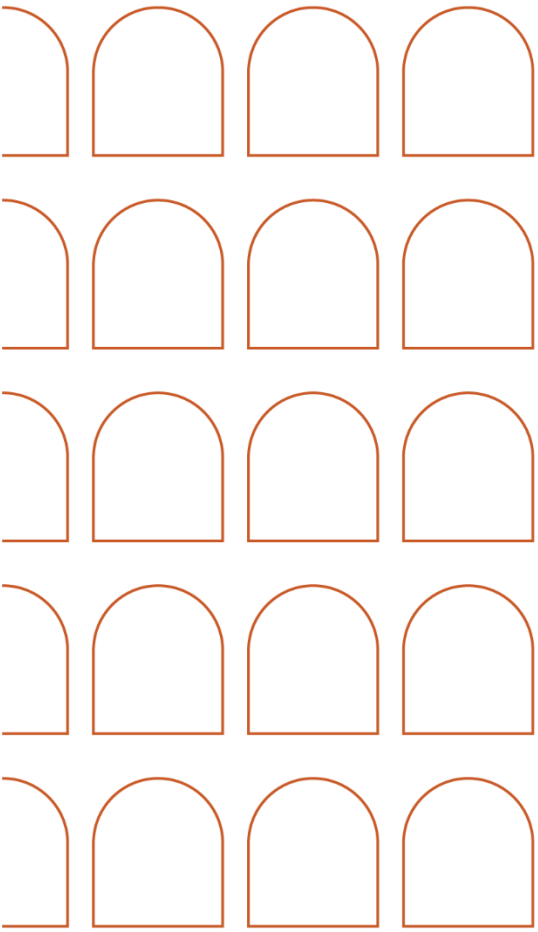
EUI DEPARTMENT OF LAW



LAW 2026/11
Department of Law

# WORKING PAPER

## National Security as Exception: The European Court of Human Rights and the Proceduralisation of Privacy in the Age of Mass Surveillance

Sophie Duroy and Martin Scheinin

European University Institute

**Department of Law**

# National Security as Exception: The European Court of Human Rights and the Proceduralisation of Privacy in the Age of Mass Surveillance

Sophie Duroy and Martin Scheinin

LAW Working Paper 2026/11

ISSN 1725-6739



Published in June 2026 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu



With the support of the Erasmus+ Programme of the European Union

The European Commission supports the EUI through the European Union budget. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.

## Abstract

This paper critically analyses European Court of Human Rights jurisprudence on bulk data collection, situating it within the Court's broader turn to proceduralism. We argue that, in cases concerning mass surveillance, the Court has effectively abandoned structured proportionality review and transformed national security from a *prima facie* legitimate aim into a *de facto* exception to Article 8. Placing this caselaw in the long shadow of 9/11 and the Court's legitimacy concerns, we assess its coherence and theoretical limitations against foundational principles of international human rights law. We then trace the detrimental consequences of the Court's proceduralist approach for the EU legal order, surveillance methods legalised by states, and the right to privacy. However, through the Court's judgment in *Podchasov* v. *Russia* (2024), the paper also argues for the recognition and functioning of an inviolable essential core of Article 8 as regards privacy, allowing for cautiously optimistic conclusions concerning a viable alternative to proceduralism.

The British Academy funded the research of Martin Scheinin (grant no. BAR00550-BA00.01).

An earlier version of this paper was presented at the 2024 Workshop of the Research Group on Constitutional Responses to Terrorism, International Association of Constitutional Law; at the British Academy Global Professorship conference: 'Addressing the Digital Realm through the Grammar of Human Rights Law' in Oxford; and at talks hosted by Paris-Lodron Universität Salzburg and Wien Universität. The authors are grateful to the participants of these events for their questions and comments. The authors are also grateful to Carla Ferstman for her comments.

## Keywords

mass surveillance; privacy; proceduralism; essence; national security

## Sophie Duroy

Dr Sophie Duroy is a Lecturer in Law at the University of Essex (UK). Her research focuses on public international law, human rights, and security, with a particular emphasis on the regulation of state violence, intelligence, and state-sponsored assassination. She is the author of The Regulation of Intelligence Activities under International Law (Edward Elgar, 2023), winner of the 2024 Polly Corrigan Book Prize, and has published in leading peer-reviewed journals and edited collections. Sophie holds a PhD in Law from the European University Institute (2020) and has held research fellowships at the KFG Berlin-Potsdam Research Group 'The International Rule of Law: Rise or Decline?' (2021-2023) and the Hamburg Institute for Social Research (2026).

## Martin Scheinin

Prof. Martin Scheinin was in 2008-2020 Professor of International law and Human Rights at the EUI and continues as EUI part-time professor. At the time of publication his EUI contract is related to the Horizon Europe project ELOQUENCE which develops AI solutions compatible with human rights and other EU values. In parallel, he is part-time professor of international human rights law at Lund University (Sweden) where his research relates to indigenous peoples' rights and to human rights erosion. Parallel to his academic career he has served as member of the UN Human Rights Committee (1997-2004), UN Special Rapporteur on human rights and counter-terrorism (2005-2011) and member of the Scientific Committee of the EU Fundamental Rights Agency (2018-2023).

## 1. Introduction

In 2013, the Snowden revelations about global mass surveillance by intelligence services[1] increased human rights awareness in respect of surveillance and counterterrorism measures.[2] For instance, the European Parliament adopted a robust resolution on electronic mass surveillance in March 2014.[3] In a follow-up resolution of 29 October 2015, the Parliament commended the SURVEILLE project[4] for developing a methodology for the 'assessment of surveillance technologies taking legal, ethical and technological considerations into account'.[5] Only two weeks later, the 13 November 2015 attacks on Paris and Saint-Denis happened, triggering the submission of a proposed EU counter-terrorism directive to the European Parliament, in haste and without a human rights assessment.[6] Momentum had been lost.

The digital age has come with unprecedented forms and levels of surveillance that intrude into the private sphere of individuals. For many, Edward Snowden's 2013 revelations came as a watershed moment. However, shock fizzled out quickly, and mass surveillance became normalised.[7] This normalisation process included the paradoxical legitimation of mass surveillance by courts, and especially the European Court of Human Rights (ECtHR or 'the Court').[8] As the opening story about the European Parliament illustrates, in the post-9/11 age, human rights and evidence-based rational decision-making have repeatedly been pushed aside in favour of hasty political posturing. Unfortunately, as we argue in this article, the ECtHR has not been immune from this phenomenon.

Digital technologies enable various forms of privacy-intrusive surveillance. The digitalisation of information and the exponential growth of technological capacity to store and process information have made possible, practical, and almost cost-free what was previously either impossible or only theoretically possible, at too much effort and cost. Digitalisation as such is not a foundational change. Rather, we consider that it represents a whole set of newly-emerged factual circumstances that challenge the preconditions for the enjoyment of the right to privacy as a person's liberty to choose what information to share and with whom.

---

[1] For a catalogue of Edward Snowden's revelations, see: https://www.lawfaremedia.org/article/catalog-snowden-revelations/.

[2] Zygmunt Bauman and others, 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8 International Political Sociology 121.

[3] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various member states and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) (2017/C 378/14).

[4] SURVEILLE 'Surveillance: Ethical issues, legal limitations, and efficiency' FP7-SEC-2011-284725.

[5] European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP)) (2017/C 355/07), para 28.

[6] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism, 2 December 2015, COM(2015) 625 final, 2015/0281(COD).

[7] Valsamis Mitsilegas and others, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2023) 29 European Law Journal 176.

[8] Félix Tréguer, 'Intelligence Reform and the Snowden Paradox: The Case of France' (2017) 5 Media and Communication 17; Sophie Duroy, 'When Intelligence Accountability Backfires: How States' Strategic Legal Justifications Undermine International Law' [2026] Global Constitutionalism 1 <https://doi.org/10.1017/S2045381726100276>.

From a human rights perspective, among the most concerning forms of digitalised surveillance are targeted surveillance,[9] bulk interception regimes ('mass surveillance'),[10] facial recognition technology,[11] algorithmic video surveillance,[12] and biosurveillance.[13] The first two rely on digital means to surveil people's *communications*, the latter three their *biometrics*.[14] Targeted surveillance through analogue and digital means forms the subject of an extensive and relatively protective caselaw.[15] In contrast, after two initial and somewhat contradictory decisions in *Roman Zhakarov* and *Szabo and Vissy*,[16] the Court's approach to bulk interception regimes was consolidated in 2021 with the Grand Chamber judgments in *Big Brother Watch* and *Centrum för rättvisa*.[17] These two judgments triggered intense academic commentary, with many scholars regretting the normalisation of mass surveillance[18] and the turn to

[9] Targeted surveillance refers to the 'upstream' surveillance of electronic communications (telephone, text messaging, email, internet browser chat, social media apps) of a known criminal suspect or intelligence target.

[10] Mass surveillance refers to the 'downstream' surveillance of electronic communications for the purpose of finding hitherto unknown targets.

[11] Facial recognition technology is a type of biometric technology that involves identifying or verifying individuals by analysing and comparing patterns on their faces. It uses algorithms to detect and recognize human faces in images or videos.

[12] Algorithmic video surveillance is a type of video surveillance system that uses artificial intelligence and machine learning algorithms to analyse video footage in real-time. These algorithms can detect and recognize specific objects, such as people or vehicles, and their behaviour patterns.

[13] Biosurveillance refers to the systematic monitoring and analysis of biosphere data for early detection and rapid response to infectious disease outbreaks, bioterrorism events, and other public health emergencies. It involves the continuous collection, integration, interpretation, and dissemination of various types of data, including clinical, laboratory, environmental, and social media data, to detect and respond to health threats in real-time or near real-time.

[14] Biometric data is defined in the General Data Protection Regulation as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person'. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 14.

[15] E.g., *Malone* v. *the United Kingdom*, App. No. 8691/79, 2 August 1984; *Dumitru Popescu* v. *Romania* (no. 2), App. No. 71525/01, 26 April 2007; *Liberty and Others* v. *the United Kingdom*, App. No. 58243/00, 1 July 2008; *Bykov* v. *Russia* [GC], App. No. 4378/02, 10 March 2009; *Ben Faiza* v. *France*, App. No. 31446/12, 8 February 2018.

[16] *Roman Zakharov* v. *Russia*, App. No. 47143/06, 4 December 2015; *Szabo and Vissy* v. *Hungary*, App. No. 37138/14, 12 January 2016.

[17] *Big Brother Watch and Others* v. *The United Kingdom* [GC], App. Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021; *Centrum för rättvisa* v. *Sweden* [GC], App. No. 35252/08, 25 May 2021.

[18] Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum För Rättvisa' [2021] EJIL: Talk! <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/>; Massimo Frigo, 'Big Brother Watch v. UK: A Landmark Judgment Missing the Mark' (*Opinio Juris*, 4 June 2021) <http://opiniojuris.org/2021/06/04/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark/>; Eliza Watt, 'Much Ado About Mass Surveillance – the ECtHR Grand Chamber "Opens the Gates of an Electronic 'Big Brother' in Europe" in Big Brother Watch v UK' (*Strasbourg Observers*, 28 June 2021) <https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/>; Monika Zalnieriute, 'Procedural Fetishism and Mass Surveillance under the ECHR' [2021] Verfassungsblog <https://verfassungsblog.de/big-b-v-uk/>.

proceduralism in the Court's caselaw.[19] While some of the Court's recent caselaw[20] shows signs of being more protective of privacy rights, it remains unclear whether this signals a new shift in the Court's approach, or a manifestation of double standards between Western and other European countries. Finally, at the time of writing, there is only one ECtHR judgment involving facial recognition technology,[21] and none concerning algorithmic video surveillance or biosurveillance.

This article traces and assesses the impact of the ECtHR's caselaw on bulk data collection and retention on the protection of privacy. Placing the ECtHR's caselaw within the broader political context and discourse and focusing on selected landmark cases to enable close doctrinal and textual analysis, we demonstrate the multifactorial nature of the Court's legitimation of mass surveillance and its consequences for privacy rights and their prospects in Europe. We focus our analysis on the ECtHR, that is, the first court to have dealt with mass surveillance under the right to privacy following the Snowden revelations that exposed the existence of bulk interception regimes. The Court of Justice of the European Union (CJEU) recently began aligning itself with the ECtHR in its caselaw concerning bulk data collection and retention by identifying a national security exemption to practices that it previously had considered inherently impermissible,[22] while other human rights courts and bodies have yet to pronounce themselves on cases involving mass surveillance.[23]

The ECtHR itself used to have a stronger stance on surveillance and privacy, as its caselaw concerning targeted surveillance exemplifies.[24] Understanding the impact of the Court's proceduralist approach to (Western states') bulk interception regimes is crucial for two main reasons. First, this allows us to assess whether and how the Court's caselaw concerning mass surveillance undermines Article 8 ECHR as a privacy-protecting clause. In this respect, we find that this caselaw has elevated national security from a *prima facie* legitimate aim that may justify limitations on privacy that are lawful, necessary and proportionate, to a *de facto* exception from human rights. Consequently, we argue that the Court's legitimation of Western states' mass surveillance apparatuses effectively empties the right to privacy of its protective characteristics.

Second, this analysis allows us to assess the detrimental effects that this caselaw may have on the protection of privacy regarding newer forms of biometric surveillance already used by several member states, including algorithmic videosurveillance, facial recognition technology,

---

[19] Monika Zalnieriute, 'Big Brother Watch and Others v. the United Kingdom' (2022) 116 American Journal of International Law 585; François Dubuisson, 'Surveillance and the European Court of Human Rights' in Russell Buchan and Iñaki Navarrete, *Research Handbook on Intelligence and International Law* (Edward Elgar Publishing 2025).

[20] *Podchasov* v. *Russia*, App. No. 33696/19, 13 February 2024; see also *Ekimdzhiev and others* v. *Bulgaria*, App. No. 70078/12, 11 January 2022; *Glukhin* v. *Russia*, App. No. 11519/20, 4 July 2023; *Škoberne* v. *Slovenia*, App. No. 19920/20, 15 February 2024; *Pietrzak and Bychawska-Siniarska and Others* v. *Poland*, Apps Nos. 72038/17 and 25237/18, 28 May 2024.

[21] *Glukhin* v. *Russia* (n 20).

[22] See Section 4.1.

[23] But see: United Nations Human Rights Committee, 'Concluding Observations on the Fourth Periodic Report of the United states of America' (23 April 2014) CCPR/C/USA/CO/4, para 22; United Nations Human Rights Committee, 'Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland' (17 August 2015) CCPR/C/UK/CO/7, para 24.

[24] See e.g., the cases mentioned at footnote 15. For a critical analysis of the Court's caselaw on surveillance, see Dubuisson (n 19).

and biosurveillance. The Court has not (yet) found biometric (mass) surveillance[25] to be compatible with Article 8.[26] However, the Court's caselaw on mass surveillance is instructive. By not drawing sufficient 'bright lines'[27] in its caselaw on bulk interception regimes, the Court has implicitly encouraged member states to increase their mass surveillance capacities, even providing them with clear procedural guidelines for making their (biometric) surveillance regimes appear ECHR-compliant.

This article contributes new evidence and analysis to a growing body of critical scholarly literature on the ECtHR's turn to proceduralism (or 'process-based review'[28]) in proportionality assessments,[29] and on possible double standards in its caselaw.[30] Nevertheless, while we remain highly critical of the Court's caselaw, which exhibits a legally unfounded level of trust in Western European states' good-faith use of mass surveillance, our conclusions become slightly less pessimistic when accounting for the Court's 2024 judgment in *Podchasov*.[31] Until *Podchasov,* the Court's abandonment of a structured proportionality test in the realm of mass surveillance had been accompanied by a complete lack of recognition that the right to privacy may contain inviolable aspects. Another significant scholarly contribution of this article thus lies in its demonstration of the existence and functioning of an inviolable essential core of ECHR Article 8 regarding privacy. In view of the impending litigation over member states' increasing use of (biometric) mass surveillance, it is notable that such a core would not be subject to a national security exemption. Hence, rather than dismissing *Podchasov* as (merely) a sign of double standards between countries, we welcome it as a crucial first step in the right direction. Yet, unless followed by a high-profile Western European case reaffirming the inviolability of the essence of privacy, *Podchasov* could well become an isolated 'good' judgment against a 'bad' country.

We begin our discussion by highlighting the contextual factors surrounding the turn to proceduralism in the Court's caselaw with the advent of electronic mass surveillance. We then analyse the Court's caselaw against the foundational principles and decades-long progressive evolution of international human rights law. Finally, we assess the direct and indirect impact of the Court's caselaw on bulk data collection on the growing potency of the national security exemption, the surveillance means legalised by states, and the right to privacy itself. We

---

[25] Biometric mass surveillance refers to the monitoring, tracking and otherwise processing of biometric data of individuals or groups in an indiscriminate or arbitrarily targeted manner, usually in publicly accessible spaces.

[26] In *Glukhin* v. *Russia* (n 20), the Court found a violation of Article 8 but was careful to state that, in this case, the 'question is not whether the processing of biometric personal data by facial recognition technology may in general be regarded as justified under the Convention' (para 85).

[27] The term 'bright-line rule' is found mostly in common law systems. In contrast with balancing tests, bright-line rules, or tests, are objective rules that resolve legal questions in a straightforward, predictable manner. Our discussion on rules and principles in Section 3.2 frames this issue by distinguishing between two categories of legal norms.

[28] Robert Spano, 'The Future of the European Court of Human Rights—Subsidiarity, Process-Based Review and the Rule of Law' (2018) 18 Human Rights Law Review 473.

[29] E.g., Dubuisson (n 18); Alain Zysset, 'A Culture of Justification or a Culture of Presumption? The Turn to Procedural Review and the Normative Function of Proportionality at the European Court of Human Rights' in Stephanie Schiedermair, Alexander Schwarz and Dominik Steiger (eds), *Theory and Practice of the European Convention on Human Rights* (Nomos Verlagsgesellschaft mbH & Co KG 2022); Oddný Mjöll Arnardóttir, 'The "Procedural Turn" under the European Convention on Human Rights and Presumptions of Convention Compliance' (2017) 15 International Journal of Constitutional Law 9.

[30] E.g., Başak Çali, 'Coping with Crisis: Whither the Variable Geometry in the Jurisprudence of the European Court of Human Rights' (2017) 35 Wisconsin International Law Journal 237; Øyvind Stiansen and Erik Voeten, 'Backlash and Judicial Restraint: Evidence from the European Court of Human Rights' (2020) 64 International Studies Quarterly 770.

[31] *Podchasov* v. *Russia* (n 20).

conclude with cautiously optimistic remarks on the potentials of the right to privacy and its essential core to constitute an antidote to the ever-growing potency of the national security exemption.

## 2. Paving the Way for the Acceptance of Surveillance Technologies: A Contextual Perfect Storm

In 2015, the SURVEILLE project demonstrated through context-specific multidisciplinary expert assessments that mass surveillance produced at best a medium 'usability score' (i.e., it was not very useful for detecting threats) while causing extremely high intrusions on human rights.[32] Mass surveillance either encroached the inviolable essential core of privacy or at least could not constitute a proportionate restriction to the right to privacy.[33] These conclusions remain highly relevant, in particular regarding downstream communications surveillance, as the same structural limitations persist despite technological improvements in machine learning and data analysis. Put simply, because the statistical incidence of terrorism is extremely low relative to the vast volume of everyday electronic communications, downstream surveillance of communication flows cannot, from a mathematical perspective, yield meaningful utility as the basis for finding actual perpetrators or plotters of terrorism. Yet, when confronted with cases concerning regimes of mass surveillance in recent years, the ECtHR has held them to be (potentially or effectively) compatible with the ECHR when the legitimate aim of protecting national security was invoked. Two interlocking contextual factors explain this contradiction: the ECtHR's legitimacy crisis and the twenty-first century security landscape.

### 2.1. The ECtHR's Legitimacy Crisis

The ECtHR, with legally binding jurisdiction over 46 member states of the Council of Europe (CoE) and with thousands of individual cases decided annually, provides for the largest and most authoritative interpretive practice under international human rights law, namely the 1950 European Convention on Human Rights and its subsequent Protocols. The geographical extension towards the east of CoE membership and the move from optional to mandatory recognition of the ECtHR's jurisdiction to receive individual cases have since the shift of the century resulted in an unprecedented caseload, backlogs, and delays in the processing of cases.[34] Over the same period, several Western European governments began contesting the ECtHR's legitimacy and sought to restrain its activity in respect of what they perceived as overreach compared to what they originally signed up for.[35] Since 2000, the ECtHR has become increasingly selective as to which cases pass even the preliminary stages, shifting its emphasis from notions such as 'real and effective rights' or 'living instrument' to practices that recite earlier caselaw and denote deference and subsidiarity in relation to national decisions. Member states further amended the ECHR to the effect of introducing the principle of a margin

---

[32] SURVEILLE (n 4). See Deliverables D2.8 and D4.10: https://surveille.eui.eu. The SURVEILLE project acknowledged the much greater utility of upstream communications surveillance, i.e., targeted measures based on pre-existing suspicion. Through that acknowledgment, the project verified the need for a structured proportionality test to prove the permissibility of some forms of surveillance.

[33] Ibid.

[34] Council of Europe, Steering Committee for Human Rights (CDDH), 'CDDH report on the longer-term future of the system of the European Convention on Human Rights' (2015) R84 Addendum I, Strasbourg.

[35] For the political outcomes of these contestations, see Committee of Ministers of the Council of Europe, 'Brighton Declaration', (2012); Committee of Ministers of the Council of Europe, 'Copenhagen Declaration', (2018); Conclusions of the Informal Ministerial Conference (10 December 2025), available at: https://rm.coe.int/informal-ministerial-conference-10-december-2025-conclusions/488029b843.

of appreciation into its text and imposing stricter requirements for the admissibility of complaints.[36] What is left of the ECtHR's approach of dynamic-evolutive interpretation has been labelled as 'incrementalism'.[37]

Even while undergoing such changes, however, the Court remained under steady criticism and backlash from several member states.[38] While part of this is related to so-called 'democratic backsliding' in a few Central and Eastern European states, criticism from Western European states mostly concerns national security matters, and in particular the fight against terrorism and concerns about irregular migration and border control.[39] Indeed, even deferential treatment still feels too intrusive for these member states when national security is invoked.[40] In their claims before the Court, as respondent states or third-party interveners, these Western European states thus advocate for a state-centric vision of the ECHR, based on subsidiarity, a low level of human rights commitments, and the minimalisation of protection of vulnerable people.[41] In sum, they repeatedly demand an increased level of deference and subsidiarity by the Court. Importantly, the increased deference the Court gives to these Western states may not be granted towards those other member states undergoing democratic backsliding. In cases against Russia, Turkey, or Hungary, for instance, the Court shows very little deference, even when national security is invoked.[42] This difference in evidentiary thresholds justifies a serious worry about incoherent caselaw that, especially when surveillance measures are at stake, reeks of double standards.

### 2.2. The Twenty-first Century Security Landscape

The development of digital technologies for surveillance purposes was encouraged by the shift to a new security landscape following the terrorist attacks of 11 September 2001 (9/11). This new landscape is characterised by a rhetorical and abstract balancing exercise. Often called the 'liberty-security conundrum', this trade-off mentality assumes or advocates the necessity to reduce rights and liberties in exchange for better security.[43] Trade-off discourses first took hold in the United States in the wake of 9/11[44] and were used to justify policies as extreme as

---

[36] Council of Europe, 'Protocol No. 14 amending the Convention on the Protection of Human Rights and Fundamental Freedoms', (13.V.2004), Strasbourg; Council of Europe, 'Protocol No. 15 amending the Convention on the Protection of Human Rights and Fundamental Freedoms', (24.VI.2013), Strasbourg.

[37] Janneke Gerards, 'Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights' (2018) 18 Human Rights Law Review 495.

[38] Vassilis P Tzevelekos, 'Has the ECHR Failed Us?' (2025) 6 European Convention on Human Rights Law Review, 275.

[39] See, e.g., *Hirsi Jamaa and Others* v. Italy, App. No. 27765/09, 23 February 2012; Othman *(Abu Qatada)* v. *The United Kingdom*, App. No. 8139/09, 17 January 2012; *A and Others* v. *The United Kingdom*, App. No. 3455/05, 19 February 2009.

[40] For an overview of debates in the post-9/11 context, see Alice Donald, Jane Gordon and Philip Leach, *The UK and the European Court of Human Rights* (Equality and Human Rights Commission 2012); see also Çali (n 29).

[41] See, for instance, the third-party interventions by the Governments of France, the Netherlands, and Norway in *Big Brother Watch* (n 17), paras 300-310, and *Centrum för rättvisa* (n 17), paras 224-235. See also, for an example of advocacy for 'balancing' under Article 3, the third-party intervention by the United Kingdom in *Saadi v. Italy* [GC], App. No. 37201/06, 28 February 2008, para 122. For an analysis of third-party interventions before the ECtHR, see Kanstantsin Dzehtsiarou, 'Conversations with Friends: "Friends of the Court" Interventions of the state Parties to the European Convention on Human Rights' (2023) 43 Legal Studies 381.

[42] Regarding privacy, see especially *Roman Zakharov* v. *Russia* (n 16); *Szabo and Vissy* v. *Hungary* (n 16); *Podchasov* v. *Russia* (n 20).

[43] Jeremy Waldron, 'Security and Liberty: The Image of Balance' (2003) 11 Journal of Political Philosophy 191.

[44] David Cole, 'Their Liberties, Our Security: Democracy and Double Standards' [2003] 31 Int'l J. Legal Info. 290-311.

imprisonment without charge[45] or torture.[46] It bears stating explicitly that we do not consider that all 'trade-offs' are impermissible *per se*, but rather that the permissibility of human rights intrusions should be assessed through the structured and analytical step-by-step tests developed in international human rights law rather than through abstract balancing exercises.

Rhetorically, the balancing exercise is captivating: to fight terrorism and ensure the security of its population, the state needs additional powers.[47] These powers require the population to give up some rights and liberties. Hence, for the promise of more security, the population agrees to reduce its liberties. However, this seemingly simple balancing exercise is ridden with logical fallacies. We outline three of them here.[48]

First, the trade-off discourse implies that the threat to human rights emanating from terrorist attacks is on balance with the threat emanating from the state, so that when one raises, the other one diminishes. On the contrary, the terrorist threat to security is complemented by and may even enhance state threats to individual security when, as is the case in many countries since 9/11, the government is granted additional powers. The state is then free (also) to use these powers against its own 'enemies', such as minorities or opposition groups. Of course, the positive obligations of the state to secure the human rights of individuals within its jurisdiction against interference by private parties (for example terrorists) have been recognised generally in respect of many rights.[49] Yet, it is absurd to infer from the existence of such positive obligations that, to realise them, the negative obligations of the state not to violate the same rights should be diminished.

Second, proponents of a balancing approach between security and liberty often emphasise the 'social good' aspect of security: we must accept to be a bit less free to be a bit more secure. This balancing discourse has been at the core of the post-9/11 counterterrorism approach. However, it fails to take into account that what is at stake, at least at the outset, is an interpersonal trade-off: those who accept, those who gain security, and those who suffer human rights harm are not the same subjects.[50] In general, those who agree to the trade-off assume that 'others' will bear the highest cost. In the short term, they are usually right: minorities and non-citizens generally pay the highest price of heightened security measures and rights reductions. In the long term, however, it often becomes clear that the state will use, or will be tempted to use, its newly acquired powers against anyone.[51]

Third, and relatedly, when in fear of an attack, citizens expect their government to act and respond to the threat. The more unusual or drastic the response, the stronger is its

---

[45] After 9/11, thousands of Muslim, South Asian and Middle Eastern men in the US were detained by the FBI, police and immigration officers and held in various prisons in New York and New Jersey. See Shubh Mathur, 'Surviving the Dragnet: "Special Interest" Detainees in the US after 9/11' (2006) 47 Race & Class 31.

[46] The case for legally allowing the torture of suspected terrorists was made most clearly by Alan Dershowitz, then professor at Harvard Law School.

[47] Waldron (n 43).

[48] The following paragraphs build upon Sophie Duroy, *The Regulation of Intelligence Activities under International Law* (2023) Chapter 1.

[49] E.g., ECtHR *Osman* v. *United Kingdom*, Application No 23452/94, [GC] Judgment, 28 October 1998, para 116; IACtHR *Velasquez Rodriguez* v. *Honduras* (Judgment) IACtHR Series C No 4 (29 July 1988) paras 172–175.

[50] Jeremy Waldron, *Torture, Terror, and Trade-Offs: Philosophy for the White House* (Oxford University Press 2010) 146; David Luban, *Torture, Power, and Law* (Cambridge University Press 2014); Cole (n 44).

[51] This argument is similar to Foucault's imperial boomerang thesis, according to which governments that develop repressive techniques to control colonial territories will eventually deploy the same techniques domestically, against their own citizens. Michel Foucault, *Society Must Be Defended: Lectures at the Collège de France, 1975-76* (Penguin).

psychological reassurance on the population.[52] The risk of a violent attack from a terrorist organisation could well still be the same, but national security will have profited in the trade-off: the position of governmental institutions is now more secure and governmental powers have increased. However, this does not mean that individuals' security has benefited in any way from this governmental capture of power. Quite the opposite, for the benefit of such psychological reassurance, civil liberties may have been traded-off, the rule of law undermined, and security as a social good and as a human right[53] damaged. In other words, liberty was sacrificed for the mere potential of security.

The post-9/11 security landscape united virtually all states against a real or imagined common enemy: terrorism. Terrorism constitutes both the root and the rationale of the twenty-first century security landscape. As the trade-off narrative emphasises, the enemy is an undefined non-state actor. It is pervasive and global, dangerous, inhumane, and the threat it poses allegedly justifies extraordinary measures to prevent it from materialising. To protect themselves against terrorism, states, governments and populations united themselves beyond usual divisions. This security landscape is thus characterised by an 'us against them' mentality, and by the perceived need for new and greater powers to face the terrorist threat.

While emerging in the wake of 9/11, the liberty-security conundrum was not restricted to the United States. On the international scene, it was first embedded in a series of Chapter VII resolutions by the UN Security Council.[54] Binding on all states, these resolutions effectively transformed the trade-off mentality into binding international law, ensuring its worldwide effect. Predictably, the resulting international counterterrorism framework lacked meaningful safeguards and legitimated a crackdown on human rights and the rule of law in the name of preventing and fighting terrorism.[55]

The influence of the liberty-security conundrum as a political and legal theory is still visible today. Exceptional measures enacted in the immediate aftermath of 9/11 have become permanent.[56] There is a strong lock-in effect of security-enhancing measures, regardless of whether they achieve their stated purpose.[57] Put simply, no one wants to be blamed for the next attack or failure; hence, no one takes responsibility over discontinuing emergency security measures. This latter point underlies much of the deference to the executive that national courts and tribunals show in matters of national security.[58] In theory, regional and international courts should be better able to extricate themselves from the pressures faced by domestic courts. However, member states' continuous questioning of the ECtHR's legitimacy and

---

[52] Waldron (n 50) 45.

[53] Despite some early caselaw by the Human Rights Committee, such as *Delgado Paez* v. *Colombia* (CCPR/C/39/D/195/1985), international human rights bodies have failed to utilize the potential of 'the right to security of the person', proclaimed in ICCPR Article 9(1) or ECHR Article 5(1). See Martin Scheinin, 'Human Dignity, Human Security, Terrorism and Counter-Terrorism' in Christophe Paulussen and Martin Scheinin (eds), *Human Dignity and Human Security in Times of Terrorism* (TMC Asser Press 2020).

[54] See especially S.C. Res. 1373 (28 September 2001); S.C. Res. 1611 (7 July 2005); S.C. Res. 1618 (4 August 2005); S.C. Res. 2133 (27 January 2014); S.C. Res. 2170 (15 August 2014).

[55] Kim Lane Scheppele and Arianna Vedaschi, 'Conclusion: The Afterlife of 9/11' in Arianna Vedaschi and Kim Lane Scheppele (eds), *9/11 and the Rise of Global Anti-Terrorism Law* (Cambridge University Press 2021).

[56] Fiona de Londras, *The Practice and Problems of Transnational Counter-Terrorism* (Cambridge University Press 2022).

[57] Sophie Duroy, 'The Regulation of Intelligence Cooperation under International Law: A Compliance-Based Theorization' in Arianna Vedaschi and Kim Lane Scheppele (eds), *9/11 and the Rise of Global Anti-Terrorism Law: How the UN Security Council Rules the World* (Cambridge University Press 2021) 189.

[58] John Ip, 'The Supreme Court and the House of Lords in the War on Terror: Inter Arma Silent Leges?' (2010) 19 Michigan State Journal of International Law.

'activist' stance has encouraged the Court to adopt a similar position in ECtHR cases involving states perceived as liberal democracies: deferring to the executive when national security is invoked.[59] After 9/11, balancing processes did not take long to emerge at the ECtHR. It bears noting that the Court did resist states' repeated claims that national security justified altering the level of protection provided by the Convention when torture and non-refoulement were at stake.[60] In contrast, the balancing rhetoric was remarkably successful regarding privacy.

Following Snowden's revelations, concerns about mass surveillance violating human rights were high.[61] Civil society's calls for increased transparency and legitimacy drove states to give a legal status to their intelligence agencies and provide a legal basis for their surveillance activities. However, this *a priori* positive development was part of a broader movement that saw states attempting to justify and legitimise their intelligence activities to various domestic and international audiences.[62] When questioned before supranational courts and bodies, states began justifying their surveillance practices in human rights terms. In essence, states' justifications construct a phenomenon (e.g., terrorism) as a threat to a legitimate interest (e.g., national security) and present their response of choice (e.g., mass surveillance) as a necessary and proportionate interference with human rights. The result is that governments often present bulk data collection and retention or spyware such as Pegasus as intrinsically lawful. Yet, the balancing mentality underlying these measures remains as fallacious today as it was two and a half decades ago.

Against the contemporary situation just described, it becomes clear that the acceptance of bulk surveillance technologies in the Court's caselaw occurred during a contextual perfect storm, combining the Court's own legitimacy crisis with the perpetuation of a fight against terrorism in a national security culture of legal rationalisation.[63] Together, these contextual factors enabled increased deference towards states' national security claims. With the CJEU gradually aligning its jurisprudence with the ECtHR's, a European trend towards proceduralism and increased legitimation of mass surveillance has surfaced.

## 3. Assessing the Court's Caselaw on Bulk Data Collection against the Foundations of International Human Rights Law

As a result of the security context and backlash against the Court, we identify an interpretive discrepancy in the Court's approach to bulk interception regimes compared to its earlier caselaw on targeted surveillance regimes. We critically analyse these developments against

[59] Duroy (n 8); Chao Jing, 'The ECtHR's Suitability Test in National Security Cases: Two Models for Balancing Human Rights and National Security' (2023) 36 Leiden Journal of International Law 295.

[60] See, e.g., *Saadi* v. *Italy* (n 41)*; A.* v. *The Netherlands,* App. No. 4900/06, 20 July 2010, para 143; *Daoudi* v. *France,* App. No. 19576/08, 3 December 2009, para 64. States' claims have recently been reiterated the Chişinău Declaration CM(2026)99-final - 135th Session, 15 May 2026.

[61] Sophie Duroy and Liliya Khasanova, 'Cyberespionage and Human Rights: A Disappointing Balance' in Antonio Segura Serrano (ed), *Global Cybersecurity and International Law* (Routledge 2024).

[62] Sophie Duroy, 'The Intelligence Community as a Normative Actor under International Law' in Russell Buchan and Iñaki Navarrete (eds), *Research Handbook on Intelligence and International Law* (Edward Elgar Publishing 2025); Duroy, 'When Intelligence Accountability Backfires' (n 8).

[63] A national security culture of legal rationalisation is a legal culture whereby public authorities are pressed to produce detailed legal justifications for *prima facie* unlawful policies. Rebecca Sanders, *Plausible Legality: Legal Culture and Political Imperative in the Global War on Terror* (Oxford University Press 2018).

the foundational concepts, distinctions and principles of international human rights law,[64] to which the Court itself greatly contributed historically. We find that, as regards mass surveillance, the Court has failed to conform to these foundations in at least two ways. First, the Court abandoned the quest for a structured proportionality test, instead turning to proceduralism. Second, the Court's inconsistent use of the concept of essence (or inviolable core) in its caselaw is puzzling and reeks of double standards rather than identical bright-line rules for all states.

### 3.1. The Turn to Proceduralism: Abandoning the Quest for a Structured Proportionality Test

The ECtHR's initial assessments of digital surveillance practices, while conducting a substantive review of the legal regimes at stake, recognised a wide margin of appreciation for states.[65] Following Snowden's revelations, the first two cases considering the specificity of non-targeted surveillance measures yielded contradictory approaches. In *Roman Zhakarov*, the Grand Chamber maintained its approach of providing states with a wide margin of appreciation, abstaining from adapting its proportionality test to bulk data collection.[66] In *Szabo and Vissy*, however, one chamber applied a 'strict necessity' approach to the assessment of proportionality, considering that the specificities of bulk data collection meant that the state no longer benefited from a wide margin of appreciation but should, instead, be able to demonstrate that mass surveillance regimes were 'strictly necessary' to protect national security.[67] Following two chamber decisions in 2018,[68] the Court's approach was consolidated with the 2021 Grand Chamber judgements in *Big Brother Watch* (BBW) and *Centrum för rättvisa* (CFR).[69] In these two cases, faced with Western states' repeated claims as to the lawfulness of their practices and their quest for increased deference in national security matters, the Court moved towards a 'balance' more deferential to states' national security arguments and claims for mass surveillance.

Only if courts perform their duty can states' justifications for human rights intrusions be legally evaluated and deconstructed. Mass surveillance constitutes a serious interference with individuals' right to privacy, among other rights. The right to privacy being non-absolute, it can be restricted. According to the accumulated jurisprudence of human rights courts and bodies, a structured permissibility test should assess whether an interference 1) leaves the essence (core) of the right unaffected; 2) is in accordance with the law; 3) serves a legitimate aim; 4) is necessary, including minimally intrusive, to achieve that aim; and 5) is proportionate to the benefit that it delivers towards the aim pursued.[70] Yet, in Europe, where the only supranational

---

[64] Here, this article follows the 'Grammar of IHRL' approach presented in Tarik Gherbaoui and Martin Scheinin, 'A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove It' (2023) 1 Journal européen des droits de l'homme - European Journal of Human Rights.

[65] See, e.g., *Kennedy* v. *United Kingdom*, App. No. 26839/05, 18 May 2010; *Liberty and Others* v. *United Kingdom*, App. No. 58243/00, 1 July 2008; *Weber and Saravia* v. *Germany*, App. No. 54934/00, 29 June 2006. For an analysis of the Court's caselaw, see Dubuisson (n 19).

[66] *Roman Zakharov* v. *Russia* (n 16).

[67] *Szabo and Vissy* v. *Hungary* (n 16), para 88.

[68] *Centrum för rättvisa* v. *Sweden*, App. No. 35252/08, 19 June 2018; *Big Brother Watch and Others* v. *The United Kingdom,* App. Nos. 58170/13, 62322/14 and 24960/15, 13 September 2018.

[69] *Big Brother Watch and Others* v. *The United Kingdom* (n 17); *Centrum för rättvisa* v. *Sweden* (n 17).

[70] For an articulation of these elements of a structured permissible limitations test, see: Human Rights Committee, General Comment No. 37 on freedom of assembly (2020), paras. 36-41. See also, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 28 December 2009, A/HRC/13/37, para 17; ECtHR, *Muhammad and*

caselaw on mass surveillance and indiscriminate data retention is to be found, the ECtHR has increasingly stopped assessing all but the second prong ('in accordance with law'), instead showing near-absolute deference to states' national security arguments and often superficial proportionality assessments. While some commentators view the Court's emphasis on formal procedural requirements as a pragmatic expression of subsidiarity and institutional restraint,[71] these justifications risk normalising broad discretion in an area where independent, substantive scrutiny remains essential.[72] As the analysis below demonstrates, such procedural requirements have become a substitute rather than a complement to structured proportionality assessments.

In its 2021 Grand Chamber judgments in BBW and CFR, the Court considered that operating a bulk interception regime is not, in principle, unlawful and/or disproportionate. The Court found that the British and Swedish bulk interception regimes were 'valuable'[73] and of 'vital importance'[74] to the security of member states—notwithstanding the lack of public evidence concerning their actual performance. On this basis, the Court held that national authorities enjoy a 'wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security'.[75] The consequence of this deferential treatment was that end-to-end safeguards were required. The Court therefore established a new eight-part test to assess the compatibility of bulk surveillance regimes with Article 8 ECHR.[76] This test focuses on the regulatory framework and procedural requirements. It assesses exclusively the 'in accordance with law' prong of the broader permissibility assessment and assumes satisfaction of the 'necessity',[77] 'legitimate aim' and 'proportionality' prongs. Both judgments exemplify the Court's

*Muhammad* v. *Romania*, App No 80982/12, 15 October 2020, with several concurring and dissenting opinions that evidence and reflect upon the need for a structured proportionality test.

[71] See, e.g., Spano (n 28); Thomas Kleinlein, 'The Procedural Approach of the European Court of Human Rights: Between Subsidiarity and Dynamic Evolution' (2019) 68 International & Comparative Law Quarterly 91.

[72] For a review of arguments for and against proceduralism in national security matters, see Daniella Lock, 'Strasbourg's Open Door to Normalisation in National Security Adjudication' [2026] European Convention on Human Rights Law Review 1 <https://doi.org/10.1163/26663236-bja10151>.

[73] BBW para 323, CFR para 237.

[74] BBW para 424, CFR para 365.

[75] BBW para 228, CFR para 252.

[76] BBW para 361, CFR para 275. The test purports to assess jointly the 'in accordance with law' and 'necessity' aspects of the surveillance regime by examining 'whether the domestic legal framework clearly defined:
the grounds on which bulk interception may be authorized;
the circumstances in which an individual's communications may be intercepted;
the procedure to be followed for granting authorisation;
the procedures to be followed for selecting, examining and using intercept material;
the precautions to be taken when communicating the material to other parties;
the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.'

[77] Although the test also purports to assess the necessity prong, it does so only in a procedural way, leaving the substantive assessment of necessity entirely up to states.

blind trust in (some)[78] states' assessment that interception, storage, and analysis of data and metadata are necessary and proportionate to protect national security.[79]

Mass surveillance has thereby become a 'question of trust', namely, trust in the professionalism and integrity of intelligence and security authorities in Western democracies, and the ECtHR's trust in the word of their governments. Notably, governments have been unable or unwilling to demonstrate the utility of downstream communications surveillance in detecting previously unknown threats. A rare but often-cited effort to substantiate actual benefits obtained through bulk surveillance is provided by a 2015 report by the UK Government's Independent Reviewer of Terrorism Legislation, tellingly titled 'A Question of Trust'. [80] It provides six very short and security-redacted descriptions of cases where bulk data interception was used successfully.[81] However, it does not show that in *any* of them the successful investigation actually originated from downstream data interception. Rather, in at least four and possibly all six cases, bulk surveillance was applied *to substantiate a pre-existing suspicion*, thereby making it a tool in the service of *upstream* surveillance. In consequence, we find it plausible that the unredacted facts of the six cases underlying the report would in fact support rather than challenge the conclusion of the SURVEILLE project that downstream communications surveillance does not have real utility.[82]

The Court's 'proceduralist approach'[83] to mass surveillance facilitates states' legitimation of their bulk data collection regimes. Indeed, formal procedural requirements have come to substitute for, rather than complement, substantive proportionality assessments.[84] Where states' regulatory frameworks satisfy the Grand Chamber's eight-part procedural test, the bulk collection regime is deemed to be in accordance with law. In practice, states only need to *present* bulk collection regimes that fulfil the procedural test as necessary and proportionate for them to be considered lawful. Based on the two judgments, it seems that whether the regime is actually 'valuable' for protecting the legitimate aim of national security in delivering an actual and proven benefit towards meeting the legitimate aim, and whether practice complies with the regulatory framework, are of virtually no importance for the outcome of a case.[85] In other words, not only is the Court conducting an abstract review of the legislation providing for the bulk collection regime,[86] but it is also only reviewing whether it meets the 'in accordance with law' prong of the broader permissibility assessment, and doing so in a purely procedural manner. Such a procedural and often superficial review amounts to what Daniella Lock termed a 'covert box-ticking' approach to reviewing ECHR compatibility.[87] Through these

---

[78] It may be interesting to note that, historically, Sweden and the UK have the lowest rate of adverse judgments. See Donald, Gordon and Leach (n 40) 38. For an analysis of recent caselaw against the UK, see Lewis Graham, 'Boldness, Caution, Avoidance: Recent Cases Against the UK Before the European Court of Human Rights' (2024) 5 European Convention on Human Rights Law Review, 65. On the Court's reluctance to rule against democratic critics, see Stiansen and Voeten (n 30).

[79] Frigo (n 18).

[80] UK Government's Independent Reviewer of Terrorism Legislation: David Anderson, A Question of Trust: Report of the Investigatory Powers Review: https://www.publicinformationonline.com/shop/82361.

[81] Ibid, Annex 9 (pp. 337-338).

[82] SURVEILLE (n 32).

[83] Zalnieriute (n 18).

[84] Lock (n 72).

[85] In a 2022 Bulgarian case, the Court nevertheless underlined that procedural safeguards should not only exist on paper but also operate in practice. Whether this also applies to mass surveillance and to all member states is, however, unclear. *Ekimdzhiev and others* v. *Bulgaria* (n 20), para 419.

[86] On abstract and concrete review, see Janneke Gerards, 'Abstract and Concrete Reasonableness Review by the European Court of Human Rights' (2020) 1 European Convention on Human Rights Law Review 218.

[87] Lock (n 72).

two judgments, the Court thus affirmed the legitimacy of mass surveillance. In so doing, it also accepted states' claims to quasi-exclusive sovereignty over national security matters.

The Court's deference towards Western states' claims effectively made redundant actual proportionality analysis performed by the Court. Any semblance of a structured proportionality assessment combining the requirement of a legal basis, a legitimate aim, and the assessment of necessity[88] and proportionality *stricto sensu*[89] is effectively bypassed in favour of procedural checks. The ECtHR now exclusively focuses on the 'in accordance with law' prong of the test and defers to states' assessments regarding the necessity and proportionality *stricto sensu* of mass surveillance regimes. Nowhere in BBW and CFR is the Court itself assessing either, or questioning the domestic authorities' assessments that their bulk collection regimes were necessary or proportionate to achieving the legitimate aim of protecting national security.[90] Similarly, proportionality is simply absent, as a category, from the Registry's factsheet on 'terrorism surveillance measures'.[91] The word 'proportionality' appears only twice in the document, in sentences describing the duties of domestic courts to assess the necessity and proportionality of the measures being taken.

Even a presumption that the fight against terrorism falls under the legitimate aim of protecting national security should not preclude the application of a structured proportionality test by the Court, beyond the verification that procedural safeguards are sufficient. Such a test requires assessing and/or measuring the benefit obtained towards the legitimate aim; assessing the human rights intrusion; and comparing the two.[92] To properly strike a balance, the weights must be measured and compared: What is the proven, or on valid grounds expected, benefit obtained towards the invoked legitimate aim from using a specific form of surveillance known to cause a privacy intrusion? And what is the proven, or on valid grounds expected, detrimental impact of such surveillance upon the enjoyment of the right to privacy? A proper 'all-things-considered' proportionality assessment can only be made when these two questions are answered. By foregoing the quest for a structured proportionality test in cases of mass surveillance and showing near-absolute deference to the Western states involved, the Court has legitimated and normalised mass surveillance, presumably for all member states.

### 3.2. The Inconsistent References to the Essence of Article 8 in Mass Surveillance Cases

The Court has also failed to recognise the inviolability of the essential core (essence) of the right to the protection of private life (or privacy) contained in Article 8 when electronic mass surveillance is at stake in Western European states. Instead, the Court has tacitly accepted these states' position that the protection of national security requires that individuals relinquish their privacy by default. After conceptualising the essential core of the right to privacy, we analyse the Court's recognition of this core in *Podchasov*.

---

[88] Necessity implies the need for a combined fact-based assessment of the effectiveness of the measure with regard to the aim pursued and of whether it is less intrusive compared to other options for achieving the same goal.

[89] Proportionality *stricto sensu* requires that the advantages resulting from the measure towards the legitimate aim must be greater than the disadvantages the measure causes for the exercise of human rights.

[90] This is confirmed by a search for the word 'proportionality' in BBW (60 occurrences) and CFR (18 occurrences). All the occurrences in the Court's assessment refer to the role of domestic authorities to assess necessity and proportionality, instead of the Court's own role.

[91] CoE Registry, Key Theme 'Terrorism Surveillance Measures' (updated 31/08/2025) : https://ks.echr.coe.int/documents/d/echr-ks/surveillance-measures

[92] Human Rights Committee, General Comment No. 37 on freedom of assembly (2020), para. 40.

### *3.2.1. Conceptualising the essential core of the right to privacy*

We assert that the right to privacy should be understood as an aggregate of rules and principles.[93] As a principle, the right to privacy has general validity within the legal system and an abstract weight commensurate to its nature as an internationally protected human right. But if its essential core is at issue, the right to privacy also applies as a rule (or set of rules) that may determine the outcome that surveillance is impermissible, irrespective of any justifications presented for it. Such rules, or 'bright lines', will usually have a narrow scope of application but secure the inviolability of the 'essence' of the right.[94]

The inviolable essential core of privacy, or one essential core attribute among several, is a Hohfeldian liberty-right (privilege).[95] It is not a (positive) claim-right or power, and neither is it a passive immunity (right to be left alone). This core can be described as *a relational privilege-right to choose what information to share with whom, and what to share with no-one*. In real-life situations, other modalities (i.e., binary relations between a rights-holder and a duty-bearer) are clustered around this essential core, especially in the form of legal remedies that come into play to protect the liberty and represent the typical three-party structure of a legal right.[96] But, importantly, the essential core of the human right to privacy is not merely a solitary *forum internum* as the catchphrase 'right to be let alone' would suggest.[97] In fact, as Yuval Shany notes, the continued relevance of the right to privacy in the digital age was helped by the theoretical shift from a dominant conception of privacy as a right to be left alone to notions of privacy involving the right to exercise control over personal data and its derivative uses, including control over inter-personal communication flows.[98]

---

[93] For *rules* and *principles* as two categories of legal norms, see, Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press 2002). For an elaboration of the roles of rules and principles in international human rights law as compared with Alexy's principle-focused theory designed for a stable constitutional system (Germany), see Martin Scheinin, 'Terrorism and the Pull of Balancing in the Name of Security' [2009] EUI Working Paper Law 2009/11 55–59 <https://doi.org/10.2139/ssrn.1555686>.

[94] The concept of 'essence' appears unsystematically and even incoherently in ECtHR caselaw. There are cases where the Court's references to it entail that, if the essence of a human right is breached, there is no need for a proportionality assessment or the application of a margin of appreciation. See, e.g., *Jureša* v. *Croatia,* App. No. 24079/11, 22 May 2018*,* para 41 (Article 6), or *Navalny* v. *Russia* [GC], App. Nos. 29580/12, 36847/12, 11252/13, 12317/13 and 43746/14, 15 November 2018, para 133 (Article 11). These cases suggest that the essential core is protected by 'bright lines', i.e., gives rise to a rule that makes unnecessary any balancing between principles. In other cases, a reference to the 'essence' merely appears to emphasise an important aspect of a human right. *Podchasov* v. *Russia* (n 20) is the first Article 8 case where the notion of essence was clearly used both for identifying an important aspect of privacy and for the outcome that no proportionality assessment should be conducted. Earlier, in *Delfi* v. *Estonia* [GC], App. No. 64569, 16 June 2015, para 110, the Court nevertheless implied that it applied the notion of essence to demarcate areas where human rights provide for 'bright lines', this time in the context of reconciling the essence of freedom of expression (Article 10) and privacy rights (Article 8).

[95] Wesley Newcomb Hohfeld, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) 23 The Yale Law Journal 16; Wesley Newcomb Hohfeld, 'Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1917) 26 The Yale Law Journal 710.

[96] Carl Wellman, *A Theory of Rights: Persons under Laws, Institutions and Morals* (Rowman & Allanheld 1985) 80–102; Carl Wellman, *Real Rights* (Oxford University Press 1995); see also M. Scheinin, 'Characteristics of Human Rights Norms', in Catarina Krause and Martin Scheinin (eds), *International Protection of Human Rights: A Textbook* (2., revised ed, Åbo Akademi Univ, Inst for Human Rights 2012) 33–35.

[97] The catchphrase is attributed to Warren and Brandeis, 'The Right to Privacy', *Harvard Law Review*, Vol. 4 (1890) but represents a simplification of their argument. For the concept and normative features of the right to privacy, see, Daniel Solove, *Understanding Privacy* (Harvard University Press 2009) and Carissa Veliz, *The Ethics of Privacy and Surveillance* (Oxford University Press 2024).

[98] Yuval Shany, 'Digital Rights and the Outer Limits of International Human Rights Law' (2023) 24 German Law Journal 461, 465.

Since trivial or manifestly non-private information may not trigger the unconditional nature of the essential core, it is necessary to include one of two alternative qualifications for when such an absolute liberty-right applies: privileged subject-matter or privileged relationship to the intended exclusive recipient of the information. We consider privileged subject-matters to include one's intimate thoughts, affections, desires, sentiments, or health issues, while privileged relationships should include those with one's spouse and family, and qualified professional relationships (lawyer, doctor, therapist, priest). We claim that this inviolable core applies in contexts of indiscriminate or mass surveillance without individualised suspicion and without the individual's liberty to decide what to share. By contrast, we would accept that targeted surveillance based on concrete legitimate suspicion may not trigger the essence and, therefore, could be proven justified, through a structured proportionality assessment between the security benefit and the human rights harm.

From this perspective, the essential core of privacy represents a 'bright line' that must not be crossed, i.e., a rule that within its own scope of application determines the outcome of the legal assessment, without a need to assess other factors such as the justification or proportionality of the intrusion.[99] In other words, even the legitimate aim of protecting national security cannot justify an interference with the essential core of the right to privacy. In addition, the protective modalities clustered around the core may include rules with the same all-or-nothing nature: the 'prescribed by law' or legality requirement and the requirement of judicial authorisation, when applicable, are also rules. The requirement of a legitimate aim served by the privacy intrusion is also technically a rule. However, in practice, the mere invocation of a legitimate aim meets the requirement of that rule.

The domain of proportionality assessment starts where the rules do *not* on their own determine that the surveillance at issue is impermissible. The proportionality assessment will determine the outcome of most but not all contestations of surveillance. Unlike the procedural test devised by the Court in BBW and CFR, a properly framed proportionality assessment is about 'weighing the nature and detrimental impact of the interference on the exercise of the right against the resultant benefit to one of the grounds for interfering. If the detriment outweighs the benefit, the restriction is disproportionate and thus not permissible'.[100] This formulation, used in a recent General Comment by the UN Human Rights Committee, represents the crystallisation of what a structured proportionality test requires according to the accumulated principles of international human rights law. In the same General Comment, the Committee was equally clear concerning the inviolability of the essence of a human right and the need to test this requirement before proceeding to a proportionality assessment.[101]

What is special about digitalised forms of surveillance is their unprecedented pervasiveness and reach resulting from technological developments. These developments make possible, practical and almost cost-free the processing of digital information about everyone, instead of needing to start from defining, on permissible grounds, an individual as a suspect or target. In consequence, it is an appropriate judicial response to the phenomenon of digitalised surveillance to categorise whole forms of digital surveillance such as 'mass surveillance', 'suspicionless surveillance', or surveillance including 'direct remote access' by security authorities as breaching the essence of privacy, or at least deserving of heightened scrutiny.[102]

---

[99] Reference is made to Robert Alexy's theory of constitutional rights (n 93).

[100] Human Rights Committee, General Comment No. 37 on freedom of assembly (2020), para. 40.

[101] Ibid. para 36.

[102] See especially: CJEU, Case No. C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650, para 94; ECtHR, *Podchasov* v. *Russia* (n 20) para 80, 'direct remote access by security authorities'; *Szabó and Vissy* v. *Hungary* (n 16), para 68 referring to the 'massive monitoring of communications' and 'masses of data'; or

This is so even if the chain of reasoning has not always been clearly articulated by courts. The conclusion that mass measures may cause the worst intrusions into individual rights may appear counter-intuitive. The inviolable essence of a human right is expected to be precise and narrow, capturing only clear cases of incompatibility. From this perspective, such a narrow essential core would be surrounded by a much larger scope of validity of the same right conceived of as a principle that is subject to a proportionality assessment. Yet, from the perspective of a specific individual, being hit by suspicionless surveillance that intrudes deep into the core aspects of privacy including its most intimate dimensions is a violation of the right to privacy, irrespective of how many other individuals are put in the same situation. Human rights violations occurring on a massive scale are still individual human rights violations.

### *3.2.2. The Court's recognition of an essential core of privacy in Podchasov*

Despite references to the essence of Article 8 being conspicuously absent from the Court's judgments in BBW and CFR, the Court did explicitly recognise its existence in the 2024 case of *Podchasov* v. *Russia*. In this case, the Court stated that the legislation at stake 'permits the public authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications'. Therefore, 'it impairs the very essence of the right to respect for private life'.[103] Interestingly, but for the emphasis on safeguards, the phrasing is identical to that of the CJEU in *Schrems I*.[104] The qualification ('and without sufficient safeguards') allows the Court to abstain from following the CJEU in declaring that such generalised access regime always or inherently impairs the essence of the right to privacy. Instead, the Court seems to preserve the possibility that, should adequate (procedural) safeguards be implemented,[105] such regimes might be found to be ECHR-compliant. Consequently, while the Court recognises an essential core of the right to privacy in *Podchasov*, procedural conditions could still define the scope of application of that substantive core.

Yet, despite the reference to safeguards, *Podchasov* can hardly be reconciled with BBW and CFR. The eight-part procedural test developed by the Court in BBW and CFR is an abstract 'in accordance with law' test rather than a test about the substantive essence of privacy and its safeguards. In *Podchasov*, the Court could have satisfied itself by applying the eight-part test and finding a violation.[106] Instead, the Court found it necessary to 'examine with particular attention whether the domestic law provides adequate and sufficient safeguards against abuse'[107] and found that the Russian legislation at stake impaired 'the very essence' of privacy, overstepping 'any acceptable margin of appreciation'.[108] The distinguishing factor put forth by the Court seems to be the combination of 'the retention of all Internet communications of all users, the security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications.'[109] Notably, *Podchasov* concerned direct, indiscriminate access to the content of communications,

---

the notion of 'bulk interception' forming the core of BBW and CFR. In BBW, Judge Pinto de Albuquerque also refers to it as 'suspicionless interception'.

[103] *Podchasov* v. *Russia* (n 20), para 80.

[104] Case No. C-362/14 (n 102), para 94.

[105] As we explain below, we do not believe that satisfying the eight-part procedural test developed in BBW and CFR would be sufficient.

[106] This is what the Court did in *Roman Zhakarov* (n 16), which concerned the same legal regime and in which the Court applied a similar procedural test to find a violation of Article 8. See *Podchasov* v. *Russia* (n 20), paras 74-75.

[107] *Podchasov* v. *Russia* (n 20), para 71.

[108] *Podchasov* v. *Russia* (n 20), para 80.

[109] *Podchasov* v. *Russia* (n 20), para 80.

whereas BBW and CFR primarily involved metadata. Here, we merely note that the qualitative distinction between content and metadata has fallen apart at least since the systematic deployment of precise location tracking, which entails determination of the precise whereabouts of an individual at a specific time, including whom they met and whether they visited privacy-sensitive services, such as a psychiatrist, an abortion clinic or a gay bar. But even disregarding that, *Podchasov* remains in tension with BBW and CFR, lest one accepts the premise that the Court does not treat all member states with equal trust. Or, more accurately, the Court seems to exhibit an extraordinary – and, in our view, legally unfounded – level of trust in Western European states' good-faith use of mass surveillance.

*Podchasov* can therefore be analysed as a step in the right direction, demonstrating that the presumption of legality is rebuttable and that a structured permissibility assessment remains possible. Such an assessment includes, as a threshold condition, the inviolability of the essence of privacy and, thereafter and if pertinent, the proportionality between the benefit delivered for the legitimate aim and the resulting human rights harm. In this regard, the Court's confirmation that Article 8 contains an inviolable essential core that, if breached, renders any proportionality assessment unnecessary is extremely significant. This recognition opens a path for new claims seeking recognition of other core aspects of the right to privacy.

## 4. The Effects of the Court's Caselaw on the Protection of Privacy

Unavoidably, the Court's permissive caselaw on digital forms of surveillance has had and will have effects on how states in Europe and even elsewhere legislate on and deploy or allow existing and future techniques of surveillance and to what extent the right to privacy remains protected. In particular, if the Court does not define sufficient 'bright lines' that states must not cross when relying on surveillance in the name of protecting their national security or other collective goals, then an erosion or withering away of privacy is in part attributable to the Court.[110]

This erosion could be described as the result of a dual extension of the post-9/11 trade-off mentality according to which the end justifies the means. The Court, in recognising that the end of fighting terrorism justifies mass surveillance means adopted by Western European states, gave a signal in favour of new means being equally justified and of the original means also being used to pursue additional ends. In this section, we analyse the practical impact of the Court's caselaw on the growing potency of the national security exemption throughout Europe, the surveillance means legalised by states, and the right to privacy itself.

### 4.1. Effects on the Potency of the National Security Exemption throughout Europe

As the ECtHR Registry's factsheet states, matter-of-factly, governments' invocations of the fight against terrorism are 'invariably' accepted as legitimate by the Court.[111] In the previous section, we demonstrated that, in its caselaw on bulk data collection, the Court's blind trust in Western states' good faith has transformed the proportionality assessment into a procedural test when mass surveillance is at stake. The procedural turn in the ECtHR's caselaw has also redefined the meaning and potency of the national security clause contained in Article 8. Since the Court does not control the suitability, necessity, or proportionality of the actual measures taken by states under the declared aim of fighting terrorism or protecting national security, this

[110] Lock (n 72).

[111] CoE Registry, Key Theme 'Terrorism Surveillance Measures' (updated 31/08/2025): https://ks.echr.coe.int/documents/d/echr-ks/surveillance-measures

'legitimate aim' has become both very vague and extremely potent. In effect, it provides states with a 'carte blanche' for increasingly intrusive surveillance measures. This is particularly the case for states perceived as democratic by the Court, whose claims and assessments are often taken at face value.[112]

Indeed, when Western European states invoke national security to justify an interference with the right to privacy, the intensity of the Court's scrutiny has become minimal. Hence, a threat to national security need not be imminent, nor does it need to be identified. It may well be potential and cumulative, and described by the state in a highly abstract way ('national security threats').[113] The means chosen by the state are also readily presumed as effective for achieving the declared aim of fighting terrorism, without any demonstrated utility or justification required.[114] In cases against some other states, in contrast, the Court is keen to examine specific arrangements with 'particular attention' due to their being 'particularly prone to abuse'[115] and to apply a 'strict necessity' test.[116] It is also more insistent that procedural safeguards should operate in practice,[117] and requires the government to 'illustrate the practical effectiveness of the supervision arrangements with appropriate examples',[118] thus showing some healthy distrust towards respondent states' claims. It can only be regretted that the Court does not exercise the same level of oversight over all states' invocations of the fight against terrorism or national security.

This is all the more regrettable since the Court of Justice of the European Union (CJEU), originally more protective of privacy rights in its caselaw on mass surveillance and data retention, has begun following suit in recognising a wide national security exemption. Its initial pronouncement in *Digital Rights Ireland*[119] annulled the Data Retention Directive[120] and rejected a model of mass surveillance based on general and indiscriminate retention of communications metadata as incompatible with the Charter of Fundamental Rights of the European Union (CFREU).[121] In this landmark judgment, the CJEU rejected the possibility that indiscriminate data retention could be a proportionate interference with the right to respect for private and family life (Article 7 CFREU) and the protection of personal data (Article 8 CFREU). The CJEU's principled opposition to mass surveillance was reaffirmed in further cases

---

[112] See, e.g., *Big Brother Watch* (n 17), para 323, and *Centrum för rättvisa* (n 17), para 237.

[113] See, e.g., the UK Government's submission (e.g., para 287) and the third-party interventions by France, the Netherlands, and Norway in *Big Brother Watch* (n 17), paras 300-310: 'hitherto unknown threats' (para 287) 'international and cross-border crime' (para 300). The Court itself uses abstract references to 'new threats' to find that states' bulk interception regimes are 'valuable' (para 323).

[114] Chao Jing, 'The ECtHR's Suitability Test in National Security Cases: Two Models for Balancing Human Rights and National Security' (2023) 36 Leiden Journal of International Law 295. While this is not the author's argument, clear patterns emerge when looking at the cases that the author identifies as 'debiasing' the Court's two models, with Russia and Turkey triggering a heightened scrutiny of national security measures under the 'human rights model' compared to Western states.

[115] *Roman Zhakarov* v. *Russia* (n 16), paras 271 and 270, *Podchasov* v. *Russia* (n 20), para 73.

[116] *Szabo and Vissy* v. *Hungary* (n 16), para 73.

[117] E.g., *Roman Zhakarov* v. *Russia* (n 16), para 263, *Ekimdzhiev and others* v. *Bulgaria* (n 20), para 419.

[118] *Szabo and Vissy* v. *Hungary* (n 16), para 88.

[119] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others (C-293/12) and Kärntner Landesregierung and Others (C-594/12) [2014] ECLI:EU:C:2014:238.

[120] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communications networks and amending Directive 2002/58/EC, OJ L105/54, 13.4.2006 (Data Retention Directive).

[121] Charter of Fundamental Rights of the European Union (2007/C 303/01).

concerning national data retention regimes in EU member states,[122] international data sharing,[123] or the transfer of Passenger Name Record data.[124]

However, in its 2020 decision in *La Quadrature du Net*[125] (LQDN), the CJEU reversed its previous principled stance by introducing a national security exemption. In LQDN, the CJEU considered that the Charter allows for general, indiscriminate preventive data retention when member states are confronted with a 'serious threat […] to national security which is shown to be genuine and present or foreseeable'.[126] Signalling a newfound convergence with the ECtHR, LQDN results in the abstract acceptance of bulk data retention (and thus bulk data collection as a necessary prior step) as a proportionate interference with human rights when the aim pursued is the protection of national security. As the ECtHR did in *Big Brother Watch* and *Centrum för rättvisa*, the CJEU attempts to restrain (rather than outlaw) bulk data retention under the national security exemption by requiring procedural safeguards. Yet, the CJEU's convergence with the ECtHR's acceptance of mass surveillance as inevitable and necessary has serious consequences for effective privacy protection in Europe.

The legitimising trend started with LQDN has been confirmed by the CJEU in several recent decisions. First, in *Ligue des Droits Humains*,[127] concerning the Passenger Name Record (PNR) Directive,[128] the CJEU approved the surveillance regime established by the PNR Directive as compatible with the CFREU. In so doing, the CJEU took a different path than it had done in *Digital Rights Ireland,* where it annulled the Data Retention Directive on the ground that indiscriminate data retention would be incompatible with fundamental rights. In *Ligue des Droits Humains*, instead, the CJEU strictly circumscribed the PNR Directive's transposition into member states' national law through a restrictive interpretation of its provisions (leading to its alteration 'beyond recognition'[129]). The difference between its landmark 2014 case and this 2022 ruling lies in the blurring of an established 'bright line' and the abstract acceptance of mass surveillance as a proportionate and legitimate measure in response to national security threats. The CJEU also reaffirmed the national security exemption in a preliminary ruling concerning Germany's telecommunications data retention law, although in this case the legislation at stake was judged non-compliant with EU law.[130] Most recently, in *La Quadrature du Net II*[131] (LQDN II) the CJEU Full Court further lowered privacy protections by exempting whole categories of data (in this case, IP addresses and identifying data) from scrutiny on the

---

[122] Joined Cases C-203/15 and C-689/15, Tele2 Sverige AB v. Postoch telestyrelsen (C-203/15) and Secretary of state for the Home Department v. Tom Watson and Others (C-689/15) [2016] ECLI:EU:C:2016:970.

[123] C-362/14 (n 102) and C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559.

[124] Case Opinion 1/15, ECLI:EU:C:2016:656.

[125] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier Ministre and Others, ECLI:EU:C:2020:791.

[126] Ibid, para 137.

[127] Case C-817/19, Ligue des Droits Humains v. Council of Ministers, ECLI:EU:C:2022:491. For a commentary, see Sophie Duroy, 'Case C-817/19, Ligue Des Droits Humains v. Council of Ministers (C.J.E.U.)' (2023) 62 International Legal Materials 611.

[128] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[129] Christian Thönnes, 'A Directive Altered beyond Recognition' [2022] Verfassungsblog <https://doi.org/10.17176/20220623-153431-0>.

[130] Joined Cases C-793/19 (SpaceNet AG) and C-794/19 (Telekom Deutschland), ECLI:EU:C:2022:702.

[131] Case C-470/21, La Quadrature du Net and Others v. Premier Ministre, ECLI:EU:C:2024:370.

basis that the privacy infringement cannot be 'categorised as "serious"'.[132] As Marco Mauer highlights, 'the [CJEU] provides detailed guidance on how to design a national regime for bulk retention of IP addresses and identifying data'.[133] Criticised both for surrendering to member states' refusal to comply with previous (more protective) rulings and for doing away with anonymity on the internet,[134] LQDN II may turn out to be as damaging to effective privacy protections as the ECtHR Grand Chamber's eight-part procedural test in BBW and CFR.

The protection of national security has thus become a powerful enough aim to justify highly intrusive bulk interception and retention regimes that were previously deemed impermissible by the CJEU. The fact that EU law provided a comparatively higher level of privacy protection against mass surveillance was so clear that Norway, intervening in BBW, 'encouraged the Court to refrain from importing concepts and criteria from the CJEU', noting in particular that 'the CJEU also formulated "proportionality" differently, using a "strict necessity" method which did not compare to that used by the Court'.[135] The CJEU's subsequent abandoning of its principled opposition to mass data collection and retention is, therefore, all the more regrettable. In this respect, the influence of the ECtHR in *decreasing* privacy protections also in the EU legal order is notable.

As a result, the European normalisation of mass surveillance may now seem complete, leaving few hopes of meaningfully constraining and curtailing the development of mass surveillance through the powerful courts of the region. Further, this shift has repercussions at the law-making level in the EU. Negotiations surrounding the AI Act initially ambitioned banning automated facial recognition in public spaces.[136] However, the AI Act passed by the European Parliament on 13 March 2024 contains numerous exceptions: automated facial recognition may be used in real time – after judicial or administrative authorisation – in cases of assault and battery, homicide, drug trafficking or to prevent a terrorist attack.[137] The leading country to push for these exceptions was France,[138] whose police had been using software with facial recognition technology enabled by default since 2018, outside any legal framework or authorisation.[139] Since the passing of the Act, several EU member states have given or

---

[132] Ibid, para 90.

[133] Marco Mauer, 'The Unbearable Lightness of Interfering with the Right to Privacy: ECJ on Data Detention in La Quadrature Du Net II' [2024] Verfassungsblog <https://verfassungsblog.de/the-unbearable-lightness-of-interfering-with-the-right-to-privacy/>.

[134] Elif Mendos Kuşkonmaz, 'Of Minor Benefits and Major Costs' (2024) Verfassungsblog <https://doi.org/10.59704/bda8dcecc2247532>; Marcin Rojszczak, 'Data Retention Laws and La Quadrature Du Net II' (2024) Verfassungsblog <https://doi.org/10.59704/7243fc81d0e53381>.

[135] *Big Brother Watch* (n 17), para 310. Though note that the ECtHR did apply a strict necessity test in *Szabo and Vissy* v. *Hungary* (n 16), para 88.

[136] Alice Giannini and Sarah Tas, 'AI Act and the Prohibition of Real-Time Biometric Identification' (2024) Verfassungsblog <https://doi.org/10.59704/a15aa6e58151c853>.

[137] European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[138] Luca Bertuzzi, 'AI Act: MEPs Mull Narrow Facial Recognition Technology Uses in Exchange for Other Bans' *www.euractiv.com* (6 November 2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-meps-mull-narrow-facial-recognition-technology-uses-in-exchange-for-other-bans/>.

[139] 'La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale' *Disclose* (14 November 2023) <https://disclose.ngo/fr/article/la-police-nationale-utilise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale/>.

announced their intention to give law enforcement the ability to use real-time facial recognition technology through cameras in public places.[140]

### 4.2. Effects on the Surveillance Means Legalised by States

By taking Western states' national security claims at face value and failing to uphold a non-negotiable bright line to protect the essential core of privacy, the ECtHR has redefined the contours of privacy in its adjudication of ECHR Article 8 complaints, thereby expanding the range of legitimate uses of digital technologies for surveillance purposes. National security is so broadly understood that invoking it legitimises more and more surveillance and digital technologies. And since actual benefits towards national security are not assessed by the Court, what is 'suitable' when fighting terrorism under Article 8 has come to include more and more intrusive means. As the Court appears to check only whether mass surveillance regimes are 'in accordance with law' and whether the legal framework fulfils its procedural test, states now have an incentive to provide a legal basis for their most intrusive surveillance practices to legitimate them. A recent yet significant limit to this development was brought by the Court's 2024 judgment in *Podchasov*, which reaffirms the existence of 'bright lines' regarding mass surveillance. However, the effects of the Court's earlier permissive caselaw have already been felt and the development and legalisation of new surveillance measures will be difficult to roll back.

Taking advantage of the permissive environment, in May 2023, France promulgated a law on the 2024 Olympic and Paralympic Games.[141] Despite its name, the law has more to do with surveillance than sports.[142] In particular, its Article 7 creates a legal basis for algorithmic video surveillance (AVS), that is, video surveillance that relies on artificial intelligence to process the images and audio of video surveillance cameras in order to identify human beings, objects, or specific situations. Individuals in public spaces in France are now subjected to algorithmic-driven identification and determination of whether their behaviour is suspicious. Factually, this was already happening in several French cities (for instance in Toulouse since 2016[143]) and in some railway services, but without any legal basis.

The legal basis for AVS provided by Article 7 legitimises a practice that ignores France's human rights obligations but, should the ECtHR apply the same procedural oversight as in BBW and CFR, may not be assessed as such by the Court. AVS constitutes a clear infringement on the right to privacy and on freedom of assembly and association. It also has a chilling effect on many other human rights.[144] Article 7 provides a legal basis for the use of AVS (in contrast with its earlier use in France that was devoid of any legal basis and, as such, was clearly unlawful under human rights law), and the aim pursued (ensuring the security of major sporting events) will certainly be recognised as legitimate. In the process of assessing human rights compliance, the issues therefore lie at the steps of necessity and proportionality.

---

[140] E.g., in March 2025, the Hungarian parliament passed three legislative amendments allowing the Hungarian police to use facial recognition technology in all types of infraction procedures; in March 2026, the Swedish government submitted Proposition 2025/26:150 to the parliament, seeking to authorise police use of artificial intelligence for real-time facial recognition.

[141] LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000046777392/

[142] The following analysis reuses material from Sophie Sophie Duroy, 'Big Brother is Watching the Olympic Games – and Everything Else in Public Spaces' [2023] Verfassungsblog <https://doi.org/10.17176/20230322-185302-0> accessed 4 October 2023.

[143] Technopolice, Fiche 'Toulouse': https://technopolice.fr/toulouse/

[144] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.

However, these may never be addressed if the Court satisfies itself by applying its procedural safeguards test. It bears emphasising here that the burden of proof should normally be on the government. Hence, the government should have to demonstrate, using appropriate data and evidence, that AVS is both effective and *the least intrusive measure* to secure national security and public order effectively. Furthermore, the government should be expected to show that restrictions upon the right to privacy and freedom of assembly and association are outweighed by the actual benefits from AVS. Such justifications are missing from both the law and the public discourse surrounding it.[145]

The effectiveness of video surveillance to counter national security threats has never been demonstrated.[146] Further, the extremely low base rate of terrorism[147] means that false positives are the norm. Based on studies of low-probability threat detection, the correct identification of a terrorist by facial recognition software would occur in fewer than one case per thousand flagged individuals, implying that over 99.9% of those identified would be false positives.[148] Since AVS and facial recognition are based on the same image analysis and biometric surveillance algorithms (the former isolates and recognises bodies, movements or objects, while the latter detects a face), this finding is particularly concerning.

Moreover, AVS arguably threatens the essence of the right to privacy and data protection, hence rendering any proportionality assessment unnecessary.[149] In fact, the human rights risks posed by AVS are so high that discussions on the EU AI Act originally envisioned a formal ban,[150] defeated only because of France's stern advocacy.[151] However, litigation before the ECtHR could prove risky. Following the Court's approach in *Podchasov* should lead to AVS being considered inherently disproportionate due to infringing the essential core of the right to privacy. However, should the Court instead apply the same lower level of oversight as in BBW and CFR, France's invocation of the protection of national security and the legal basis and safeguards provided in the Olympics law might be considered sufficient for AVS to be deemed compatible with Article 8 ECHR.

France was the first EU member state to legalise AVS, creating a worrisome precedent and participating in normalising biometric mass surveillance in Europe. Despite the statement contained in the law that AVS will not 'use any biometric identification system, process any biometric data or implement any facial recognition technique', its very functioning implies the collection and processing of biometric data. Biometric data is defined in the General Data Protection Regulation (GDPR) as 'personal data resulting from specific technical processing

---

[145] For an analysis, see Félix Tréguer, *Technopolice: la surveillance policière à l'ère de l'intelligence artificielle* (Éditions Divergences 2024).

[146] Alois Stutzer and Michael Zehnder, 'Is Camera Surveillance an Effective Measure of Counterterrorism?' (2013) 24 Defence and Peace Economics 1.

[147] Marc Sageman, 'The Implication of Terrorism's Extremely Low Base Rate' (2021) 33 Terrorism and Political Violence 302.

[148] Alexander Schulan, 'Behavioural Economics of Security' (2019) 4 European Journal for Security Research 273 Table 2. While modern facial recognition systems have improved, these figures illustrate the inherent challenges posed by low-base-rate events, rather than representing the performance of any specific current system.

[149] 'Open Letter | France: Proposed Olympic Surveillance Measures Violate International Human Rights Law' <https://www.statewatch.org/news/2023/march/france-proposed-olympic-surveillance-measures-violate-international-human-rights-law/>.

[150] See: Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))(1): https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

[151] La Quadrature du Net, 'EU AI Act Will Fail Commitment to Ban Biometric Mass Surveillance' *La Quadrature du Net* (18 January 2024) <https://www.laquadrature.net/en/2024/01/18/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance/>.

relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person'.[152] AVS cannot be used for detecting suspicious events in public space without collecting and processing the physical, physiological and behavioural features of the individuals present. The effectiveness of the system further rests on the possibility to isolate individuals in a crowd, thereby leading to their 'unique identification' – regardless of whether their name or ID number is known. Hence, Article 7 of the Olympics law constitutes an effective legalisation of biometric mass surveillance. In addition, while the use of AVS is presented as an experiment in the law, experience and research clearly show the strong lock-in and mission creep effects of national security measures.[153]

The Court is not responsible for individual member states' decisions to adopt intrusive surveillance measures, and it remains possible that it would deem France's use of AVS incompatible with the ECHR. However, when the Court granted a high degree of legitimacy to the British and Swedish bulk interception regimes, deeming them 'valuable' and 'vital', it also provided a veil of legitimacy to other member states' mass surveillance regimes. By not recognising the essence of the right to privacy and not drawing any bright line in BBW and CFR, the Court implicitly encouraged member states to increase their mass surveillance capacities, even providing them with clear procedural guidelines for making them appear ECHR-compliant. The partial reversal brought by *Podchasov* might, in this respect, simply be too little too late unless followed soon by a high-profile Western European case reaffirming the inviolability of the essence of privacy.

### 4.3. Effects on the Human Right to Privacy

Through its permissive caselaw on mass surveillance, the Court redefined the contours of privacy in its adjudication of Article 8 complaints, putting into question the substantive scope of individuals' right to privacy and states' corresponding obligations. By default, national security claims are now assumed to be legitimate. In turn, this implies that it is accepted that individuals are all assumed to be potential national security threats, meaning that they must relinquish their privacy by default. Article 8 now applies in a reverse fashion when it comes to digital surveillance. The burden of proof has been put on the individual to show that they deserve privacy in respect of ubiquitous digital surveillance, while the secrecy surrounding its operation makes it impossible for them even to gather and present their evidence. National security has been elevated from a *prima facie* legitimate aim that may justify lawful, necessary and proportionate limitations on privacy, to a *de facto* exception to human rights.

Invoking the national security exemption gives states a wide margin of appreciation in the choice of 'suitable' means to achieve the aim. However, most surveillance techniques are also capable of being used beyond their stated purpose of 'fighting terrorism' or 'maintaining public order'. Consequently, the declared purpose and aim of national security measures do not necessarily constrain governments and may never be assessed by the Court. When a technique or measure has been considered lawful, it will be tempting to use it beyond the original objective and to justify it through procedural safeguards.

As explained earlier, it is a misperception that the right to privacy or its core content would be a 'right to be left alone', demarcating a solitary individual and strictly personal sphere. As all human rights, the right to privacy is relational and dynamic. It is primarily a liberty (privilege),

[152] General Data Protection Regulation (n 14), Article 14.

[153] The French Government already attempted to extend the use of AVS to public transportation absent any major sporting or similar event, but this disposition was censored by the constitutional council for procedural reasons. Article 15 (censored) of LOI n° 2025-379 du 28 avril 2025 relative au renforcement de la sûreté dans les transports.

namely a person's protected freedom to decide what information to share, and with whom. Its correlative is the duty of the state (and others) not to overrule that freedom of choice. However, the shifting of the burden of proof onto the individual, now responsible for showing why they deserve privacy, has rendered moot this conceptualisation.

The first foreseeable, yet extremely chilling, effect of this development is that seeking to ensure one's privacy can be interpreted as evidence of criminal conduct or intent. In a recent criminal trial against left-wing activists, the Paris tribunal convicted seven individuals for the offense of participation in a 'criminal terrorist association'[154] despite no discernible terrorist or violent project having been uncovered, the 'members' of the group not all knowing one another, and them not being linked to any known terrorist organisation.[155] One of the key elements underpinning the convictions was the lawful use of privacy-protecting applications.[156] In a blunt reversal of the burden of proof, the court treated the use of encrypted chat applications and privacy-preserving search engines as indicative of criminal intent and activity.

This trend extends beyond the courtroom. Many states now require individuals to provide encryption keys to their devices or social media accounts at border checks[157] or during police custody.[158] While the CJEU has clarified that judicial authorisation is required for access, it has also affirmed that police access to telephone data is not limited to serious offenses.[159] In practice, when the police invoke national security or public order to request access, privacy protections are rendered largely meaningless. In France, for example, refusal to comply with such requests constitutes a separate infraction, independent of the offense under investigation. In the above-mentioned trial, three of the defendants were additionally charged with "refusing to hand over a secret convention for deciphering a means of cryptology" [160] after they declined to provide telephone or email passwords, citing the right to respect for their private life.

The ECtHR's deferential balancing exercise may not have intended this but, as it legitimated states' mass surveillance apparatuses, it may have emptied the right to privacy of its protective characteristics in relation to the invocation of national security. While the recognition of an essential core of the right to privacy – and of the importance of encryption measures to safeguard this right[161] – in *Podchasov* is most welcome, the effects of the Court's earlier

---

[154] In French: 'association de malfaiteurs terroriste'. This offense is repressed by Article 421-2-1 of the French code pénal. It is generally viewed as controversial as adherence to any criminal plan is not a condition for participation in a terrorist criminal association.

[155] For a report on the unpublished decision, see 'Affaire « du 8 décembre 2020 » : sept militants d'ultragauche condamnés pour association de malfaiteurs terroriste, dans une ambiance tendue' *Le Monde.fr* (22 December 2023) <https://www.lemonde.fr/societe/article/2023/12/22/affaire-du-8-decembre-2020-sept-militants-d-ultragauche-condamnes-pour-association-de-malfaiteurs-terroriste-dans-une-ambiance-tendue_6207364_3224.html>.

[156] La Quadrature du Net, 'Encryption Discussion during the 8 December Trial: From Myth to Reality' *La Quadrature du Net* (15 December 2023) <https://www.laquadrature.net/en/2023/12/15/encryption-discussion-during-the-8-december-trial-from-myth-to-reality/>.

[157] See, e.g., Samuel Singler, 'Surveillance Evangelism: Private Technology Companies and the Digital Futures of Crimmigration Control' (2025) 29 Theoretical Criminology 365; Sebastian Weydner-Volkmann, 'Using Open, Public Data for Security Provision: Ethical Perspectives on Risk-Based Border Checks in the EU' (2023) 8 European Journal for Security Research 25.

[158] Case C-548/21*, Bezirkshauptmannschaft Landeck*, ECLI:EU:C:2024:830.

[159] Ibid.

[160] Article 434-15-2 of the French code pénal. This offense is punishable by three years in prison since a 2022 Court of Cassation judgment: Cour de cassation, Pourvoi n° 21-83.146, Assemblée plénière, 7 novembre 2022, ECLI:FR:CCASS:2022:PL90659.

[161] *Podchasov* v. *Russia* (n 20), para 76.

caselaw on the right to privacy have permeated states' practices and domestic laws so deeply that this development will be extremely hard to reverse.

## 5. Conclusion: An Attempt at Cautious Optimism

From the perspective of substantive human rights protection, the main strand of development in European caselaw on digitalised means of surveillance is extremely worrisome. We discussed the wide-ranging damaging effects and continuities between the ECtHR Grand Chamber cases of *Big Brother Watch*[162] and *Centrum för rättvisa*[163] and the 2024 CJEU Full Court ruling in *La Quadrature du Net II*.[164] As we demonstrated, this judicial acceptance of contemporary surveillance regimes falls in the long shadow of 9/11. European courts, and especially the ECtHR, have adopted a highly deferential approach to Western European states that are presumed democratic and human-rights-compliant. As we explained in the previous section, this caselaw has already had detrimental effects on the protection of privacy in Europe. In consequence, we fear that the ECHR system cannot be trusted to constitute a suitable framework for the effective protection of individuals against increasingly intrusive surveillance through digital technologies.

However, our analysis of the 2024 *Podchasov*[165] chamber judgment by the ECtHR drives us to temper slightly our pessimistic outlook. Rather than dismissing the case as a manifestation of double standards *because* it was a Russian case, we suggest that, in human rights law, cases from 'bad countries' may instead produce good caselaw precisely because they provide the judges with an opportunity to draw or reaffirm bright lines that must not be crossed. Hence, we wish to acknowledge the merits of the ruling and allow ourselves to be cautiously optimistic as to its role in helping the ECtHR to clarify the law now and in the future.

This article's main contribution in respect of the theoretical foundations of IHRL relates to our criticism that, in its case law on surveillance, the ECtHR has shied away from the foundational concepts, distinctions and principles of international human rights law. We showed that the Court has abandoned the quest for a structured proportionality test, instead turning to proceduralism. Further, the Court's inconsistent use of the concept of essence of Article 8 in its caselaw reeks more of double standards than it establishes bright-line rules for all states. As we argued in our analysis, the solution to the problems created by the Court's deference and proceduralist approach, as exemplified by BBW and CFR, would be a better 'theory' of the right to privacy and the permissibility of limitations thereof. We have sought to show that this theory requires upholding and reinforcing a structured test of permissible limitations, acknowledging that it includes the legal basis (including quality of the law) as a threshold requirement (a rule), but also the inviolability of the essence as another threshold requirement (also a rule) and then, if these two requirements have been met, a structured assessment of proportionality (between principles) where demonstrated benefit towards the legitimate aim is a *sine qua non* condition of proportionality.

Such seems to be the path that the Court has chosen to follow in *Podchasov*. In consequence, we welcome *Podchasov* as a promise to return to the proper toolkit of IHRL in respect of mass surveillance. Proceduralism, manifesting itself as the Court's self-limitation to assess only legality, may have become the default approach to digital surveillance. However, for an

[162] *Big Brother Watch and Others* v. *The United Kingdom* (n 17).

[163] *Centrum för rättvisa* v. *Sweden* (n 17).

[164] Case C-470/21 (n 131).

[165] *Podchasov* v. *Russia* (n 20).

optimist, *Podchasov* shows that the presumption that the Court will automatically defer to national authorities' assessments can be rebutted by presenting a good reason to do so. This is indeed what transpires from the Court's highlighting of the 'extremely broad duty of retention' and law-enforcement authorities' 'direct remote access to all Internet communications and related communications data' in *Podchasov*.[166] Confirming the existence of bright-line rules that trigger a finding of a violation of Article 8 without a need to conduct a proportionality assessment, the ECtHR endorsed the principled and conceptually important view that the right to privacy contains an inviolable essential core. Hence, in *Podchasov*, the Court found that, because it allows access to the content of electronic communications 'on a generalised basis and without sufficient safeguards', Russia's regime of electronic mass surveillance 'impairs the very essence of the right to respect for private life under Article 8 of the Convention'.[167] This finding closed the case, and no further questions needed to be addressed.

The heuristic value of *Podchasov* is crucial. By returning to the foundations of international human rights law and endorsing the existence of an inviolable essential core of the right to privacy, the ECtHR has invited applicants, lawyers and social movements to come forward with additional good reasons for rebutting the presumption that a proceduralist approach would be sufficient when assessing the permissibility of mass surveillance regimes. Now that one element of the inviolable essential core of Article 8 has been confirmed, there will be a quest for claims that there are others.

[166] *Podchasov* v. *Russia* (n 20), paras 70 and 72.

[167] *Podchasov* v. *Russia* (n 20), para 80.