European Papers – A Journal on Law and Integration
Vol. 10, No. 3, 2025, pp. 779–801

The Future of Digitalisation in EU Law Enforcement
***edited by* Niovi Vavoula**

Dancing in the Dark: Policy Transformations Through Obfuscating Contestations in the Case of Prüm II

Nina Amelung[*] *and Helena Machado*[**]

ABSTRACT: In December 2021, the European Commission proposed amendments to the Prüm system on the exchange of different categories of personal data for stepping up cooperation for combating terrorism and cross-border crime (Prüm II). The proposal aimed to increase automation of the sharing of data, add new categories of data for exchange, namely facial images and police records, and prepares the integration of the Prüm system into the interoperability framework which interconnects the six large-scale IT systems in the European Union Area of Freedom, Security and Justice (AFSJ). In this article we analyse the public consultation process on these planned reforms to the Prüm II system, and we focus on two particular prospective changes: interoperability and

[*] Post-doctoral research fellow (Sociologist), Instituto de Ciências Sociais, Universidade de Lisboa, nina.amelung@ics.ulisboa.pt.

[**] Coordinator Researcher at CIES-Center for Research and Studies in Sociology, Iscte-University Institute of Lisbon, helena.cristina.machado@iscte-iul.pt.

Alphabetical order, equally contributing authors. Nina Amelung receives funding from the Fundação para a Ciência e Tecnologia in the context of the 'Fundação para a Ciência e Tecnologia' (with the reference number CEECIND/03611/2018/CP1541/CT0009), which funds the research project of Nina Amelung entitled 'Affected (non)publics: Social and political implications of transnational biometric databases in migration and crime control (AFFECT)'. Helena Machado acknowledges funding from the European Union through the European Research Council (ERC Advanced Grant, fAIces. Facial Recognition Technologies. Etho-Assemblages and Alternative Futures, Grant agreement ID: 101140664). Views and opinions expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

ISSN 2499-8249
doi: 10.15166/2499-8249/854

exchange of facial images. We argue that the public consultation process related to prospect changes to the Prüm system has functioned as 'technologies of democracy' by which policy transformations obfuscate tensions and conflicts around complex and contested public problems. Specifically, in the context of Prüm II, we assert that public consultation efforts fall short of addressing the concerns of the affected publics. Instead, they sideline and suppress alternative yet reasonably anticipated concerns, thereby fortifying dominant security frameworks.

KEYWORDS: Prüm II – interoperability – facial images – public consultation – technologies of democracy – stakeholders.

1. Introduction

Council Decision 2008/615/JHA and Council Decision 2008/616/JHA – the Prüm Decisions –[1] require Member States to step up cross-border cooperation by ensuring the availability of DNA, fingerprint and vehicle registration data from their national databases to assist in combating terrorism and cross-border crime. Since 2018, the Prüm Decisions have been subject to technical and political negotiations and reconfigurations, which were channelled into a Commission proposal for a Prüm II system, adopted on 8 December 2021.[2] On 8 February 2024, the European Parliament approved the rules on Prüm II and the Regulation 2024/982 (Prüm II Regulation) was adopted on 13 March 2024.[3]

The Prüm II Regulation aims to modernise the legal framework by increasing automation in the personal data exchanges, adding new categories of personal data that can be exchanged, namely facial images, police records, and driving licence data, standardizing the format in which data can be shared, setting new standards on data quality, transfers, and other largely technical elements, and creating a legal basis for searches for missing persons and unidentified human remains, irrespective of whether they have been initially collected for criminal or civil identification purposes.[4] Another novelty of the Regulation is the integration of Prüm II into the interoperability framework. The latter links the six large-scale IT systems established

[1] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime; Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[2] See, Council of the EU Press Release, 'Council Adopts Two General Approaches and a Recommendation to Improve Operational Police Cooperation and Information Exchange, Press Release' (10 June 2022), at www.consilium.europa.eu.

[3] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (Prüm II Regulation).

[4] EDRI, 'Respecting Fundamental Rights in the Cross-Border Investigation of Serious Crimes' (7 September 2022), at edri.org.

in the EU Area of Freedom, Security and Justice merging migration and mobility control on the one hand, and crime control on the other hand.[5]

Before the implementation of the Prüm system, literature pointed out important fundamental rights challenges regarding the protection of personal data, respect for private life, and the presumption of innocence.[6] These critical approaches gained new impetus as the Prüm system was being implemented – a process that lasted no less than 15 years.[7] Additional concerns were voiced regarding the significant heterogeneity in national legislations and police operations, as well as the accuracy, reliability, and accountability of the technical and operational governance regimes set up to facilitate the Prüm system.[8] Other studies took a broader approach to societal, cultural and political implications of the Prüm system, reflecting on the role of science and technology in the EU security agendas and policy making and implications on citizenship and democracy.[9] Democratic deficits were identified as key shortcomings in the process of implementing the Prüm regime, as the European Parliament

[5] C Blasi Casagran, 'Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU' (2021) 21 *Human Rights Law Review* 433.

[6] T Balzacq, D Bigo, S Carrera, and E Guild, 'Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats' (CEPS Working Document No. 234-2005).

[7] S Hufnagel and C McCartney, 'Police Cooperation Against Transnational Criminals' in N Boister and R Currie (eds), *Routledge Handbook of Transnational Criminal Law* (Routledge 2014) 107; S Matos, 'Privacy and Data Protection in the Surveillance Society: The Case of the Prüm System' (2020) 66 *Journal of forensic and legal medicine* 155; C McCartney, 'Opting in and Opting Out: Doing the Hokey Cokey with EU Policing and Judicial Cooperation' (2014) 77 *The Journal of Criminal Law* 543; C McCartney, E Topfer and R Granja, 'Biometric Forensic Identity Databases: Precariously Balanced or Faulty Scales?' in A Roberts, J Purshouse and J Bosland (eds), *Privacy, Technology and the Criminal Process* (Routledge 2023).

[8] F Santos, H Machado and S Silva, 'Forensic DNA Databases in European Countries: Is Size Linked to Performance?' (2013) 9 *Life Sciences, Society and Policy* 1; F Santos and H Machado, 'Patterns of Exchange of Forensic DNA Data in the European Union through the Prüm System' (2017) 57 *Science & Justice* 307–313; H Machado, and R Granja, 'Police Epistemic Culture and Boundary Work with Judicial Authorities and Forensic Scientists: The Case of Transnational DNA Data Exchange in the EU' (2019) 38 *New genetics and society* 289; V Toom, 'Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision' (Study for the LIBE Committee 2018); V Toom, R Granja and A Ludwig, 'The Prüm Decisions as an Aspirational Regime: Reviewing a Decade of Cross-Border Exchange and Comparison of Forensic DNA Data' (2019) *Forensic Science International: Genetics* 41, 50.

[9] N Amelung, R Granja, H Machado, *Modes of Bio-Bordering: The Hidden (Dis)integration of Europe* (Springer 2021); N Amelung, and H Machado, '"Bordering" Processes in the EU: De-Bordering and Re-Bordering along Transnational Systems of Biometric Database Technologies' (2019) 5 *International Journal of Migration and Border Studies* 392; H Machado, R Granja, N Amelung, 'Constructing Suspicion through Forensic DNA Databases in the EU. The Views of the Prüm Professionals' (2019) 60 *The British Journal of Criminology* 141; H Machado and R Granja, *Genetic Surveillance and Crime Control: Social, Cultural and Political Perspectives* (Taylor & Francis 2022) 212; B Prainsack and V Toom, 'The Prüm Regime: Situated Dis/empowerment in Transnational DNA Profile Exchange' (2010) 50 *The British Journal of Criminology* 1117; B Prainsack and V Toom, 'Performing the Union: The Prüm Decision and the European Dream' (2013) 44 *Studies in History and Philosophy of Science Part C: Studies in History and Philosophy of Biological and Biomedical Sciences* 71.

and the European Court of Justice were for years excluded from exercising democratic and judicial control. After all, the Prüm Decisions fell under the former third pillar or police and judicial cooperation in criminal matters. Thus, issues around the lack of democratic 'legitimacy and guarantees that all the public interests were equally balanced' had been problematized from early on.[10]

Regarding Prüm II, various stakeholders have raised diverse concerns about the planned restructuring arguing that it may pose challenges to the protection of fundamental rights.[11] However, we observe that these diverse concerns relating to the Prüm II proposal have played a limited role in the negotiating procedure. This observation prompts our interest to enquire in this article how public consultation processes as part of the regulatory process of Prüm II prefigure and (dis)enable the enactment of particular political visions for law enforcement cooperation relying on biometric data exchange in the EU.

The current transformations towards an expanded Prüm system require a closer look at the various 'consultation activities' or 'consultation strategy', set up by the European Council and the Commission assessing the limitations of current Prüm system and preparing for the Prüm II proposal. Public consultations have become a standard tool in the 'good governance' repertoire of the Commission over time.[12] We will address the selected public consultation activities with stakeholders and the wider publics that have accompanied the legislative process of the Prüm II proposal as sequences of staged performances of conflict resolution that fail to satisfy concerned publics.[13] Laurent has referred to such public participation forms as 'technologies of democracy', in the sense that they require material and cognitive investments to generate their intended outcomes, publics and collective problems.[14] They 'allocate public roles for citizens, define rules for legitimate actions of public and private actors, and identify suitable public issues for collective examination'. The objective of analysing organized consultations is 'to make explicit the political constructions they enact' and to reveal 'conflicts, oppositions and potential alternatives

[10] N Vavoula, 'Police Information Exchange - The Future Developments Regarding Prüm and the API Directive' (Study for the LIBE Committe 2020), at www.europarl.europa.eu.

[11] C McCartney, E Topfer and R Granja (n 7).

[12] AS Binderkrantz, J Blom-Hansen, M Baekgaard and S Serritzlew, 'Stakeholder Consultations in the EU Commission: Instruments of Involvement or Legitimacy?' (2023) 30 *Journal of European Public Policy* 1142; C Quittkat and B Kohler-Koch, 'Involving Civil Society in EU Governance: The Consultation Regime of the European Commission' in B Kohler-Koch and C Quittkat (eds), *De-Mystification of Participatory Democracy. EU Governance and Civil Society 41–61* (Oxford University Press 2013); AS Binderkrantz, AS Blom-Hansen and R Senninger, 'Countering Bias? The EU Commission's Consultation with Interest Groups' (2021) 28 *Journal of European Public Policy* 469.

[13] M Hajer, 'Setting the Stage: A Dramaturgy of Policy Deliberation' (2005) 36 *Administration & Society* 624; J Oomen, J Hoffman, and M Hajer, 'Techniques of Futuring: On How Imagined Futures become Socially Performative' (2022) 25 *European Journal of Social Theory* 252.

[14] B Laurent, 'Technologies of Democracy: Experiments and Demonstrations' (2011) 17 *Science and engineering ethics* 649, 651.

that are in tension with otherwise stable dominant constructions of democratic order'.[15] In light of the above, our aim is to investigate the staged processes and the framing of problems and solutions, and the situated and contingent framings of stakeholders' roles and the values guiding their approaches to Prüm II.

The article is structured as follows: in the next section we briefly outline the incremental regulatory evolution from Prüm to Prüm II. Then, we analyse the consultation process set up prior to the adoption of the Prüm II proposal. Afterwards, we explore the heterogeneous views on the planned reforms to the Prüm system focusing on two aspects: the preparation for its integration into the interoperability framework and the inclusion of facial images for exchange among police forces of the EU Member States. These selected examples serve to illustrate some characteristics and limitations of the process of consultation. We conclude by arguing that consultations activities have functioned as 'technologies of democracy' emphasizing the engineering and technocratic character of these processes oriented to demonstrate deliberation, consensus and agreement, embedded in, and co-constituting the governance of complex and contested public problems in pre-scripted ways.[16]

2. From Prüm to Prüm II

In 2018, ten years after the adoption of the Prüm Decisions and while not all Member States had implemented them in full, the European Council began to consider reforming the Prüm system, using the term 'Prüm Next Generation', later referred to as Prüm II.[17] Two driving forces behind the proposed reforms can be identified; on the one hand, legal, technical and operational shortcomings, and, on the other hand, the desire to include additional types of personal data, such as facial images and police records, as well as streamlining the IT architecture of the Prüm system with other existing database systems.

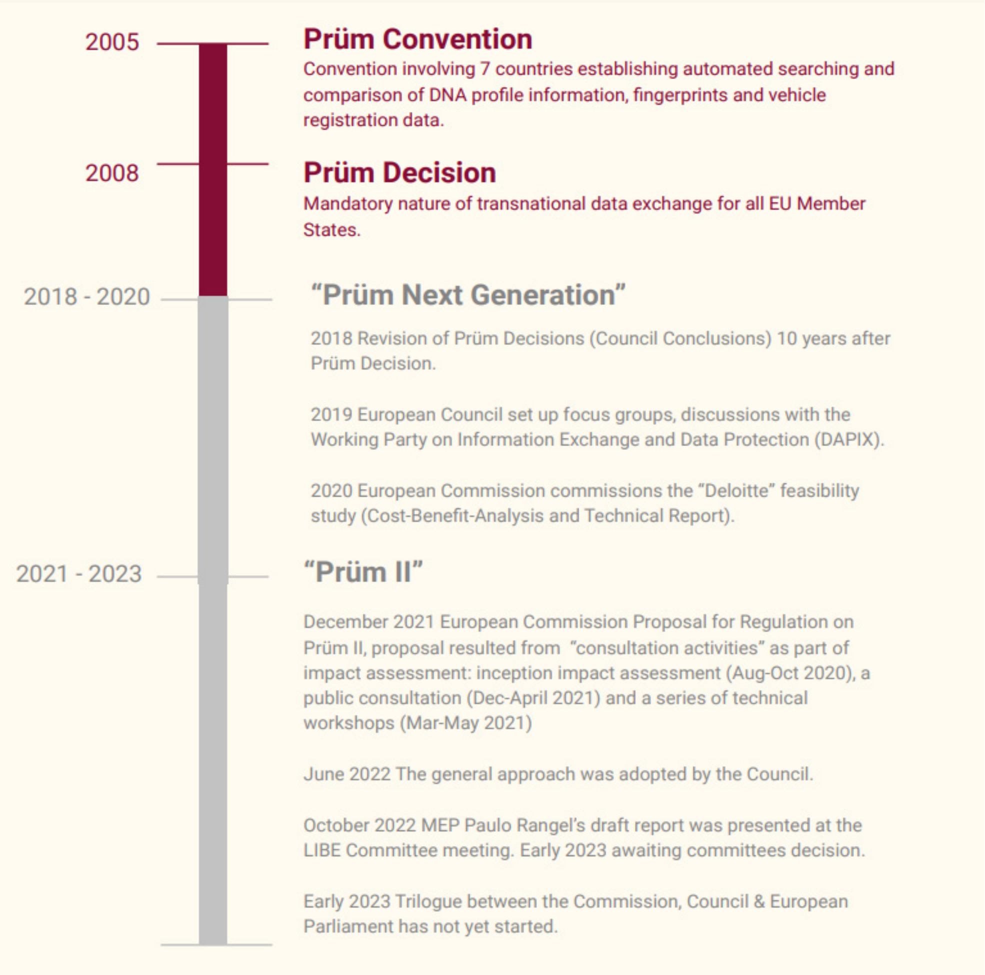
The first steps towards preparing a reform of the Prüm system took place (under the label of 'Prüm Next Generation') between 2018 and 2020 and was driven by the Council of the EU. The initial phase included focus groups on the different forensic modalities of fingerprints, DNA, Vehicle Registration Data (VRD) and facial images, discussions with the Working Party on Information Exchange and Data Protection, and from 1 January 2020, the Working Party on Justice and Home Affairs

[15] *Ibid.* 650–651.

[16] *Ibid.*

[17] Proposal COM(2021) 784 final for a Regulation of the European Parliament and of the Council of 8 December 2021 on automated data exchange for police cooperation ('Prüm II'), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council.

Information Exchange (IXIM) as well.[18] Additionally, the Commission commissioned a feasibility study from Deloitte a ‘feasibility’ on ‘improving information exchange’ under the Prüm decisions which incorporated a technical report accompanied by a cost-benefit. In response, the LIBE (Committee on Civil Liberties, Justice and Home Affairs) Committee of the European Parliament commissioned its own study to provide background information and to assess fundamental rights implications of the Prüm Next Generation project in-the-making.[19]



2005

Prüm Convention

Convention involving 7 countries establishing automated searching and comparison of DNA profile information, fingerprints and vehicle registration data.

2008

Prüm Decision

Mandatory nature of transnational data exchange for all EU Member States.

2018 - 2020

“Prüm Next Generation”

2018 Revision of Prüm Decisions (Council Conclusions) 10 years after Prüm Decision.

2019 European Council set up focus groups, discussions with the Working Party on Information Exchange and Data Protection (DAPIX).

2020 European Commission commissions the “Deloitte” feasibility study (Cost-Benefit-Analysis and Technical Report).

2021 - 2023

“Prüm II”

December 2021 European Commission Proposal for Regulation on Prüm II, proposal resulted from “consultation activities” as part of impact assessment: inception impact assessment (Aug-Oct 2020), a public consultation (Dec-April 2021) and a series of technical workshops (Mar-May 2021)

June 2022 The general approach was adopted by the Council.

October 2022 MEP Paulo Rangel’s draft report was presented at the LIBE Committee meeting. Early 2023 awaiting committees decision.

Early 2023 Trilogue between the Commission, Council & European Parliament has not yet started.

Figure 1: From Prüm to Prüm II (Authors’ compilation).

[18] Council of the European Union, Note 13511/19 from the German delegation to the Working Party on Information Exchange and Data Protection (DAPIX) on Next generation Prüm (Prüm.ng) - Reports from focus groups / Report on DNA data exchange.

[19] N Vavoula (n 10).

During the COVID-19 pandemic, the Commission initiated the second phase of preparations for the Prüm II proposal including public consultation activities, with the term 'Prüm Next Generation' being dropped. An online public consultation designated as 'inception impact assessment' was launched by the Commission for 8 weeks between August and October 2020; in early 2021, a de facto online questionnaire was set up online for 12 weeks, and a series of technical workshops took place between March and May 2021.[20] The Commission's proposal of Prüm II was adopted in December 2021, and the Council adopted the general approach in June 2022.[21] Additionally, on their own initiative, the European Data Protection Supervisor (EDPS) released two opinions,[22] European Digital Rights (EDRi) issued two position papers[23] and the European Economic and Social Committee published its opinion.[24] In the European Parliament, the Committee on Budgets which had been designated to give an opinion, opted for not giving one.[25] In May 2023, the LIBE Committee adopted its report[26] and in June 2023, the European Parliament entered into the interinstitutional trilogue negotiations. In February 2024, an agreement was reached and the Prum II Regulation was adopted on 13 March 2024.

The Regulation introduces profound changes compared to its precursor. The scope of personal data exchanged includes facial images and police record index numbers of suspects and convicted persons, in case Member States opt in to share the data.[27] When permitted by national law, Member States could also exchange data for the search of missing persons, identification of unidentified human remains, and for humanitarian purposes.[28] The follow-up procedure to a data match needs to be happening within a deadline of 48 hours, with the exception when national judicial authorisation requires

[20] Proposal COM(2021) 206 final for a Regulation of the European Parliament and of the Council of 21 April 2021 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts.

[21] Proposal COM(2021) 784 final (n 17).

[22] European Data Protection Supervisor, Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation (Prüm II); Opinion 5/2022 on the Proposal for a Directive on information exchange between law enforcement authorities of Member States.

[23] EDRI, 'EDRi Challenges Expansion of Police Surveillance via Prüm' (24 March 2021), at edri.org; EDRI (n 4); EDRI, 'Automated Data Exchange in Prüm II: The EU's Securitisation Mindset Keeps Encroaching on our Fundamental Rights' (6 February 2024), at edri.org.

[24] European Economic and Social Committee, *Opinion on Security Union package/Schengen package* (19 May 2022), at www.eesc.europa.eu.

[25] European Parliament, *Legislative Observatory 2024*, at oeil.secure.europarl.europa.eu.

[26] European Parliament, 'REPORT on the Proposal for a Regulation of the European Parliament and of the Council on Automated Data Exchange for Police Cooperation ("Prüm II"), Amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council' (2023); European Parliament Press Release, 'Police co-operation: MEPs Adopt Law on more Efficient Data Exchanges' (8 February 2024), at www.europarl.europa.eu; European Parliament, Legislative Observatory 2024, at oeil.secure.europarl.europa.eu.

[27] Prüm II Regulation (n 3) Art 1.

[28] *Ibid*. Art 2.

a longer time period.[29] The solutions found suggest that Member States may adopt and progress within a range of expansive versus restrictive data exchange possibilities impacting on the type of data exchange, the purposes of data exchanges as well as the conditions to attend to substantive measures of validation procedures.

In the next section we analyse the diverse expert, stakeholder and public consultation activities, which accompanied the legislative process to illustrate how processes and possibilities to raise critical issues and diverse viewpoints were designed.

3. Stakeholders' consultation

As noted by several scholars, open consultations should be designed to elicit the interests, preferences, and pursued policy norms of key stakeholders in the security field, viewed as legitimate and bias-reducing, leading to successful policy outcomes.[30] On the surface, public consultations aim to foster the inclusion of citizens' and civil societies' stakeholders feedback. Binderkrantz et al. have pointed to the common use of public consultations as means of governance processes of the European Commission.[31] They differentiate between three types of instruments used for public consultations of the EU Commission that vary with regards to their openness and access for diverse stakeholders and their ability to facilitate enduring interactions: open online consultations, stakeholder conferences, expert groups.

We find these instruments in the preparation for the Prüm II revision. As mentioned earlier, the Commission organized consultation activities to mobilize experts and invited different stakeholders in two phases. In the first phase, the Commission along with the Council of the EU held expert groups focus group meetings focussing on stakeholders they classified as 'current and potential new end-users or other directly related stakeholders of the Prüm framework', e.g. Member States' authorities, EU agencies, EU institutions.[32] In an early version of a published 'consultation strategy' additional approaches are listed as 'consultation activities' that include the research methodologies used for the additionally commissioned feasibility study carried out by Deloitte.[33] The ambiguous use of the label 'consultation activities' to

[29] *Ibid*. Art 47.

[30] T Baird, 'Who Speaks for the European Border Security Industry? A Network Analysis' (2017) 26 *European Security* 37; A Bunea and R Thomson, 'Consultations with Interest Groups and the Empowerment of Executives: Evidence from the European Union' (2015) 28 *Governance: An International Journal of Policy Administration and Institutions* 517; A Bunea, 'Designing Stakeholder Consultations: Reinforcing or Alleviating Bias in the European Union System of Governance?' (2016) 56 *European Journal of Political Research* 46.

[31] AS Binderkrantz, A S Blom-Hansen and R Senninger (n 12).

[32] Commission Staff Working Document Impact Assessment SWD(2021) 378 final Accompanying the proposal for a regulation of the European Parliament and of the Council on automated exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council.

[33] *Ibid*.

refer to the nature of these processes becomes visible when this early phase ex-post became renamed as processes which 'have contributed to establishing a sound knowledge about the benefits and shortcomings of the existing Prüm framework' and was included into the Annex 2: Stakeholder consultation of the Impact Assessment Report accompanying the Prüm II proposal.[34]

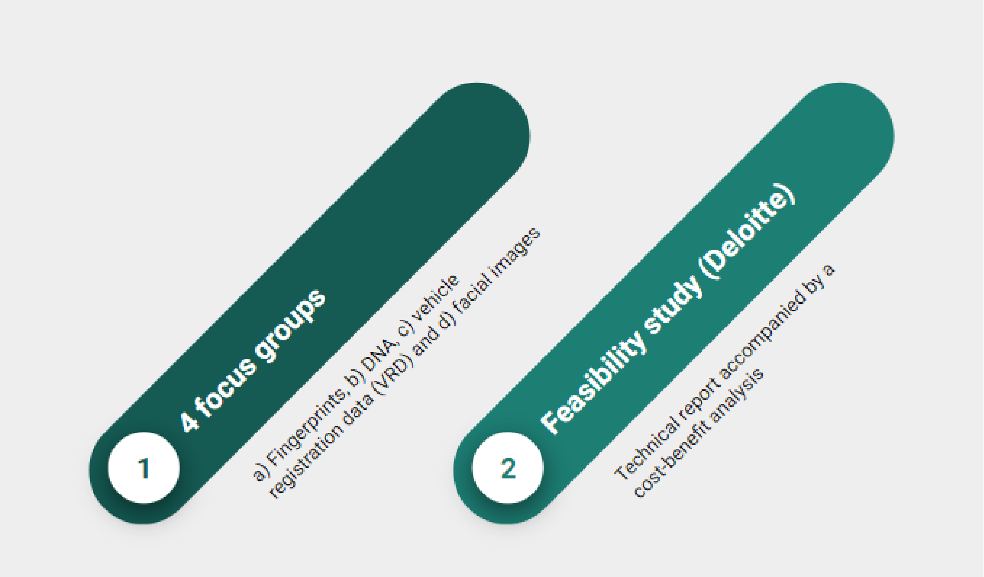

1
4 focus groups
a) Fingerprints, b) DNA, c) vehicle registration data (VRD) and d) facial images
2
Feasibility study (Deloitte)
Technical report accompanied by a cost-benefit analysis

Figure 2: 'Consultation activities' between 2018 to-early 2020 (Authors' compilation).

In the second phase, the Commission aimed at conducting more structured consultation processes, including selected NGOs, networks and the wider public. The pandemic was used as a justification of different methodologies rather than the organization of in person meetings; in effect, 'the consultation activities focus on alternatives such as online surveys, semi-structured phone interviews, as well as meetings via video conference'.[35] The Commission, as the main driving force and designer of these processes, decided on the formats, the participants, and the agenda of these consultations. Thereby, it defined what expertise and concerns could become included as relevant, as well as which issues would be opened up for more public consultation, and which ones might be reserved for deliberation among expert groups.

[34] Council of Europe, 'Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a regulation of the European Parliament and of the Council on automated data exchange for police cooperation ('Prüm II'), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council' (2021) 14204/21.

[35] European Commission, 'Consultation Strategy for the Initiative on Strengthening the Automated Data Exchange under the Prüm Framework' ec.europa.eu 4.

In the course of the consultation activities specific framings of the policy and technical problems at stake and solutions to deal with them were established and manifested, reflecting security industry driven language and rationalities. The feasibility study serves as an excellent example in this respect. Listing a consulting service of a private consulting agency as a 'consultation' clearly demonstrates the bias leaning towards private consultation instead of public ones. The feasibility study was outsourced to Deloitte, which provides audit, consulting and financial and risk advisory services. The major changes proposed by the private firm were: *a)* improving the automated data exchange through the inclusion of missing persons and the identification of deceased persons); *b)* improving the follow-up procedure to a hit called 'step-2' procedure, which regulates what obligatory personal 'core data' is exchanged; *c)* introducing new data categories including facial images, driving licences and biographic data; *d)* introducing a new IT architecture by implementing a new central route, which implied to move from a decentralized data exchange system to a centralized data exchange system; and *e)* exploring the possibility to link Prüm to the EU large-scale IT systems and embedding interoperability solutions, which was entailed the involvement of Europol, Interpol and other third countries.

This outsourced consulting service shows an understanding of reforming Prüm as a business case which was assessed with a framing of a cost-benefit analysis, rather than an emphasis on the possible challenges for fundamental rights. This is also evidenced from the fact that the Commission preferred the conduct of a feasibility study instead of an impact assessment. This does not mean that business actors drive policy development, since the powers of agenda-setting and legislative decision-making still rest with Member States and the EU institutions. However, as suggested by many scholars researching on EU security policy making, industry gains political legitimacy through strategic communication of its preferences and interests in order to co-construct policy norms alongside EU institutions.[36] As noted by Baird, this raises the question of 'how to address alternative frames in the debate on EU border security, frames which bring into account alternative world views and interpretations of social contexts that move beyond the categories, logics, and practices of business actors'.[37]

[36] T Baird (n 30); AW Chalmers, 'Getting a Seat at the Table: Capital, Capture and Expert Groups in the European Union' (2014) 37 *West European Politics* 976; D Coen, 'Empirical and Theoretical Studies in EU Lobbying' (2007) 14 *Journal of European Public Policy* 333; D Lowery, FR Baumgartner, J Berkhout, JM Berry, D Halpin, M Hojnacki, H Kluver, B Kohler-Koch, J Richardson, and KL Schlozman, 'Images of an Unbiased Interest System' (2015) 22 *Journal of European Public Policy* 1212; S Roura, 'The Role of the Private Sector in EU Internal Security' (High-Level Conference on a Renewed EU Internal Security Strategy Speech to Be Released 2014).

[37] T Baird (n 30).

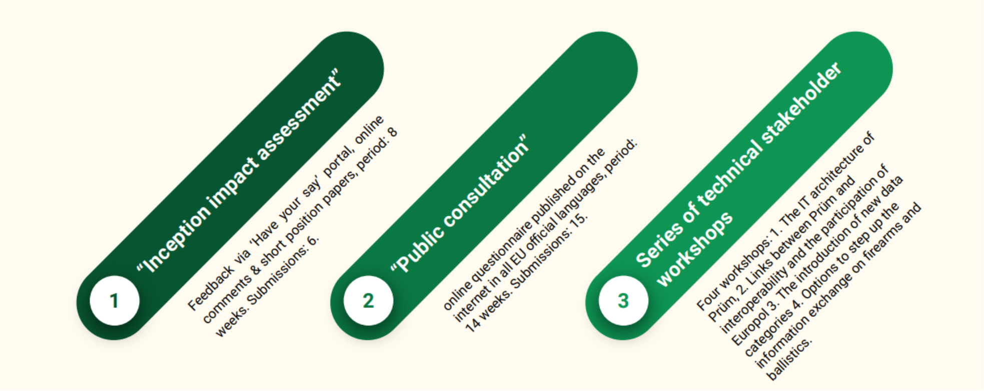

1
"Inception impact assessment"
Feedback via 'Have your say' portal, online comments & short position papers, period: 8 weeks. Submissions: 6.
2
"Public consultation"
online questionnaire published on the internet in all EU official languages, period: 14 weeks. Submissions: 15.
3
Series of technical stakeholder workshops
Four workshops: 1. The IT architecture of Prüm, 2. Links between Prüm and interoperability and the participation of Europol 3. The introduction of new data categories 4. Options to step up the information exchange on firearms and ballistics.

Figure 3: 'Consultation activities' between August 2020 and May 2021 (Authors' compilation)

In explaining the attributed roles to participating actors invited as 'concerned stakeholders' the Prüm II proposal states: 'The preparation of this proposal involved targeted consultations of concerned stakeholders, including end-users of the system, namely Member States' authorities using the Prüm automated data exchange ranging from law enforcement and judicial authorities, national vehicle registration authorities, to national database custodians and forensic laboratories. Europol and eu-LISA were also consulted in view of their respective expertise and their potential role in the new Prüm framework'.[38]

Other stakeholders were the European Union Agency for Fundamental Rights (FRA), the non-governmental organization European Digital Rights (EDRi) and Eucaris (European car and driving licence information systems).

The 'inception impact assessment' launched by the European Commission, published on 11 August 2020, serving to inform stakeholders and citizens about the initiative, and the 'public consultation' activities drew very limited number of responses.[39] In the Annex attached to the proposal, which documents these consultation activities, the reasons behind the limited number of responses were speculated 'due to the technical nature of the instrument'.[40] The policy issues at stake were scripted as of 'technical nature', an approach which stresses the necessity and legitimacy of relying on expert expertise. Taking the technicality of the issue at stake as a given also easily serves as a reasonable explanation for not investing in providing wider public access, information and education or further public consultations.

[38] European Commission, Strengthening the Automated Data Exchange under the Prüm Framework, Have your Say - Public Consultation and Feedback, at ec.europa.eu; European Commission, 'Combined Evaluation Roadmap/Inception Impact Assessment' (2021), at ec.europa.eu.

[39] *Ibid.*; Six for the inception impact assessment, and 15 for the public consultation, with the large majority of them provided by public authorities in the field of security and law enforcement.

[40] Council of Europe (n 34).

Citizens and stakeholders were invited to provide their views on foresight scenarios and policy options to ‘successfully prevent and investigate serious crimes’. The likely social impacts were described as follows: ‘Improved information exchange between European law enforcement authorities leads to a greater number of successful investigations and convicted criminals, and will consequently lead to a safer society’.[41] With regard to the impact on fundamental rights, first, there was a reference to the expansion of new categories of data, which were anyway ‘already collected’.[42] Second, the impact on fundamental rights was in fact depicted solely in a positive manner, suggesting that Prüm II will enhance data security and privacy protection. In this regard, it was stated:

> ‘…one of the aims of this initiative is to update and strengthen the Prüm framework in the light of the new European data protection regime, especially the Law Enforcement Directive. Improving the efficiency of the Prüm framework, and improving the security of the system by modernising the technical requirements, will lead to improved possibilities for the identification of criminals and more efficient criminal investigations that will contribute to the security of the society’.[43]

Any potential challenges to fundamental rights, for example along the alternative positions expressed by Vavoula and EDRi, raising concerns that fundamental rights are increasingly threatened by the way data is made available and increasingly exchanged, for instance with stakeholders, such as Europol did not feature.[44]

While critical voices have been raised beyond those fora of ‘invited’ consultations, they hardly find their way into any of the assessment reports and considerations of the Prüm II proposal. Even in the limited cases where they are mentioned,[45] there is no meaningful engagement with the critical issues they raise. Such issues are for example the lack of common shared technical standards about matching rules that lead to hits and follow up validation procedures. Fingerprint comparisons conducted on the basis of as few as six or seven loci are susceptible to false positives and consequently require subsequent validation procedures to definitively exclude such outcomes. Another issue is the lack of meaningful statistical data compiled from the Prüm system to provide evidence for its efficiency and effectiveness. Thus, ‘uninvited’ participation becomes marginalized and certain forms of contestations can get protracted and silenced. Even when ‘invited’, critical voices are also sidelined to give way to the positive effects.

[41] *Ibid.*

[42] *Ibid.*

[43] *Ibid.*

[44] N Vavoula (n 10); EDRI (n 23); EDRI (n 4); EDRI (n 23).

[45] V Toom, ‘Cross-border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision’ (Study for the LIBE Committee 2018), at www.europarl.europa.eu.

In sum, the public consultations were non-inclusive and provided a space for shaping the views of the Commission, through the rhetoric of 'openness' to policy learning opportunities, using direct channels of communication.[46] De facto, they functioned as means to diffuse critique or resistance while reinforcing power asymmetries and hegemonic discourses about fighting criminality. These public consultations performed what Laurent has called 'technologies of democracy'.[47]

The relevance of including diverse views may be best illustrated along issues that remain highly contested, and yet have gained little visibility along the organized consultation processes. The following section portrays two examples of matters of concern which have been marginalized by how the consultations were organized and whose voices get heard throughout these processes. These examples concern two reforms with significant ethical and fundamental rights concerns, namely integrating the Prüm system into the interoperability architecture, making diverse database systems – these of migration control and of law enforcement – interoperable, and second, integrating new types of biometric data such as facial images. Both areas raise substantial ethical and regulatory issues according to the critical views of diverse stakeholders, and have not yet sufficiently found recognition in the governance process towards Prüm II and the legal provisions outlined in the draft regulation.

4. Reforming the Prüm system: matters of concern and underexplored substantial challenges they raise

4.1. In the name of 'interoperability': unsettling data sovereignty of Member States and bringing together centralized with decentralized systems of information exchange

At the heart of the transformation of Prüm is its refurbishment from a decentralized system of information exchange to a partially centralized one. The logic of centralized database infrastructures can be found in other existing systems, such as the Visa Information System (VIS) and the Schengen Information System (SIS), set up in the AFSJ (Area of Freedom, Security and Justice) for immigration control, that process personal data primarily of third-country nationals. Centralized databases aggregate personal data collected by Member States' authorities into one repository and at EU level have been typically created in the context of asylum, migration and border management.[48] Europol databases store data from multiple sources, including other Agencies and private parties. In turn, in the field of law police cooperation in crimi-

[46] T Baird (n 30).

[47] B Laurent (n 14).

[48] V Mitsilegas and N Vavoula, 'Databases' in V Mitsilegas (ed), *EU Criminal Law* (2nd edition, Hart 2022).

nal matters, emphasis has been placed on decentralized avenues of cross-border information exchange of Prüm as the rationale has been to make Member States' law enforcement data from (mostly pre-existing) national databases available across Member States.[49] Because of its decentralized data exchange and cross-jurisdictional nature, the Prüm system represents an information exchange tool that exemplified Member States' sovereignty, autonomy and ownership of data governance.[50] The emphasis on decentralized systems is also shaped by the diversity of national legislations, the multitude of practices related to the operation and maintenance of domestic law enforcement databases, as well as the heterogeneous functioning of criminal justice systems and policing practices across EU Member States.

Prüm's decentralized structure has kept data as the 'property' of the Member State where they are collected.[51] The Prüm system contains large amounts of biographical information, as well as biometric – thus sensitive – data of mostly EU citizens, referring to national databases with mostly data of EU nationals. The attempt to introduce more centralizing components comes with the introduction of a central router.

The creation of a central router is presented as a 'hybrid approach between a decentralized and centralized solution without any data storage at central level'.[52] All national databases in each Member State shall connect to the central router instead of connecting to one another.[53] Via the newly installed central router, the Prüm data exchange will be connected to the backbone that holds together the whole interoperability architecture of the meta-database system, the Common Identity Repository (CIR).[54] The CIR contains individual files created for each person that is registered in one or many of the other existing databases. These files are established for the purpose of facilitating the correct identification of persons registered across different databases. The EU Agency responsible for the management of large-scale IT Systems (eu-LISA) is entrusted with the task of developing the central router, as

[49] *Ibid.*

[50] N Amelung, R Granja, H Machado (n 9).

[51] This does not mean that the in centralized systems the Member States storing the data do not have any ownership.

[52] Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council cit. 4.

[53] Art 35 of the Prüm II Regulation.

[54] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA; Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, Arts 17–21.

it is the hosting and facilitating entity for the interoperability project. The CIR initially aimed at centrally storing basic biographic and biometric information of third-country nationals from VIS, Eurodac, the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Record Information System for Third-country Nationals (ECRIS-TCN) which then is available for search and comparison by the authorities and agencies that are granted access to the system. The inclusion of Prüm entails including data not only from third-country nationals, but from EU citizens who fall under the categories relevant for exchange. The paradigm shift of distributing powers to coordinate data exchange to EU agencies such as the EU agency for Large Scale IT Systems (eu-LISA) in more centralized manners is significant in terms of sharing data sovereignty of Member States.

Interoperability is a term that originates from computer science and constitutes the response to users' needs for shared access across multiple autonomous databases developed and operated in silos. In EU terms, this means that separate, EU-wide IT systems should become interconnected.[55] Interoperability reinforces the political intentions behind the development of the Prüm system to harmonize and minimize the divergence of Member States' situations. In that respect, the Prüm II proposal states that based on previous evaluations of the Prüm system not all Member States have sufficiently implemented the Prüm Decisions, and that differences in national rules and procedures caused delays and inefficiencies in the information exchange and thus hindering law enforcement measures to identify criminals.[56]

Overall, considering that almost all the large-scale IT systems to which Prüm is interconnected process biometric data, namely dactyloscopic data and facial images, the revised regime aims at the mass exchange of biometric data at the borders and beyond. This in line with attempts to expand biometric data exchange and establish 'borderlessness' for data flows and to overcome the logics of nation state boundaries as part of data governance. The aim of interoperability is to diminish technical, scientific, operational and legal obstacles, resulting in increasingly permeable bio-borders.[57]

This seemingly technical change – imagined as possible to be separated from political dimensions – of IT architecture towards interoperability had been a potential scenario since the beginning, as Vavoula outlined.[58] The EDPS raised this point

[55] R Bellanova and G Glouftsios, 'Formatting European Security Integration through Database Interoperability' (2022) 31 *European Security* 454, 455.

[56] Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council cit. 5.

[57] N Amelung, and H Machado (n 9) 396.

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

clearly: The EDPS is convinced that interoperability should be viewed first and foremost as a policy choice, not as a technological solution, due to its far-reaching legal and societal consequences. [...] However, the EU legal framework must ensure that any limitations to the fundamental rights of all affected individuals apply only in so far as is strictly necessary'.[59]

The political dimension of these paradigm changes in the case of Prüm is a shift towards vertical integration and re-negotiation of data sovereignty. The centralization and integration of Prüm into a wider set of centralized IT systems clearly shifts the data sovereignty of Member States which had been a core principle in the data management of law enforcement authorities in the AFSJ. While also in centralized systems Member States have national rules and responsibilities to which the use of data exchange needs to correspond to, the bottom up approach building on national databases of the Prüm system so far allowed for a wider range of sovereign procedures which includes for instance different standards of validation processes, also taking different timings for that into consideration.[60] As the shared Biometric Matching Service (sBMS), another interoperability component, will store fingerprints and facial images, it is here where the EDPS reminds of the multi-layered context of performing biometric data collection and analysis. The EDPS exemplifies the problematic consequences of diverse origins of biometric data collection for different purposes for the case of facial images:

> 'Furthermore, the EDPS draws the attention to the fact that facial images from the national databases, subject to automated searches in the context of Prüm, may differ from the ones stored in the EU large scale IT systems (e.g. VIS, EES) in terms of format and quality. In this regard, there are questions about the performance of the biometric matching algorithm of sBMS when matching facial images of data of suspects captured under different conditions, e.g. by a security camera, with facial images taken in a controlled environment, e.g. in a booth during visa procedure. Appropriate measures should be developed and implemented to address the risks stemming from low performance of matching algorithms'.[61]

The paradigm shift disguising a political transformation as a technology and innovation oriented takes place by also subscribing to the vision of 'digital transformation' which Trautmansdorff and Felt identified already in the context of the interoperability initiative as the driving mission for eu-LISA's attempt to harmonize and incorporate various forms of identity management.[62] The latter demonstrates the dominant role of IT experts in the transformation towards interoperability of both

[59] European Data Protection Supervisor, Opinion 4/2018 of 16 April 2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 15.

[60] *Ibid.*

[61] *Ibid.*

[62] P Trauttmansdorff and U Felt, 'Between Infrastructural Experimentation and Collective Imagination: The Digital Transformation of the EU Border Regime' (2023) 48 *Science, Technology & Human Values* 635.

decentralized and centralized systems which contribute to narratives that frame the project rather as a mere technical and less political matter. The vision of 'digital transformation' together with specific technical solutions such as the router also get mainstreamed across different data exchange systems. The regulatory reform of the Advance Passenger Information (API) system also foresees the introduction of a central router coordinated by eu-LISA to introduce centralizing components on a previously existing system which imposes on air carriers to transmit API data prior to flights' take off. Similarly, the new layer to Prüm is the digital aspect of linking decentralized databases into the interoperability project via the central router and the link to the CIR allowing to verify and cross-validate identity records across various databases. The latter moves identity management into a new and still unknown digital space which lives from its promise to be assumed to be reliable.[63] This change facilitates the delegation and relies on accumulated powers of IT expertise.

The additional 'formatting' of the system to be ready for interoperability implies the inclusion of additional biometric data such as facial images, and the widened access for additional actors of law enforcement, in particular by Europol.[64] Furthermore, it is the integration across different databases at the intersection of migration and law enforcement and streamlining processes, such as speeding up the follow up processes to a hit which then includes the exchange of personal data via law enforcement agencies (the so-called 'step 2 process') in stricter defined short timelines. The data transactions measured along the central router then will be reported and transformed into technical statistics of the system intended to be published by eu-LISA in the future. Here, the EDPS pointed to the relevance to go beyond pure technical statistics and turn such a tool into meaningful statistics to prove the efficiency and efficacy of the Prüm system for its defined purposes: 'The EDPS believes that reporting on the accuracy of hits by the requesting Member State / Europol, would be highly valuable to measure the effectiveness of Prüm, particularly where it concerns matches of biometric data, such as facial images. Therefore, he recommends including explicitly this element in the statistics'.[65]

Concerns have also rightly been raised that once there is a central router together with the 72 hours period to share personal core data (step two process) in place that there are no sufficient safeguards for accuracy and veracity in place to prevent false positives which immediately impact on risks for privacy.[66] Finally, Europol access has also been contested on two grounds; its lack of necessity – notably there has not been a single explanation as to why Europol should have access to that data and

[63] L Leese, 'Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU' (2022) 27 *Geopolitics* 113.

[64] R Bellanova and G Glouftsios (n 55) 456.

[65] EDPS Opinion 4/2022 (n 22) 16.

[66] EDRI (n 4) 25.

concerns abou the lack of robust safeguards in place to prevent data reaching third countries via their cooperation with Europol.[67]

4.2. Matters of inclusion of new biometric data: facial images

The second reform of interest relates to the introduction of new data categories for exchange across EU Member States, such as the addition of searches for missing people and unidentified remains and new types of data, in particular facial images and police records. The implicit assumption in the Prüm system is that the more data are exchanged, the more useful they are.[68] The 'profoundly ideological role of beliefs in the power of data' is materialised by the fact that data matter more than ever, through their gathering, further processing and sharing, in the control of crime of borders, and migration.[69] For the purpose of this article, in this section we focus on a particular aspect of expansion of categories of sensitive data, the addition of facial images, understood at the visual representations of a person's face captured through photographs or video frames.

The Prüm II Regulation foresees in Arts 22(2) and 24 the introduction of automatic search of facial images: The requesting Member State automatically receives a list of matches concerning likely candidates. One matter of concern involves the possibility of using facial recognition technologies that utilize algorithms and computer vision to analyse and identify unique facial features within these images[70] Facial Recognition Technologies (FRTs) can be applied on videos (e.g. CCTV) or photographs to authenticate or to identify a person, and may be used for various purposes, including to search for persons in police watch lists or to monitor a person's movements in the public space.

This concern is more than rhetorical or hypothetical. As of December 2020, the TELEFI project, funded by Internal Security Fund – Police of the Commission, has found that facial recognition for law enforcement purposes has been implemented in several EU Members and beyond.[71] A typical use case of facial recognition by law

[67] *Ibid.*

[68] H Machado and R Granja, (n 9) 212.

[69] J Van Dijck 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology' (2014) 12 *Surveillance & Society* 197, 201; G Glouftsios and S Scheel, 'An Inquiry into the Digitisation of Border and Migration Management: Performativity, Contestation and Heterogeneous Engineering' (2021) 42 *Third World Quarterly* 123; L Leese (n 63).

[70] FRTs use digital images of faces (i.e. a person's face that is captured using a device such as a camera or a scanner). The image is then stored in a database, and can be processed and analysed using computer algorithms.

[71] According to the TELEFI study, facial recognition technologies were already implemented in eleven EU Member States (Austria, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, The Netherlands and Slovenia), in the UK and by Europol and Interpol. Seven Member States (Croatia, Cyprus, Czech Republic, Estonia, Romania, Spain and Sweden) have reached the stage of preparing for implementation and expect to start using the technology within one to two years. Nine EU Member States (Belgium, Bulgaria, Denmark, Ireland, Luxembourg, Malta, Poland, Portugal and

enforcement authorities in the Member States, in the United Kingdom (UK), or by Europol and Interpol is to use it as a retrospective tool during an investigation, where the facial image associated with a criminal event is examined after the crime has been committed. The facial image of interest is searched against a database that contains known individuals with an aim to identify the 'unknown' person within the image. The search result is a list of suspect candidates. No EU Member State has implemented live facial recognition for routine use, but it is routinely used in the UK.

While calls to ban facial recognition are proliferating at European level,[72] the technology has been speedily rolled out at EU's borders and is seen as an essential tool of policing.[73] In sum, despite huge controversies raised by FRTs there is a large global scale use of them.

Non-governmental organisations critically engaging with the development of surveillance technologies and expansion of police databases have reported ethical and social concerns with facial recognition, considered to be highly intrusive and human rights violating. Euroactive, Statewatch, EDRi and other civil society organizations have called on the European Commission, the European Parliament, and Member States to ensure that facial recognition technologies are comprehensively banned in both law and practice throughout the EU.[74] The problematic plans on the table to exchange facial images within the Prüm system raise serious concerns that Prüm II could therefore facilitate automated exchange of sensitive data without putting in place adequate safeguards to ensure that this cannot be done spuriously, arbitrarily or for politically-motivated reasons. During the consultation phase, EDRi strongly opposed the plans for extension of the Prüm framework with facial images in Member States' criminal investigation databases. EDRi urged for a democratic debate on facial recognition and for refraining to impose the roll out of facial recognition in policing through the Prüm framework potentially leading to 'biometric mass surveillance'.[75]

Scholars alert that with the evolution of Artificial Intelligence (AI), particularly with the development of machine-learning algorithms, there has been significant progress in the field of image recognition that expands the potential for unscrupulous

Slovakia) did not present solid plans for implementation; TELEFI, 'Summary Report of the Project "Towards the European Level Exchange of Facial Images"' (2020), at www.telefi-project.eu.

[72] The EU Artificial Intelligence Act, unveiled in April 2021, has reached a provisional agreement between the European Parliament and the Council in 8 December 2023, after months of intensive trilogue negotiations. In the AI Act, one banned AI application is untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases. Recognising the potential threat to citizens' rights and democracy posed by certain applications of AI, the co-legislators agreed to prohibit its use but agreed on 'law enforcement exceptions'.

[73] C Aradau and T Blanke, 'Algorithmic Reason: The New Government of Self and Other' (Oxford University Press 2022) 160; L Urquhart and D Miranda, 'Policing Faces: The Present and Future of Intelligent Facial Surveillance' (2022) 31 *Information & Communications Technology Law* 194.

[74] EDRI (n 4); M Monroy, 'Facial Recognition and Police Records: European Biometric Systems to be Expanded' (27 January 2022), at digit.site36.net.

[75] EDRI (n 23) 4.

use of this technology.[76] The use of facial images in Prüm II might enable large-scale data processing, and it also opens new paths for racial bias and other discriminatory outcomes in sensitive contexts such as security, border control, or asylum management or enabling very problematic uses such as predicting how likely it is for an individual to commit a future crime.[77]

In the context of AI, the European Parliament has already warned about the risks arising from law enforcement uses of facial recognition, calling to prohibit uses which would constitute biometric mass surveillance (EPRS, 2021). Commission's AI Act prohibited real-time facial recognition in publicly accessible spaces, while permitting narrowly defined exemptions for law enforcement to search for missing children, dangerous criminals, or suspected terrorists.[78]

FRTs are also considered as inducing the risk of discrimination and false results. As one of the most deployed AI applications, the errors of facial recognition appear frequently in public debates. According to a report by the civil liberties organization Big Brother Watch in the UK, facial recognition systems used by the police were wrong nine times out of ten. Errors in facial recognition are systematic rather than accidental, revealing underlying patterns of bias and discrimination (Matzner, 2018: 41). Algorithms can 'automate' racial and class relations, presenting them as natural and objective (Buolamwini and Gebru, 2018).[79]

Vavoula stressed the challenges to the protection to private life and protection of personal data, the potential for discrimination and profiling against certain groups of people, the risks of false positive matches due to problems with data quality and accuracy of the technology, concluding that:

> 'If this option goes forward, the sources of facial images require clarity and data protection safeguards must be embedded so that the quality of facial images is high enough to

[76] C Bueno, 'The Face Revisited: Using Deleuze and Guattari to Explore the Politics of Algorithmic Face Recognition' (2020) 37 *Theory, Culture & Society* 73.

[77] L Introna and D Wood, 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems' (2004) 2 *Surveillance & Society* 177; S Kloppenburg and IVD Ploeg, 'Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences' (2020) 29 *Science as Culture* 57; J Angwin, J Larson, S Mattu, 'Machine Bias: There's Software used Across the Country to Predict Future Criminals. And it's Biased Against Blacks' (2016) *ProPublica.Org*.

[78] Final Regulation (EU) 2024/1689, adopted in March–May 2024 (with entry into force July 2024 and full applicability by dates up to August 2026). Under Art 5(1)(d) of Regulation (EU) 2024/1689 (the Artificial Intelligence Act, in force 1 August 2024), 'real-time' remote biometric identification systems (e.g. live facial recognition) in publicly accessible spaces are generally prohibited when used for law enforcement purposes; exceptions may be authorized *only* in specific, serious circumstances—namely, the targeted search for missing persons (including children), prevention of an imminent terrorist threat, or identification and prosecution of serious criminals—only after appropriate court or administrative authorization at national level.

[79] J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (FAT* 2018), *Proceedings of Machine Learning Research* 81, pp 77–91.

> prevent the risk of increased false matches, which may lead to discriminatory practices. The specific purposes for searching facial images should also be circumscribed so as to prevent wide-ranging surveillance practices at the national level. Separation of images on the basis of their sources and their quality (mug-shots v probe images) should be considered as well'.[80]

The European Data Protection Board (EDPB) also alerted on the use of facial recognition technology in the areas of law enforcement to the necessity to consider carefully the challenges of reliability and efficiency of facial recognition, as well as the overall issue of quality and accuracy of data sources, since they entail particular significant or serious risks for data subjects concerned in the area of law enforcement.[81] The EDPB's pronouncement illustrates how public concerns with 'errors' and lack of quality of data sets used to training algorithms have been enacted in regards to controversies of facial recognition in the following statement:

> 'the EDPB considers it important to recall that FRT [i.e. facial recognition technologies]. facial recognition technologies, the authors], whether used for the purposes of authentication or identification, do not provide for a definitive result but rely on probabilities that two faces, or images of faces, correspond to the same person. [...] Numerous studies have also highlighted that such statistical results from algorithmic processing may also be subject to bias, notably resulting from the source data quality as well as training databases, or other factors, like the choice of location of the deployment'.[82]

From the perspective of developers of facial recognition, the controversies triggered so far have been the result of a mere lack of technical accuracy and hence these errors can and must be solved by employing better training data sets for machine learning.[83] As noted by Bueno, from this perspective, a properly trained algorithm accompanied by adequate technical solutions is presented by AI developers as 'less racist than human-to-human interactions', therefore obliterating historical systemic racism and social logics of power and discrimination.[84]

In the same line of reasoning, Aradau and Blanke propose to unpack the emergence of 'accountability by error' in global scenes of controversy around facial recognition and their respective 'politics of optimization and trust'.[85] In their view, accountability has been enacted triggered through error detection when different publics have encountered algorithmic malfunctions, misrecognitions, failures, or

[80] Vavoula (n 10) 51.

[81] European Data Protection Board (EDPB), Guidelines 05/2022 of 12 May 2022 on the use of facial recognition technology in the area of law enforcement 14.

[82] *Ibid.*

[83] F Pasquale, 'The Algorithmic Self' (2015) 17 *The Hedgehog Review* 14.

[84] Bueno (n 76) 75.

[85] Aradau and Blanke (n 73) 166–171.

other fallibilities: 'These forms of accountability through error enact algorithmic systems as fallible but ultimately correctable and therefore always desirable. Errors become temporary malfunctions, while the future of algorithms is that of indefinite optimization'.[86] In this context, to have 'better' facial recognition technologies ('better algorithms') might mean to assemble larger and larger data to optimise algorithms, and in this way logics of power are obfuscated and extensive surveillance is normalized.

5. Conclusions

This article focussed on selected components of the policy process leading from Prüm to Prüm II. We emphasized on the preparatory process between 2018 to 2021 which included different consultation activities led by the Commission, and then selected two areas which are subject of contestation to discuss some characteristics and limitations of the process of regulating the follow-up process which expands, modifies and reformats the Prüm system.

The political rationale of public consultation activities set up by the European Commission to reform the Prüm system aimed to provide a regulation in line with fundamental rights and dedicated to the public good of security of EU citizens. However, it was done through particular framings of the procedural democratic (consultations) and technical (technology assessment) steps. We argue that the process suffers from various limitations. It is driven by a monopoly of actors who are involved in the governance of possible futures of the Prüm system which consists of regulators, specific EU agencies such as Europol and eu-LISA which had themselves interests in magnifying their powers, law enforcement authorities, and selected Member States. The hegemonic governance that creates and manifests Prüm builds on specific ascribed meanings of security and underpinning assumptions of security governance, configures what is conceived as risks and threats, who is assumed in need to become protected and by what means, and whose voices and expertise are considered and whose are silenced in the decision making of governing this continuously emerging technological system. Thereby power asymmetries between actors drive the settings for consulting activities, but are also confirmed and manifested by them.

By focussing on the orchestrated policy deliberations and public consultations in the context of the Prüm II preparations this article improves the understanding of why certain governance arrangements claiming to be participatory fail to satisfy institutions and concerned publics.[87] With such staged and orchestrated forms of consultation, opportunities for alternative anticipatory practices — such as predictions,

[86] Ibid. 171.

[87] M Hajer, 'Setting the Stage: A Dramaturgy of Policy Deliberation' (2005) 36 *Administration & Society* 624; M Hajer, 'Rebuilding Ground Zero. The Politics of Performance' (2005b) *Planning Theory & Practice*, 6:4, 445.

forecasts, and scenarios informed by 'ecologies of participation' (i.e., the dynamics of diverse, interrelating collectives and spaces of participation) — are often missed.[88] The still scarce attention paid to critical issues in the governance towards Prüm II provokes us to ask if there are possibilities for alternative governance forms which suggest being more attentive to ethical and democratic concerns. We suggest to continuing the exploration of the following questions: How can hegemonic security narratives be contested? How may alternative positionings, that are attentive to claims about additional or alternative ethical and human rights issues, be heard and incorporated into the governance of Prüm? What forms of anticipatory governance can and shall accompany incremental technology change policy process leading from Prüm to Prüm II?

With this article, we aim to contribute to scholarship which sensitizes readers to the finding that policy and engagement processes with the objective to arrive at decision making and political choices on security issues are political in themselves and need to be reconsidered and re-opened to define legitimate public problems and acceptable ways to deal with them. In order to be legitimate, they need to seriously consider the various articulations of reasonable public contestations.

[88] J Chilvers, H Pallett, T Hargreaves, 'Ecologies of Participation in Socio-Technical Change: The Case of Energy System Transitions' (2018) 42 *Energy Research & Social Science* 199.