempo crucial. No entanto, essas medidas deveriam sempre submeter-se a um posterior controle judicial. Nesse caso, o Tribunal entendeu que o art. 8º da CEDH havia sido violado pelo regime legal de retenção de dados aplicado de forma desproporcional nesse Estado, assim como pela ausência de uma decisão judicial prévia autorizando a medida de vigilância dos recorrentes, unida ao fato de que essa medida tampouco contava com um controle judicial *ex post*[36].

2.1.4 O caso *ByLock*

No caso *Yüksel Yalçinkaya v. Turquia*[37], também conhecido como caso *ByLock* ou o «*EncroChat* turco», aborda-se, entre outras questões,

---

[35] *Pietrzak e Bychawska-Siniarska e outros v. Polonia,* Appl. nos. 72038/17 y 25237/18, de 28 de maio de 2024.

[36] A intervenção judicial só estava prevista se as medidas de vigilância secreta fossem posteriormente prorrogadas após expirar o período inicial de três meses. Portanto, nem a adoção da medida nem a sua aplicação no período inicial de três meses estiveram sujeitas a alguma revisão por um organismo independente. O Tribunal já havia indicado que a autorização de medidas de vigilância secreta por um órgão não judicial poderia ser considerada compatível com a Convenção, desde que o órgão fosse suficientemente independente do executivo. E neste caso não era, pois se tratava de um membro do executivo com responsabilidades políticas.

[37] *Yüksel Yalçinkaya v. Turquia*, Appl. nº. 15669/20, de 26 de setembro de 2023. Sobre esta sentença del TEDH e outras relacionadas ao mesmo tema, vid. o informe da Statewatch elaborado por Turkut e Yıldız, «ByLock Prosecutions

a admissibilidade da prova e sua conformidade com os arts. 6º e 8º da CEDH com relação à prova obtida a partir do acesso a um sistema de comunicação criptografado. No contexto de uma investigação em matéria de terrorismo, as autoridades afirmaram que todos os usuários de ByLock – um sistema criptografado de mensagens para telefone móvel – pertenciam a uma organização criminosa e que, ademais, esse sistema era utilizado exclusivamente por membros de referida organização. Com base nisso, o acusado foi condenado. O recorrente alegou que a falta de controle judicial na obtenção e tratamento dos dados do ByLock havia impossibilitado a verificação da autenticidade e integridade dessas comunicações eletrônicas. Esse defeito seria agravado pelo fato de que as autoridades não haviam apresentado uma relação das medidas tomadas para garantir a integridade dos dados de maneira verificável. A juízo do recorrente, todas essas circunstâncias levavam a concluir que os dados do ByLock não podiam ser considerados confiáveis e nem conclusivos para fins probatórios. O recorrente também apresentava outros dados que indicavam que os registros oficiais de usuários não coincidiam com as pessoas identificadas como tais. E acrescentava que, apesar de ser uma prova incriminatória determinante, não havia podido questionar a fiabilidade, a autenticidade e a legalidade (parágrafos 284-286).

Antes de valorar as circunstâncias desse caso em concreto, o TEDH recordou sua doutrina geral em matéria de admissibilidade de provas, reiterando que a valoração da prova cabe essencialmente aos tribunais nacionais e que ao Tribunal só compete analisar se a prova foi irrazoável ou arbitrária, pois o TEDH não é uma quarta instância. O TEDH comprova se foram respeitados, em termos gerais, a *fairness* do processo e a esse propósito enumera alguns de seus fatores tomados em consideração para avaliar o respeito ao direito a um processo equitativo: se o recorrente teve a possibilidade de impugnar as provas e opor-se à sua utilização; se as provas favoráveis ou contrárias ao acusado foram apresentadas de maneira que garantisse um juízo justo, o qual pressupõe

and the Right to Fair Trial in Turkey: The ECtHR Grand Chamber's Ruling in *Yüksel Yalçınkaya v. Türkiye*», publicado em março de 2024. Disponível em: https://www.statewatch.org/publications/reports-and-books/bylock-prosecutions-and-the-right-to-fair-trial-in-turkey-the-ecthr-grand-chamber-s-ruling-in-yuksel-yalcinkaya-v-turkiye.

o desenvolvimento de um processo com contraditório e paridade de armas (parágrafos 303 e 304); e a qualidade das provas, tomando em consideração o modo de sua obtenção e se há dúvidas acerca de sua fiabilidade ou autenticidade. A motivação da sentença nacional deveria lançar luz a esses extremos.

Depois de analisar o modo de obtenção da prova, as garantias adotadas para sua integridade e autenticidade e a resposta aos recursos do acusado, o TEDH concluiu que foi violado o art. 6.1 da CEDH. O Tribunal de Estrasburgo não questionou o acesso à plataforma ByLock, ao contrário, afirmou que «o recurso a provas eletrônicas que confirmam que um indivíduo está utilizando um sistema de mensagens criptografado que foi especialmente desenvolvido e utilizado exclusivamente por uma organização criminosa nas comunicações internas de uma organização criminosa pode ser muito importante na luta contra o crime organizado» (parágrafos 312 e 344).

O Tribunal reconheceu que o uso e a valoração das provas eletrônicas em processos penais podem implicar dificuldades particulares para os juízes, devido à complexidade dessas provas, o que pode interferir na capacidade dos tribunais nacionais para determinar sua autenticidade, exatidão e integridade. Ademais, o manejo de provas eletrônicas, em particular quando se trata de dados criptografados e/ou de grande volume ou alcance, pode criar problemas práticos e processuais graves para as autoridades policiais e judiciais, tanto na fase de investigação, quanto na fase judicial (parágrafo 312).

Afirmou também o Tribunal que, nos processos penais, s pode-se recorrer cada vez mais a dados eletrônicos ou outros dados coletados por serviços de inteligência, cujas atividades a esse respeito podem ou não estar sujeitas às normas que regulamentam a obtenção de prova no processo penal (parágrafo 315). Pois bem, nesses casos, se a obtenção ou processamento desses dados não está submetida a uma prévia autorização ou supervisão independente, ou a uma revisão judicial *ex post factum*, ou quando não está acompanhada de outras garantias processuais ou não está corroborada por outras provas, é mais provável duvidar de sua fiabilidade.

Portanto, o TEDH ponderou se a falta de acesso do recorrente às fontes de prova havia sido compensada com garantias processuais adequadas e se acusado teve uma oportunidade adequada para preparar sua

defesa, como exige o art. 6º da Convenção (parágrafo 330), concluindo que essas garantias faltaram.

Desse caso é muito importante destacar que, em sua análise, o Tribunal de Estrasburgo não questionou o uso de informação de inteligência como prova, o qual deixa nas mãos da legislação nacional. Centrou sua análise na existência de suficientes garantias que sirvam para equilibrar as desvantagens causadas para a defesa pela falta de acesso à integralidade das fontes de prova. Nesse contexto, em que a valoração dessa prova eletrônica reveste especial complexidade – que os próprios juízes, de regra, não estão em condições de entender – e não pode estar submetida ao contraditório pleno, conferir-lhe um valor determinante para a condenação do sujeito acusado infringe o art. 6.2 da CEDH.

2.2 A interceptação em massa de comunicações e o caso *EncroChat*

No âmbito da prova transnacional e da admissibilidade da prova obtida através de uma interceptação em massa de comunicações, quiçá não exista nenhum caso com tanta repercussão quanto o conhecido caso *EncroChat*, sobre o qual se pronunciou o TJUE na sentença de 30 de abril de 2024[38].

É preciso destacar que não é o único caso em que houve acesso e registro de todo um sistema de comunicação criptografado mediante um registro em massa ou indiscriminado, o qual podemos situar entre as medidas de vigilância próprias das atuações em âmbito preventivo ou de segurança nacional e as medidas de interceptação de comunicações que são utilizados numa investigação criminal. O sistema *EncroChat* não é o único serviço de troca de mensagens criptografado, pois similares problemas foram levantados em relação a muitas outras plataformas de mensagens criptografadas.

Há alguns anos, houve operações em diferentes países da União Europeia – e também fora dela – dirigidos precisamente a bloquear ou registrar sistemas de comunicação criptografados sobre os quais existia

[38] STJUE, de 30 de abril 2024, caso C-670/22 - M.N. (*EncroChat*), ECLI:EU:C:2024:372.

uma suspeita de que fossem usados por sujeitos criminosos. A operação sobre o sistema EnnetCom – com servidores no Canadá, porém com grande parte de usuários localizados em território holandês – dirigida pela polícia holandesa em 2016, levou à detenção do dono da companhia pelos delitos de lavagem de dinheiro e tráfico ilícito de armas, entre outras atividades delitivas[39]. As operações relativas à SkyECC, uma companhia com sede nos Estados Unidos e no Canadá, que comercializada telefones móveis, com a câmera, o microfone e o GPS desabilitados, nos quais havia sido instalada uma aplicação de mensagem criptografada que unicamente permitia a comunicação com outros telefones com o mesmo sistema de criptografia. Os servidores que davam assistência à aplicação se encontravam na Europa e contavam com aproximadamente 170.000 usuários identificados mediante um código alfanumérico (ID) de 6 caracteres[40]. E também as plataformas de An0m – criada pelos próprios serviços de inteligência dos Estados Unidos na operação «*honey pot*» de controle e vigilância, que legou à detenção de uns 800 suspeitos de delitos graves na Europa em 2021[41]. O Exclu, com servidor localizado na Alemanha[42].

Não é esse, naturalmente, o lugar para abordar um estudo pormenorizado de todos os aspectos e implicações dos dados de comunicações obtidos por meio do acesso a um sistema criptografado fundamentalmente para trocar mensagens escritas. Estas páginas concentram-se no caso *EncroChat*, sem prejuízo de que muitas das considerações jurídicas – em

---

39 Vid. *The Guardian*, 22 de abril de 2016. Disponível em: https://www.theguardian.com/world/2016/apr/22/dutch-police-ennetcom-shut-down-owner-arrested.

40 *SwissInfo,* de 20 de maio de 2022. Disponível em: https://www.swissinfo.ch/spa/la-investigación-de-sky-ecc-revela-los-métodos-despiadados-de-los-narcotraficantes-en-europa/48100996.

41 Sobre este último vid. a sentença do *Oberlandesgericht* de Frankfurt, de 22 de novembro de 2021, NJW 2022/710. Disponível em: https://dejure.org/dienste/vernetzung/rechtsprechung?Text=1%20HEs%20427/21. Vid. também o comunicado da Europol à imprensa de 8 de junho de 2021. Disponível em: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication.

42 *Irish Independent*, de 14 de fevereiro de 2023. Disponível em: https://www.independent.ie/irish-news/crime/german-police-target-george-the-penguin-mitchell-in-encrypted-phone-network-investigation/42341287.html.

particular as que afetam o direito de defesa – sejam aplicáveis nos processos em que se valora a prova obtida através do registro em massa de outros sistemas de comunicação criptografados.

Para além da indubitável atualidade deste caso no marco da luta contra o crime transnacional na União Europeia, interessa mencionar aqui este caso porque assenta algumas bases que deverão ser respeitadas para que seja admissível como prova a informação obtidas no acesso em massa aos dados de uma plataforma de troca de mensagens, efetuada pelos serviços policiais com a colaboração dos serviços de inteligência de um Estado[43].

Tal e como se reflete no STJUE no caso *EncroChat*[44], «no âmbito de uma investigação levada a cabo pelas autoridades francesas, foi revelado que alguns investigados utilizavam telefones móveis criptografados que funcionavam sob uma licença denominada "EncroChat" para cometer delitos relacionados principalmente com o tráfico de drogas. Esses telefones móveis permitiam, graças a um "*software*" especial e a um material modificado, estabelecer, através de um servidor instalado em Roubaix (França), uma comunicação criptografada de ponta a ponta que não pode ser acessada mediante métodos tradicionais de investigação».

No fim de dezembro de 2018, e posteriormente em outubro de 2019, as autoridades francesas solicitaram a autorização do Tribunal Penal de Lille para conservar esses dados. Em 2020, a França e a Holanda, junto com a Europol[45] e a Eurojust, estabeleceram uma Equipe Conjunta de Investigação (*Joint Investigation Team*, *JIT*) para levar a cabo a operação de intervenção do sistema de comunicação criptografada de ponta a ponta no qual não se podia intervir com os métodos de investigação convencionais.

---

[43] Como já foi indicado, o sistema *EncroChat* não é o único serviço de troca de mensagens encriptadas, pois problemas similares foram levantados em relação a muitas outras plataformas de mensagens criptografadas. Também foram levantados problemas similares em relação ao sistema "Anom" desenvolvido pelo FBI. Sobre este último, vid. a sentença do *Oberlandesgericht* de Frankfurt, de 22 de novembro de 2021, NJW 2022/710. Disponível em: https://dejure.org/dienste/vernetzung/rechtsprechung?Text=1%20HEs%20427/21.

[44] Vid. parágrafo 19 da sentença.

[45] A Europol declarou que não havia desenvolvido *software* para interceptar comunicações trocadas por meio da rede *EncroChat*. O apoio da Europou envolveu análise operacional, apoio técnico e experiência para o JIT.

A utilização de um «*trojan*» para acessar ao sistema foi autorizada também pelo Tribunal Penal de Lille[46]. Essa medida afetou «32.477 usuários – de um total de 66.134 usuários registrados no sistema – distribuídos entre 122 países, 4.600 deles na Alemanha»[47]. Esta medida permitiu detectar que nos telefones celulares do sistema *EncroChat* se alojavam comunicações de milhares de sujeitos relacionados com atividades delitivas, principalmente com o tráfico de drogas. Especificamente, a decodificação parcial inicial de 3.477 arquivos de texto criados como «notas» revelou que quase todo o material era referente a comunicações relacionadas com atividades delitivas perpetradas por organizações criminosas.

No início desse caso e diante da clara relevância transnacional, organizou-se uma reunião de coordenação na Eurojust para informar essas descobertas e, a partir daí, começou-se a distribuir o material interceptado entre os Estados membros para que o utilizassem em suas investigações próprias, através do sistema SIENA de transferência segura de informação policial[48]. Essa operação originou milhares de prisões em toda a União Europeia e também numerosas condenações penais, baseadas em grande parte na prova obtida por meio da medida adotada na França.

Sem entrar em todos os detalhes – o caso *EncroChat* poderia dar origem a várias monografias[49] – o «hackeamento» desse sistema de comu-

---

[46] O registro desses telefones celulares e o acesso e preservação das comunicações foram feitos em conformidade com o art. 706-102-1 do *Code de procédure pénale* francês e a decisão judicial foi motivada quando aos requisitos de necessidade, adequação e proporcionalidade.

[47] STJUE, parágrafo 20.

[48] Os países com maior número de telefones celulares afetados foram, nesta ordem: Holanda, Espanha, Reino Unido, Alemanha e Itália.

[49] Uma descrição detalhada das atuações e resoluções adotadas na Alemanha sobre esse caso pode ser vista tanto na STJUE de 30 de abril de 2023, como na ST do *Bundesgerichtshof* de 2 de março de 2022, já citada. Vid. também: WAHL, Thomas. Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren. *Zeitschrift für Internationale Strafrechtsdogmatik*, v. 7–8, pp. 452-461, 2021, p. 453; OERLEMANN Jan-Jaap; VAN TOOR, Dave. Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law and Criminal Justice*, v. 30, n. 3-4, pp. 309-328, 2022; LINDEMAN, Joep; LUCHTMAN, Michiel; VAN TOOR, Dave. Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair-Trial Rights in the Netherlands. *In*: BACHMAIER WINTER, Lorena; SALIMI, Farsam. (Ed.) *Admissibility of Evidence in EU*

nicação coloca, entre outras, a questão acerca de quais são as condições de admissibilidade da prova transnacional e dos efeitos da transmissão desses dados obtidos em outro Estado membro através de uma Ordem Europeia de Investigação (OEI).

O debate gira fundamentalmente em torno dos seguintes pontos:

1) Se a medida adotada na França – «intervenção de todo um sistema de comunicações» – resulta lícita, ao não existir uma investigação penal concreta pela prática de um delito baseada em suspeitas frente a um sujeito concreto. Nesse contexto, cabe questionar se se trata de informação de inteligência à qual se acessa por motivos de segurança ou, melhor, de uma investigação penal que se dirige frente a um número massivo de sujeitos não identificados. A fronteira não está clara.

2) Se foram cumpridas as normas previstas no art. 31 da Diretiva sobre a Ordem Europeia de Investigação (DOEI) que exige que se autorize em um Estado membro a interceptação de comunicações no território de outro Estado membro «cuja assistência técnica não seja necessária para levar a cabo a intervenção, o Estado que realiza a intervenção deverá notificar à autoridade competente do Estado no qual há é feita referida intervenção». Essa notificação deverá ser feita previamente se é sabido que o sujeito cujas comunicações se interceptam está em outro Estado membro, ou *ex post* se esse fato só é conhecido posteriormente. Tendo em vista a notificação, o Estado «notificado» poderá ordenar a suspensão da medida ou denegar a possibilidade de utilizar como prova as comunicações interceptadas no caso de a intervenção não poder ter sido acordada num caso nacional semelhante no Estado «notificado».

3) Admitida a prova em um processo penal, se os direitos de defesa do acusado foram respeitados adequadamente, permitindo que pudesse questionar a licitude da prova obtida em outro Estado.

Aqui, vou me concentrar no desenvolvimento do caso *Encro-Chat* na Alemanha por ser um dos primeiros países que enfrentou essas questões em um processo de diversos acusados pelo delito de tráfico de drogas e no qual foram proferidas as primeiras sentenças condenatórias

Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights. Oxford: Hart Publishing, 2024, p. 118 e ss.

baseadas nessas interceptações[50]. Também por ser o primeiro em que um juiz formulou uma prejudicial ao TJUE para resolver a questão acerca da possível violação ao direito da União Europeia no caso *EncroChat*, especificamente a interpretação que deve ser dada a diversos preceitos da Diretiva da Ordem Europeia de Investigação.

2.2.1 O caso *EncroChat* nos tribunais alemães

Voltando ao caso *EncroChat,* de forma geral, os tribunais alemães não apresentaram obstáculos à admissibilidade, como prova, dos dados extraídos do sistema *EncroChat,* obtidos por meio da cooperação policial e judicial internacional com a França. Contudo, a posição dos tribunais de primeira instância não foi sempre unânime. Por exemplo, o Tribunal Regional de Berlim (*Landgericht* Berlin), em decisão de 1º de julho de 2021, negou a abertura do julgamento oral contra o acusado, ao considerar que a prova apresentada pela acusação — as comunicações obtidas do *EncroChat* e enviadas pelas autoridades francesas — não era admissível. Em resposta, o Ministério Público interpôs recurso perante o Tribunal Superior Regional de Berlim (*Kammergericht,* equivalente a um *Oberlandesgericht*), que acatou o recurso em decisão de 30 de agosto de 2021[51], alinhando-se à posição dos demais tribunais superiores regionais dos *Länder*.

Um aspecto curioso dessa decisão do *Kammergericht* de Berlim é um dos argumentos utilizados para não questionar a legalidade das ações das autoridades francesas na interceptação do sistema *EncroChat*. Especificamente, após constatar que o caso envolvia crimes graves e que a obtenção da prova não comprometeu o núcleo essencial do direito fundamental à vida privada, o tribunal reforçou sua ponderação em favor da admissibilidade da prova com a seguinte afirmação: "não utilizar as informações obtidas legalmente pelas autoridades da República da França — não apenas um membro fundador da União Europeia, mas também

---

[50] Sentença do *Bundesgerichtshof* de 2 de março de 2022 – 5 StR 457/21.

[51] *KG Berlin Strafkammer*, de 30 de agosto de 2021, 2 Ws 93/21. Disponível em: https://dejure.org/dienste/vernetzung/rechtsprechung?Text=2%20Ws%2093/21.

um dos países que constituem a base da concepção moderna dos direitos humanos — na persecução de crimes tão graves quanto os presentes, também configuraria uma ofensa ao senso de justiça da população que respeita a lei."[52]

Embora este argumento seja peculiar para sustentar o princípio da confiança mútua, é relevante examinar os principais argumentos apresentados pela defesa contra a admissibilidade das provas do *EncroChat*. Em primeiro lugar, argumentou-se que tais interceptações de comunicações eletrônicas não poderiam ter sido autorizadas em um processo interno na Alemanha, dado que a legislação alemã exige suspeitas graves e concretas da prática de um ato criminoso para permitir medidas de interceptação de comunicações eletrônicas (On-line Durchsuchung). No caso em questão, segundo a defesa, tal condição não teria sido atendida, já que a interceptação massiva não foi direcionada contra um suspeito específico.

Este argumento foi refutado pelos tribunais superiores, que afirmaram existir indícios de que o serviço de telefonia móvel *EncroChat* estava sendo utilizado por redes de criminalidade organizada, fato reconhecido por vários acusados perante os tribunais franceses. Além disso, tratava-se de aparelhos celulares que não podiam ser adquiridos por meios comerciais regulares, mas apenas via eBay, a um custo de 1.610 euros. Diante dessas evidências e outros elementos suspeitos, as autoridades francesas realizaram a «invasão» do servidor e, posteriormente, acessaram as comunicações nos dispositivos vinculados ao sistema *EncroChat*.

Em segundo lugar, a defesa alegou que o direito de defesa foi comprometido, já que não foi possível verificar o método de obtenção das provas, o que restringiria o direito a um processo contraditório e com todas as garantias. Frente a essas alegações, o recurso de cassação (Revisionsverfahren) apresentado ao Supremo Tribunal Federal

[52] Tradução feita no DeepSeek: «A não utilização de informações obtidas legalmente pelas autoridades da República da França — não apenas um membro fundador da União Europeia, mas também um dos países berço da compreensão moderna dos direitos humanos — sobre crimes tão graves violaria, de forma significativa, o senso geral de justiça da população que respeita a lei», (parágrafo I.2.c da sentença).

(Bundesgerichtshof, BGH)[53] confirmou a admissibilidade das provas obtidas pela interceptação do sistema *EncroChat*. Vale destacar que a legislação alemã não prevê restrições expressas ao uso de dados obtidos no exterior por meio de assistência jurídica internacional. Em particular, o artigo 100e(6) do Código de Processo Penal Alemão (StPO), que regula os requisitos e procedimentos para medidas de interceptação de comunicações, não se aplica diretamente a provas obtidas no exterior.

O BGH rejeitou o recurso com base no seguinte raciocínio: a admissibilidade de provas, incluindo aquelas obtidas no exterior, é regida pelas normas de direito interno; no âmbito da cooperação judicial internacional em matéria penal, aplica-se o princípio "locus regit actum", e não compete aos tribunais nacionais verificar o cumprimento das normas estrangeiras pelas autoridades de outro país. Conforme a Decisão de Ordem Europeia de Investigação (DOEI), não há exigência de que o Estado solicitante examine se o Estado requerido obteve as provas em conformidade com os padrões de suas próprias normas processuais. Além disso, não há razões para recusar a admissibilidade das provas por questões de ordem pública ou de direito internacional público, visto que a França autorizou o uso das provas por ela obtidas nos tribunais alemães. O modo como as provas foram obtidas no território francês não contraria os princípios constitucionais do direito alemão. Considerando que o ordenamento jurídico alemão não prevê normas rígidas de exclusão de provas relacionadas à forma de obtenção das mesmas (abhängige Beweisverwertungsverbote), e que, neste caso, não havia motivos processuais ou constitucionais para a exclusão da prova, tampouco à luz da jurisprudência do TEDH, o BGH rejeitou o recurso.

Um ponto especialmente relevante para análise é a declaração do BGH de que o caso em questão não se trata de vigilância massiva realizada por serviços de inteligência, ainda que estes possam ter participado e alguns aspectos da obtenção das provas permaneçam confidenciais. Segundo o tribunal[54], não se trata de um caso de «vigi-

---

[53] O recurso foi apresentado perante a sentença de condenação prolatada pelo *Oberlandesgericht* de Hamburgo, de 15 de julho de 2021. Disponível em: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2022&nr=127966.

[54] Ver parágrafos 37 e 38 da decisão.

lância massiva e avaliação indiscriminada de dados sem um objetivo ou motivação concreta», característica das interceptações realizadas por serviços de inteligência. Conforme argumentaram as autoridades francesas, a investigação no caso *EncroChat* não foi direcionada a um modelo de negócio completamente normal e legal (oferta de um serviço de telefonia móvel criptografada para aumentar a segurança contra invasões), utilizado por apenas alguns criminosos. O objetivo foi acessar um serviço projetado desde o início para facilitar atividades criminosas, sendo uma rede operativa secreta, amplamente utilizada por redes de tráfico de drogas, conforme evidenciado ao longo da investigação.

Do ponto de vista das autoridades francesas, a presunção de que os dispositivos *EncroChat* eram utilizados quase exclusivamente para fins criminosos foi confirmada ao longo da investigação, tanto após o primeiro acesso aos dados quanto após a análise de outras informações de usuários a partir de janeiro de 2020. Com base nessas suspeitas e evidências, um juiz autorizou e supervisionou a coleta temporária de todos os dados dos usuários do *EncroChat,* por razões repressivas e preventivas relacionadas à obrigação constitucional de garantir a segurança dos cidadãos contra riscos graves, como o tráfico de drogas e o crime organizado.

À luz de todo o exposto, o BGH concluiu que não houve violações graves aos princípios do Estado de Direito, nem aos direitos humanos fundamentais ou aos valores e princípios do direito europeu. Após várias condenações proferidas por diferentes tribunais — não apenas na Alemanha —, e diante da jurisprudência uniforme dos Oberlandesgerichte, o Tribunal Regional de Berlim, em decisão de 19 de outubro de 2022, submeteu uma questão preliminar ao TJUE (C-670/22).

Enquanto a questão preliminar estava pendente de decisão no TJUE, a possível violação de direitos fundamentais pela admissão das comunicações do *EncroChat* como prova pelos tribunais alemães foi também levantada no Tribunal Constitucional Alemão (Bundesverfassungsgericht), em relação a outro processo penal em que as mensagens do *EncroChat* foram usadas como prova. Nesse caso, o recorrente, condenado por tráfico de drogas pelo Landgericht de Rostock por uma sentença de 23 de julho de 2021 (depois de esgotar todos os recursos ordinários),

apresentou recurso constitucional em 24 de março de 2022.[55] Em seu recurso, argumentava que haviam sido violados o artigo 101.1 e 2 da *Grundgesetz* alemã (direito ao juiz natural), ao considerar que os tribunais nacionais deveriam ter submetido a questão preliminar ao TJUE e, ao não fazê-lo, estavam privando o juiz natural de sua competência.[56] Além disso, alegava-se a violação dos artigos 7 (direito ao respeito pela vida privada e familiar) e 8 (direito à proteção de dados pessoais) da Carta dos Direitos Fundamentais da União Europeia. O recurso não foi conhecido em decisão de 9 de agosto de 2023, especialmente por não ter invocado as supostas infrações em instâncias judiciais anteriores.

2.2.2 A questão preliminar no TJUE

Na questão preliminar apresentada ao Tribunal de Justiça da União Europeia (TJUE), apresenta-se, em primeiro lugar, a problemática referente à autoridade emissora: especificamente, se, para efeitos do artigo 6.º da Decisão-Quadro relativa à Ordem Europeia de Investigação (DOEI) e em conformidade com o artigo 2.º, alínea c), da mesma decisão, a "autoridade emissora" competente para emitir essa ordem pode ser um procurador. Sem adentrar aqui em uma análise detalhada, é suficiente observar que o TJUE concluiu que um procurador pode ser considerado autoridade emissora para solicitar a execução de uma DOEI visando a obtenção de provas que já se encontram sob posse do Estado de execução, desde que, nos termos do direito nacional, o procurador também tivesse competência para emitir tal ordem em um caso interno. Ressalta-se que, no caso *EncroChat* na Alemanha, a DOEI foi emitida para que as autoridades francesas enviassem arquivos de comunicações que já estavam sob sua posse, como resultado da interceptação prévia do sistema. O pedido alemão, portanto, não buscava a execução de uma nova medida de interceptação de comunicações, mas apenas a transmissão de dados já coletados, o que foi determinante para

---

[55] *Bundesverfassungsgericht* 2 BvR 558/22, de 9 de agosto de 2023. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/08/rk20230809_2bvr055822.html.

[56] Art. 101, 1 e 2 da *Grundgesetz*.

concluir que a DOEI poderia ser emitida por uma autoridade judicial que não fosse um juiz.

O segundo ponto relevante refere-se ao objetivo e às funções da notificação prevista no artigo 31.º da DOEI. O TJUE inicialmente analisou a aplicação desse dispositivo ao caso em questão, indicando que a medida adotada pelas autoridades francesas — o registro de comunicações armazenadas em um servidor e o acesso aos dispositivos móveis — equivale, para fins de notificação, a uma «interceptação de comunicações». Assim, essa notificação seria exigível em relação à medida realizada.

Essa interpretação parece lógica, pois o sigilo das comunicações é afetado tanto em interceptações de comunicações orais quanto no registro de comunicações escritas, independentemente de as normas aplicáveis para cada tipo de interferência serem distintas. Em ambos os casos, há uma ingerência no sigilo das comunicações, o que fundamenta a conclusão do TJUE de que o artigo 31.º da DOEI se aplica ao caso.

Entretanto, essa inferência entra em aparente contradição com a abordagem do próprio TJUE em relação à autoridade emissora: para fins de emissão da DOEI, não se trata de uma interceptação de comunicações — que exigiria a autorização de um juiz —, mas sim para fins da notificação prevista no artigo 31.º. Essa contradição aparente pode ser resolvida ao considerar que o TJUE aborda dois níveis distintos: os requisitos aplicáveis às autoridades alemãs, enquanto Estado emissor, e os requisitos que devem ser cumpridos pelas autoridades francesas, enquanto Estado executor da medida.

Ainda assim, a aplicação prática do artigo 31.º da DOEI levanta algumas dúvidas. Este dispositivo estabelece que um Estado-membro, ao interceptar comunicações que ocorram em outro Estado-membro sem assistência técnica deste, deve notificá-lo. O Estado «notificado», por sua vez, pode autorizar a medida ou proibir o uso das comunicações como prova. Assim, a pergunta do tribunal alemão ao TJUE não se refere diretamente à utilização da prova na Alemanha, mas à obrigação das autoridades francesas de notificarem os demais Estados-membros sobre essas interceptações. A notificação condicionaria a utilização das provas obtidas por meio do registro do *EncroChat* na França, visto que os Estados «notificados» poderiam vetar a admissibilidade dessas comunicações em processos judiciais franceses.

Nesse contexto, surge uma questão: qual o interesse do tribunal de Berlim em determinar se essas provas seriam válidas na França na ausência da notificação prevista no artigo 31.º da DOEI? Embora possa parecer desnecessário à primeira vista, esse questionamento ganha relevância à luz das regras gerais sobre admissibilidade de provas transnacionais. A regra geral é que se aplica o princípio da *lex loci*: se a prova foi obtida de forma legal no Estado de execução, ela deveria ser admitida no tribunal de foro. Perguntar sobre a exigibilidade da notificação do artigo 31.º implica verificar se a obtenção da prova na França cumpriu os requisitos legais, isto é, se respeitou o princípio da *lex loci*. Ao decidir que o artigo 31.º é aplicável, o TJUE também determina que essa notificação é parte integrante das exigências legais para validar a obtenção da prova na França.

De qualquer forma, sendo as autoridades alemãs as interessadas na utilização das provas obtidas na França, não parece provável que elas se opusessem à sua utilização em território francês. É verdade que o artigo 31 da DOEI prevê a possibilidade de que o Estado «notificado» se oponha à medida que tem efeitos em seu território, já que o artigo 31.3 da DOEI especifica que, se tal medida não estiver autorizada em um caso interno semelhante, esse Estado «poderá» se opor à execução dessa medida ou à utilização do que foi obtido por meio dela como prova.

O significado e o alcance do artigo 31 da DOEI não estão isentos de debates, mas este não é o momento para abordá-los.[57] É importante, contudo, destacar que o TJUE acrescenta que o objetivo dessa notificação não é meramente informativo ou uma questão de cortesia internacional, mas também «visa proteger os direitos dos usuários afetados por uma medida de "interceptação de telecomunicações", conforme o significado desse artigo».[58]

---

[57] Remeto-me aqui ao que já mencionei anteriormente em: BACHMAIER WINTER, Lorena. Mutual recognition and cross-border interception of communications: the way ahead for the European Investigation Order. *In*: BRIÈRE, Chloé; WEYEMBERGH, Anne. (Ed.). *The needed balances in EU Criminal Law*: Past, present and future. Oxford: Hart Publishing, 2017, p. 313-336.

[58] STJUE M.N., caso C-670/22 (*EncroChat*), de 30 de abril de 2024, em sua parte dispositiva, parágrafo 132, 4). Em sentido diverso se expressa a sentença já citada do BGH, na qual se entende que a proteção conferida pelo artigo 31 da DOEI é limitada: ela se destina principalmente a proteger a soberania do Estado interceptado, e o indivíduo estaria protegido por essa notificação

Adicionalmente, o TJUE abordou outra questão relevante: a admissibilidade das provas obtidas na França por meio do registro do *EncroChat,* em conformidade com o artigo 14.º, n.º 7, da DOEI, que obriga a respeitar os direitos de defesa e a equidade na avaliação das provas obtidas por meio de uma DOEI.

Nesse sentido, o tribunal alemão questionou se seria compatível com o direito a um julgamento justo emitir uma OEI quando a integridade dos dados obtidos por meio dessa ordem «não pudesse ser verificada devido à confidencialidade dos elementos técnicos utilizados para a coleta de informações, o que poderia impedir a defesa de contestar efetivamente os dados no processo penal posterior» (parágrafo 83 da STJUE *EncroChat*). O TJUE respondeu que a questão da verificação da integridade dos dados não afeta a emissão da OEI, mas deve ser considerada pelo tribunal de julgamento no momento de avaliar as provas, de modo a garantir o direito a um processo equitativo (parágrafo 90). O tribunal nacional deve excluir provas quando a parte acusada não puder efetivamente contestar os dados ou quando essas provas influírem de forma decisiva na apreciação dos fatos.

Segue aqui o TJUE o critério já adotado na jurisprudência do TEDH[59] e em sua própria jurisprudência em matéria de retenção de dados[60], embora na jurisprudência sobre conservação de dados também

---

apenas na medida em que os dados fossem utilizados como prova no país interceptador (neste caso: França). Mesmo que tivesse sido violada a obrigação de notificação, o interesse do Estado no processamento prevaleceria sobre essa violação.

[59] Veja, entre outros, as SSTEDH *Bykov v. Rússia*, Appl. nº. 4378/02, de 10 de março de 2009, parágrafos 88-90; *Huseyn e Outros v. Azerbaijão*, Appl. nºs. 35485/05 e 3 mais de 26 de julho de 2011, parágrafo. 199, 200 e 211; *Murtazaliyeva v. Rússia* [GC], Appl. nº. 36658/05, de 18 de dezembro de 2018. *SA-Capital Oy v. Finlândia*, Appl. nº 5556/10, de 14 de fevereiro de 2019, parágrafo 78, *Kobiashvili v. Geórgia*, Appl. nº. 36416/06, de 14 de março de 2019, parágrafo 5

[60] SSTJUE WebMindLicenses, caso C-419/14, de 17 de dezembro de 2015; Processo penal contra H.K., caso C-746/18, de 2 de março de 2021; La Quadrature du Net a.o. c. Primeiro-Ministro e Ministro da Cultura, caso C-470/2 ("La Quadrature du Net II"), de 30 de abril de 2024; Procuradoria da República junto ao Tribunal de Bolzano, caso C-178/22, ("Bolzano"), de 30 de abril de 2024. Sobre este tema, veja os capítulos: MARTÍNEZ SANTOS, Antonio Martínez. Conservación, cesión y utilización con fines probatorios de

se faça referência à falta de conhecimentos específicos na matéria por parte do tribunal de julgamento, algo que é omitido no pronunciamento da sentença *EncroChat*.

Fica por esclarecer como deve ser interpretada essa causa de inadmissibilidade de prova definida pelo TJUE. O que significa concretamente poder «comentar eficazmente» sobre a prova?

Na matéria de obtenção de prova eletrônica, o direito de defesa gira em torno da possibilidade de verificar a legalidade, autenticidade, integridade e proporcionalidade da prova. Como isso se articula no caso de prova transnacional e, neste caso específico, em relação ao acesso massivo às comunicações realizado pelas autoridades francesas no âmbito de uma norma processual penal, mas que claramente ultrapassa o objeto do delito investigado? Como podem ser verificados os protocolos de acesso e conservação das comunicações interceptadas, quando nesse registro foi utilizada tecnologia informática e sistemas de descriptografia que, por motivos de segurança nacional, não podem ser compartilhados com a defesa no processo penal? Como pode ser verificada a integridade dos dados se não se pode acessar a totalidade deles? Comentar efetivamente implicaria um direito de acesso aos dados brutos?

Sem a intenção de analisar cada uma dessas questões, quero ressaltar aqui que o STJUE responde a algumas dessas questões, mas não sobre como deve ser articulado o direito de defesa em casos de prova eletrônica transnacional obtida por meio de um registro massivo de uma plataforma de comunicação criptografada.[61]

Neste ponto, é importante lembrar que o TEDH já declarou que o direito de acesso às fontes de prova — e, portanto, o direito de

---

los metadatos derivados de las comunicaciones electrónicas y digitales en el proceso penal. *In*: BACHMAIER WINTER, Lorena. (Coord.). *Prueba penal y derecho de defensa en la era digital*: Nuevos paradigmas y nuevos retos. Madri: Aranzadi, 2024; e LASAGNI, Giulia. Admisibilidad de pruebas en el procedimiento penal: Lecciones de la jurisprudencia del TJUE en materia de conservación de datos. *In*: BACHMAIER WINTER, Lorena. (Coord.). *Prueba penal y derecho de defensa en la era digital*: Nuevos paradigmas y nuevos retos. Madri: Aranzadi, 2024.

[61] Enquanto escreviam-se estas páginas, estavam pendentes no TEDH dois recursos relativos a EncroChat, *A.L. Lewis-Turner v. Francia* Appl. nº. 44715/20 y *E.J. Jarvis v. Francia*, Appl. Nº. 47930/21.

comentar efetivamente sobre as mesmas — não é um direito absoluto, e pode ser objeto de limitações. Afirma o TEDH que, em um processo penal, podem existir interesses contrapostos, como a segurança nacional ou a necessidade de manter em segredo os métodos de investigação policial, que poderiam justificar que as fontes de prova ou o modo de sua obtenção não sejam revelados integralmente. Portanto, ao avaliar o acesso às fontes de prova à luz do direito a um processo equitativo, esses interesses devem ser ponderados em relação aos direitos do acusado.[62] Aplicando isso ao caso *EncroChat,* o fato de a defesa não poder acessar a totalidade dos dados ou verificar o software utilizado no registro da plataforma não implicaria automaticamente uma violação do direito a um processo justo. Se o modo de proceder na obtenção ou na transmissão dessas provas suscitar dúvidas sobre a confiabilidade da prova, isso cabe ao tribunal de julgamento, e entra dentro de sua liberdade de apreciação.

3. *Mass surveillance* e análise de dados abertos: os desafios para o processo penal

Identificar indivíduos como "pessoas de interesse" com base no risco potencial de cometerem crimes, submetendo-os a vigilância contínua, transforma-os não apenas em fontes de informação, mas também, de certa forma, em objetos de prova, à medida que os dados obtidos dessa vigilância podem adquirir relevância probatória. Por meio de mecanismos de monitoramento ativados sem uma suspeita concreta e prévia de prática delituosa, mas baseados em perfis, no *predictive policing* e em programas de avaliação de riscos – conhecidos como *Automated Suspicion Algorithms* (ASAs) –, é possível coletar elementos probatórios contra essas pessoas.[63] Embora esse modo de proceder não seja uma novidade, o

[62] Sobre os princípios gerais dessa matéria, vid. *Jasper v. Reino Unido* [GC], Appl. nº. 27052/95, de 16 de fevereiro de 2000, parágrafo 52.

[63] Vid. RICH, Michael. Machine learning, automated suspicion, algorithms and the Fourth Amendment. *University of Pennsylvania Law Review*, v. 164, pp. 870-929, 2016; e também BRAYNE, Sarah. Algorithmic Suspicion and Big Data Searches: The Inadequacy of Law in the Digital Age. *In*: BRAYNE, Sarah. *Predict and Surveil*: Data Discretion and the Future of Policing. Oxford: Oxford University Press, 2020, pp. 118 ss.

problema atual reside no fato de que a *mass surveillance* aplicada a dados e comunicações com fins preventivos possibilita a criação de perfis de indivíduos potencialmente perigosos, submetendo-os a uma vigilância muito mais invasiva do que a vigilância física tradicional.

Ademais, a análise massiva de dados pode ser desencadeada sem a necessidade de demonstrar, perante uma autoridade judicial, a existência de uma suspeita específica sobre um indivíduo. Muitas vezes, basta uma avaliação de risco realizada por um algoritmo. Os ASAs são programas que analisam, de forma massiva, dados de indivíduos para determinar a existência de suspeitas potenciais. É sabido que grandes empresas prestadoras de serviços na internet vendem dados a empresas privadas, que os utilizam para monitorar o comportamento dos consumidores em suas campanhas de publicidade e marketing. Esses dados, somados às informações publicadas por usuários em redes sociais e aos dados mantidos por autoridades públicas[64] e *data brokers*, possibilitam a construção de perfis de comportamento e risco cada vez mais sofisticados. A utilização de inteligência artificial para analisar essa massa de dados dá origem aos ASAs, cujas análises fundamentam as políticas e ações das forças policiais e de outras agências de segurança. Assim, as forças policiais tornam-se clientes dos *data brokers*, adquirindo análises que identificam não apenas riscos potenciais, mas também indivíduos que podem ser classificados como suspeitos. Os ASAs, portanto, substituem os informantes e as tradicionais atividades de vigilância policial, ampliando exponencialmente seu alcance, mas sem que os juízes disponham de critérios claros para avaliar sua confiabilidade.[65]

Essa nova dinâmica altera profundamente os fundamentos para a abertura de investigações penais. Inicialmente, realiza-se uma avaliação de riscos por meio da análise de grandes volumes de dados. Com base nessa análise, identificam-se «pré-suspeitos», que, após a definição de seus perfis, podem ser classificados como «pessoas de interesse» e submetidos a uma

---

[64] Dentre as ferramentas que cita RICH, estão: *mass surveillance*, *data mining*, *intelligence-led policing technology*, *fusion centers*, *offender registries*, *social media surveillance*, *social network analysis*, *biometrics*.

[65] No mesmo sentido: RICH, Michael. Machine learning, automated suspicion, algorithms and the Fourth Amendment. *University of Pennsylvania Law Review*, v. 164, pp. 870-929, 2016, p. 908.

vigilância mais intensa para coleta de indícios ou provas. Uma vez obtidos esses indícios, os elementos que fundamentam uma suspeita concreta são apresentados à autoridade judicial para a expedição de ordens que autorizem medidas processuais, como interceptação de comunicações ou acesso a dados digitais, cujos resultados podem ser admitidos como provas no processo. Essa prática suscita preocupações, pois permite a abertura de investigações invasivas com base em análises massivas de dados para fins de segurança, mesmo sem uma suspeita prévia concreta.

Não se afirma, com isso, que tal atuação seja generalizada ou que os serviços de inteligência estejam agindo à margem da lei. Nas democracias europeias, há indícios de que, mesmo quando capazes de realizar coleta massiva de dados, os serviços de inteligência enfrentam limitações de tempo, recursos e prioridades, operando de forma geral dentro dos limites legais e com base em critérios objetivos. A vigilância direcionada (*targeted surveillance*), por sua vez, é submetida a controles rigorosos e diversos níveis de supervisão. Contudo, sistemas de vigilância que carecem de transparência e publicidade devem ser submetidos a escrutínio rigoroso, pois a ausência de controles adequados no processo de obtenção de inteligência e na seleção de alvos pode comprometer as salvaguardas do sistema de justiça penal. A conquista de direitos fundamentais no âmbito do processo penal pode ser ameaçada pela *mass surveillance* e pela dinâmica do "Big Brother".

A interceptação massiva de comunicações e a retenção dos dados obtidos representam uma violação significativa ao direito à privacidade, mesmo que esses dados não sejam analisados de forma concreta.[66] A mera existência de sistemas de vigilância massiva de metadados de comuni-

[66] Isto é algo já indiscutível. A esse respeito, veja, por exemplo, a sentença do Tribunal de Justiça da União Europeia (TJUE) GC de 8 de abril de 2014, *Digital Rights Ireland v. Ministro das Comunicações, Marinha e Recursos Naturais e Outros e Kärntner Landesregierung e Outros* (casos C-293/12 e C-594/12), na qual o TJUE declarou que a Diretiva EU 2006/24/CE era incompatível com o princípio da proporcionalidade e, portanto, a legislação nacional que prevê a conservação de dados de comunicações deve ser considerada também contrária aos artigos 7 e 8 da Carta dos Direitos Fundamentais da UE, a menos que essa legislação seja complementada com suficientes garantias sobre o acesso aos dados. Sobre esta sentença, vid., entre outros: OJANEN, Tuomas. Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. *In*: COLE, David D.; FABBRINI,

cação é um assalto à nossa privacidade que afeta o comportamento dos indivíduos, exerce um efeito inibidor sobre a liberdade de expressão[67] e compromete o desenvolvimento pleno da vida privada. Além disso, os riscos de abuso associados à vigilância massiva representam uma ameaça não apenas aos direitos individuais, mas também à preservação da democracia e do Estado de Direito.[68]

Naturalmente, os riscos são ainda maiores quando, devido aos critérios de seleção aplicados, determinadas pessoas se tornam alvos e o conteúdo de suas comunicações é monitorado e analisado. Não devemos esquecer que esses mecanismos são projetados para detectar ameaças e, portanto, são ativados diante de alvos desconhecidos; ou seja, podem afetar qualquer cidadão, mesmo que não exista suspeita prévia sobre ninguém em particular. Este é precisamente o fator que levou o TJUE a questionar a proporcionalidade das técnicas que permitem intervir e armazenar todas as comunicações para, posteriormente, selecionar aquelas que merecem ser submetidas a uma análise mais aprofundada.

Apenas se discute a utilidade das interceptações em massa para as operações de segurança, e a abordagem proativa para identificar ameaças à segurança nacional se houver um fim legítimo e razoável.[69] No entanto, considerando que, ao contrário de uma investigação criminal, tal invasão de nossa privacidade não tem um objetivo específico e opera com base em critérios de seleção (não está, portanto, vinculada a uma suspeita prévia), é compreensível questionar se ela respeita o princípio da proporcionali-

---

Federico; SCHULHOFER, Stephen. (Ed.). *Surveillance, Privacy and Transatlantic Relations*. Oxford: Hart Publishing, 2017, pp. 13-30.

67 Sobre o «chilling effect», vide o Informe do Conselho da Europa (CoE) do Comissionário para Direitos Humanos «Democratic and effective oversight of national security services», de maio de 2015. Disponível em: https://rm.coe.int/1680487770, p. 25. No mesmo sentido, destacando a escassez de estudos empíricos sobre o tema: MURRAY, Daragh; FUSSEY, Pete. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*, v. 52, n. 1, pp. 31-60, 2019, p. 43-47.

68 Vid. Informe do Conselho da Europa «Democratic and effective oversight of national security services», cit., p. 26.

69 Assim apontou a Comissão de Veneza em seu Informe «On the Democratic Oversight of Signals Intelligence Agencies», de 15 de dezembro de 2015, CDL-AD(2015)011, p. 47.

dade, e também se o critério de proporcionalidade nesses casos deveria ser diferente do que se aplica no processo penal.

São dois os elementos básicos que diferenciam claramente os níveis de garantias no processo penal e no sistema de prevenção voltado para a segurança: a exigência do requisito de suspeita prévia no âmbito da investigação penal e a necessidade de que as medidas de investigação e obtenção de provas que impliquem uma intrusão nos direitos fundamentais exijam, como regra, uma autorização judicial prévia. Essa autorização, como é sabido, serve não apenas para controlar a legalidade da medida e os critérios de proporcionalidade, mas também para verificar se existem indícios ou suspeitas suficientes contra uma pessoa determinada. Obviamente, o controle judicial continua operando de forma ordinária em todas as etapas do processo, até mesmo posteriormente, por meio dos mecanismos para questionar a admissibilidade e a licitude da prova.

No caso da "non-targeted surveillance" (vigilância não direcionada), o enfoque difere desse esquema, pois não há uma decisão judicial inicial baseada em suspeitas prévias contra indivíduos específicos, simplesmente porque não há um objetivo específico, já que nenhum suspeito é identificado[70]. Como afirmou o TEDH, "a interceptação massiva, por definição, não tem um objetivo específico, e exigir uma 'suspeita razoável' tornaria impossível o funcionamento de tal esquema".[71] De maneira semelhante, o requisito de "notificação posterior" pressupõe a existência de objetivos de vigilância claramente definidos, o que não ocorre em um regime de interceptação massiva.[72]

Poder-se-ia argumentar que a vigilância massiva não tem como finalidade colher provas para fins penais, pois se concentra na prevenção. Mas será que isso significa que a expectativa de privacidade não é aplicável? E se, finalmente, esses dados forem utilizados para desencadear uma investigação criminal e, portanto, forem justamente os dados que permitem estabelecer a «suspeita razoável» e obter a ordem judicial para obter provas, não estaríamos diante de um círculo vicioso? Primeiro, acessam-se os dados de forma massiva, depois filtram-se e realiza-se uma

---

70 Vide. *Big Brother Watch*, parágrafo 317.

71 Ibid., parágrafo 317.

72 Ibid.

análise desses *big data* e, com base nessa análise —feita por algoritmos—, estabelece-se o que nos Estados Unidos se denomina "probable cause"[73] (causa provável). Estabelecido assim o motivo fundado ou a suspeita razoável, já é possível solicitar a ordem judicial para acessar dados e comunicações, os quais poderão ser utilizados como prova no processo. Não seria esta uma forma de burlar as garantias processuais destinadas precisamente a evitar que as pessoas sejam submetidas a medidas intrusivas quando não existe uma suspeita razoável?

O uso dos algoritmos de avaliação de suspeitas que já está sendo feito em certos países apenas confirma esses riscos.

4. Novo paradigma, novas garantias?

O tratamento massivo de dados por meio de algoritmos e inteligência artificial demanda não apenas um fortalecimento das garantias processuais existentes no modelo processual liberal, mas também, possivelmente, a criação de novos mecanismos de proteção ao cidadão. Atualmente, qualquer pessoa pode ser submetida a uma inspeção massiva de seus dados pessoais, uma vez que, com base apenas em informações de fontes abertas (*open source*), é possível traçar um perfil detalhado de praticamente todos os aspectos de sua vida privada. Caso, de acordo com o algoritmo utilizado, um indivíduo seja categorizado como "pessoa de interesse", basta um pequeno passo para que esses mesmos dados sirvam como fundamento para a instauração de um processo penal, sua apresentação como prova e, eventualmente, sua aceitação para justificar a condenação penal do indivíduo.

Tal realidade pode exigir uma reconsideração do sistema de garantias processuais, tradicionalmente centradas no modelo liberal, que enfatiza a publicidade e oralidade da fase de julgamento, momento no qual o contraditório atinge sua máxima expressão na prática probatória. Contudo, torna-se cada vez mais difícil questionar a licitude e a

[73] Sobre o requisito da *probable cause* na Constituição norte-americana, ver. BACHMAIER WINTER, Lorena. *Probable cause* y la Cuarta Enmienda de la Constitución estadounidense: una garantía tan imprecisa como necesaria. *Quaestio Facti*, v. 4, n. 1, pp. 191-220, 2023, p. 195 e ss.

confiabilidade dos dados eletrônicos obtidos, especialmente quando não se tem acesso ao software utilizado nem ao entendimento do algoritmo empregado na análise e busca desses dados. Além disso, em muitos sistemas processuais, o julgamento oral tornou-se uma fase quase excepcional, acionada somente quando não há acordo entre as partes. E, quando os dados obtidos por vigilância ou rastreamento massivo são contundentes, a defesa frequentemente opta pelo "mal menor", ou seja, uma sentença negociada, em vez de enfrentar um julgamento oral cujo foco pode estar excessivamente voltado para a análise pericial informática.

Nesse contexto, talvez fosse pertinente questionar se não seria adequado reconsiderar o sistema de garantias e reforçar os pressupostos que podem levar à abertura de uma investigação penal contra um indivíduo específico. Refiro-me a abrir um debate mais profundo sobre o significado que adquire, em um mundo de vigilância massiva e de conservação massiva de dados, o fato de que basta consultar os dados existentes sobre qualquer indivíduo — ou empresa — para fundamentar uma suspeita que possibilite transformar esses dados em provas incriminatórias. Se com base em uma quantidade avassaladora de dados eletrônicos já existentes sobre cada cidadão pode-se elaborar uma "suspeita fundada", não seria necessário antecipar as garantias processuais para esse momento, em vez de centrá-las no desenvolvimento de um julgamento oral, que provavelmente não ocorrerá? Não seria oportuno repensar o papel dos conceitos de «indícios racionais» ou «suspeitas fundadas», ou, para usar o termo da Quarta Emenda norte-americana, a "probable cause"?

Já tive a oportunidade de analisar em detalhes o conceito de "causa provável" na Constituição norte-americana em relação aos conceitos análogos nos processos penais europeus, como o "Tatverdacht" do art. 102 do Código de Processo Penal alemão, ou os "indizi criminali" ou o "motivo fondato" do art. 247 do Código de Processo Penal italiano, ou as "suspeitas razoáveis" dos arts. 543, 579 ou 588bis e ter da Lei de Processo Penal espanhola.[74] Sem intenção de reiterar aqui o que já foi expresso nesses e outros trabalhos, acredito ser conveniente lembrar

[74] BACHMAIER WINTER, Lorena. Probable cause y la Cuarta Enmienda de la Constitución estadounidense: una garantía tan imprecisa como necesaria. *Quaestio Facti*, v. 4, n. 1, pp. 191-220, 2023.

alguns aspectos desses conceitos. Em primeiro lugar, deve-se destacar sua vaguidade, pois não contêm um padrão de prova que possa ser definido, nem sequer de forma aproximada. A Suprema Corte norte-americana reconhece que não é fácil determinar esse padrão fundamental para a proteção do indivíduo contra intromissões do Estado em sua liberdade e privacidade, o que constitui uma garantia fundamental dos princípios do Estado de direito. Trata-se de algo mais do que uma simples suspeita e algo menos do que a situação de «além de toda dúvida razoável», que é o padrão probatório para fundamentar uma sentença condenatória;[75] o determinante é que exista «um motivo razoável para a convicção ou para a culpabilidade» (*a reasonable ground for belief or guil*t)[76]. Portanto, estamos diante de um termo ambíguo, que faz referência a um cálculo de probabilidades, a uma probabilidade não quantitativa ou estatística que se move dentro de uma faixa variável. A conclusão é que o termo «provável» não nos dá um parâmetro concreto sobre qual é o limite que permite adotar medidas restritivas de direitos fundamentais com fins de investigação penal contra um indivíduo;[77] a própria Suprema Corte norte-americana o considera um padrão impreciso «baseado no senso comum»[78]. Esse conceito se diferencia do termo ou padrão de «suspeita razoável», que exige um grau menor de suspeita; seria como um estágio anterior à "causa provável", embora sejam termos fluidos: o primeiro faz referência a uma mera possibilidade e o segundo a uma probabilidade. Mas como já destaquei em outro lugar:

> «Traçar uma distinção clara na prática entre ambos os padrões não é fácil, embora suas repercussões jurídicas sejam claramente diferentes. Em primeiro lugar, porque não é muito claro o que se quer dizer com "possibilidade". Em sentido estrito, algo é possível apenas quando não é impossível, então é possível que um fato tenha ocorrido, embora não haja nenhum dado que o comprove. E em um sentido mais amplo, possível é sinônimo de provável, de

---

[75] *Brinegar v. United Sates*, 388 U.S. 160, 174 (1949). Ibid., p. 203

[76] *Brinegar v. United Sates,* p. 174.

[77] BACHMAIER WINTER, Lorena. Probable cause y la Cuarta Enmienda de la Constitución estadounidense: una garantía tan imprecisa como necesaria. *Quaestio Facti*, v. 4, n. 1, pp. 191-220, 2023, p. 203.

[78] *Steel v. United States*, 267 U.S. 498, 504-505 (1925).

> forma que, interpretado assim, não se distinguiria a «reasonable suspicion" da "probable cause"; a não ser que se fixe a diferença no grau de probabilidade (não matemática), mas então seria necessário alguma concretização desse grau, além da distinção entre possibilidade e probabilidade.»[79]

O requisito de "probable cause" também é o que se aplica atualmente ao acesso e apreensão de dados eletrônicos.[80]

No âmbito europeu, talvez não seja errado afirmar que o padrão de «suspeita razoável», definido pelo TEDH para realizar uma detenção, equivaleria *mutatis mutandis* ao padrão de "probable cause". Mas não encontramos uma definição desse padrão em relação às interferências na esfera da privacidade, pois ao avaliar se são atendidos os requisitos do art. 8º da CEDH, o TEDH parte, geralmente, da premissa de que já foi analisado o limiar de «suspeita razoável» que permite a abertura de um processo penal. No contexto do processo penal espanhol, o art. 546 exige que haja indícios racionais da prática de um crime ou, no caso da medida de entrada e registro, indícios de que o suspeito ou elementos de prova possam ser encontrados no local.[81]

No entanto, para iniciar um processo penal, basta a mera probabilidade — no sentido de possibilidade — de que um fato criminoso tenha sido cometido. E, como assinalou o Tribunal Supremo espanhol, para isso não é necessário que se constate indícios racionais de criminalidade; é suficiente a «notitia criminis sustentada por uma suspeita fundada em circunstâncias objetivas de que um crime tenha podido ser cometido, esteja sendo cometido ou será cometido»[82].

---

[79] Tradução livre. Ibid. p. 205.

[80] *Riley v. California*, 573 U.S. 373 (2014). E posteriormente, em *Carpenter v. United States*, 585 U.S.__ (2018), a Suprema Corte determinou que, para obter os dados de geolocalização de um telefone móvel de uma empresa de telecomunicações, era necessário comprovar causa provável, pois esses dados afetam o direito à privacidade protegido pela Quarta Emenda.

[81] Vid. STS153/2015, de 18 de março.

[82] STS 32/1995, de 4 de dezembro de 1995. Ibid., p. 215. Sobre o pressuposto da notitia criminis e o julgamento sobre a mesma para a instauração do processo penal e sua relação com os riscos da abertura de causas gerais sem

Diante da indeterminação do padrão — «suspeita razoável» — para iniciar um processo penal, assim como para adotar medidas de investigação penal que afetem os direitos fundamentais (embora essas devam ser submetidas aos critérios de necessidade, adequação e proporcionalidade), a ativação de um algoritmo para identificar/elaborar, por meio do processamento massivo de dados, poderia estabelecer esses indícios ou suspeitas praticamente sobre qualquer indivíduo. Se, além disso, for possível dispensar a «suspeita razoável» no âmbito da prevenção, isso significa que o Estado pode coletar informações e dados eletrônicos relativos a qualquer sujeito e, uma vez processados, estabelecer o critério de "probable cause" para cumprir os padrões exigidos para a investigação criminal no processo penal.

Dito de outra forma, o padrão para ativar medidas de investigação baseadas no processamento de Big Data, ou no acesso a bancos de dados nos quais se conservam indiscriminadamente dados pessoais de todos os usuários, deve ser reforçado se quisermos continuar mantendo as tradicionais garantias do processo penal.

Ainda poderíamos confiar que se apliquem regras de exclusão de prova a esses dados obtidos previamente a um processo penal, ou que sejam declaradas nulas as provas obtidas com base em «suspeitas razoáveis» oriundas de uma vigilância massiva. Mas não é o que acontece: primeiro, porque são poucos os ordenamentos jurídicos que aplicam regras estritas de exclusão de provas;[83] e segundo, porque para condenar

---

objeto concreto, ver. AGUILERA MORALES, Marien. *Proceso penal y causa general*: La inquisitio generalis en el Derecho español. Madri: Aranzadi, 2008, pp. 64 e ss.

[83] Sobre as diferenças com relação às regras de exclusão de provas, ver, entre outros, THAMAN, Stephen C. Balancing Truth Against Human Rights: A Theory of Modern Exclusionary Rules. *In*: THAMAN, Stephen C. (Ed.). *Exclusionary Rules in Comparative Law*. Londres: Springer, 2013, pp. 403-446. Este autor destaca que apenas algumas jurisdições «particularmente aquelas que surgiram recentemente em regimes totalitários ou autoritários» excluíram toda ponderação com relação ao uso de provas obtidas ilicitamente, p. 441. Ver também GLESS, Sabine; RICHTER, Thomas. (Eds.), *Do exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules*. Londres: Springer, 2019. Mais recentemente, BACHMAIER WINTER, Lorena; SALIMI, Farsam. (Eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*. Oxford: Hart

já não é necessário apresentar provas incriminatórias em um debate contraditório, considerando que cerca de 60% das condenações na Europa se baseiam em acordos de conformidade (nos Estados Unidos, esse percentual chega a mais de 95%). Será suficiente confrontar o acusado com toda a bateria de dados disponíveis pela acusação para convencê-lo a aceitar a condenação. E esses dados, cuja retenção ainda não está, na prática, limitada em muitos países[84], e cujo acesso na maioria dos casos foi consentido pelos próprios usuários das redes, serão um elemento convincente para dobrar a vontade do acusado e fazê-lo renunciar ao julgamento, talvez em troca de uma redução da pena.

A título de conclusão

Diante desse panorama inquietante, apresento três breves conclusões. A primeira — embora óbvia, mas ainda assim essencial — é a necessidade de continuar lutando pela proteção das garantias processuais. A segunda é a urgência de redefinir os requisitos que permitem ao Estado acessar e processar nossos dados com fins preventivos, assim como estabelecer controles mais rigorosos sobre o critério de «suspeita razoável». Em um sistema eminentemente preventivo e tecnológico, tal critério pode acabar sendo a única barreira efetiva para impedir a abertura de investigações penais que convertam dados previamente obtidos em provas incriminatórias. Por fim, a terceira conclusão reconhece que, embora a proteção de direitos fundamentais tradicionalmente tenha se voltado contra o poder avassalador do Estado, o poder das empresas privadas — particularmente as que prestam serviços de internet e gestão de dados — exige uma reavaliação de seu papel na investigação penal.

Publishing, 2024; e o informativo «Study on cross-border use of evidence in criminal proceedings» de março de 2022, responsável pela Comissão Europeia a Milieu. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/2815b94e-9165-11ed-b508-01aa75ed71a1/language-en.

84 Assim, por exemplo, na Espanha, onde a STJUE de 8 abril 2014, *Digital Rights Ireland and Seitlinger and others* (casos C-293/12 e C-594/12) («*Digital Rights Ireland*»), não teve praticamente nenhum impacto quanto à limitação da conservação dos dados. Ver a STS 3436/2015 de 7 de julho 2015; o STS 5140/2015 de 23 novembro 2015.

O debate sobre sua responsabilidade como garantidoras da privacidade dos usuários, além das obrigações previstas nas legislações de proteção de dados, e seu papel como colaboradoras nas investigações penais, precisa ser aprofundado.

Em relação ao uso de sistemas de comunicação criptografados, o TEDH destacou expressamente que o mero fato de baixar ou usar um sistema de comunicação criptografado, ou até mesmo o uso de qualquer outro método para proteger a natureza privada das mensagens trocadas, não pode, por si só, constituir um crime, nem tampouco pode ser considerado automaticamente um elemento probatório capaz de convencer um observador objetivo de que se está realizando uma atividade ilegal ou cometendo um crime.[85] No entanto, como vimos, isso não impediu que, na prática, se estabelecesse, como uma suspeita razoável para acessar o sistema, o fato de que alguns — poucos ou muitos — criminosos utilizam essas plataformas de comunicação. De acordo com o TEDH, o uso dessas plataformas é legal e faz parte do direito à privacidade de comunicar com quem cada pessoa desejar e através do sistema legal que escolher, mas isso não impede que o uso de tais plataformas gere desconfiança nas autoridades que atuam na área de inteligência ou na investigação criminal. Portanto, esse uso é considerado um elemento que abre a porta para decifrar o sistema e acessar as comunicações dos usuários.

Diante dessa situação, a defesa só pode invocar seu direito de "comentar efetivamente" sobre as provas obtidas dessa maneira, o que, como vimos anteriormente, não necessariamente implica o direito de revisar a integridade dos dados interceptados ou de conhecer o software utilizado para acessar as suas comunicações. Diante desse desequilíbrio entre os poderes do Estado de interferir em nossa esfera de privacidade e os direitos do usuário (suspeito, pré-suspeito ou simples usuário de um sistema criptografado), só pode ser invocado o cumprimento dos protocolos adequados para garantir a autenticidade, integridade e proporcionalidade

[85] STEDH *Akgün v. Turquía,* Appl. nº. 19699/18, de 20 de julho 2021, parágrafo 160: «que não existia nenhum elemento de prova apto a persuadir um observador objetivo de que ele poderia ter cometido o crime do qual foi acusado. Em particular, o interessado alega que a utilização que fez do ByLock não poderia justificar sua prisão».

das provas eletrônicas. Por isso, hoje mais do que nunca, o direito de defesa deve ser fortalecido, também com ferramentas digitais e software adequado, pois, caso contrário, não será possível cumprir o princípio do contraditório como sistema de formação da prova. Os tribunais devem estar preparados para conceder à defesa as possibilidades de não apenas verificar como se teve acesso à prova digital, mas também, como aponta Rich, para questionar a confiabilidade dos *Automated Suspicion Algorithms* (Algoritmos de Suspeita Automatizada) e, se for o caso, excluir a prova obtida com base nesses algoritmos.[86]

Em todo caso, a existência de uma suspeita prévia para ativar medidas notavelmente intrusivas em nossa esfera de privacidade não parece ser um pressuposto absoluto que nos proteja contra as vigilâncias massivas. Quando a prevenção se dilui e se confunde com a repressão do crime, é muito difícil estabelecer fronteiras entre a informação de inteligência e a obtenção de prova penal, especialmente no âmbito da proteção de dados e do acesso às comunicações. Nisso, concordo com o que afirmaram, em seu voto particular, os juízes Lemmens, Vehabović e Bošnjak: «É provável que, em um futuro não tão distante, ao explorar esse terreno em particular, a investigação criminal possa passar da vigilância direcionada para a interceptação massiva de dados»[87]. E me pergunto: não é isso o que estamos vendo no caso *EncroChat?*

Essa tradução mantém os detalhes e as nuances do texto original, abordando o contexto legal e as questões de vigilância e privacidade no uso de tecnologia criptografada, especialmente no que se refere ao direito de defesa e ao controle judicial de provas obtidas em investigações de segurança.

---

[86] RICH, Michael. Machine learning, automated suspicion, algorithms and the Fourth Amendment. *University of Pennsylvania Law Review*, v. 164, pp. 870-929, 2016, p. 929: «os Tribunais devem estar preparados para fornecer orientações e condições aos acusados para questionamento da credibilidade dos ASA e para excluir provas obtidas com base em ASA não certificados ou em ASA cuja confiabilidade não for provada».

[87] Voto dissidente conjunto parcialmente concomitante com a decisão do TEDH *Big Brother Watch and others v. Reino Unido*, *Grand Chamber*, 25 de maio 2021, parágrafo 29.

Referências

AGUILERA MORALES, Marien. *Proceso penal y causa general*: La inquisitio generalis en el Derecho español. Madri: Aranzadi, 2008.

ALCALÁ ZAMORA, Niceto. Liberalismo y autoritarismo en el proceso. *Boletin Mexicano de Derecho Comparado*, v. 1, n. 2-3, pp. 559-600, 1968.

ASHWORTH, Andrew; ZEDNER, Lucia. *Preventive Justice*. Oxford: Oxford University Press, 2014.

BACHMAIER WINTER, Lorena; SALIMI, Farsam. (Eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*. Oxford: Hart Publishing, 2024.

BACHMAIER WINTER, Lorena. Countering Terrorism: Suspects without suspicion and (Pre-)Suspects under surveillance. *In*: SIEBER, Ulrich; MITSILEGAS, Valsamis; MYLONOPOLUS, Christos; KNUST, Nandor. (Eds.). *Alternative systems of Crime Control*. Berlim: Duncker & Humblot, 2018.

BACHMAIER WINTER, Lorena. Información de inteligencia y proceso penal. *In*: BACHMAIER WINTER, Lorena. (Coord.). *Terrorismo, proceso penal y derechos fundamentales*. Madri: Marcial Pons, 2012.

BACHMAIER WINTER, Lorena. Mutual recognition and cross-border interception of communications: the way ahead for the European Investigation Order. *In*: BRIÈRE, Chloé; WEYEMBERGH, Anne. (Ed.). *The needed balances in EU Criminal Law*: Past, present and future. Oxford: Hart Publising, 2017, pp. 313-336.

BACHMAIER WINTER, Lorena. Probable cause y la Cuarta Enmienda de la Constitución estadounidense: una garantía tan imprecisa como necesaria. *Quaestio Facti*, v. 4, n. 1, pp. 191-220, 2023.

BACHMAIER WINTER, Lorena. Proportionality, surveillance and criminal investigation: Strasbourg Court facing Big Brother. *In*: BILLIS, Emmanouil; KNUST, Nandor; RUI, Jon Petter. (Ed.). *The Principle of Proportionality in Crime Control and Criminal Justice*. Oxford: Hart Publising, 2021.

BILCHITZ, David. The Right to Privacy, Surveillance and the Global Obligations of Corporations. *In*: COLE, David D.; FABBRINI, Federico; SCHULHOFER, Stephen. (Eds.) *Surveillance, Privacy and Trans-Atlantic Relations*: Hart Studies in Security and Justice. Dublin: Bloomsbury Publishing, 2017.

BRAYNE, Sarah. Algorithmic Suspicion and Big Data Searches: The Inadequacy of Law in the Digital Age. *In*: BRAYNE, Sarah. *Predict and Surveil*: Data Discretion and the Future of Policing. Oxford: Oxford University Press, 2020.

BRAYNE, Sarah. *Predict and Surveil*: Data Discretion and the Future of Policing. Oxford: Oxford University Press, 2020.

CAMERON, Iain. *National Security and the European Convention on Human Rights*. Haia: Kluwer Law, 2000.

DERENCINOVIC, Devor, GETOS, Anna-Maria. Cooperation of law enforcement and intelligence agencies in prevention and suppression of terrorism. European perspective. *Revue internationale de droit pénal*, v. 78, pp. 79-112, 2007.

GALISON, Peter; MINOW, Martha. Our Privacy, Ourselves in the Age of Technological Intrusions. *In*: ASHBY WILSON, Richard. (Ed.). *Human Rights in the 'War on Terror'*. Cambridge: Cambridge University Press, 2005.

GALLI, Francesca. The freezing of terrorists' assets: preventive purpose with a punitive effect. *In*: GALLI, Francesca; WEYEMBERGH, Anne. (Ed.). *Do labels still matter*? Blurring boundaries between administrative and criminal law. The influence of the EU. Bruxelas: Editions de l'Université de Bruxelles, 2014.

GLESS, Sabine; RICHTER, Thomas. (Eds.), *Do exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules*. Londres: Springer, 2019.

HIRSCH, Marianne F. H. Terrorism Causing a Shifting Responsibility in Criminal Pre-Trial Investigation: from Repression to Prevention. *In*: HIRSCH, Marianne F. H. et al. (Ed.). *Shifting Responsibilities in Criminal Justice*. Haia: Eleven International Publishing, 2012.

LASAGNI, Giulia. Admisibilidad de pruebas en el procedimiento penal: Lecciones de la jurisprudencia del TJUE en materia de conservación de datos. *In*: BACHMAIER WINTER, Lorena. (Coord.). *Prueba penal y derecho de defensa en la era digital*: Nuevos paradigmas y nuevos retos. Madri: Aranzadi, 2024.

LINDEMAN, Joep; LUCHTMAN, Michiel; VAN TOOR, Dave. Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair-Trial Rights in the Netherlands. *In*: BACHMAIER WINTER, Lorena; SALIMI, Farsam. (Ed.) *Admissibility of Evidence in EU Cross-Border Criminal Proceedings*: Electronic Evidence, Efficiency and Fair Trial Rights. Oxford: Hart Publishing, 2024.

MARTÍN MORALES, Ricardo. El principio constitucional de intervención indiciaria. *Revista de la Facultad de Derecho de la Universidad de Granada*, n. 2, pp. 341-506, 1999.

MARTÍNEZ SANTOS, Antonio Martínez. Conservación, cesión y utilización con fines probatorios de los metadatos derivados de las comunicaciones electrónicas

y digitales en el proceso penal. *In*: BACHMAIER WINTER, Lorena. (Coord.). *Prueba penal y derecho de defensa en la era digital*: Nuevos paradigmas y nuevos retos. Madri: Aranzadi, 2024.

MITSILEGAS, Valsamis. The Security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law. *In*: CARRERA, Sergio; MITSILEGAS, Valsamis. (Ed.). *Constitutionalising the Security Union*. Effectiveness, Rule of Law and Rights in Countering Terrorism. Bruxelas: CEPS, 2017.

MURRAY, Daragh; FUSSEY, Pete. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*, v. 52, n. 1, pp. 31-60, 2019.

OERLEMANN Jan-Jaap; VAN TOOR, Dave. Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law and Criminal Justice*, v. 30, n. 3-4, pp. 309-328, 2022.

OJANEN, Tuomas. Administrative counter-terrorism measures – a strategy to circumvent human rights in the fight against terrorism?. *In*: COLE, David; FABBRINI, Federico; VEDASCHI, Arianna. (Ed.). *Secrecy, National Security and the Vindication of Constitutional Law*. Cheltenham: Edward Elgar Publishing Limited, 2013.

OJANEN, Tuomas. Rights-based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. *In*: COLE, David D.; FABBRINI, Federico; SCHULHOFER, Stephen. (Ed.). *Surveillance, Privacy and Transatlantic Relations*. Oxford: Hart Publishing, 2017

RADEMACHER, Timo. Predictive Policing im deutschen Polizeirecht. *Archiv des öffentlichen Rechts*, v. 142, n. 3, pp. 366–416, 2017.

RATNER, Steven R. Corporations and Human Rights: A Theory of Legal Responsibility. *Yale Law Journal*, v. 111, n. 3, pp. 443-545, 2001.

RICH, Michael. Machine learning, automated suspicion, algorithms and the Fourth Amendment. *University of Pennsylvania Law Review*, v. 164, pp. 870-929, 2016.

SIEBER, Ulrich. Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt: eine Analyse der Vorfeldtatbestände im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten". *Neue Zeitschrift für Strafrecht*, v. 29, n. 7, pp. 353-364, 2009.

SIEBER, Ulrich. Risk prevention by means of criminal law – On the legitimacy of anticipatory offenses in Germany's recently enacted counter-terrorism law. *In*: GALLI, Francesca; WEYEMBERGH, Anne. (Eds.), *EU counter-terrorism offences:*

What impact on national legislation and case-law?. Bruxelas: Editions de l'Université de Bruxelles, Bruselas, 2012.

THAMAN, Stephen C. Balancing Truth Against Human Rights: A Theory of Modern Exclusionary Rules. *In*: THAMAN, Stephen C. (Ed.). *Exclusionary Rules in Comparative Law*. Londres: Springer, 2013.

WAHL, Thomas. Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren. *Zeitschrift* für *Internationale Strafrechtsdogmatik*, v. 7–8, pp. 452-461, 2021.

WESTIN, Alan. *Privacy and Freedom*. Nova Iorque: Atheneum, 1967.

Authorship information

Lorena Bachmaier Winter. Professora Catedrática de Direito Processual da Universidade Complutense de Madrid, Espanha. Doutora em Direito. l.bachmaier@der.ucm.es

Additional information and author's declarations (*scientific integrity*)

Acknowledgement: I want to express my sincere gratitude to Fernanda Vilares e Luiz Eduardo Cani for the translation into Portuguese of this article and to Prof. Dr. Vinicius Gomes de Vasconcellos for its final revision.

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

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

Declaration of originality: This article is a revised and updated translation of a prior article published in Spanish: "La lucha por las garantías procesales y el cambio de paradigma en materia de prueba: del proceso penal liberal a la mass surveillance", L. Bachmaier Winter (ed.), *Prueba penal y derecho de defensa en la era digital. Nuevos paradigmas y nuevos retos*, Aranzadi, Cizur Menor, 2024, pp. 21-64. The author assures that the text here published in Portuguese has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; she also attests that there is no third party plagiarism or self-plagiarism.

Editorial process dates (https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 12/11/2024
- Editorial review and plagiarism check: 10/12/2024
- Final version: 07/02/2025
- Final editorial decision: 08/02/2025

Editorial team

- Editor-in-chief: 1 (VGV)

How to cite (ABNT Brazil):

BACHMAIER WINTER, Lorena. A luta pelas garantias do devido processo e a mudança de paradigma na teoria da prova: do liberalismo à *mass surveillance* no processo penal europeu. *Revista Brasileira de Direito Processual Penal*, vol. 11, n. 1, e1164, jan./abr. 2025. https://doi.org/10.22197/rbdpp.v11i1.1164