

Case Discussion

Commentary on the Judgment *Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” v. Colombia* – Emphasizing Informational Self-Determination as a Condition for the Exercise of the Right to Defend Human Rights

Lucas Reckziegel Weschenfelder¹ 

¹Universität Hamburg 

Contents

- I. Facts of the Case –
Members of CAJAR v.
Republic of Colombia
- II. Reasoning of the Court
- III. Commentary on the
Judgment
- IV. Conclusion
Vita

Citation:

Lucas Reckziegel Weschenfelder,
Commentary on the Judgment *Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” v. Colombia*, in:
MRM 31 (2026) 1, pp. 38–56.
<https://doi.org/10.60935/mrm2026.31.1.34>.

Received: 2026-02-12

Accepted: 2026-06-05

Published: 2026-08-13

Permissions:

The copyright remains with the authors.
Copyright year 2026.

Unless otherwise indicated, this work is licensed under a [Creative Commons License Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/). This does not apply to quoted content and works based on other permissions.

Summary – Unofficial Headnotes

(1) The establishment of a regime of state intelligence and surveillance without prior adoption of clear laws and legal norms – defining procedures, limiting access and data sharing, and ensuring that intelligence activities serve purposes consistent with the normative standards of a democratic society – is incompatible with the American Convention on Human Rights (ACHR).

(2) The exercise of state intelligence inherently tends to interfere with the rights to privacy, confidentiality, data protection, and informational self-determination. Accordingly, for an intelligence framework to be compatible with the ACHR, it must establish objective structures that comply with human rights standards and, moreover, create space for the exercise of individual rights.

(3) State surveillance structures must coexist harmoniously with the protection of human rights and with activities functionally linked to that purpose. States have not only a negative obligation to refrain from hindering the work of human rights defenders, but also a positive obligation to actively ensure safe and stable conditions in which such actors can carry out their activities without risks to their lives or those of their families.

(4) The Republic of Colombia failed to establish an adequate normative framework for state intelligence, particularly with respect to ensuring and promoting the protection of privacy, data protection, and informational self-determination of human rights defenders (Art. 11 para. 2, 3, Art. 13 para. 1), as well as safeguarding their function and, consequently, the right to defend human rights in the country (Art. 1 para. 1, Art. 4 para. 1, Art. 5 para. 1, Art. 8 para. 1, Art. 13 para. 1, Art. 16 para. 1, Art. 25 para. 1 ACHR).

(5) The Republic of Colombia, actively engaged in conduct that violated the human rights of human rights defenders, including their informational rights, as well as their rights to life (Art. 4 ACHR), personal integrity (Art. 4 para. 1, Art. 5 para. 1, 2 ACHR), freedom of expression and association (Art. 13 para. 1, Art. 16 para. 1 ACHR), honor (Art. 11 para. 1 ACHR), the right to know the truth (Art. 13 ACHR), freedom of movement and residence (Art. 22 para. 1 ACHR), protection of the family (Art. 17 para. 1 ACHR), and the rights of the children (Art. 19 ACHR), right of access to justice and judicial protection (Art. 8 para. 1, Art. 25 ACHR), and women’s rights and the corresponding duty to protect those rights, as set forth in the Convention of Belém do Pará (CBP) (Art. 1 para. 1, 2 CBP).

Human Rights (IACtHR) was consolidated with the condemnatory ruling of 18 October 2023, followed by an interpretative judgment on 16 October 2024, issued after requests for clarification by the parties.²

1. Factual Background

The proceedings concern a pattern of conduct spanning from the 1990s to 2020, affecting more than sixty identified victims, including family members and children. Colombian intelligence bodies – namely, the military forces, the National Police, and the Administrative Department of Security (DAS), all linked to the Executive – collected, processed, and stored intelligence data concerning multiple aspects of the victims’ private lives (para. 1). The factual record further indicates that the Colombian state engaged in sustained acts of violence, intimidation, harassment, and threats against members of CAJAR, persisting from the 1990s to the time of judgment (para. 1). State intelligence and law enforcement agencies also engaged as or with constituent members of paramilitary groups, resulting in an overlap between state and paramilitary structures aimed at creating an atmosphere of surveillance directed against members and human rights defenders associated with CAJAR (para. 1).

I. Facts of the Case – Members of CAJAR v. Republic of Colombia

The judgment in *Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” – CAJAR v. Republic of Colombia*¹ before the Inter-American Court of

2. Procedural History – the Commission’s Decision

The Commission on Human Rights (CIDH) acknowledged that while many acts of harassment by the state lacked clearly identified authorship (i.e., which agents were involved, what procedures were followed,

¹ IACtHR, *Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia* (Series C No. 506), judgment of 18 October 2023.

² IACtHR, *Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia* (Series C No. 544), judgment (interpretation sentence) of 16 October 2024.

and under what legal basis), given the nature of state intelligence operations,³ this lack of identification could not undermine the claims. Moreover, despite the absence of identified perpetrators, explicit statements and actions by state authorities contributed to the violence, including the provision of information to paramilitary groups and stigmatizing remarks linking CAJAR members to guerrilla groups. These measures, according to the CIDH, constituted not only a serious breach of the duty to protect, but were also openly contrary to that duty.⁴ The CIDH found that the Colombian state acted omisively by failing to conduct a serious and rigorous investigation into the facts, which would have enabled the clarification of the truth, the identification of those responsible, and the uncovering of “the sources of risk faced by CAJAR”.⁵

Moreover, the victims were denied access to effective procedural remedies capable of ensuring access to justice, including access to information and data held within state intelligence databases related to the events.⁶ Finally, the Commission noted that the experiences endured by the victims generated a broad sense of physical and psychological insecurity—a “well-founded fear”—which led to the exile of many CAJAR members and their families, including minor children.⁷

³ CIDH, *Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia* (Serie C No. 506), Informe No. 57/19 of 4 May 2019, para. 1.

⁴ Ibid.

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.

II. Reasoning of the Court

1. Summary of the Parties’ Arguments – Procedural Openness Over Time

a) The Victims’ Claims

In essence, the victims’ claims are grounded in the normative assertion that they were subjected to persecution by intelligence agents and paramilitary structures over varying periods, due to their status as human rights defenders (para. 1). The forms of persecution, harassment, and intimidation—both individual and collective (as an association) directed at them, their relatives, and their children (para. 326) were perpetuated through the instrumentalization of technological and computational tools, including surveillance, image and communication capture, data storage, and information sharing (paras. 195–302). These practices were accompanied by the dissemination of false information linking the work of human rights defenders to criminal-paramilitary groups (paras. 171–194), as well as concrete acts threatening their lives, in addition to forms of symbolic intimidation, such as vehicles following members, the presence of unidentified individuals in public spaces, as well as their entry into private premises without judicial authorization, letters containing objects, and telephone calls—generally carried out anonymously.

They further contend that the Colombian state not only acted affirmatively in enabling such practices, but was also omisive in failing to establish an adequate normative framework for the protection of human rights defenders. In particular, the state failed to conduct proper investigations into internal complaints, to elucidate the underlying facts, and to identify the public agents involved—including in instances of unlawful data and information

sharing—while also neglecting to afford adequate judicial and administrative protection to human rights defenders, and, furthermore, full and adequate access to the intelligence agency's database, which was denied through multiple avenues of access to information, thereby also violating, from another perspective, the right to access of information and informational self-determination.

Within the limits of this section, it is not possible to enumerate all the claims. Particular emphasis is warranted, however, on the situation of women human rights defenders and their children (a gender-based dimension) (para. 881). One victim – who was both a woman and a mother – for example, received a defaced doll bearing burn marks and red stains in specific areas, including intimate parts of the human body, accompanied by a letter stating that her family was “very beautiful” and that she should take care not to “sacrifice” them (para. 888).

For this reason, the victims alleged that the Colombian state violated their human rights to privacy; data protection and informational self-determination (Art. 11 para. 2, 3, Art. 13 para. 1); the right to defend human rights (Art. 1 para. 1, Art. 4 para. 1, Art. 5 para. 1, Art. 8 para. 1, Art. 13 para. 1, Art. 16 para. 1, Art. 25 para. 1); the right to life (Art. 4); personal integrity (Art. 4 para. 1, Art. 5 para. 1, 2); freedom of expression and association (Art. 13 para. 1, Art. 16 para. 1); the right to honour (Art. 11 para. 1); the right to know the truth (Art. 13); freedom of movement and residence (Art. 22 para. 1); the right to family protection (Art. 17 para. 1); and the rights of children (Art. 19) and right of access to justice and judicial protection (Art. 8 para. 1, Art. 25) of the American

Convention on Human Rights (ACHR),⁸ added to the violation of women's rights and of the state's duty to eradicate violence of any kind, insofar as the state actively acted against such rights and also tolerated actions aimed at that end, as provided for in Art. 1 para. 1 and 2 of the Convention of Belém do Pará (CBP).⁹

b) The Colombian State's Submissions

The Colombian state argued that it was not responsible for the alleged violations and asserted that it had established a normative framework and concrete institutional structures capable of protecting the rights of human rights defenders. In particular the Colombian state asserted that, in the course of the Commission's investigation, it adopted appropriate public policies to ensure the security of human rights defenders,¹⁰ as well as new legislation and an administrative structure capable of effectively investigating, prosecuting, and holding accountable those responsible for actions deemed to violate human rights.¹¹ Furthermore, it claimed to have implemented additional measures, considered appropriate, to prevent intelligence agencies from engaging once again in illegal or abusive conduct.¹²

Notably, one of the state's principal defence strategies incorporated the very dynamics of the intelligence operations – characterized by anonymity, the absence

⁸ American Convention on Human Rights of 22 November 1969, UNTS vol. 1144, p. 123.

⁹ Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women of 9 June of 1994.

¹⁰ IACtHR, *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia* (Series C No. 506), Written final submissions of the Colombian state of June 2022, p. 78.

¹¹ *Ibid.*, p. 81.

¹² *Ibid.*, p. 53.

of identifiable agents, unlawful data and information sharing (without traceability), and a multiplicity of acts affecting multiple victims – that in part constitute the human rights violations. The Colombian state, as a preliminary matter, argues that it should not be held responsible because it is not possible to identify all the acts, their respective actors, and the actions that the victims claim to have suffered. What is occurring here, therefore, is the state instrumentalizing these situations – in essence, surveillance without a prior legal framework; information sharing without the possibility of traceability; unidentified public agents; and the exchange of information and actions involving unidentified para-state agents and actors – in order to construct a procedural narrative aimed at preventing the claim from being admitted and, ultimately, at avoiding state responsibility in the event of adjudication.¹³

Additionally, the state failed to provide access to all data and information contained in its intelligence archives, which include relevant evidence pertaining to the case. It invoked confidentiality and public-interest grounds to obstruct the victims' access to materials likely capable of clarifying the facts, substantiating their claims, and supporting their defence and potential reparations.

2. Findings of the Court

The considerations of the IACtHR, can be divided between the specific human rights violations established in the judgment and the structural measures ordered by the IACtHR to the Colombian state. These measures form an integral part of the judgment and set forth conditions of reparation, including preventive actions –

aimed at ensuring that such events do not recur – as well as promotional, symbolic, and media-oriented measures related to the case and to other human rights defenders in the country.

a) The Human Rights Violations Identified by the IACtHR

The IACtHR concluded that the Colombian state violated the victims' rights: (i) to life and personal integrity, as recognized in Art. 4 para. 1 and Art. 5 para. 1 ACHR (para. 5); (ii) to personal integrity under Art. 5 para. 2 ACHR (para. 6); (iii) to personal integrity and the rights of the child, as recognized in Art. 5 para. 1 and Art. 19 ACHR (para. 7), coupled with violations of women's rights, insofar as the state failed in its duty to refrain from acts or practices of violence against women and in its obligations to respect and ensure such rights, pursuant to Art. 1 para. 1 ACHR and Art. 7 lit. a CBP (para. 7); (iv) to personal integrity under Art. 5 para. 1 in relation to Art. 1 para. 1 ACHR (para. 8); (v) to judicial guarantees and judicial protection under Art. 8 para. 1 and Art. 25 para. 1 ACHR; (vi) to privacy under Art. 11 para. 2 and Art. 11 para. 3 ACHR; (vii) to freedom of thought and expression under Art. 13 para. 1 ACHR; (viii) to honour under Art. 11 para. 1 ACHR; (ix) to the rights of the child under Art. 19 ACHR; (x) to freedom of thought and expression in conjunction with freedom of association, under Art. 13 para. 1 and Art. 16 para. 1 ACHR; (xi) to freedom of movement and residence under Art. 22 para. 1 ACHR; and (xii) to protection of the family under Art. 17 para. 1 ACHR (paras. 900–989).

Innovatively – and this is the analytical angle emphasized in this article – the Court (by a majority of four votes to one) held the Colombian state internationally responsible for violating the right to informational

¹³ Ibid., pp. 71–76.

self-determination, grounded in Art. 11 para. 2 and Art. 13 para. 1 ACHR, "in relation to the obligations to respect and ensure rights and to adopt domestic legal provisions established in Articles 1.1 and 2 of the same instrument," with respect to members and former members of CAJAR (para. 13).

In conjunction with this finding, the Court unanimously concluded that the Colombian state was internationally responsible for violating the right to know the truth, linked to the right of access to information under Art. 13 para. 1 ACHR, in relation to the obligations set forth in Art. 1 para. 1 ACHR (para. 14). The judgment further articulated these informational rights as a condition for the creation of a stable environment for the exercise of the right to defend human rights, thereby including them as 'prerequisites' for the effective enjoyment of such rights, holding unanimously that the state violated the right to defend human rights, as derived from Art. 4 para. 1, Art. 5 para. 1, Art. 8 para. 1, Art. 13 para. 1, Art. 16 para. 1, and Art. 25 para. 1 ACHR (para. 20).

The condemnatory judgment further allows individuals who did not formally participate in the proceedings to be recognized as victims and rights-holders within the legal relationship examined by the IACtHR, in which the Colombian state was found responsible for violations of the human rights of members of the CAJAR, thereby entitling them to the reparations established in the judgment (para. 95). This determination is adopted in light of the temporal dimension of the facts underlying the case, which span more than forty years, as well as the material conditions that characterize it, including the potential number of individuals involved, the functions performed in the defence of human rights, the environment created

by the state itself through actions and omissions, and the resulting difficulty in identifying all members of CAJAR and their families, as well as relevant facts, data and information that the Colombian state failed to investigate and to provide to the victims, their representatives, and the CIDH (para. 95).

b) Structural Measures Imposed

The judgment establishes a set of structural measures to be implemented by the Colombian state, coherently addressing the informational rights violations identified in the context of state intelligence activities over time. First, within a reasonable period, the state must investigate and clarify all acts of violence, threats, intimidation, and harassment perpetrated against the victims, as well as the functioning of intelligence activities carried out by various public bodies during the 1990s, and, where appropriate, prosecute and sanction those responsible (para. 22).

Additionally, the state must purge its intelligence archives in order to guarantee the effective exercise of the victims' right to informational self-determination with respect to data held about them (para. 23). It must also designate a competent authority to facilitate access, following such data cleansing, for other CAJAR members and their families – recognized as victims – to the individual reparations ordered by the Court, ensuring their effective implementation (para. 24).

Furthermore, the state is required to implement a system for collecting data and statistics on cases of violence against human rights defenders. For this, it is obligated to undertake normative adjustments to the national body of law concerning the legal structuring and regulation of state

intelligence activities.¹⁴ For example, the Court mandated the adoption of new legislation establishing reasonable, expeditious, free, and effective procedures to enable individuals to access and control their personal data contained in state intelligence archives, in accordance with the scope of the right to informational self-determination. The state must also revise its internal intelligence protocols and manuals (paras. 31–37).

These measures – centred on informational rights – constitute structural obligations incumbent upon the state and will be further examined in subsequent sections. Alongside these, the judgment imposes duties of material and psychological reparation, including the provision of healthcare to victims, training of state agents on human rights defence, the establishment of a national day honouring human rights defenders, the implementation of nationwide awareness campaigns addressing violence and stigmatization against such defenders (including audiovisual programs), and the creation of a fund dedicated to the prevention, protection, and assistance of human rights defenders in situations of risk (para. 1050).

III. Commentary on the Judgment

The IACtHR advanced multiple lines of reasoning in holding the Colombian state internationally responsible for violations against CAJAR members, as summarized above. This commentary focuses on a central dimension of the case, crucial for contemporary state – intelligence – citizen

relations, particularly regarding human rights defenders. Although the IACtHR has previously addressed issues related to privacy, data protection, informational self-determination, and access to information,¹⁵ this appears to be the first case articulating a normative link between informational self-determination as an autonomous right and the human right to defend human rights.

This commentary seeks not only to present the nuances of the case – within certain limits and perspectives, given the extensive number of facts, identified human rights violations, and victims – but also to demonstrate how the IACtHR, in an innovative manner, adopts a data-oriented approach to address violations of the rights of human rights defenders. It advances a specific argument intended to be generalizable to other regions of global society: in the absence of a systemic guarantee of informational self-determination – beyond its strictly subjective dimension – there is a concrete and indirect detriment (*chilling effect*) to the defence of human rights and to the very right to defend them.

1. The Right to Defend Human Rights: Conditions for Its Exercise and (the Specific) Violations by the Colombian State

The IACtHR understands that the status of a human rights defenders derives from the activities performed, regardless of whether the individual is a public official or a private actor, and irrespective of the category of rights protected. This status is not necessarily permanent and may arise

¹⁴ Republic of Colombia, Law No. 1621 of 2013; Republic of Colombia, Decree No. 2149 of 2017

¹⁵ IACtHR, *Claude Reyes y otros v. Chile* (Series C No. 151), judgment of 19 September 2006, para. 77; IACtHR, *Flores Bedregal y otras v. Bolivia* (Series C No. 467), judgment of 17 October 2022, para. 132.

from occasional actions (paras. 468–470). In this respect, the IACtHR adopts a functional criterion grounded in the activities carried out, recognizing as defenders not only lawyers but also other professionals involved in protecting victims. Given its broad and flexible nature, the concept includes legal assistants, political scientists, communication professionals, specialists from other fields, and technical and administrative staff whose functions contribute to the promotion and protection of human rights (paras. 468–470).

It further emphasizes that the effectiveness of human rights largely depends on the guarantees that enable defenders to act freely, as their activities are crucial for preventing impunity and for complementing the role of states and the Inter-American system (paras. 471–476). Moreover, international instruments, such as the United Nations Basic Principles on the Role of Lawyers¹⁶ and the Escazú Agreement¹⁷, the latter being directly binding on the states parties, and the former only indirectly, e.g., when incorporated into domestic legal systems or used as a source of law in national judgments and in decisions rendered by the IACtHR, both reinforce the states' obligations to ensure a safe environ-

ment and to prevent and sanction attacks against these actors (paras. 471–476).

The IACtHR establishes that states must ensure adequate conditions for the exercise of human rights advocacy, including by providing the necessary means for its exercise, protecting human rights defenders from threats, and refraining from creating obstacles to their work. States must also conduct serious and effective investigations into violations, thereby combating impunity. The IACtHR underscores that attacks against human rights defenders have both individual and collective effects, as they hinder society's access to the truth. For this reason, human rights defenders are recognized as essential to democracy and the rule of law, which imposes upon states a special duty of protection (paras. 477–478). The IACtHR further held that the state's actions and omissions were decisive in significantly affecting the regular activities of the human rights organization, insofar as they generated a chilling effect¹⁸ on CAJAR members in the exercise of their rights – particularly the freedom to practice their profession, freedom of expression, and freedom of association.

The decision of the IACtHR indicates that human rights defenders were exposed to a constant risk, manifested in multiple forms of violence, including attacks against life and privacy, repeated threats, interference with professional activities, as well as harassment, persecution, stigmatization, and unlawful surveillance by state authorities. Many of these acts appear to have remained unpunished, in light of deficiencies in effective investigations and the inadequacy of protection measures, thereby exacerbating the risk.

¹⁶ United Nations Basic Principles on the Role of Lawyers, UN Doc. A/RES/144/28 of 07 September 1990.

¹⁷ Regional Agreement on Access to Information, Public Participation and Justice in Environmental Matters in Latin America and the Caribbean of 4 March 2018, UNTS vol. 3388, p.16 (Escazú Agreement). The IACtHR makes specific reference to Art. 9 of the Escazú Agreement, which has binding force and establishes rights in favor of human rights advocates, and obligations for states parties to ensure, protect, and promote the human rights of human rights defenders, particularly in the field of environmental and climate protection (although generalizable to other areas, such as that of the present case) (para. 474).

¹⁸ Jonathon W. Penney, *Chilling Effects: Repression, Conformity, and Power in the Digital Age*, 2026, p. 111.

Moreover, within the context of armed conflict, the reasoning of the judgment suggests that defenders were frequently associated with the “internal enemy,” a legal and social conception adopted within the Colombian national system and linked to the doctrine of national security that emerged in the country during the 1960s, which, in turn, contributed to facilitating their persecution (paras. 462–486).

Although the situation evolved after 2016, risks persisted, particularly in areas with limited state presence. The Court also identified a pattern of attacks and delegitimization, including accusations of links to insurgent groups and intelligence operations aimed at neutralizing defenders. Accordingly, it concluded that members of CAJAR have faced, since the 1990s, a continuous situation of risk and extreme vulnerability (paras. 485–501).

2. Informational Self-Determination, Access to Information, and the Objective Framework for the Materialization of their Normativity

The rights to informational self-determination and access to information are interpretatively derived by the IACtHR from Art. 11 para. 2 (Right to Privacy, Honor, and Dignity) and Art. 13 para. 1 (Freedom of Thought and Expression) ACHR. The former provides that “No one may be the object of arbitrary or abusive interference with his private life, family, home, or correspondence, nor of unlawful attacks on his honour or reputation”. The latter establishes that “Everyone has the right to freedom of thought and expression. This right includes the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of

art, or through any other medium of one’s choice”.

a) Access to Information and Informational Self-Determination: Two Sides of the Same Coin

The reasoning of the IACtHR may be interpreted as seeking to establish a normative correlation between informational self-determination and the right of access to information. In this regard, the judgment articulates a judicial framework centered on access to data and information through organized, effective, diligent, expeditious, and cost-free procedures, both at the administrative and judicial levels – thus linking this line of reasoning to the broader right to judicial protection and guarantees. Furthermore, the decision can be read as acknowledging that, in contexts such as the present case, certain state-imposed limitations may arise, which may be considered valid and legitimate, particularly with respect to data and information contained in intelligence archives (para. 601).

That is why we can see that, in the judgment, there is an affirmation that the right to informational self-determination, alongside the right to access to information, requires both an objective and a subjective structure, including for the validation of potential limitations on access – especially in cases involving intelligence-related data.¹⁹ According to the Court’s reasoning, grounded in its prior jurispru-

¹⁹ Organization of the American States, Updated Principles on Privacy and Personal Data Protection, Resolution OEA/Ser.D/XIX.20 of 31 of December 2021; African Union, African Union Convention on Cyber Security and Personal Data Protection, Resolution EX.CL/846 of 27 June 2014; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 of 28 January 1981.

dence²⁰ and further developed for the present case, any limitation on the right of access to information must be previously established by law in a clear and precise manner, specifying the types of documents and information concerned, the conditions of their storage, and their retention period (para. 601). Such limitations must be exceptional, duly reasoned, and consistently oriented toward a legitimate aim aligned with the normative standards of a democratic society (para. 602).

With respect to the sharing of information with third parties, the competent authority must establish safeguards ensuring that unlawful or improper disclosure is effectively prevented. The mere fact that data or information is linked to state intelligence activities does not, in itself, constitute sufficient grounds to deny access. The state must adopt a clear and exceptional legal and regulatory framework defining the categories of data, their purposes, the grounds for their processing, and any justified restrictions on access by data subjects. A general and abstract assertion that data processing is connected to state intelligence is insufficient to justify denial of access (para. 603).

Limitations may be legitimate and valid in accordance with the jurisprudence and relevant international and domestic standards, such as the Tshwane Principles (Principle 9),²¹ the Inter-American Model Law on Access to Public Informa-

tion (Art. 34),²² and the Johannesburg Principles (Principle 12).²³ These limitations must satisfy the criteria of suitability, necessity, and proportionality in light of the circumstances of the case. Examples include information concerning military capabilities or communications systems, as well as measures aimed at protecting national territory or institutions against concrete threats requiring confidentiality – consistent with the logic of safeguarding national security within a democratic society (paras. 605–606).

These declarations and normative instruments are not, in themselves, legally binding. However, when the Inter-American Court of Human Rights (IACtHR) incorporates them into its legal reasoning, the Court, through the exercise of its adjudicatory authority, effectively confers binding force upon them. In simplified terms, this occurs because of the binding nature of both the Court's judgments and the American Convention itself, whose normative content has been progressively expanded through the Court's interpretative activity. Through this process, the Court continually develops and renews the Convention's normative framework. Consequently, these standards are, in a sense, transformed through a form of normative alchemy into binding legal standards.

This form of judicial articulation, adopted by the IACtHR, serves to create a framework in which member states may, under

²⁰ IACtHR, *Caso Manuela e outros vs. El Salvador* (Series C No. 441), judgment of 2 November of 2021, para. 202; UN Doc. A/HRC/39/29, para. 202.

²¹ Open Society Justice Initiative, *The Global Principles on National Security and the Right to Information (The Tshwane Principles)* of 12 June 2013, p. 19, available at: <https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles> (last visited 27 April 2026).

²² Organisation of American States, *Inter-American Model Law 2.0 on Access to Public Information*, Resolution OEA/Ser.D/XIX.12 of 7 August 2020, p. 52.

²³ ARTICLE 19, *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information* of 1 October 1995, p. 12, available at: <https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf> (last visited: 27 April 2026).

certain circumstances, limit or restrict – either totally or partially – access to data and information, particularly when linked to intelligence services. At the same time, it establishes requirements ensuring that such restrictions remain conventional in nature, supported by proportional and appropriate justifications in each case, and thus aligned with the applicable conventional framework in a comprehensive manner.

Limitations on access to data and information on intelligence grounds must not be used strategically for improper purposes, such as favouring or undermining specific state or civil society activities, whether for political reasons or any other form of discrimination (para. 607). Where access is restricted on the basis of intelligence protection, the data must be duly safeguarded to prevent alteration, loss, unauthorized transmission, or access, insofar as their retention is justified. Moreover, in cases involving human rights violations and, confidentiality or non-disclosure based on public interest, intelligence, or national sovereignty cannot be invoked to justify refusals to comply with requests from judicial or administrative bodies tasked with investigation and fact-finding (paras. 607–608). Decisions concerning the classification and retention of data and information must not be made by the same entity that originally determined their secrecy, nor in situations where members of a decision-making body denying access are themselves implicated as potential perpetrators in the conduct under investigation.

The regime governing data retention and confidentiality cannot be indefinite. It must remain exceptional, and any denial of access should be confined to the period strictly necessary to achieve a previously defined legitimate aim. This entails the institutionalization of periodic review

mechanisms to reassess both the continued necessity of confidentiality and the justification for restricting access (paras. 607–608). Within the sphere of access to information concerning state intelligence, a legal framework is required that ensures structured processes for review, declassification, and, where appropriate, the subsequent public disclosure of intelligence archives once the grounds for confidentiality cease to exist.

Such a framework must also establish fixed periods for the automatic declassification of data or information while safeguarding sensitive data or information whose disclosure depends on the consent of the data subject. Furthermore, in line with the right to informational self-determination, the legal system must ensure procedural avenues enabling individuals to challenge, before judicial authorities, the grounds invoked by administrative bodies for denying access. This includes the establishment of effective remedies allowing for the review of such decisions. In the context of judicial review, courts must be empowered to examine the substantive content of the data or information to which access has been denied (para. 608).

b) Informational Self-Determination and Its Hybrid Character: Objective Structure and Subjective Exercise

Such considerations are intrinsically related to the analysis through which it was recognized that the absence of predefined structures and concrete limitations capable of preventing the unchecked and abusive exercise of intelligence powers, as well as the lack of oversight by a competent and functionally independent authority, are incompatible with the Convention. These deficiencies directly implicate the structural, objective dimension of the violated rights. Legality, the establishment of

a specific regulatory framework governing intelligence conduct, and the creation of autonomous and independent administrative oversight mechanisms constitute indispensable elements of the normative architecture required in this domain (paras. 672–673).

Illustratively, in order to ensure that intelligence activities are formally regulated in conformity with informational self-determination and data protection, the IACtHR delineated several guidelines. These include statutory provisions establishing formal, specific, and non-abstract procedures; the identification of processes and methods employed in intelligence operations; comprehensive registration of all operational stages; and the maintenance of historical records of access to electronic systems, where applicable. The IACtHR further required that such procedures be documented in periodic reports submitted to appropriate oversight bodies.

Concerning the processing of personal data gathered by intelligence agencies, there is an articulation of minimum requirements, with the imposed specific obligations: authorities must maintain records that (i) identify the officials responsible for data processing; (ii) specify the purposes of collection, including the data's origin and category; (iii) indicate the legal basis for the operations; (iv) establish retention periods; and (v) describe the techniques employed in processing. Chronological records must document access, alteration, consultation, deletion, or disclosure of data, along with the identification of individuals who accessed the information. Inter-agency information exchanges are subject to the same safeguards. Where surveillance techniques entail access to non-public databases or information systems, prior judicial authorization is mandatory (paras. 673–674).

Regarding urgent scenarios, it is acknowledged that intelligence agencies may, in cases of proven urgency and necessity, immediately monitor the electromagnetic spectrum, that is, communications. Nonetheless, they must submit the operation for judicial review within twenty-four hours, thereby ensuring effective oversight, whether the surveillance is targeted or large-scale. Should the judiciary determine that the operation was unlawful, all data obtained must be destroyed (paras. 675–677).

These normative structures represent specific and structural safeguards that the IACtHR deemed essential to the matter under consideration. The subjective dimensions of data protection and informational self-determination are intrinsically linked to objective institutional arrangements designed to secure their effective existence and exercise. This American human rights perspective is particularly relevant in contemporary society. Furthermore, the decision articulates concerns capable of broader transregional projection, offering culturally and juridically adaptable parameters with potential global relevance.

In addition, the IACtHR addressed issues relating to state intelligence archives containing data and information that were, and remain, relevant to the victims' pursuit of truth and access to the record of actions carried out to their detriment. In both its merits judgment and its subsequent interpretative decision, the IACtHR reaffirmed that "all possible efforts must be undertaken to carry out the process of purging intelligence archives, both of the DAS and of other state bodies, which constitutes a determining element for guaranteeing the effective exercise of the right to informational self-determination" (para. 26). This process must be conducted by an independent authority. Where vic-

tims or other directly or indirectly affected persons request the deletion, suppression, or cancellation of data contained in intelligence archives that also bear relevance to human rights issues or possess historical value, a careful balancing of interests is required. Such assessment must consider the informational self-determination of data subjects, particularly where sensitive data is involved. Anonymization emerges as a principal instrument, alongside other reasonable and practicable measures, including the creation of specific procedures to safeguard the confidentiality and privacy of third parties referenced in such archives (paras. 56–59).

In the present case, the Colombian state failed to establish effective conditions for access to information (and to related actions and their purposes of defence and reparation), advancing insufficient justifications to deny access or to grant it only partially. This occurred in response to both individual and collective requests, including within judicially mandated procedures and in proceedings before the CIDH, at different historical moments and under various statutory and regulatory frameworks – from the 1990s through the 2020s.

The IACtHR, upon identifying administrative – and, more decisively, judicial – conduct that was insufficient and not aligned with ACHR-based normative standards, found that such deficiencies impeded the clarification and investigation of facts, including in the judicial sphere. This resulted in violations of the right to informational self-determination, in conjunction with the right to access to information, particularly regarding personal data contained in intelligence archives. The IACtHR concluded that the judicial authorities, in particular, failed to exercise conventionality control, which requires

the harmonized interpretation of domestic law with international law, with the aim of privileging the normative framework most conducive to the protection, guarantee, and effective realization of human rights. Both the IACtHR previously established normative standards and those developed for the present case were disregarded (paras. 649–651).

It follows that this normative dimension – grounded in the application of Art. 2 ACHR (the duty to adopt domestic legal provisions) – is directly engaged in the reasoning of the IACtHR. The finding concerning the Colombian state is best understood in light of its failure, even after being prompted by the Commission during the proceedings to implement reforms to its internal framework for the organization and cleansing of data and information, to establish an administrative structure capable of: (i) developing a regulatory framework governing access to, and the proper cleansing of, data and information contained in intelligence archives; and (ii) instituting an independent civilian authority endowed with oversight and administrative ordering powers over such a data structure.

Notwithstanding the fact that the Colombian state amended its domestic legislation and created the National System for the Cleansing of Data and Intelligence and Counterintelligence Archives, a thorough assessment revealed that this administrative body lacks the requisite independence and does not conform to applicable conventional normative standards. On this basis, the IACtHR further concluded that the Colombian state violated Art. 11 para. 2 and Art. 13 para. 1 in conjunction with Art. 2 ACHR, due to the failure to bring its domestic legal order into conformity with its international obligations (paras. 692–693).

3. The Need to Establish *Ex Ante* and *Ex Post* Regulation of Informational Self-Determination as an Autonomous Human Right, Coupled with the Right to Defend Human Rights

The judicial examination of the case outlined above, together with the normative dimension of informational self-determination and the right of access to information, is of paramount importance. This section seeks to advance a commentary on an additional normative framework articulated in the case under analysis, which establishes an innovative approach within the Court's jurisprudence by recognizing the right to informational self-determination as both a constitutive element and a condition of possibility for the exercise of the right to defend human rights. As we can observe in the separate opinion of Judge Rodrigo Mudrovitsch: "In this regard, the present case encompassed the recognition of the right to informational self-determination and the right to defend human rights as autonomous rights that are directly enforceable" (para. 250).

Particularly from the perspective highlighted in this commentary, this constitutes a diagnosis of the systemic conditions and challenges inherent to the defence of human rights in the region. It underscores the extent to which such challenges are embedded in broader structural dynamics affecting the protection of individuals engaged in human rights advocacy. In particular, the case draws attention to the unrestrained and abusive use of both digital and analog mechanisms to capture, process, share, and generate data and information about individuals – especially

human rights defenders.²⁴ These practices are frequently carried out without prior or subsequent controls that ensure compliance with legality and with conventional normative standards, occurring both within the sphere of the state and in the realm of private initiative.²⁵

Consequently, this commentary intends to highlight a singular, critical angle: the increasingly intensive practice of state and private surveillance in a digitizing society. Within this context, the dogmas of personal data protection and the concept of informational self-determination emerge as essential discursive elements that must be integrated into the specific framework of human rights, as emphasized by the IACtHR. While this is not the first case to address the legal and relational dynamics of state intelligence violence against human rights defenders, it represents a significant evolution in jurisprudence, regarding data relations. In prior cases – as recognized by the Court²⁶ – an analysis was undertaken regarding the proportionality of intelligence activities and their inherent potential to infringe upon "private life" (paras. 520–521). This concept has been broadly construed and reinterpreted so as to encompass the protection of both physical spaces (such as the family home) and communications in digital and

²⁴ *Unwanted Witness*, State of Security for Human Rights Defenders in a Digital Era, Ugandan Case: Perception and Practices, 2018, available at: <https://www.unwantedwitness.org/download/uploads/State-of-Security-for-HRDs-In-a-Digital-Era.pdf> (last visited: 27 April 2026).

²⁵ UN Doc. HRC/A/RES 58/23; European Commission, Report on a rule of law and human rights compliant regulation of spyware, Report Doc. CDL-AD(2024)043 of 6–7 December 2024.

²⁶ IACtHR, *Case Ituango Massacre vs. Colombia* (Serie C No. 148), judgment of 1 July 2006, paras. 193–194; IACtHR, *Case Sales Pimenta vs. Brazil* (Serie C No. 454), judgment of 30 June 2022, para. 89.

analog forms (including letters and other forms of correspondence). Traditionally, the notions of privacy or private life have been employed to establish a protective barrier against abusive or arbitrary interference by third parties or public authorities.²⁷ While such approaches are significant and maintain a connection with the broader language of data protection, they have remained relatively limited, lacking a specific and structured focus on data as such. In this context, the concept of informational self-determination has been invoked as a means of strengthening a normative framework capable of reconstituting objective spheres of protection, which, in turn, enable the effective exercise of (informational) rights in their subjective dimension (paras. 521–522).

a) Informational Self-Determination in and for the Protection of Human Rights Defenders

Beyond the gravity of the violations and the suffering inflicted upon the victims, the case under brief examination conveys a significant message to those engaged in Human (and Fundamental) Rights Law in an increasingly digital age, as well as in the progressively mutable – and still insufficiently theorized – relationships between citizens (in casu, human rights defenders) and the state (including its so-called state intelligences). At the doctrinal level, informational self-determination (*informationelle Selbstbestimmung*²⁸), a foundational concept in personal data protection

law, encompasses a comprehensive protective structure. It grants individuals both active and passive spheres of authority, enabling them to act within increasingly asymmetric social, private, and state-related data environments characterized by pronounced informational power imbalances.²⁹

Furthermore, deriving from the normative structure of this conception, its normativity extends beyond the individual sphere; it becomes necessary to broaden its scope to encompass both state and private structures, as well as their multiple interrelations and dimensions. This is because, within the dogmatic language of human and fundamental rights – an approach long since superseded, yet still worth recalling – the subjective and objective dimensions of rights operate in a self-reinforcing manner, whereby one dimension creates the conditions for the exercise (and continuous critique) of the other. Accordingly, rights are understood as a structural ensemble, both within and across relationships among individuals, as well as between individuals and the state, and further extending to international private and inter-state structures.³⁰ This underscores the need to establish objective frameworks capable of addressing the complexity of data relations and of providing effective conditions for the exercise of the subjective dimension of this right. It is possible to see a framework capable of fulfilling this condition, while remaining open to contextual and even temporal adaptations, in accordance with the devel-

²⁷ IACtHR, *Case Ituango Massacre vs. Colombia* (Series C No. 148), judgment of 1 July 2006, paras. 193–194; IACtHR, *Case Sales Pimenta vs. Brazil* (Series C No. 454), judgment of 30 June 2022, para. 89.

²⁸ Marion Albers, *Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen*, in: Michael Friedewald/Jörn Lamla/Alexander Roßnagel (ed.), *Informationelle Selbstbestimmung im digitalen Wandel*, 2017, pp. 11–35.

²⁹ Indra Spiecker gen. Döhm, *The More the Merrier: A Dynamic Approach Learning From Prior Misgovernance in EU Data Protection Law*, in: Matthias C. Kettemann/Alexander Peukert/Indra Spiecker gen. Döhm (ed.), *The Law of Global Digitality*, 2022, pp. 77–95 (79).

³⁰ Dieter Grimm, *Die Zukunft der Verfassung*, 1991, p. 221.

opment of the sociotechnical relations at issue.

Within the present judicial context, informational self-determination is scrutinized in one of its most sensitive domains: the relationship between citizens and state intelligence. The IACtHR adopted a firm position in favour of applying the normative dimension of informational self-determination in such circumstances, drawing upon constitutional and legal sources from member states, as well as international elements, within a dynamic process of cross-fertilization in the judicial construction of normativity (para. 600). This constitutes a relevant approach, as the IACtHR – acting as an entity responsible for providing one of the authoritative interpretations of all the American conventional framework – signals to society and to other courts in the region the need for an openness capable of fostering continuous learning between national jurisdictions and the Inter-American system, as well as among regional and national jurisdictions in other parts of the global community. This is neither a naïve measure nor a posture detached from the cultural, political, and legal conditions of each context; rather, it represents a means of generating cognitive openness aimed at strengthening the normativity of human rights, as well as the very American networks and structures that ultimately seek to consolidate, in an effectively manner, their socio-normative programs at both the preventive and promotional levels.

The case illustrates the importance of a dialogue among rights, a process emphasized throughout this commentary, in which informational self-determination is conceived as a co-structuring normative element intrinsically connected to other dimensions of human rights protection, particularly the right to defend human rights. This renewed production of human

rights normativity aligns with an era that aspires to define itself as “digital”, updating the discursive structure of the relevant legal dogmatics while simultaneously confronting concrete, empirical situations.³¹ Such situations, through their symbolic force and tangible consequences, reveal an urgent need to rethink state intelligence structures and, concurrently, to reaffirm the relevance of informational self-determination within this normative sphere, especially for those operating at the forefront of human rights defence against both state and private actors.

In recognizing the defence of human rights as essential to democratic regimes, the IACtHR imposes a stringent and unavoidable scrutiny upon public-private digital and computational infrastructures. Unrestrained surveillance and the indiscriminate collection of data and information on citizens – particularly on human rights defenders – constitute an institutional and social phenomenon incompatible with both democratic governance and the ACHR. States, especially in relation to their intelligence agencies, must establish clear, public criteria and concrete internal regimes to ensure that the core values of a

³¹ IACtHR, *Case Sales Pimenta vs. Brazil* (Serie C No. 454) of 30 June 2022; Supremo Tribunal Federal (Brasil), *Rede Sustentabilidade vs. Ministro de Estado da Justiça e Segurança Pública* (ADPF 722), judgment of 16 May 2022: “The Court, by majority, upheld the claim brought in the action for the breach of a fundamental precept and, confirming the precautionary measure previously granted, declared unconstitutional acts of the Ministry of Justice and Public Security involving the production or sharing of information concerning the personal life, personal and political choices, and civic activities of citizens, as well as federal, state, and municipal public servants identified as members of an antifascist political movement, university professors, and any other individuals who, acting within the bounds of legality, exercise their rights to freedom of expression, assembly, and association” (translation).

democratic society are effectively embedded within their normative architectures and intelligence practices. Informational self-determination emerges, in this context, as a reflexive and dynamic principle – one that is not fixed in time or space, but remains open to institutional regeneration within the conditions of highly complex modern societies.

From a systemic standpoint, the judgment introduces a reconfigured understanding of state–citizen relations, emphasizing a specific duty of ‘data-related’ care. Moreover, its binding force extends beyond Colombia’s international responsibility, projecting normative effects upon all states parties to the ACHR. These states are required to observe the *ratio decidendi* of the ruling, potentially adopting legislative measures in analogous domestic situations and exercising conventionality control over legal frameworks that do not conform to this paradigm. The decision thus transcends its immediate factual and inter-state dimensions, deepening normative integration across the legal orders of all states parties.

b) Self-Referential State Intelligence and the Reflexivity Enabled by Informational Self-Determination

A proper reading of the reasoning of the IACtHR supports the view that state intelligence activities – by virtue of the means employed and the collection and processing of personal data – constitute interferences with individual rights. Accordingly, such activities must conform to pre-established legal frameworks (formal dimension) and pursue legitimate aims that meet the requirements of suitability, necessity, and proportionality, as measures “necessary in a democratic society” (material dimension) (paras. 622–623).

By their very nature, intelligence operations carry an inherent potential to infringe privacy, data protection, and informational self-determination, even though they may simultaneously pursue legitimate objectives related to the protection of the state and its sovereignty. This overlap of distinct legal realities demands heightened theoretical and institutional reflection. It is therefore unsurprising that contemporary legal scholarship has advanced proposals to revisit the classical doctrine of the separation of powers, reconceptualizing it as a form of informational separation of powers in order to reassess the internal objective structures of the state and their potential excesses.³²

Recalling the structural measures imposed by the IACtHR – particularly those aimed at establishing ex ante and ex post data governance frameworks for state intelligence practices that respect data protection and the informational self-determination of human rights defenders – a broader critique is warranted. In my view, it is insufficient to create detailed legal authorizations for specific intelligence activities and internal controls governing which and how data are processed, stored, and shared.

In an increasingly integrated, globalized context, restrictions on data processing

³² Ingo Wolfgang Sarlet/Gabrielle Bezerra Sales Sarlet, *Separação Informacional de Poderes na Ordem Jurídico-Constitucional Brasileira*, 2023; Jürgen Wolter, *O inviolável e o intocável no direito processual penal. Reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal*, 2018; Gabrielle Bezerra Sales Sarlet/Lucas Reckziegel Weschenfelder, *The Brazilian State and Human Rights: Citizen Identification and Informational Separation of Powers*, in: Preeti Raghunath (ed.), *Critical Political Economy and Southern Approaches to AI*, 2026, pp. 121–152.

must be expanded and translated into the very infrastructures that enable such data relations. This requires attention to large-scale, infrastructural conditions: the regulatory models adopted by states, the gaps that may arise not only in legislation but also in public and private contractual arrangements, and the limits of jurisdiction and sovereignty in relation to acts originating from other states or outsourced to private entities. Equally critical are the forms of engagement with private companies providing infrastructural services and how these actors interact with other firms, civil society, and states. A further issue that arises, and which appears closely connected to contemporary debates on sovereignty and digital sovereignty, concerns the possibility of certain states deploying digital systems with global reach to surveil human rights defenders and, potentially, to fabricate false or misleading situations that affect them psychologically or even compromise their physical integrity, acting outside their legal competences or exceeding them – through an abuse of right – by extending their reach beyond national borders, or beyond their international competences, which are limited to legitimate intelligence purposes.

Domestic regulation is a necessary first step, but it is not sufficient. In a complex and highly global and interconnected techno-industrial environment, internal restrictions and prohibitions are often circumvented or rendered ineffective – particularly in contexts involving human rights defenders. The chilling effect experienced by these actors does not stem solely from state conduct; it also arises from the actions of private companies and broader societal dynamics that endorse and reproduce narratives capable of translating into concrete forms of pressure or harm.

Although the case centres on the relationship between citizens – specifically human rights defenders – and the state, contemporary realities reveal an increasingly common convergence between state intelligence services and private corporate actors. Even though the decision does not directly address this phenomenon, merely touching upon it in light of state intelligence relationships, paramilitary activities, and the political instrumentalization of such narratives in a polarized environment, the normative parameters it establishes should be extended to this hybrid public–private surveillance environment, particularly where intelligence agencies outsource or delegate essential operational functions to private entities (para. 571).³³

We jurists tend – this being a recurrent blind spot – to focus on actions framed within normative standards and protocols. However, interactions between the state and private companies, especially in intelligence contexts, often occur through public procurement of services in democratic societies. These services are typically based on infrastructural elements such as technical systems, equipment, databases, safeguards, and cybersecurity. The risk lies in their capacity to circumvent legal frameworks. Although formally presented as supportive services, they may constitute core intelligence activities outsourced to private entities, operating at the margins of – or in disregard of – the law. For example, private data brokers, capable of capturing images, geolocation

³³ The Court merely touches upon the issue, without developing it more comprehensively, as doing so would fall outside the specific scope of the case. It nevertheless explicitly states: “In this regard, the standards set out below, although they could be applicable within the spheres of competence of the entire public administration and of private actors (...)” (para. 571).

data, communications, and behavioural patterns, may provide direct or indirect surveillance services to intelligence agencies.

Such practices enable the evasion of safeguards, such as judicial authorization for accessing sensitive data, while bypassing internal oversight mechanisms. The result is a generalized public–private surveillance environment,³⁴ largely insulated from societal scrutiny and, at times, even from internal control bodies.

IV. Conclusion

This brief analysis has sought to underscore the significance of a landmark decision within the Inter-American human rights system, in which informational self-determination is consolidated as a protective barrier against state arbitrariness, especially in the sphere of intelligence activities. As a core element of the normative grammar of human rights – and of the right to defend them – informational self-determination opens a decisive normative horizon in an age marked by digital arbitrariness. The case constitutes a normative threshold in the Court’s jurisprudence regarding future state–citizen relations in the intelligence domain. The parameters articulated, although formulated within the delicate context of state–citizen interaction, warrant transposition to the contemporary landscape of intertwined public–private surveillance, particularly where intelligence agencies rely upon private corporations not merely for infrastructural support but for the execution of

essential public functions. Such normative and political vigilance is indispensable to aligning indispensable state intelligence activities with elevated and digitally updated human rights standards.

Vita

The author is a PhD researcher at Universität Hamburg (2026), at Pontifical Catholic University of Rio Grande do Sul (2022–2026) and at Insper Institute – São Paulo (2025–2026), completed a doctoral internationalization period at Goethe University (2023–2024) and served as a Visiting PhD Researcher at the University of Cologne (2024–2025) and the Max Planck Institute for Legal Theory (2025), with a research focus on regulatory law, human and fundamental rights, and emerging technologies, as well as legal theory and the interaction between law and science.

³⁴ *Andrew Guthrie Ferguson, Your Data Will Be Used Against You: Policing in the Age of Self-Surveillance*, 2026.