Bits, Bytes, Searches, and Hits:

Logging-in Accountability for EU Data-led Security

Curtin, D.M.; de Goede, M.

DOI
10.1093/oso/9780198874195.003.0006

Publication date
2023

Document Version
Final published version

Published in
Data at the Boundaries of European Law

6

Bits, Bytes, Searches, and Hits: Logging-in Accountability for EU Data-led Security

*Deirdre Curtin and Marieke de Goede**

1. Introduction

The EU security model for fighting terrorism and organized crime, cybersecurity, countering terrorism financing, and border security depends in large measure on cross-border (intra-EU and external EU) information exchange and the creation, operation, and interconnection of specialized databases, with acronyms such as SIS, VIS, ETIAS, EU-PNR, TFTP, IRU and others.[1] The EU Security Union works through a paradigm of 'preventive justice' that is heavily reliant on 'the collection of personal data and the cooption of the private sector'.[2] Data-led security is crucial to current EU policies and practices of security integration, in particular through the building and interoperability of databases. In this context, the model of EU data-led security poses profound challenges to democratic control and to the normative principles of legal protection and accountability. Under the guise of supposedly value-neutral and apolitical support for information sharing, the technological solutions inherent in database interoperability reflect deeper policy choices

* The authors wish to thank Asma Balfiqih and Sarah Tas for research assistance and help with compiling the figures and tables in this chapter. Thanks to all participants in the online workshop 'Data at the Boundaries of Law' held at the European University Institute in April 2021, and special thanks to Niovi Vavoula and Mariavittoria Catanzariti for their generous and helpful comments on an earlier version of this paper.

Prof de Goede's work on this paper received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (research project 'FOLLOW: Following the Money from Transaction to Trial', Grant No. ERC-2015-CoG 682317).

[1] SIS (Schengen Information System), VIS (Visa Information System), ETIAS (European Travel Information and Authorization System), EU-PNR (EU passenger name record), TFTP (Terrorist Finance Tracking Program), and IRU (Internet Referral Unit). Commission Communication 673 final on The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (2010).

[2] S. Carrera and V. Mitsilegas (eds), *Constitutionalising the Security Union: Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime* (2017), at 12; E. Fahey and D. Curtin (eds), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders* (2014); M. de Goede, *Speculative Security: The Politics of Pursuing Terrorist Monies* (2012).

Deirdre Curtin and Marieke de Goede, *Bits, Bytes, Searches, and Hits: Logging-in Accountability for EU Data-led Security* In: *Data at the Boundaries of European Law*. Edited by: Deirdre Curtin and Mariavittoria Catanzariti, Oxford University Press.
DOI: 10.1093/oso/9780198874195.003.0006

that have a significant impact on individuals' fundamental rights.[3] Our normative view is that adequate mechanisms of accountability for data-led security are indispensable in democratic governance: they allow citizens, parliaments, and many other fora to assess and pass judgment on the actions of government as well as private actors engaged in the public domain.[4] Yet the question of how accountability mechanisms could or should look in the context of 'data at the boundaries of law' is a particularly challenging one as we explain in this chapter. In the broader agenda of generating 'data justice', accountability for algorithmic decisions in general and data-led security in particular, is a pressing puzzle that has given rise to a large and growing literature.[5] Meanwhile, actual data-led security practices in Europe and elsewhere are developing apace and are creating novel forms and ad hoc arrangements of accountability that will generate new standards by default.

This chapter maps and analyses the concrete mechanisms and practices that are taking shape in EU data-led security, and assesses to what extent these are—what we call—'logged-into' actual data practices. EU data-led security is giving rise to hybrid accountability arrangements and single institutions, as well as pivotal EU agencies with various specific databases under their management.[6] Novel data-led security programmes are creating limited oversight and accountability structures that work to generate new standards. The purpose of this chapter is to explore and analyse these structures and standards from the perspective of their encounter with data. The most specific and in many ways most far-reaching creation that could provide a future model for accountability in other areas is in the field of external relations. In June 2012, the Directorate-General for Migration and Home Affairs (DG Home) of the European Commission recruited for an entirely new position: a deputy overseer to work inside the US Treasury in Washington. The role of the deputy overseer is to assist 'in the oversight and monitoring mission' of the EU as

[3] Rijpma, 'Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum', in M. Cremona (ed.), *New Technologies and EU Law* (2017) 197, at 203; Galli, *Interoperable Law Enforcement: Cooperation Challenges in the Area of Freedom, Security, and Justice*, 15 EUI Working Paper RSCAS (2019), at 3.

[4] Bovens, Goodin, and Schillemans, 'Public Accountability', in M. Bovens, R. E. Goodin, and T. Schillemans (eds), *The Oxford Handbook of Public Accountability* (2014), 1.

[5] Taylor, 'What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally', *Big Data & Society* (2017) 1; Amoore and Raley, 'Securing with Algorithms: Knowledge, Decision, Sovereignty', 48 *Security Dialogue* (2016) 1; Kosta, 'Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights', *Regulation and Governance* (2020) 1.

[6] Sullivan and de Goede, 'Between Law and the Exception: The UN 1267 Ombudsperson as a Hybrid Model of Legal Expertise', 26(4) *Leiden Journal of International Law* (2013) 833; Sullivan, 'Transnational Legal Assemblages and Global Security Law: Topologies and Temporalities of the List,' *Transnational Legal Theory* (2014), 5(1): 81–127.

agreed in Article 12 of the 'EU-US Terrorism Financing Tracking Agreement on the Processing and Transfer of Financial Messaging Data' (TFTP Treaty). This Agreement enables and regulates the transfer of financial transaction (SWIFT) data from the EU to the US in the context of counterterrorism. The TFTP Treaty established the role of an EU overseer to work inside the CIA and monitor the operation of the programme in the context of the Treaty stipulations. The remit of the overseer and his deputy is to 'review, analyze and verify the legitimacy of data searches' that are carried out by the US Treasury in the context of the TFTP. The overseer and his deputy are allowed to block searches if they judge them to be not compliant with Agreement provisions. According to the vacancy text, suitable candidates for the deputy overseer position were expected to have 'well-proven professional experience in counterterrorism' and eligibility for US security clearance.[7]

The creation of the overseer and deputy overseer positions illustrates the challenges of accountability in EU data-led security politics that are also transatlantic in nature and involve the creation of new and in-between oversight bodies that have access to the data used in security decision-making. The TFTP Overseer positions form an entirely new part of EU governance architectures that is understudied and little known. They are generally seen as an important EU achievement in the context of what was previously a secret and unaccountable US security programme. They have been negotiated as part of an international relations exercise and not as internal EU governance with full involvement of the European Parliament. Nonetheless, these new positions are innovative and may even contain the seeds of something that could possibly be transplanted more broadly within the EU, as our chapter will argue. An overseer with security clearance can closely observe the ways in which data are handled, shared, and analysed, and can be logged-into the data-driven nature of security analysis and decisions as part of the public administration. An overseer presumably has access to all data immediately with the power to actually block searches before they happen or are ongoing.

However, there is much that is unknown about how the TFTP overseers actually operate in practice within the TFTP, and much that can be challenged about their practices. The secrecy surrounding their identity and the procedures of data sharing and analysis is striking when compared to staff in other EU oversight institutions, such as the EU Ombudsman or the European Data

[7] Selection of temporary staff for Directorate-General Home Affaires (HOME) COM/TA/HOME/12/AD8, https://www.mzv.cz/file/827535/Vacancy_note_TA_2A___EN.pdf (last visited 16 December 2021).

Protection Supervisor (EDPS), who operate in very visible and well-regulated ways.[8] The TFTP overseers work *inside* the US Treasury and in close collaboration with Treasury and CIA officials. Despite being the very face of EU accountability in relation to the TFTP, secrecy reigns even with regard to entirely non-operational facts, such as the actual identities of the overseer and his deputy, which have never been in the public domain. The requirement that they have substantial experience in counterterrorism, rather than, for example, in data protection, influences their expertise and their practical orientation. In this sense, the overseers are fully part of the security structure of the TFTP (and of the US government)—whereby personal financial transactions data are shared transatlantically and algorithmically mined—but they seem to remain rather isolated and 'logged-out' of wider structures of accountability towards a European public.

The TFTP overseer is external in terms of EU governance and accountability structures, and this is unusual although it has now been the case for a decade. Other data-led security regulatory initiatives also focus on imposing obligations on external actors, including private actors. TERREG, for example, authorizes social media service providers to police and remove terrorist-related utterances from their platforms. This raises distinct accountability challenges but ones that can presumably—within limits—be supervised by EU institutions. Newer data-led security initiatives create new databases (for example, ETIAS, European Criminal Records Information System—Third Country Nationals [ECRIS-TCN]) that are interoperable with various existing actors and other databases—as a matter only of EU governance—and rely on existing EU institutions in terms of accountability, in particular on one increasingly important EU agency in this field, eu-LISA.

This chapter analyses the ad hoc practices and processes of accountability that are developing in relation to the actors and instruments in (a number of) EU security programmes, and assesses their 'loggedness' in relation to data. Our aim is twofold. First, we offer a mapping exercise in relation to accountability practices for a selection of established and emerging database configurations in the EU security realm. Second, in a manner not previously done in the literature, we assess the extent to which the selected mechanisms are 'logged-in' to the work of data analysis that they are expected to give account of (as opposed to logged-out or not connected). The term 'logging' is pivotal in

[8] V. Abazi, *Official Secrets and Oversight in the EU: Law and Practices of Classified Information* (2019); de Goede, 'The SWIFT Affair and the Global Politics of European Security', 50 (2) *Journal of Common Market Studies* (2012), 214-230.

this context as it refers to the practice of creating a record, reporting, noting, or registering information in the present that may be used to retrace current or past decisions in the future. Key to the practice of logging is that it uses a standardized format, on the basis that it is not presently known what actions, decisions, or factors are needed to account for a future emergency or control. Like with a ship's logbook, logging can help establish the causality of events in retrospect.

In this chapter, we show that logged-out accountability is typified by: (1) transfer of reporting, transparency and accountability to the private sector or to public security authorities; (2) an emphasis on public reporting and narrative justification on the actors' *own terms*, trumping independent investigation and request for information; and (3) a lack of ways in which accountability fora can actually be assembled, to look at, for example, concrete complaints or causes of harm. The term 'logged-out' suggests our hypothesis that the form of accountability, which is planned or in operation, risks being out-of-the-loop and possibly below par. The ideal practice, one that is aligned to the nature of the data as object, is that the accountability mechanisms and practices are 'logged-in'.

Our departure point on giving meaning to the concept of accountability is the well-known definition that describes accountability as 'a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgment, and the actor may face consequences'.[9] We start by examining how all elements of this definition—actor, conduct, and forum—are challenged in data-led security. Our chapter then develops a theoretical approach that moves beyond understanding accountability as a normative principle to seeing it as a concrete mechanism and practice, that we call rendering 'account-able'.[10] Subsequently, the chapter maps and analyses how accountability mechanisms have taken shape in relation to four different EU data-led security programmes (and the actors behind them). This mapping enables us to draw conclusions concerning the characteristics of what we describe as 'logged-out accountability', and to reflect on what a fuller, more meaningful 'logged-in' accountability in relation to data-led security could and should look like both in terms of institutions

[9] Bovens, Curtin, and 't Hart, 'Studying the Real World of EU Accountability: Framework and Design', in M. Bovens, D. Curtin, and P. 't Hart, *The Real World of EU Accountability: What Deficit?* (2010) 31, at 35.

[10] Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism', 33 *West European Politics* (2010) 946, at 951. The term account-able draws on the work of Daniel Neyland, 'Bearing Account-able Witness to the Ethical Algorithmic System', 41(1) *Science, Technology, & Human Values* (2016).

and digital practices. One promising avenue we consider in more detail is the notion of an EU-overseer in the field of data-led security who is independent, specifically created, and logged-into the data-led environment in which the office would exercise a supervisory role.

2. EU Data-led Security: In Uncharted Administrative Territory

The rise of both interoperable and algorithmic governance presents unprecedented challenges to preserving, let alone strengthening, the practices of accountability we have inherited from past generations of administrative and constitutional lawyers. This section discusses the challenges that data-led security poses to established notions of accountability. It charts why and how the focus on database interoperability, that is so prominent in contemporary EU security, poses particular questions of accountability.

Database interoperability is crucial to EU data-led security. It enables the (partial) connection of different actors and (pre-existing) databases in decentralized ways.[11] Such interconnections can be realized across different jurisdictions, different institutions, and across public–private spaces. In each concrete case, interoperability is based on specific techno-juridical arrangements that allow (pre-existing) databases to connect and communicate.[12] Thus, database interoperability is redrawing many pre-existing constitutional and political boundaries of EU governance and the place of national authorities, EU institutions, and data subjects in it.[13] EU authorities—paradigmatically, eu-LISA—may appear in a mediating role, as they perform tasks auxiliary to the exchange of personal data by Member States' authorities, such as developing the technological infrastructure required to facilitate data exchanges. Other EU agencies such as Europol and Frontex manage to put themselves more prominently on the map of interoperable systems by gaining ever-increasing

[11] Curtin, '"Accountable Independence" of the European Central Bank: Seeing the Logics of Transparency', 23 *European Law Journal: Review of European Law in Context* (2017) 28; Carrera and Mitsilegas (n. 2).

[12] M. Gutheil *et al.*, *Interoperability of Justice and Home Affairs Systems*, Study for the LIBE Committee, European Parliament (2018); Galli, 'Interoperable Database: New Cooperation Dynamics in the EU AFSJ?', 26(1) *European Public Law* (2020) 109; Brouwer, 'Large-Scale Databases and Interoperability in Migration and Border Policies: The Non- Discriminatory Approach of Data Protection', 26(1) *European Public Law* (2020) 71; Aden, 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy', 26(1) *European Public Law* (2020) 93; Leese, 'Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU,' *Geopolitics*, 27:1 (2022), 113–133.

[13] Curtin and Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue', 26(1) *European Public Law* (2020) 59.

access to data shared by others and for broader purposes.[14] Moreover, interoperability produces a form of networked administration characterized by the sharing of sensitive personal data within domains—such as security and border management—that are themselves politically sensitive. In this light, it becomes evident that the EU's bet on technological solutions in security is enhancing European administrative power in that area.[15] This is true both of the various agencies involved but also of the Commission which has increased considerably its power to legislate (for example, on ETIAS) through delegated and implementing acts.[16]

However, enhanced power requires enhanced safeguards of public accountability and it is not clear that they are sufficiently in place and sufficiently adapted to match the data-led nature of security cooperation. As Harlow and Rawlings aptly put it, the bureaucratic use of artificial intelligence (AI) in particular is 'moving us fast into uncharted administrative territory, one in which prior achievements in terms of rights protection and the good governance triad of transparency, accountability and participation may be restricted, even reversed'.[17] Interoperability relies on AI and algorithmic matching in many crucial respects but can also take place more mechanically.[18] For example, sharing information across decentralized databases in security programmes is often done on the basis of algorithmic matching of records or specific search terms.

The challenges to practising accountability in relation to EU data-led and interoperable security are substantial, for at least three reasons. First, there are challenges of secrecy and the availability of information. Without information to hold the power wielder to account, citizens and non-citizens cannot hope to attain accountability for the actual decision taken which may be of a transient

[14] Quintel, 'Interoperable Data Exchanges within Different Data Protection Regimes: The Case of Europol and the European Border Coast Guard Agency', 26(1) *European Public Law* (2020) 205.

[15] D. Bigo *et al.*, *The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda* (2015); D. Bigo *et al.*, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law* (2013); E. Guild, *EU Counter-Terrorism Action: A Fault Line between Law and Politics?* (2010).

[16] Art. 89 ETIAS Regulation (EU) 2018/1240 OJ L 236/1, e.g. the Commission delegated Regulation (EU) 2019/946 on the allocation of funding from the general budget of the Union to cover the costs for the development of ETIAS (2019) or the Commission delegated Regulation (EU) 2021/916 establishing a ETIAS as regards the predetermined list of job groups used in the application form (2021); S. Alegre, J. Jeandesboz, and N. Vavoula, *European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection* (2017), at 27.

[17] Harlow and Rawlings, 'Proceduralism and Automation: Challenges to the Values of Administrative Law', in E. Fisher, J. King, and A. Young (eds), *The Foundations and Future of Public Law: Essays in Honour of Paul Craig* (2020) 275, at 297; Ulbricht and Yeung, 'Algorithmic Regulation: A Maturing Concept for Investigating Regulation of and through Algorithms', 16(1) *Regulation & Governance* (2021), 3; Yeung, 'Algorithmic Regulation: A Critical Interrogation', 12(4) *Regulation & Governance* (2018), 505.

[18] C. Dumbrava, *Artificial Intelligence at EU Borders—Overview of Applications and Key Issues* (2021).

nature, for example, exclusion from the territory of a Member State/EU. In many cases, such decisions (for example, exclusion from a territory) will not lead to a full judicial hearing where the data relied on is scrutinized at the national level.[19] This is of course tricky in the context of police cooperation as the data in question are not usually shared outside policing networks, not even for the purposes of public accountability. At the supranational level, when data are retained in databases and subsequently shared, there are inevitably operations that are invisible not only to outsiders but also to insiders. Secrecy is fostered by data protection laws and the legal requirement of not sharing personal data and this may operate as an accountability inhibitor in a more substantive sense.

The second challenge to practising accountability in EU data-led security is the complex and multilevel landscape of EU security governance, involving different layers of EU institutions on the one hand and Member States on the other. Moreover, EU security governance involves complex webs of transatlantic cooperation and information sharing, as well as processes of 'agentification'.[20] Thus, the setting of data-led police and security cooperation is profoundly multilevel and this is of direct influence on the possibility of accountability. Information sharing takes place in a setting where the information asymmetry is systemic and particularly accentuated, also in terms of the participants within the conclave of governance, let alone when it comes to the possibility of external accountability. The very nature of the subject matter is fragmented and invisible: shared personal data by police and other associated authorities in a non-national setting. In this arena, executives anyway enjoy a wide strategic and operational discretion where 'normal' accountability mechanisms do not traditionally apply.[21] The position of third-country nationals whose data is contained in EU databases and shared is particularly weak.[22] The strong executive governance impacts on the conceptualization and implementation of accountability practices in the Area of Freedom, Security and Justice (AFSJ) that need to be adapted to the actual ownership of data and exercise of power to be effective. In this context, 'post hoc accountability', in the form of explanation and justification 'in retrospect', is becoming a key mode of (democratic) control and legitimation.[23]

[19] E. Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (2008), at 289.

[20] Busuioc and Curtin, 'The Politics of Information in EU Internal Security: Information-Sharing by European Agencies', in T. Blom and S. Vanhoonacker (eds), *The Politics of Information* (2014).

[21] C. Moser, *Accountability in EU Security and Defence: The Law and Practice of Peacebuilding* (2020), at 119.

[22] Vavoula, 'Interoperability of EU Information Systems: The Deathblow to the Rights of Privacy and Personal Data Protection of Third-Country Nationals?', 26(1) *European Public Law* (2020) 131.

[23] D. Curtin, P. Mair, and Y. Papadopoulos (eds), *Accountability and European Governance* (2012).

Third, and perhaps most importantly, the fact that EU data-led security works in large measure through database interoperability (as discussed above), means that anchor points for accountability need to be located in complex public–private networks of cooperation and data sharing.[24] Interoperability exacerbates a number of issues including perceived mutual trust in national administrations and trust in technologies.[25] It aggravates the obscurity and difficult accountability that results from the fragmented character of composite administration, where the EU administration enjoys status of a 'second order' administration that is only answerable to other administrations, if at all.[26] It becomes hard to pinpoint at exactly what level of administration mistakes are made. It is also close to impossible for the public or for institutions not involved in the interoperable (law enforcement) networks to demand access and understand how the processing of data results in concrete security decisions.[27] As the intelligence networks in AFSJ contain both personal and non-personal data this implies for the individuals whose data is being shared within interoperable networks and databases that they lose control over their own personal data. The fact is that the data in question are largely collected by the administrative authorities of the Member States using a variety of methods and sources, including information that may have been in many instances collected originally by private parties.

3. Accountability as Mechanism and Practice: Logging-in Overseers

As the example of the TFTP overseers and databases discussed in our introduction shows, EU data-led security is creating novel mechanisms and devices of accountability in a relatively fragmentary fashion. Even if existing concepts and structures of accountability are challenged through data-led security and its reliance on interoperability, new ad hoc practices are emerging. The translation of ideal-typical accountability into concrete practices is the result of complex processes of negotiation in a multilevel setting. The overseer positions have, for example, been designed in a unique and path-dependent process of

[24] Curtin and Brito Bastos (n. 13).

[25] Vavoula, 'Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust', 22(3) *German Law Journal* (2021) 391.

[26] Curtin, 'The EU Automated State Disassembled', in E. Fisher, J. King, and A. Young (eds), *The Foundations and Future of Public Law: Essays in Honour of Paul Craig* (2020) 233, at 252.

[27] Huysmans, 'What's in an Act: On Security Speech Acts and Little Security Nothings', 42(4–5) *Security Dialogue* (2011) 371.

negotiation between the EU and the US, involving multiple levels and layers of EU decision-making. New institutions like the overseer office might offer creative solutions to address accountability deficits in relation to novel security programmes, but they are also legal hybrids that need further critical attention. How do these new institutions and mechanisms actually work? What kind of accountability documents, devices, and outputs do they entail? What kind of knowledge do they produce, and what remains obfuscated? Do they deliver the key principles of accountability in terms of explanation, justification, and sanction, and if so, how?

As Bovens argues, the social relationships that constitute accountability work through concrete 'mechanism[s] that involve an obligation to explain and justify conduct'.[28] The emphasis on *mechanisms* is relevant here: it directs attention away from accountability as an ideal-typical legal norm towards an examination of how accountability mechanisms work in actual practice (which can then be assessed on a normative basis). Literatures in Science-and-Technology studies (STS) are helpful to grasp such (technological) practices analytically, as they distinguish *accountability* as a political and ethical principle from *account-ability* understood as the material practices that render an order's actions 'observable-reportable'.[29] *Account-ability* in this sense goes beyond an analysis of the mechanisms identified by Bovens to understand accountability as being made up of the concrete, material, sedimented practices through which ideal-typical accountability takes shape. It is made up of everyday activities like 'keeping records, following instructions, justifying actions in relation to guidelines'.[30] It involves choices concerning forms and timing of reporting, technical specifications of what and how to report, priorities in justification, and the specification of appropriate modes of public questioning.

Three key mechanisms of accountability have been identified in the literature. According to the accountability definition of Bovens, the provision of information is the first stage of the accountability process upon which all further stages rest—no accountability without information.[31] The power holder needs 'to inform the forum about his or her conduct'.[32] Providing information changes the allocation of power both for those who take decisions (the power wielders) and those who want to hold them to account for that use of

[28] Bovens (n. 10) 951.
[29] Neyland, 'Bearing Account-able Witness to the Ethical Algorithmic System', 41(1) *Science, Technology, & Human Values* (2016) 55; Marres and Lezaun, 'Materials and Devices of the Public: an Introduction', 40(4) *Economy and Society* (2011) 489.
[30] Neyland (n. 29) 55.
[31] Moser (n. 21) 125.
[32] Bovens (n. 10) 952.

information. Without information, the power wielders cannot have a basis for their decision and its accuracy is otherwise put to account. In this sense information is both an instrument of empowerment and, through withholding it from those outside the enclave, dis-empowerment. At the level of EU databases, the information holder is at the European level and subject to its rules and regulations and the data is transferred/shared with an information recipient that is different to the information provider (the Member State that owns the data). In this information triangle, the common outsider is the individual whose data is at stake. Without information to hold the power wielder to account, the individual cannot hope to attain accountability for the actual decision taken, which may be of a transient nature, for example, exclusion from the territory of a Member State/EU, and in many cases will not lead to a full judicial hearing where the data relied on is scrutinized at the national level.

The second principle of accountability is explanation, which is closely coupled to justification. According to Bovens, the citizen forum 'needs to be able to interrogate the actor' and the actor needs to be able to explain choices and justify courses of action.[33] Again, it is useful to think concretely about how such justifications are performed in practice and how they are rendered materially possible. Boltanski and Thévenot suggest that we examine the concrete 'operations' that are performed in order to link an actor's decisions to general normative principles.[34] How are specific judgments related and explained with reference to the common good? As new and hybrid accountability institutions and practices emerge within EU data-led security, it is imperative to examine critically the concrete operation of justification.

The third and final principle of accountability is the crucial question *for what* an actor can be held to account/sanctioned by an appropriate accountability forum, and whether and how they may 'face consequences'.[35] Is it for the quality or quantity of information provided or for the actual conduct that has been undertaken on the basis of the data accesses by the (national) actor? The power of a forum to sanction for the content of the account is what Philip called a 'contingent condition of accountability'.[36] The obligation to provide information is on this analysis the *necessary* condition of accountability. In the area of police cooperation and shared information in interoperable databases and otherwise, as we shall see, there are a number of characteristics that are

[33] Ibid. 953.
[34] Boltanski and Thévenot, 'The Reality of Moral Expectations: A Sociology of Situated Judgment', 3 *Philosophical Explorations* (2000) 208.
[35] Bovens (n. 10) 952.
[36] Moser (n. 21) 125.

quite specific and might lead to the conclusion that one of the fundamental reasons why accountability is inhibited in these enclaves is that the mechanisms of accountability are quite simply 'logged-out' or disconnected from the content and use of the data in question (as opposed to its retention and collection). This customization of existing notions of accountability to interoperable AFSJ databases and agency cooperation may lead to novel conceptualizations of what accountability can mean in this context.

In relation to data-led security, these three principles of accountability are more complex than the literature initially presumed. As we have discussed elsewhere, data-led security can be understood as a chain-like process, where each analytical step in the chain feeds into the next, in bits, bytes, searches, and possible hits. In such chain-like processes, data are captured (often from commercial systems), they are curated into transferable datasets, they are shared across systems or jurisdictions (through techno-juridical arrangements), and they are analysed (with the aid of trained algorithms).[37] Alternatively, in models of interoperability, databases remain decentralized, but can be queried and connected through specific nodal points and techno-juridical arrangements. These chain-like workflows ultimately produce particular security decisions, whereby the outcomes of one link in the chain feed into the next step in the process. Consequently, data-led security decisions are not momentary or hidden inside an algorithmic 'black box', but they are processual and iterative. Security decisions are dispersed across iterative processes of data curation, transfer, and analysis.

Subsequently, we find that questions of accountability in data-led security too often focus on unpacking the inner workings of the algorithm, by seeking to 'open the black box' of the algorithm.[38] Till Straube has argued that the metaphor of opening the algorithmic black box is a seductive fallacy that 'appeals to the researcher's fantasy of bringing the (dark) secrets of an elusive object to light … [Yet] even if we succeed, what we usually find is more black boxes'.[39] In contrast, if data-led security is understood as a technical-juridical *process*, the

[37] de Goede, 'The Chain of Security', 44 *Review of International Studies* (2018) 24; Bellanova and de Goede, 'The Algorithmic Regulation of Security: An Infrastructural Perspective', *Regulation & Governance* (2022) 16 (1), 102–118; L. Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (2020).

[38] What M. Ziewitz calls 'the algorithmic drama' in Ziewitz, 'Governing Algorithms', 41(1) *Science, Technology & Human Values (*2020) 3; Koivisto, 'Thinking Inside the Box: The Promise and Boundaries of Transparency in Automated Decision-Making', 1 *EUI Working Paper AEL 2020/01* (2020) https://cadmus.eui.eu/bitstream/handle/1814/67272/AEL_2020_01.pdf? 11; also Koivisto, Chapter 3, this volume.

[39] Straube, 'The Black Box and its Dis/Contents', in E. Bosma, M. de Goede, and P. Pallister-Wilkins (eds), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork* (2020) 175, at 178 and 182.

challenges to accountability are dispersed across the iterative, socio-technical process of data-led sensemaking.

These challenges thoroughly problematize the actor–forum–relation triad that Bovens theorizes. First, it is not always clear who the *actor* to be held to account is. Data-led security involves complex public–private cooperation and the use of mundane, commercial data for security analytics.[40] Actors are not always (national) governments or governmental institutions but can be transnational agencies or public–private collaborations that have been institutionalized with complex data architectures and interlinking databases. Interoperability generates the (partial) connection of different actors and (pre-existing) databases in decentralized and ways. There is almost always a multiplicity of public–private actors involved in data-led security programmes, from the commercial providers who compile and curate databases, to public actors who are able to retrieve hits from interconnected databases that inform their security analysis and actions. The key challenge to accountability is not simply how to hold an actor to account, but how to log into the processual collaboration of multiple actors and databases, to enforce specific moments or processes of public visibility and giving account.

Second, the citizen *forum* to which account must be given is not a national citizenry but a multinational and dispersed public. The public forum, as we know from the work of Marres and Lezaun, is not independent from its material gathering, like, for example, a hearing or a court procedure. An approach informed by STS asks about the 'materials and devices of public participation', instead of defining 'publics and their politics largely in discursive . . . or procedural terms'.[41] So this means that we need to be attentive to how accountability fora are able to emerge; where questions can be posed and an investigation can take place. Concretely then, one question for data-led security is how complaints or cases of harm can be heard; how they can be rendered visible and audible to the extent that they become a matter of concern around which a public can assemble?[42]

Third, the *relation* between the actor and the forum in EU data-led security is multilevel and complex. The political science literature that analyses the rise of

[40] L. Amoore, *The Politics of Possibility* (2013); Amoore and de Goede, 'Transactions after 9/11: The Banal Face of the Preemptive Strike', 33(2) *Transactions of the Institute of British Geographers* (2008) 173; Bures and Carrapiço, 'Private Security Beyond Private Military and Security Companies', 67(3) *Crime, Law and Social Change* (2017) 229; Mitsilegas, 'Transatlantic Counterterrorism Cooperation and European Values' in E. Fahey and D. Curtin (eds) *A Transatlantic Community of Law* (2014) 289.

[41] Marres and Lezaun (n. 29) 490.

[42] B. Latour, *What Is the Style of Matters of Concern? Two Lectures in Empirical Philosophy* (2008); Marres, 'Front-Staging Non-Humans: Publicity as a Constraint on the Political Activity of Things', in B. Braun and S. J. Whatmore (eds), *Political Matter: Technoscience, Democracy, and Public Life* (2010).

European administrative networks in general points out that the dispersion of tasks within such networks dilutes political responsibility; and that those networks' weak visibility 'insulates them from public scrutiny'.[43] Yet these issues are exacerbated in the chain-like processes of interoperability in particular. As was mentioned before, the very dataflows and the infrastructure created to enable them involve sensitive information, either because that information concerns personal data or because the purposes for which such data are collected and processed, more specifically security purposes, can often not be reconciled with total transparency to the public at large. Accountability does require that a forum exists to pass judgment on the actions of authorities; yet the secretive and highly technical nature of interoperability makes the accountability fora more exclusive, more remote and therefore in practice limited, not logged-in to the chain-like processes. To a large extent, and where they are provided for at all, the accountability mechanisms of interoperable sharing and automated processing of personal data are designed to be deployed away from the eyes of the public and often away from the eyes of public accountability forums. This may be more a form of shielded accountability to privileged forums or entities rather than any reasonable understanding of public accountability. This will be explored in the following sections, both in terms of mechanism and in actual logging practice.

4. Account-ability in EU Data-led Security: Logged-out Mechanisms and Practices

The remainder of this chapter examines how the concrete mechanisms of account-ability are taking shape in relation to selected EU data-led security programmes. This will allow us to theorize trends and critically analyse the limits to accountability in security database interoperability. The focus, first, is on mapping and analysing the concrete practices through which specific security programmes seek to render their actions account-able. What kind of documents, devices, and offices have been created within these security programmes to offer public information and (a measure of) justification for actions and decisions taken? What are the technical and legal forms of narrative justification that are being designed? In this context, it is equally important to

[43] Mastenbroek and Sindbjerg Martinsen, 'Filling the Gap in the European Administrative Space: The Role of Administrative Networks in EU Implementation and Enforcement', 25(3) *Journal of European Public Policy* (2018) 422, at 429.

map the aspects of such security programmes that remain invisible, and that are not able to be accounted for. As a growing literature points out, silences and obfuscation in international politics can be part of 'strategic ignorance', which distributes responsibility in specific ways.[44] Furthermore, what kind of sanctions or consequences could actors face, if any, in case their accounts are rejected by European publics? Is it possible at all for public fora to be assembled through the mechanisms and devices created within these programmes?

In these empirical sections, we focus on four selected EU data-led security programmes. First, the TFTP is a transatlantic security programme whereby financial transactions data of the financial telecommunications company SWIFT are shared transatlantically with US security authorities in the context of counterterrorism investigations. It is based on a 2010 EU–US specifically negotiated Treaty (the TFTP Treaty).[45] Second, TERREG is a recently adopted EU Regulation for 'Preventing the Dissemination of Terrorist Content Online', which came into force in May 2021.[46] It authorizes social media service providers to police and remove utterances from their platforms, and enables the use of EU-led 'referrals' whereby European police authorities flag suspicious content to providers. Both TERREG and TFTP entail a security practice whereby commercial data are shared and algorithmically analysed in the context of counterterrorism, leading to concrete security decisions to alert security authorities, freeze financial transactions, or take content offline. Third, ETIAS is an automated data-led border control system, specifically to register visitors from countries who do not need a visa to enter the Schengen Zone. ETIAS gathers and analyses personal data (including travel documents and criminal records) and screens against existing watchlists (such as the Europol information system, VIS, Eurodac, SIS II, and the new Entry/Exit System [EES]), with the objective 'to make sure that these people are not a security threat'.[47] The personal data processed through the ETIAS Central System, a new database, is not simply checked against *existing* lists of 'persons of interest', but mined and used to profile prospective travellers based on data that already exists about *other* individuals.[48] ETIAS is expected to become operational in 2022. Finally, 2019

[44] McGoey, 'Strategic Unknowns: Towards a Sociology of Ignorance', 41 *Economy and Society* (2012) 1; McGoey, 'The Logic of Strategic Ignorance', 63 *The British Journal of Sociology* (2012) 533.

[45] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172/79.

[46] The European Parliament approved TERREG with a vote in the plenary on 28 May 2021. The Regulation entered into force on 6 June 2021 and will apply as of 7 June 2022.

[47] European Travel Information and Authorisation System (ETIAS), https://www.schengenvisainfo.com/etias/ (last visited 15 December 2021); on the politics of watchlist screening, Sullivan and de Goede (n. 6).

[48] Alegre, Jeandesboz, and Vavoula (n. 16) 24.

saw the adoption of the Regulation establishing ECRIS-TCN, the European Criminal Records Information System that allows the exchange of criminal conviction data concerning third-country nationals.[49] Unlike the previously existing ECRIS system, which basically interconnects the national criminal records on EU nationals, ECRIS-TCN facilitates finding the Member State that holds information on the criminal records of third-country nationals.[50]

Of these four programmes, only one, the TFTP, is relatively well-developed with established practices both of reporting and accounting, while in the other three this is still emerging. TERREG, ETIAS, and ECRIS-TCN have little to no actual practice yet in the form of logging, reporting, and accounting beyond what is prescribed in the foundational instruments and some institutional dialogue prior to and at the time of creation. Yet, all four of these EU security programmes have complex constellations of actors: national and supranational, public and private, as well as complex techno-juridical processes of data transfer and/or database interoperability. They are, however, negotiated by different actors and embedded in different (accountability) structures. Whereas the TFTP belongs in the external relations space (via a specific Treaty of the EU with a third state, the US), the other three programmes are largely internal to the EU. TERREG is the most explicit in the relationship with and imposition of obligations on private actors while the other two, ETIAS and ECRIS-TCN, essentially involve relationships among various types of institutions and agencies at different governance levels. TERREG involves an ongoing relationship with the EU agency Europol, whereas both ETIAS and ECRIS-TCN, exist by virtue of the little-known EU agency, eu-LISA. eu-LISA maintains these databases and is also largely responsible for account giving in the sense of reporting, such as it is, on both large-scale programmes. The relationship of these agencies with other core institutional actors at the EU level is also key in terms of to whom the account giving is made. Beyond the bare words of the founding regulations we extrapolate as to both the future role of and accounting by Europol on TERREG and the future role of and accounting by eu-LISA on ETIAS and ECRIS-TCN from the practice that has already developed by these relatively long-standing EU agencies with regard to other similar programmes/databases (Europol IRU in the case of TERREG and SIS II, VIS and Eurodac in the case of the other two newer databases).

[49] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 OJ L 135/1.

[50] For an overview of ECRIS-TCN, see Brouwer (n. 12).

In our view, this 'first cut' mapping of emerging accountability practices is not only a useful exercise in and of itself but it also provides pointers to the nature of the accountability arrangements in place for highly data specific programmes that follow their own internal logic and sharing practices that may not be visible at all to the outside world (or even to parts of the inside world) unless windows are opened in a timely and/or strategic fashion to targeted audiences that may evaluate what has happened and reveal no operational details publicly. ETIAS also makes provision for the algorithmic profiling of third country travellers in a sophisticated manner. ETIAS and ECRIS-TCN are two distinct information systems, with many structural similarities in how they are organized, as well as the fact that they are intended for the exchange and processing of information on third country nationals, with the purpose of public security in mind.

The four data-led security programmes are distinctive in terms of set-up, scale, sharing arrangements, and regulatory framework. In terms of commercial data, the TFTP and TERREG most clearly work with data captured and mined from private actors (SWIFT in the case of the TFTP and internet platforms in the case of TERREG). In contrast, both ETIAS and ECRIS-TCN are border management and judicial cooperation programmes (primarily for security purposes) that are basically public databases that share data gathered by various public authorities. In the case of ECRIS-TCN this is relatively straightforward but ETIAS is much more open for example through the European Search Portal in gathering data from public databases through a system of interoperability. Personal data has been gathered for largely specific purposes (e.g. visas, etc.) unrelated to the purposes for which they will be used, and connected though the auspices of the new ETIAS. Part of the cross-checking of ETIAS applications will be against data held by Europol. Europol databases include data gathered from private parties and, under the latest proposal, it will have even more opportunities to gather and share such data.

In all of our cases, we see that EU agencies play a crucial role in developing technical infrastructures, presenting themselves as offering 'merely' technical support. However, it should be clear that the design and operation of technical infrastructures for data sharing entails political choices and consequences for the operation of accountability (or lack thereof).[51] For example, eu-LISA is responsible for the operational management of both ETIAS and ECRIS-TCN. In

[51] Bellanova and de Goede (n. 37); Bellanova and Glouftsios, 'Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance,' 27:1 *Geopolitics* (2022) 160–184.

ETIAS, two other EU agencies play an important role. Frontex will be setting up and running the ETIAS Central Unit, and Europol will be contributing to and reviewing the ETIAS watchlist.[52] This is the main role that these interoperable information systems attribute to eu-LISA, the EU's large-scale information systems agency. eu-LISA is comparatively old, having been established in 2011 and starting its activities in 2012. It was envisaged as a type of management authority entrusted with all the activities necessary to keep large-scale IT systems such as VIS, Schengen etc. alive and took over tasks in the early years from the Commission, in particular DG HOME. Whereas as yet there is no actual reporting in place for ETIAS and ECRIS-TCN we look below by analogy to the reporting by eu-LISA of VIS and other systems to understand the kinds of issues that arise and the approach (that may be) taken. TFTP and TERREG, by comparison, do not work through eu-LISA, but have technical infrastructures that work through Europol. For example, Europol serves as point of contact for TFTP-related leads that are shared to and from the US Treasury in the context of counterterrorism investigations.

All four programmes involve the transnational interoperability of national databases that contain sensitive personal data. Three of them (excluding ECRIS-TCN) involve complex chains of public–private data sharing and collaboration, which challenge and complicate traditional mechanisms of accountability. As discussed in the first part of this chapter, traditional mechanisms of transparency and redress are difficult to operationalize when security decisions are taken across databases, jurisdictions, and across public and private spaces with lack of clear responsibilities for private companies and public actors. In the sections that follow, we map the ways in which practical account-ability processes and mechanisms are taking shape, in order to reflect on the characteristics and limits of what we call 'logged-in accountability' and possible solutions in the future.

A. Information

The availability of information in EU data-led programmes security consists primarily of self-reporting by the various actors involved, whereby crucial

[52] Arts 75 and 77 ETIAS Regulation (EU) 2018/1240; 'EU: Construction of the European Travel Information and Authorisation System (ETIAS): Progress Reports from Frontex and Europol', *Statewatch News* (2019), https://www.statewatch.org/news/2019/may/eu-construction-of-the-european-travel-information-and-authorisation-system-etias-progress-reports-from-frontex-and-europol/ (last visited 16 December 2021).

'strategic unknowns' are generated.[53] To some extent, we see the transfer of reporting obligations away from the public, towards the private sector, or in other cases made in a non-public way to selected public actors. Because actors themselves select what to disclose, important elements remain publicly unknown—this is not simply an omission but the political production of strategic unknowns. This section maps and analyses the practices, documents and procedures for the provision of information that are in place or will soon be in place (or are by analogy in place in other areas) in our four selected data-led security programmes. It shows if and how information about the scope and numbers of personal data, the technical operations of data transfer, and the processes of accessing and retaining personal data, are being presented and made accessible either in a non-public way or publicly.

The extent to which the various data-led security programmes have a body of empirical data that is publicly available as to their various activities, searches, and hits and otherwise, varies considerably across the cases. This has something to do with the timeline involved but also the actors and regulatory structures put in place at varying moments over the course of the past 12 years. TFTP gives an account of itself through two mechanisms. First, as stipulated in Article 10 of the TFTP Treaty, the parties to the Treaty conduct a regular Joint Review, including a 'proportionality assessment of the Provided Data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing'.[54] This regular review has led to five Joint Review reports to date, yet these are not an independent audit or oversight, but conducted by the Treaty parties themselves. For example, the 2019 EU–US TFTP Joint Review teams included two officials from the European Commission, two representatives of European data protection authorities and seven US officials, from the Departments of Justice and the Treasury, and from the Office of the Director of National Intelligence (Civil Liberties Protection Officer).[55] Second, the TFTP is subject to the Europol independent oversight body, the Joint Supervisory Board (JSB) until 2019, and subsequently the EDPS from 2019. The Europol oversight is a full independent oversight structure, yet it applies only to *part of* the TFTP activities, namely Europol's role in Article 4 of the Treaty, which regulates the US data requests that are the basis of the transatlantic data transfer. It does not examine the practices inside the US Treasury and it does not examine the data transfers on the basis of Articles 9 and 10 of the TFTP Treaty. Moreover,

[53] McGoey, 'Strategic Unknowns' (n. 44); McGoey, 'The Logic of Strategic Ignorance' (n. 44).
[54] Art. 10(1) Terrorist Finance Tracking Programme (TFTP) Treaty.
[55] Commission Report 342 final on the TFTP Joint Review (2019), at 21.

the Annexes to the JSB Reports, in which the substantial evaluation of the programme and its data transfers processes is set out, are classified as EU-Secret and therefore not available publicly or for research purposes, even if the short concluding sections of the JSB Reports are available.

At first glance, then, the publicly available *information* on the TFTP is really quite substantial: five Joint Review reports have been released since the start of the TFTP Treaty (2010) and at least two JSB Reports (even if partially classified). At the time of writing, collectively these reports offer over 200 pages of information and evaluation of a relatively secret security programme. The *information* in these so-called Joint Reviews includes details on the process of evaluation (the review process), as well as details on the nature, number, and results of the searches of personal financial data. In line with examining account-ability as a practice, it is useful to know what information is (not) made available through the Joint Review reports, as this reveals something about the ways in which reporting, analysing, numbering, and accounting is done in practice in the name of accountability. Key information that has become available through the Joint Review reports is the number of *searches* conducted monthly in the TFTP database. These searches have to be based on a 'nexus to terrorism or its financing' (Article 5b of the TFTP Treaty). On the basis of a piece of personal data, for example, a name, address, credit card number, wire transfer, or social security number, searches can pull strings of network information from the TFTP database. Figure 6.1 summarizes the number of searches that are detailed in the

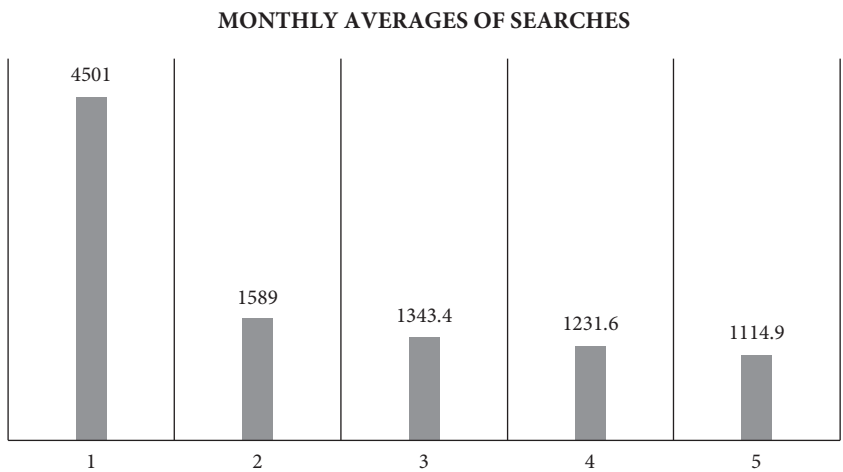

Figure 6.1: Monthly average of searches in the TFTP database per review period. (Data compiled by Asma Balfiqih from Joint Review reports.)

successive review reports between 2010 and 2020. For example, the First Joint Review Report notes that there were 27,000 searches in the first five months of the programme.

Another key piece of information in the Joint Review reports concerns the number of leads shared from the US Treasury with EU Member States and with Europol. There are two ways in which TFTP-derived intelligence can find its way its way back to Europe: first, leads that are voluntarily pushed by the US Treasury/CIA to European counterparts (Article 9). Second, leads that are shared after European requests for information and searches to be done within TFTP (Article 10 requests). The latter was widely criticized as a type of intelligence 'outsourcing', though as we can see in Figure 6.2, this type of request has increased substantially in the most recent review period (2016–2018). The increasingly active use of European intelligence services (via Europol) of the TFTP, is now used as an argument concerning its value and legitimacy.

The TFTP reports are also very useful as they provide indications as to the type of statistical information that is expressly *not* included in the review reports. In the TFTP example, this relates to the data actually requested from SWIFT (the designated provider) and transferred to the US Treasury. We do know that this information is not known, because its existence is addressed and explained in the reports, and its absence constitutes a visible point of contention between the EU and the US. In other words, the size of transatlantic data transfers is no longer a 'deep secret' as it was in the years after 9/11, when

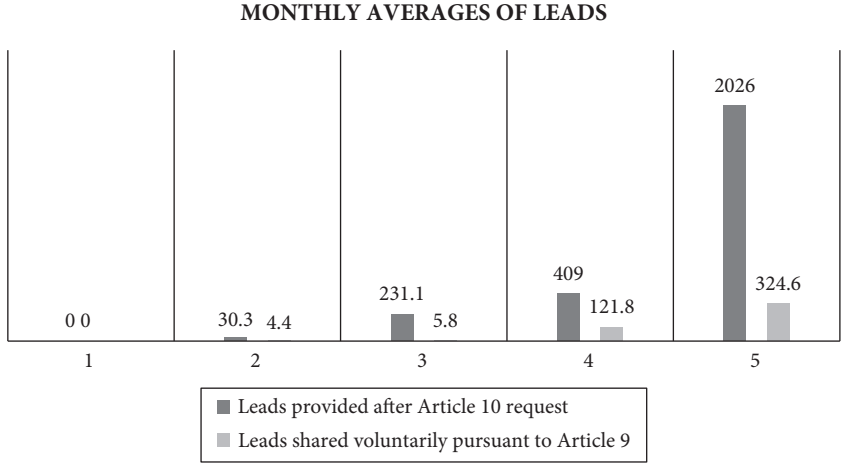

Figure 6.2: Monthly average of leads shared per review period. (Data compiled by Asma Balfiqih from TFTP Joint Review reports.)

it was simply not known that these data transfers took place at all.[56] About this 'overall volume of data provided [by the Designated Provider],' the First Joint Review Report says: 'there is a clear interest from many sides to be informed on this point in order to fully understand the scope of the programme, its possible implications on civil liberties, and thus its proportionality'.[57] However, the US has consistently and explicitly refused to render this information public through the Joint Review process or by other means. This is more than a mere contestation over the publicity of numbers. At the root of the disagreement over the question of whether the scope of data transfers should be public is a deeper disagreement over the nature and definition of 'proportionality' as a data protection measure. The US maintain that the broad scope data transfers are necessary, defined as sets of transactions of a particular message type, within a given timeframe, and to/from particular geographical areas. While the requests detailing these parameters have become ever more substantive (see below), it is not known whether this has led to more tailored and more limited data transfers.

TERREG, by comparison, is wholly within the authority of the EU and it is foreseen that by June 2023 a detailed programme for monitoring the outputs, results, and impacts of TERREG shall be established by the EU Commission.[58] In this sense, the contours of oversight and public reporting are still in the making, even if the Regulation came into force in May 2021. TERREG also stipulates that annual transparency reports by platforms are legally required to record publicly how many pieces of terrorist-related content have been removed. This is important because the deletion and storage of suspect social media content affects the contours of online public space.[59] The definition of what counts as terrorism in social media policing, however, is broad and lacks juridical precision. It can affect broad batches of online user-generated content.[60] Europol IRU—here considered to be a precursor of the impact of TERREG— explicitly advocates the take-down of what it calls 'non-violent terrorist content' including material on terrorist groups' 'alleged utopian aspects',

[56] Abazi (n. 8); de Goede and Wesseling, 'Secrecy and Security in Transatlantic Terrorism Finance Tracking', 39 *Journal of European Integration* (2017) 253.

[57] Commission Report 342 final on the Joint Review of the TFTP (2011), at 7.

[58] Art. 21(2) of TERREG (EU) 2021/784.

[59] S. T. Roberts, *Behind the Screen: Content Moderation in the Shadows of Social Media* (2019); De Gregorio, 'Democratising Online Content Moderation', 36 *Computer Law & Security Review* (2019) 1; Helberger, Pierson, and Poell, 'Governing Online Platforms: From Contested to Cooperative Responsibility', 34 *The Information Society* (2018) 1.

[60] Van Hoboken, 'The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications', *Transatlantic Working Group on Content Moderation Online and Freedom of Expression* (2019) 1.

but also poetry and song lyrics that can be linked to groups like IS.[61] Clearly, such a broad approach to content removal raises questions concerning the scope and application of future TERREG impact.[62]

TERREG stipulates that social media providers publish transparency reports, with information on the measures taken to remove content, the numbers of items removed, the ways in which prevention of re-upload is done ('in particular where automated tools have been used') and the number and outcome of complaints.[63] These transparency reports have to be provided by private platforms, because the decision to remove content ultimately remains a private decision, even if it is steered in content and governed in procedure by public authorities. We may glimpse how such transparency reports will look in practice once TERREG comes into force in June 2022 by examining a similar entity operating under the auspices of Europol, the EU IRU, which also publishes transparency reports. Three have been published to date (2017, 2018, and 2019) and offer valuable information on the number of pieces of 'terrorist content' that are assessed and deleted. On the one hand, we get some quantitative information concerning removals of online content. For example, in the 2018 report, it is noted that: 'A total of 86,076 pieces have been assessed, which triggered 83,871 decisions for referral. The content was detected across 179 online platforms.'[64] On the other hand, the reports do not define how a 'piece of terrorist content' is defined or (algorithmically) recognized. The reports use a lot of jargon concerning the new policies and instruments that are being developed in the context of IRU, discussing for example 'intelligence notification', 'cross-match reports', etc., without explaining and contextualizing what these 'products and services' entail. It may, however, be queried how useful this information is and it seems not to be forwarded to anyone for discussion or debate. Articles 7 and 8 of TERREG prescribe the obligation of annual transparency reports by hosting services and social media platforms, detailing the nature of the information to be included in such reports. Remedies and redress mechanisms are to be designed by the companies themselves, and no mention is made in the Regulation of an independent forum where the transparency

[61] EU IRU, *On the Importance of Taking-Down Non-Violent Terrorist Content*, VoxPol, (2019), https://www.voxpol.eu/on-the-importance-of-taking-down-non-violent-terrorist-content/ (last visited 10 December 2021).

[62] Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; The Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; Van Hoboken (n. 60).

[63] Section III, Arts 7–8 TERREG (EU) 2021/784.

[64] EU IRU, *Transparency Report 2019* (2020), at 5.

reports are assembled or examined, or where disputes concerning the legitimacy of removal can be taken.

When it comes to ETIAS but also ECRIS-TCN, we move into an assessment of interoperable EU and national information systems that are less obviously connected to private actors in the way the previous two examples are, although ETIAS involves airline companies in pre-boarding checks. The specific nature of the activities of the public authorities involved in interoperable data sharing for security purposes involves the processing of very large amounts of personal data. ETIAS does not process biometric data, but it does process some information on criminal records (also deserving special safeguards). ECRIS-TCN, by contrast, processes both biometric data (fingerprints and potentially facial images) and some information on criminal records (the existence of a criminal record as such).[65]

Both the supervision by the EDPS and the reporting obligations in question require the actors involved in the use, management, and development of ETIAS and ECRIS-TCN—and above all, the concrete mediator, eu-LISA—to continually offer information and explanation about how the two information systems are functioning, and whether they function appropriately in view of data protection and fundamental rights standards.[66] These are undoubtedly practices of account-ability and show how accountability is given concrete shape in these programmes. They require that eu-LISA—and in some instances the European Border and Coast Guard Agency (EBCGA) (in relation to ETIAS and its Central Unit which it houses)—give account of how data is processed and of the lawfulness of their everyday data-sharing practices.

eu-LISA is, in its management and development of both ETIAS and ECRIS-TCN, also subject to a number of accountability practices specifically in this regard. It is, for instance, obliged to regularly report to the Member States and to the Commission on issues it encounters when carrying out quality checks on the data stored in the information systems.[67] It also has to inform the EDPS on measures it takes notably with regards the security of the processing or the lawful use of the data in the systems.[68] This is an important requirement and has analogies in other regulations of large-scale data information schemes such

[65] Arts 67 and 92 ETIAS Regulation (EU) 2018/1240; Arts 29 and 36 ECRIS-TCN Regulation (EU) 2019/816; on the need for supervision, see Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention', 2 *University of Luxembourg Law Working Paper* (2018) 1; On ETIAS, Michéa and Rousvoal, 'The Criminal Procedure Out of Itself: A Case Study of the Relationship Between EU Law and Criminal Procedure using the ETIAS System', 6(1) *European Papers* (2021) 473.

[66] Art. 67(3) ETIAS Regulation (EU) 2018/1240; Art. 29(3) ECRIS-TCN Regulation (EU) 2019/816.

[67] Art. 11(13) ECRIS-TCN Regulation; Art. 74(5) ETIAS Regulation (EU) 2018/1240.

[68] Art. 59(5) ETIAS Regulation (EU) 2018/1240; Art. 13 ECRIS-TCN Regulation (EU) 2019/861.

as SIS II and VIS.[69] Moreover, whereas the national supervisory authorities ensure that the data transmitted to and from ECRIS-TCN and ETIAS at national level is lawfully processed under data protection law, eu-LISA is specifically subject to the supervision of the EDPS. The latter ensures that an audit is carried out of eu-LISA's personal data processing activities every three years, and that a report on that audit is sent to the European Parliament, the Council, the Commission, eu-LISA, and the supervisory authorities. eu-LISA is specifically required to cooperate with the EDPS by giving him the information she or he requests.[70]

eu-LISA must also report at regular intervals on the operation of the two databases. These reporting duties already start in the development phase of the information systems, and continue afterwards. In fact, Article 36 of ECRIS-TCN Regulation sets out that during its design and development phase, eu-LISA must report to the European Parliament and the Council on the state of development of the information system every six months.[71] The same goes for ETIAS. Article 92 of the Regulation notes that during the development phase, eu-LISA, but also Europol and the European Border and Coast Guard Agency (Frontex) are required to report twice a year on the progress made on the implementation and development of the Regulation.[72] While eu-LISA's reporting focuses among others on the evolution of the Central Unit and the communication infrastructure, the reporting of Frontex and Europol deals essentially with the costs incurred. After the start of ECRIS-TCN and ETIAS operation in 2022, and every two years thereafter, eu-LISA must submit a report on the technical functioning of the systems, including on issues of security, to the Commission.[73]

With regard to the European Commission, the Regulations state that every four years, it will produce a report on the evaluation of the databases.[74] Whereas the evaluation of ECRIS-TCN shall focus on the application of the Regulation, the results achieved, and the impact on fundamental rights, the evaluation of ETIAS also addresses the screening rules and the potential need to modify the mandate. The reports are based on information given to it by eu-LISA and the Member States. It may include recommendations or legislative

[69] Arts 15, 60(3) and 74 SIS II Regulation (EU) 2018/1862 on police and judicial cooperation in criminal matters OJ L 312/56; Arts 45 and 60 SIS II Regulation (EU) 2018/1861 on border checks OJ L 312/14; Art. 16 SIS II Regulation (EU) 2018/1860 on return of illegally staying third-country nationals OJ L 312/1; Arts 29 and 50(3) VIS Regulation (EU) 2021/1133 OJ L 248/1.

[70] Art. 67 ETIAS Regulation (EU) 2918/1240; Art. 29 ECRIS-TCN Regulation (EU) 2019/861.

[71] Art. 36(3) ECRIS-TCN Regulation (EU) 2019/861.

[72] Art. 92(2) ETIAS Regulation (EU) 2018/1240.

[73] Art. 92(4) ETIAS Regulation (EU) 2018/1240; Art. 36(8) ECRIS-TCN Regulation (EU) 2019/861.

[74] Art. 92(5) ETIAS Regulation (EU) 2018/1240; Art. 36(9) ECRIS-TCN Regulation (EU) 2019/861.

proposals to the European Parliament and the Council, and is sent to the European Parliament, the Council, the EDPS, and the FRA. One could say that, indirectly, the Commission's obligations to report to the remaining relevant EU institutions renders eu-LISA accountable to it, as eu-LISA must explain how the databases are functioning, so that the Commission may do the same. As of today, no practice can be found on reporting of these two databases, and it remains thus unclear what the control will look like. By analogy, one can analyse the evaluation reports made by the Commission on the SIS II and VIS.[75] These include statistical reports, studies, questionnaires, and interviews, and followed an assessment of the following criteria—effectiveness, coherence, efficiency, relevance, and added value. Thus, the future evaluation on ECRIS-TCN and ETIAS shall presumably follow the same approach.

ETIAS has a particularity in the sense that the overall framework for the processing of personal data is the responsibility of eu-LISA (as is the case with ECRIS-TCN), but it is for the EBCGA to set up the ETIAS Central Unit. The actual processing of personal data is the responsibility of the national authorities involved. Even if the involvement of the EU agencies in concrete, individual instances of data sharing will remain comparatively limited, the EBCGA and eu-LISA are nevertheless subject to various accountability mechanisms. The ETIAS Central Unit, which is established within the EBCGA, must publish an annual activity report that must include several statistics. The reports include notably the numbers of travel authorizations automatically issued by the ETIAS Central System, the numbers of applications verified by that unit, the numbers of applications manually processed per Member State, as well as the numbers of applications of third country nationals that were refused, along with the grounds for that refusal. In addition to such statistical information, the annual activity report by the ETIAS Central Unit must provide general information on the functioning of the ETIAS Central Unit and the challenges that it faces in exercising its tasks. The report is to be submitted to the European Parliament, the Council, and the Commission for information and possible debate.[76] Finally, ETIAS also devotes more attention to the accountability mechanisms that should apply to eu-LISA. It regularly reports to the Member States, the European Parliament, the Council, and the Commission, but also to ETIAS

[75] For example, European Commission 880 final, Report from the Commission to the European Parliament and the Council on the evaluation of the second-generation SIS II (2016); European Commission 328 final Staff Working Document (2016), Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the VIS and the exchange of data between Member States on short-stay visas (VIS Regulation) of 14 October 2016.

[76] Art. 7(3) ETIAS Regulation (EU) 2018/1240.

Central Unit, when carrying out quality checks on the data contained in the ETIAS Central System.[77]

We have discussed present and future modes of reporting and public information as they exist within TFTP and IRU, and as they are taking shape in relation to TERREG, ECRIS-TCN, and ETIAS. A tabular summary of this discussion is provided in Table 6.1. Based on this overview, our preliminary conclusions are threefold. (1) Across the board, it seems that the provision of information is done by actors themselves, on their own terms, and using their own terminology and criteria. That terminology is (or may in the future) often be obfuscated and imprecise, and not easy to discern for a wider public. For example, what is a 'piece of terrorist-related content' in TERREG? What does 'transparency' and 'accountability' mean when used by eu-LISA in a telegraphic and self-referential way? (2) The provision of information is post hoc and focused on recounting technical facts (for example, numbers of searches, numbers of hits, numbers of pushes). In the case of ETIAS, ECRIS-TCN, and TERREG there is no actual practice yet of logging and reporting so reliance is placed on how Europol and eu-LISA have performed similar kinds of reporting in other data-driven environments. These deal essentially with the technical aspects of the infrastructure and the system, but also touch upon broader issues of security, data protection, and interoperability. (3) It is not clear to what extent there is an obligation for the institutional actor or accountability forum to debate, write a report on or investigate further through questioning of, for example, the Director of EU agencies (Europol and eu-LISA) after receiving the annual activity report or other less frequent evaluation reports. The role of the EDPS seems to be a limited one in these programmes, as does that of the national data protection authorities. This is not surprising given their limited resources and lack of technical knowledge.[78] The European Ombudsman does not seem to have a role in this context and the fact that already now there is such scarce information on actual supervision in practice of the existing databases feeds the expectation that this trend will continue in the future with the systems now emerging in the pipeline.

The depth of the analysis presented as well as the subsequent accountability trajectory in terms of dialogue will now be examined under the related accountability criteria of 'justification' and sanction and/or consequence imposed by another actor (public accountability forum).

[77] Art. 75(5) ETIAS Regulation (EU) 2018/1240.

[78] Lynskey, 'The Europeanisation of Data Protection Law', 19 *Cambridge Yearbook of European Legal Studies* (2017) 252, at 252–253.

Table 6.1 Information practices in TFTP, TERREG, ETIAS, and ECRIS-TCN.

	Report available and limitations	Who gives the information
TFTP	- Five review reports (Joint Reviews) including details on the process of evaluation, on the nature, number, and results of the searches, number of leads shared, etc. - JBS/EDPS Reports. - Crucial information is not included in the review reports (e.g. number data actually requested from SWIFT). - JSB/EDPS Reports are EU-Classified with the exception of their short concluding parts.	Joint Review Team (EU–US) Europol Oversight bodies.
TERREG	- Annual transparency reports by platforms include how many pieces of terrorist-related content have been removed, overview of complaint procedures, etc. - No definition of 'a piece of terrorist content'.	Report provided by private platforms.
ETIAS	- Reports during the development phase by eu-LISA, Europol, and Frontex, twice per year on the state of development and progress made. - Reports by eu-LISA once ETIAS is in operation on the technical functioning of the system (including security issues). - Audits by the EDPS on eu-LISA and the system. - ETIAS Central Unit, established within the EBCGA, publishes an annual activity report which includes several statistics. - eu-LISA regularly reports to Member States, the Commission, and EDPS on quality checks and security issues. - Report of the Commission on the evaluation of the system.	eu-LISA offers information and explanation on how the information system functions.
ECRIS-TCN	- Reports during the development phase by eu-LISA on the state of development and progress made (twice per year). - Reports by eu-LISA once ECRIS-TCN is in operation on the technical functioning of the system (including security issues). - Audits by the EDPS on eu-LISA and on the system. - eu-LISA regularly reports to Member States, the Commission, and EDPS on quality checks and security issue. - Report from the Commission on the evaluation of the system.	eu-LISA offers information and explanation on how the information system functions. Frontex accounts on how data is processed and the lawfulness of the everyday data-sharing practices.

B. Justification

The second mechanism of accountability is that of justification, which is needed before deliberation by an accountability forum is possible. Which decisions and choices are justified by the actor(s) involved, and how? Which decisions and choices simply remain unknown? Who is in charge of the narrative explanation concerning the actions and decisions made within data-led security programmes? And what are the normative terms of reference that are mobilized to justify a programme or a programme's actions? We find that the self-reporting by security authorities affects the manner in which explanation is structured and limited. As Ida Koivisto argues, algorithmic transparency often works through 'iconophilia', meaning that it focuses on 'illustrations, statistics, reports, memoranda etc.', that may prioritize visibility over explanation and justification.[79]

First, let us examine arguments and examples on effectiveness that are mobilized in relation to the TFTP and that justify it. In this programme, we can observe the emergence of specific narratives of justification that appeal to the effectiveness of the programme in relation to counterterrorism, but that ultimately reveal very little information on how algorithmic security works in the TFTP. It has become widely claimed that the TFTP is effective in its operations, yet public information that demonstrate the effectiveness remains limited. In the First Joint Review Report questions about the 'added value' of the TFTP to terrorist investigations were raised, and the report stated:

> the EU review team is of the opinion that efforts should be made to further substantiate the added value of the program, in particular through more systematic monitoring of the results … Treasury should seek feedback from the agencies which receive TFTP derived information on a systematic basis in order to verify the added value of the information.[80]

In response to this call, from the Second Joint Review Report onward, the reporting includes case examples where TFTP-derived information ostensibly played an important role. These are important cases, mostly of well-known terrorist plots and suspects, that have been identified and, in some cases, prosecuted. For example, the 2017 Joint Review report mentions several so-called 'value examples' where TFTP information was used in cases of specific named

[79] Koivisto, 'Thinking Inside the Box' (n. 38) 11; also Koivisto, this volume (n. 38).
[80] TFTP First Joint Review Report (n. 57) 6.

terrorist suspects, terrorist perpetrators, and those advocating or recruiting for the conflict in Syria.[81] Yet at the same time, the precise link between these named cases and the algorithmic analysis within TFTP remains unclear.[82] It is not known which information about a case is TFTP-derived, and how such information was shared with national authorities. As such, the information in the case examples of the Joint Reviews cannot be independently verified by observers and researchers, and the question of whether TFTP-derived information was decisive, crucial, tangential, marginal, or irrelevant to a case, remains unanswerable. The generic case examples offered in review reports offer narrative justification that seems to underscore the effectiveness of the programme. However, the narratives are on the actors' own terms and cannot be independently verified. They fall (far) short of 'algorithmic accountability' that could log into the TFTP system to explain how TFTP search terms are linked to particular automated outcomes.

Similar considerations are very likely to apply to the use of algorithms in the context of ETIAS screening. Indeed, it may often be near-impossible to determine the exact causal links between a multitude of different human agents that fed the training data to the algorithm and how that algorithm actually worked later on in practice.[83] Engstrom and Ho aptly capture the nature of the problem at stake here: '[O]n the one hand, the body of law that governs how agencies do their work is premised on transparency, accountability and reason-giving. … On the other hand, the algorithmic tools that agencies are increasingly using to make and support public decisions are not, by their structure, fully explainable.' The opacity of the algorithms that public agencies deploy inevitably becomes a matter of the opacity and accountability of the agencies themselves.[84]

Second, looking at IRU and TERREG, we ask how the effectiveness of these programmes is elaborated and justified. When it comes to the narrative justification of interventions and removals, the IRU reports offer cryptic formulations and little detail. For example, the 2017 IRU report notes that: 'The EU IRU supported 167 EU MS operations and produced 192 operational products.'[85] As previously mentioned, it remains unclear what 'operations' and 'operational

[81] Commission Report 31 final on the Fourth Joint Review Report of the TFTP (2017) at 41–43.

[82] M. Wesseling, 'The European Fight Against Terrorism Financing' (2013) (PhD dissertation, University of Amsterdam).

[83] Hayes, Van de Poel, and Steen, 'Algorithms and Values in Justice and Security', 35 *AI & Society* (2020) 533.

[84] Freeman Engstrom and Ho, 'Algorithmic Accountability in the Administrative State', 37 *Yale Journal on Regulation* (2020) 19, at 21–22.

[85] EU IRU, *Transparency Report 2017* Report (2018) at 7.

products' are in the context of flagging and removing online content. It remains to be seen how service providers will explain and justify operations and take-downs once TERREG mandated reports are issued. Removals have to be publicly reported and appeal mechanisms for mistakes and incorrect removals have to be designed, but this is to be done *by* the company and *within* the company, not through a broader, independent or publicly managed platform.

When it comes to ETIAS we can only deduce for now from the types of justification that are given on similar kinds of material by other mediating actors such as Europol and eu-LISA in other contexts. For example, when it comes to knowing the access of Europol to SIS II and the numbers of searches and hits then numbers are 'logged' in various reports. It is a matter of patching it together through the reporting by Europol itself as eu-LISA does not cover Europol access when it provides its general report on the operation of SIS II.[86] Not only is justification as such not given nor in any sense the practice by either agency but the amount of explanation given for any key choices is minimal, perhaps even non-existent. For example, a key choice was to install the capability to launch automated batch searches that facilitates more structured cross-checking of large amounts of relevant Europol data against the SIS.[87] It simply says: 'Schengen Information System (SIS) II: the batch search functionality was installed at the end of 2016. The efficiency of the process had a positive impact on the ability of Europol to utilize the system in supporting operations, with searches moving from 630 in 2016 to 21,951 from 1 January until 11 September 2017.'[88] No information on Europol access is included in the eu-LISA general reports.[89] A one word justification in the form of efficiency is all there is. This is paradigmatic for the kind of reporting that takes place in annual activity reports and database specific reporting by eu-LISA, such as on SIS II. The success of SIS II 'lies in its flexibility, vague wording and wide discretion to define the outer limits of who constitutes part of the risk population and be subject to surveillance of movement'.[90] Creating links between alerts may lead to situations where persons who were previously innocent become connected with crime or criminal networks, with adverse effects on their status.[91] Given the size and nature of SIS II this is of concern. When ETIAS comes into

[86] eu-LISA, *SIS II—2020 Statistics* (March 2021) notes that: 'However, the statistics on access to SIS II by the EU agencies are not included within the scope of this document […]'.

[87] Europol, *Europol Programming Document 2018–2020* (2018) at 35–36.

[88] Europol, *2017 Consolidated Annual Activity Report* (2018), at 20.

[89] eu-LISA (n. 86) 5.

[90] N. Vavoula, *Immigration and Privacy in the Law of the European Union—The Case of Databases* (2019) at 135.

[91] F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice, towards Harmonized Data Protection Principles for Information Exchange at EU-Level* (2012) at 266.

operation, this concern multiplies many times given the nature of the interoperability envisaged. ETIAS promises to deliver a 'justification of the refusal' to rejected applicants, yet it remains to be seen how such justifications are narrated and substantiated, especially as cases concerning lack of explanation in visa rejections have previously been brought before the EU courts.[92] In principle, the justification shall include the reason for the denial, reference to the ETIAS National Unit that refused the application and information on the right to lodge an appeal, but the basis of the decision will remain unknown (Europol data, from an alert, etc.).[93]

When it comes to ECRIS-TCN, not much is said about justification. It is only mentioned once in the Regulation: 'The log of consultations and disclosures shall make it possible to establish the justification of such operation.'[94] Thus, justification as such is not given in any sense; however, it shall be made possible at a later stage.

With regard to eu-LISA and its key mediating role creating and managing large-scale databases including both SIS II, VIS, and ETIAS and ECRIS-TCN its practice is to produce periodic reports as to their operation. Yet if one studies the reports that have been made for the other databases that will be interoperable with ETIAS and ECRIS-TCN once it comes into operation, there is a practice and technique of logging what are effectively the bits and bytes of data, the searches that have been made (and if applicable, the hits). There is certainly no justification given for why operations were carried out (even in procedural terms or according to substantive criteria in a way that are not individually operationally specific) and this will make the work of accountability fora such as the data protection authorities and the EDPS very difficult indeed. Such reports are then sent to certain core EU institutions for information. Only when the Commission has to do a four yearly evaluation may it engage in a more pro-active way with eu-LISA in terms of the information it requires. Similar evaluations were conducted on SIS II and VIS, in which the Commission assessed the relevance, effectiveness, efficiency, coherence, and added value of the system.[95] To do so, the Commission based itself on evidence and opinions from national authorities, Europol, the EDPS, and eu-LISA, as

[92] ETIAS, 'The ETIAS Application Process: How it works?' (2021), https://www.etiasvisa.com/etias-news/etias-application-how-it-works (last visited 16 December 2021).

[93] ETIAS, 'Why an ETIAS Application Could Be Denied' (2020), https://www.etiasvisa.com/etias-news/can-etias-be-refused (last visited 16 December 2021).

[94] Art. 31(3) ECRIS-TCN Regulation (EU) 2019/861.

[95] Commission report 880 final on the evaluation of the second generation SIS II (2016); Commission Staff Working Document 328 final, Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the VIS and the exchange of data between Member States on short-stay visas (VIS Regulation) (2016).

well as questionnaires, surveys, and interviews, notably with eu-LISA's staff. The EDPS, in conducting its audits, has access to all the documents and the premises from eu-LISA.[96] The audits include the verification of on-the-spot compliance and the checking of the security and operational management of the databases. eu-LISA has in this regard a real obligation to assist EDPS inspectors.

When it comes to the European Parliament, its ability to engage substantively and to deliberate on the basis of the information provided by eu-LISA is limited by a number of factors. First the Parliament is a generalist institution that does not possess the kind of specialized knowledge needed to deliberate on the necessity and efficiency of complex data-driven operations and the procedures in place in that regard (or only to a very limited extent). Second, its powers of active investigation are limited and can only be triggered at present in a non-autonomous fashion and most likely only if information is leaked or there is a whistle-blower.[97] Third, much of the information it may hypothetically require access to will have been classified and there are no arrangements in place, as in other areas, for example, Customs Freight Simplified Procedures (CFSP), for it to obtain privileged access in a non-public and controlled fashion even if eu-LISA was willing to engage in this manner. The latter is not likely given its own rhetoric and justification for its mediating role and the fact that it merely facilitates and manages the technical sides of large-scale infrastructures.

Table 6.2 summarizes the justification practices of the four programmes discussed in this section. Secrecy is the elephant in the room. It looms large in this area of data-led security programmes. The argument is always that, for reasons of security and also for efficiency and operational reasons, no access can be given to data other than the logging that is reported in various activity reports by a number of actors. But actually, the secrecy system is deeper than this. One of the areas where there is some public visibility (through the website and various documents included) are the security rules and the rules on classifying documents.[98] There are two points to note. First, the rules are factual, largely aligned with EU-wide rules and offer little if any 'justification'. Second, a system is put in place as is usual in systems of classified information where there is only a small cohort of officials internal to the agencies in question who

[96] Art. 67(3) ETIAS Regulation (EU) 2018/1240; Art. 29(3) ECRIS-TCN Regulation (EU) 2019/816.

[97] See, for example, with regards to Frontex, ECRE, 'Frontex: One Investigation Closes as Another Begins and the Agency's Role in Return and Ability to Purchase Firearms under Scrutiny' (2021), https://ecre.org/frontex-one-investigation-closes-as-another-begins-and-the-agencys-role-in-return-and-ability-to-purchase-firearms-under-scrutiny/ (last visited 16 December 2021).

[98] See, for example, for eu-LISA, Decision of the Management Board on the Security Rules for Protection EU Classified Information in eu-LISA (2019) 273.

Table 6.2 Justification practices in TFTP, TERREG, ETIAS, and ECRIS-TCN

TFTP	- Emergence of specific narrative of justification that appeal to the effectiveness of the programme. - Case examples included in the reports where TFTP info was used **BUT** very little information on how algorithmic analysis and algorithmic security works, and how links are made.
TERREG	- Overview of numbers of removals and referrals. **BUT** little detail and cryptic formulations, lack of meaningful narrative justification
ETIAS	- Promise to deliver a 'justification of the refusal' that includes reason for denial, reference to ETIAS National Unit that refused the application and information on the right to lodge an appeal. **BUT** it is unclear how such justification is narrated and substantiated. The basis of the decision will remain unclear (alert, Europol data …).
ECRIS-TCN	- Possibility to establish the justification. **BUT** unclear how the justification is narrated and substantiated.

have access to (all) information above a certain level. It is not clear what the connection is in this regard between similarly situated officials in one institution or agency and other similarly situated officials in other institutions and agencies. There is no information available on this, perhaps unsurprisingly. It follows from the highly classified systems in place that information on data in terms of justification will almost never be available, other than certain raw components. Where visibility does exist—for example, in relation to number of searches (in TFTP), number of rejections (of visa applications in ETIAS), and number of removals (of online content pursuant to TERREG)—there is the question of whether numerical visibility constitutes meaningful justification, especially if the reports cannot themselves be independently verified and/or questioned and scrutinized in the European Parliament. As Koivisto puts it, 'transparency is not enough to guarantee understandability'.[99]

C. Sanction/Public Fora

The third mechanism of accountability is that of consequences. Questions here are not just about the consequences for actors, like penalties, disruptions, or fines that they may face in case their explanations are rejected by the public. Questions can also be raised about the concrete ways in which cases may be

[99] Koivisto, 'Thinking Inside the Box' (n. 38) 11.

heard and public fora may be assembled to address mistakes, bias, or abuse *in the first place*. Is it possible at all for cases of harm or wrongdoing in our selected security programmes to appear before a public accountability forum, and if so how?

First, the TFTP is a multi-actor system, in which a private company (SWIFT as the designated provider) works with public authorities on both sides of the Atlantic to generate data analytics and policing leads. As such, it demonstrates the challenges that algorithmic security poses to traditional models and mechanisms of accountability, for there is not one territorially-based actor that can be sanctioned or penalized in case of accountability breaches. Yet, the TFTP does show how multi-jurisdictional models of accountability could work. Under the conditions of the Treaty, it is possible for overseers to interrupt and even cancel TFTP searches when the scope conditions of the Treaty are not fulfilled. However, in all years of its existence, TFTP searches have never been stopped periodically, even during the time that strong transatlantic controversy over the programme's legitimacy took place. In the current, Treaty-based regulation of TFTP accountability, it does however happen that individual searches are blocked and delayed, when additional information is requested by the TFTP overseer(s). Most often, additional information is requested post hoc, thus without interrupting the searches.[100] However, search interruptions do take place within the TFTP: for example, the Fourth Review Report (covering the period 2014–2015) notes that 45 searches were blocked by the overseers (out of a total of 27,095 searches), because 'the search terms … were considered to be too broad'.[101] By comparison, during the period of the Fifth Review Report (2016–2018), 53 searches (out of 39,000) were blocked for the same reason, and 645 searches were queried by the overseers.[102]

Yet, beyond the interruption of searches, there is very little by way of sanctions when TFTP operations breach accountability or operate unfairly, for example, by engaging in discrimination of certain groups. Arguably, the TFTP is discriminatory in nature, because its data requests are always directed at transfers to and from particular geographic regions and countries. However, the lack of algorithmic accountability in the programme means that neither the public nor even the relevant security authorities are aware whether and how particular police leads, interventions, or raids are TFTP-derived. Operators who receive intelligence do not know that these leads are TFTP-derived. This

[100] Commission Staff Working Document 301 final on the Fifth Joint Review of the TFTP (2019) 27.
[101] Commission Staff Working Document 17 final on the Fourth Joint Review of the TFTP (2017) 14.
[102] Commission Staff Working Document Fifth Joint Review TFTP (n. 100) 12.

means that sanctions in case of unfair or disproportional targeting and discrimination cannot be effected.

Furthermore, although the TFTP formally offers the possibility for data subject rectification and redress, it is practically impossible for cases of concern regarding TFTP to be heard publicly. If a citizen sends a request to access and verify their personal data held in the system, they will be told that *either* the question cannot be addressed because data cannot be extracted from the black boxed database because there is no known 'nexus' to terrorism *or* the question cannot be addressed because personal data have been extracted from the black boxed database, in which case the subject is considered suspect and not entitled to further information. In addition, security authorities who receive TFTP-derived information or leads typically do not know about the information's origin.[103] Consequently, it is impossible in practice to bring cases of harm, mistakes, or abuse to a public forum. In terms of formal oversight, the EDPS—as supervisory body of Europol—does have a mandate in relation to TFTP, but only as it concerns Article 4 of the Treaty, which sets out the procedure for US data request that 'shall be tailored as narrowly as possible'.[104] In this regard, the 2019 EDPS Report concludes, inter alia, that: 'Europol only relies on the US claims that such assessment has been conducted without actually having access to this analysis.'[105]

When it comes to TERREG, it is crucial to understand that it seeks to shape and govern the *private accountability mechanisms* of platforms and service providers. In TERREG, the 'duty of care' is a key concept that intends to strengthen and harmonize platforms' efforts in counterterrorism-related removal and to help shape the private reporting on removal actions.[106] Section III of TERREG sets out 'safeguards and accountability': these are aimed at guiding the formulation of private Terms-of-Service Regulations. Concerning redress, for example, Article 10 TERREG stipulates that: 'service providers shall establish effective and accessible mechanisms allowing content providers whose content has been removed … to submit a complaint against the action of the hosting service provider'. How this will be shaped in practice remains unclear: currently, platforms do not habitually have complaint or redress procedures for users whose contents is removed. Article 18.4 of TERREG foresees penalties

[103] Commission TFTP First Joint Review Report (n. 57) 12.
[104] Art. 4(2) of the TFTP Treaty.
[105] EDPS case number 2018-0683, TFTP Inspection Report, The Hague, (2019) at 2.
[106] Bellanova and de Goede (n. 37); Bellanova and de Goede, 'Co-producing Security: Platform Content Moderation and European Security Integration', *Journal of Common Market Studies* (2021).

for online service providers who fail to comply with its obligations of 'up to 4% of the hosting service provider's global turnover of the last business year'.

Ultimately, TERREG (in the future) and IRU (currently) place any sanctions for incorrect removals on private platforms and services. Concretely, Europol IRU does not actually remove online content, but focuses its work on producing *referrals* for private companies to take action under their own Terms-of-Service Regulations. These referrals are perhaps even more important for smaller platforms than they are for larger ones, because small platforms lack the means and resources for continuous, real-time monitoring of their content. Any removal decision is ultimately a private, platform decision, for which platforms are responsible and accountable. In terms of logged-out accountability, the TERREG case shows how accountability is a complex practice of public–private coproduction, whereby the EU is seeking to shape the removal actions and Term-of-Service regulations of private providers. For citizens affected by removal decisions, however, the landscape of redress is complex and privatized, and full algorithmic accountability of how online content is assessed and classified remains lacking.

The ETIAS Regulation establishes an independent ETIAS Fundamental Rights Guidance Board, which is composed of the Fundamental Rights Officer of EBCGA and of representatives of the EDPS, of the European Data Protection Board, and of the European Union Agency for Fundamental Rights. Initially, the European Parliament required the Board to perform audit duties, but this was not accepted in light of the EDPS role.[107] The ETIAS Fundamental Rights Guidance Board must produce an annual report on the observance of fundamental rights in ETIAS. The fact that the ETIAS Regulation specifically requires that reports be public suggests that they must be accessible and comprehensible to citizens at large.[108] It is highly likely that in these reports justifications will be given one way or another for the conclusions that are reached so that a deliberation can be made and, if appropriate, consequences imposed. ECRIS-TCN does not establish such an independent board, but the EDPS and Commission play a key role in the monitoring of the processing activities.

The EDPS, moreover, fulfils an important role in monitoring the personal data processing activities of eu-LISA, Europol, and the European Border and Coast Guard Agency related to ETIAS. The EDPS ensures that an audit of eu-LISA's and the ETIAS Central Unit's personal data processing activities is carried out in accordance with relevant international auditing standards at least

[107] K. Gál (European Parliament rapporteur), *Report on the proposal for ETIAS Regulation* (2017).
[108] Arts 10(1) and (5) ETIAS Regulation (EU) 2018/1240.

every three years. Based on the information resulting from that audit, the EDPS must draft a report, in which it offers recommendations in order to ensure, for example, higher data protection and security of the system. The EDPS shall submit the report to the European Parliament, to the Council, to the Commission, to eu-LISA, and to the supervisory authorities.[109] eu-LISA and Frontex can comment on the report. The same applies to ECRIS-TCN, with the exception of the role of the Central Unit and consequently Frontex's role in it. None of the audits on eu-LISA, Europol, or Frontex are publicly available.

The specific accountability mechanisms that apply within ETIAS and ECRIS-TCN are in addition to those that already exist in the general legal framework of eu-LISA. eu-LISA—along with the ETIAS Central Unit for ETIAS—must provide the Commission with all the information it requires, so that it may evaluate ETIAS and ECRIS-TCN every four years and submit a report on that evaluation to the European Parliament, the Council, the EDPS, and the European Agency for Fundamental Rights. That evaluation includes, for instance, the results, impact, effectiveness, and efficiency of ETIAS' performance, along with an assessment of its security and its impact on fundamental rights.[110] The Commission thus has the opportunity every four years to examine if eu-LISA is fulfilling its role effectively and in compliance with its founding Regulation. The findings of the Commission in this respect may lead it to propose legislation changing eu-LISA's mandate or even to suggest abolishing the agency altogether. This would obviously be the most severe judgment possible on the performance and indeed necessity of eu-LISA and clearly represents a tool of accountability that seems reserved for use in only extreme circumstances of mismanagement, maladministration, or incompetence.[111] Less stringent recommendations may include changes at the management and organizational level, such as changing the rules of procedures. Interim reports are required every year to evaluate the progress made in the implementation of the planned activities.

This section has mapped the possible consequences and sanctions built into the accountability mechanisms of our four selected data-led security programmes, as summarized in Table 6.3. We have also asked how public fora may

[109] Art. 67 ETIAS Regulation (EU) 2018/1240.

[110] Arts 92(5) and (7) ETIAS Regulation (EU) 2018/1240.

[111] See, for example, on Frontex's mismanagement, the reaction of the European Commission that asked for clarifications and supported the European Parliament's investigations, Liboreiro and McCaffrey, 'EU Migration Chief Urges Frontex to Clarify Pushbacks Allegations', *Euronews* (2021), https://www.euronews.com/2021/01/20/eu-migration-chief-urges-frontex-to-clarify-pushback-allegations (last visited 16 December 2021).

Table 6.3 Sanctions practices in TFTP, TERREG, ETIAS, and ECRIS-TCN

TFTP	- Multi-actor system and multi-jurisdiction models of accountability. - The overseer(s) can interrupt and cancel TFTP searches. - Individual searches can be blocked and additional info requested, and it is possibility for data subject to ask for rectification and redress. However, **impossible** to be hear publicly. - Formal oversight from the EDPS remains limited.
TERREG	- Shapes and governs private accountability mechanisms of platforms and service providers. - Redress possible: submit a complaint against the actions of the hosting service provides (practice is unclear). - Removal and redress remain *private* mechanisms and decision which leads to complex public–private coproduction.
ETIAS	- ETIAS FRA Guidance Board publishes a public report and may impose consequences. - EDPS monitors eu-LISA, Europol, and Frontex's processing of personal data (with recommendations). - Commission's evaluation can recommend changes at management and organizational level, legislative changes, or the abolishment of the agency.
ECRIS-TCN	- EDPS monitors eu-LISA and offers recommendations. - Commission's evaluation can recommend changes at management and organizational level, legislative changes, or the abolishment of the agency.

assemble to address questions of accountability in data-led security. We draw the following overall conclusions. First, there are examples of (possible) sanction within these programmes, from the interruption of searches in TFTP to the discontinuation of the eu-LISA agency (in theory). However, and this is our second conclusion, in data-led security, the actor and the forum to which an account is to be offered are profoundly disconnected. There is a lack of concrete mechanisms through which cases can be heard before a forum. Indeed, it is often difficult, if not impossible, for citizens to know whether and how their data were captured and analysed, and how algorithmic analytics led to certain outcomes (like visa rejections or criminal prosecutions). This is due not just to the classification or secrecy of the processes of data analytics; it is also because algorithmic logic generally affects the relation between cause and effect, in order to govern through anomaly.[112] Machine learning programmes do not necessarily operate with a predefined notion of deviance to be identified, but

[112] Aradau and Blanke, 'Governing Others: Anomaly and the Algorithmic Subject of Security', 3 *European Journal of International Security* (2018) 1; Amoore, 'Machine Learning Political Orders', *Review of International Studies* (2022) 1.

instead let 'anomaly' be found and defined through the data analytics themselves. The behaviour or transaction that is anomalous is not a predefined wrong or harm, but an outcome generated through the analytic process itself, and determinable only in relation to seemingly normal patterns of behaviour. Such 'machine learning political order' affects the sequence between cause and effect, and obfuscates the relation between personal data and security outcomes.[113] The very invisibility of the information-sharing process means that citizens have real challenges in obtaining access to legal remedies, for example, for a breach of the purpose limitation principle which foresees that personal data should not be used for purposes other than those originally foreseen, one of the most core principles of data protection in Europe.[114]

5. In Search of Logged-in EU Security Oversight

In this chapter, we have mapped the concrete mechanisms and practices of 'giving account' that are in operation and in design in four data-led security programmes. We have shown how these remain largely 'logged-out' of the algorithmic processes—overall, they rely on industry self-reporting, they prioritize visibility over explanation,[115] and explanability is severely limited by the secrecy and obfuscation that accompanies security programmes more generally. In all of our cases, it is not clear how public accountability forums can be assembled to foster genuine public deliberation concerning the (far-reaching) security decisions taken within these programmes. In some of our cases, new laws and oversight mechanisms are still being developed and it remains to be seen how these will function in practice. By focusing on the precursors of new programmes (IRU in the case of TERREG; SIS II in the case of ETIAS), we have been able to make a preliminary assessment. Thus, we have shown how information, justification, and sanction are taking shape in practice in new EU data-led security programmes. These emerging practices are only partially able to give a meaningful account of security decisions that can have major impacts on people's lives (including the denial of visas, or the sharing of their financial transaction information).

[113] Amoore (n. 112).

[114] Brouwer, 'Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation', in L. F. M. Besselink, S. Prechal, and F. Pennings (eds), *The Eclipse of the Legality Principle in the European Union* (2011) 273; Vavoula (n. 25).

[115] Koivisto, this volume (n. 38).

In this conclusion, we ask what a 'logged-in' accountability might look like, and what the conditions are for meaningful oversight of EU data-led security practices. This fits into a broader question concerning 'data justice', which asks how to 'determine ethical paths in a datafying world'.[116] The involvement of the EDPS, and indeed of other, national, data protection supervisors, represents a relatively obvious feature of accountability in interoperable information sharing. In the past, some scholars have noted how information systems generate serious problems from the point of view of judicial protection, given that there is generally 'no remedy against the use and computation of information once it has entered administrative networks, as long as this information does not lead to a final decision either on the European or the Member State level'.[117] Besides that issue, which results from the EU judicial system's focus on the review of legal acts, adopted in the exercise of decision-making powers, the very multitude of authorities linked through interoperable databases also makes it hard to determine which would be the competent jurisdiction to initiate judicial proceedings.

The difficulties in using other common accountability tools—such as independent judicial review—justifies the development of others, that may also prove more appropriate in light of the specific nature of the activities of the authorities involved in interoperable data-sharing for security purposes. Since those activities involve the processing of very large amounts of personal data, much of which is sensitive biometric data, and since the relatively novel character of interoperability requires continual improvement and scrutiny, it is logical that ETIAS and ECRIS-TCN emphasize in particular two types of accountability mechanisms: first, supervision by data protection watchdogs (the EDPS more specifically) and, second, reporting obligations to expert bodies (such as again the EDPS and the EU FRA) and institutional actors (such as the European Parliament, the Council, and the Commission), which would be involved in any political process leading to legislative reform of either ETIAS or ECRIS-TCN.[118]

[116] Taylor (n. 5) 2.

[117] Hofmann, 'Composite Decision Making Procedures in EU Administrative Law', in H. C.H. Hofmann and A. H. Türk, *Legal Challenges in EU Administrative Law* (2009) 136, at 161; Hofmann, 'Legal Protection and Liability in the European Composite Administration', in O. Jansen and B. Schöndorf-Haubold (eds), *The European Composite Administration* (2011) 441.

[118] Arts 67 and 92 ETIAS Regulation (EU) 2018/1240; Arts 29 and 36 ECRIS-TCN Regulation (EU) 2019/816; on the need for supervision, see Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention', 2 *University of Luxembourg Law Working Paper* (2018) 1; On ETIAS, Michéa and Rousvoal, 'The Criminal Procedure Out of Itself: A Case Study of the Relationship Between EU Law and Criminal Procedure using the ETIAS System', 6(1) *European Papers* (2021) 473.

Both the supervision by the EDPS and the reporting obligations in question require the actors involved in the use, management, and development of ETIAS and ECRIS-TCN—and above all, eu-LISA—to continually offer information and explanation as to how the two information systems are functioning, and as to whether they function appropriately in view of data protection and fundamental rights standards. These are undoubtedly instruments of accountability: they require that eu-LISA—and in some instances the EBCGA—give account of how data is processed and of the lawfulness of their everyday data-sharing practices.

But this description and the investigation carried out more generally in this chapter of all four programmes shows the limits of this approach, with bits of accountability not keeping pace with the bytes, searches, and hits in the real world of security practice, which are then potentially shared with a variety of actors at different governance levels. The panoply of institutions or forums that are presented with what are essentially logging reports (except when less frequent periodic evaluations are made publicly available) are not able to deliberate in substance on the raw information they receive. It seems to be more of a box ticking exercise than anything else. This does not mean that other accountability forums might not get involved on their own initiative (perhaps subsequent to leaking or whistleblowing). For example, the European Ombudsman has opened an investigation with regard to Frontex, and her powers enable her to actively investigate and question and request and receive detailed and targeted information in a way that other accountability forums that are provided with logging reports cannot. Another example is that of the Court of Auditors which recently, on its own initiative and outside of its normal auditing function of approving the annual accounts of each of the EU agencies (including those which house significant databases), prepared a report on general large-scale information systems.[119] The conclusions are on the nature of the data collected and the need for more focused and timely data. The exercise mainly involved an evaluation and assessment of border data from the point of view of efficiency and entailed detailed consideration of the information systems in question. The investigations of both the European Ombudsman and the European Court of Auditors involved post hoc examinations with, at best, some recommendations for the future that may or may not be implemented.

What the EU system lacks is one or more EU overseers specifically for data-driven accountability programmes. A broad analogy could be made with the

[119] European Court of Auditors Special Report No. 20/2019 on EU information systems supporting border control—a strong tool, but more focus needed on timely and complete data.

idea of having an information commissioner in pre-digital times, pre-large-scale information systems that are interoperable in nature and practice. The focus of a 'data-led security overseer office' would be specifically on real-time data infrastructures inside specific agencies, examining how data are requested, searched, accessed, and shared. As the name implies, data-led security programmes would need an external insider 'overseeing' what is happening and why, with the power to stop searches or require further more targeted justification. In this sense, the EU TFTP overseer is a unique and promising model, with the ability to examine and block algorithmic searches in real time, yet it is a model that currently still has profound shortcomings, especially the secrecy of the overseers' names and reports, and the lack of public information on the size and scope of data transfers.

What we call 'data-led security overseers' would be logged-into the algorithmic processes of analysis and intervention. They could be subject to not only reporting requirements but also the obligation to go before a general accountability forum (e.g. the European Parliament), answer questions, and engage, within limits, in a dialogue. An EU data-led security overseer can be conceptualized as a type of internal ombudsman, but one who is an expert in the technical data-driven nature of the programmes and with experience of relationships of accountability and the need for some public justification on the procedures in place, at the very least. An EU data-led security overseer would supervise adequate and practicable redress mechanisms and their public visibility. With the power to stop searches, interrupt programmes, and document rights infringements across programmes, an EU data-led security overseer office could be a genuine counterbalancing power to the proliferation and sometimes hasty and ad hoc design of European data-led security powers.