A technological and legal investigation into how smart states deploy collective intelligence for security and surveillance purposes

Diana M. POPA,
Delft University of Technology, The Netherlands
d.m.popa@tudelft.nl

Abstract
The paper examines challenging cases for the balancing act between privacy and protection of individual rights on one side and protection of public and national security on the other. In doing so, the article refers to the main privacy protection legislation – the GDPR and specifically article 23, the AI ACT and its relevant exceptions, the LED, and newly proposed pieces of legislation aiming at giving more manoeuvre capabilities to law enforcement and intelligence agencies when it comes to conducting activities for the purpose of protecting the public and national security. The article debates the relation between data protection and public and national security in democratic states and shows how the evolving threat landscape influences both the practice and the legislative process around personal data protection and deployment of emerging technologies and use of collective intelligence for security purposes. The way this relationship is shaped in each (smart) state is influenced by political, technological factors as well as the specific threat landscape. The deployment of AI for surveillance of the public space, the way it is both regulated and contested are discussed, with practical cases such as the use of smart surveillance during the 2024 Paris Olimpic games being analized. When looking at surveillance technologies deployed in the public space, the article also articulates a new physical and digital intertwined dimension of the public space, making the argument that both within and outside the visible boundaries of constructed geography, there is digitally field space, either vertically or horizontally, that can represent a resilience enabler factor but can also become a threat if exclusively depended upon or if not secured against malicious interference.

Keywords: privacy, security, AI, surveillance, article 23, Smart State.

1. Introduction
In advanced rule of law democracies, sates have long faced the challenge of accommodating conflicting priorities. One such intensely debated conflict of values is the one between protection of fundamental rights and national security interests. The debate on national security versus protection of fundamental rights has had its firm supporters on both sides, as data protection becomes a test for democracies, both from the technical perspective and the perspective of the impact on fundamental rights and values. In accordance with the rule of law, states have to restrain themselves in regards with the large scale deployment of advanced technological solutions if these come at the expense of severe interference with the private sphere and privacy of the population. In the same time, the state also has the obligation of assuring the security of its population and of its territory, for which it can deploy technological advancements and state monopoly on violence. With the advancement of emerging technologies such as the AI, the debates around the lawful and ethical deployment of technology for the protection of state interests is more and more debated, due to the technologies complexity and black box effects, due to the fact that technological development precedes in speed legislative maturity and robustness and due to the possibility of open debates around conflicting values or value prioritization in democratic states occurs in a top-down or lateral manner. In many cases deployment of

public security enhancing technology came under public scrutiny post-factum (cases of predicting policing deployed in the US) but also ex-ante, such as the debates concerning the legislative project (at that time) of deploying intelligent surveillance in France on the occasion of the 2024 Olympic Games. In addition to the state controlled deployment of technology in the public space there is also a less structured invasion of the public space for smaller scale security purposes, that unfortunately is less visible in an overall perspective, namely that of individually owned and deployed technologies that can be used for surveillance or behaviour monitoring purposes and that are privacy intrusive but less visible to regulating and sanctioning authorities due to lack of oversight. These later cases are not the subject of this article, although their deployment could at the same time be a valuable source of aggregated information and an increased risk, especially considering the potential for data leakage due to (for example) system built-in backdoors. The article focuses on cases of technologies deployed by the government or for governmental purposes (i.e. public and national security), how these have been regulated so far and how new legislation is being adopted in order to answer the changing internal and external threat landscape.

2. Deploying legislation and technology in response to the threat landscape

The balancing act between the protection of individual (human) rights to which privacy belongs and public and national security that falls under the responsibility of the state is brought under constant scrutiny once new legislation is proposed or implemented or breaches of privacy come to the attention of the public. Lawyers and human rights advocates criticize what they see as that state prioritizing national security over protection of fundamental rights, claiming that fundamental values are sacrificed in the name of national security. As the right to security is also a fundamental right, defenders of its supremacy might also argue that this is a non-issue. However, the constant tug of war between security and privacy should be seen as a marker of a healthy democratic system where the public and civil society are both socially and politically active and digitally educated, with questions on how much we want or need to normalize general surveillance (given a certain risk level or risk profile of a certain country) being part of the debate. The debates are that more visible to the public in advanced rule of law countries, where there is burden sharing regarding protection of data. In this perspective data protection is a test for democracies, who need to maintain an increased security posture while preventing rule of law slippages. At global level as well, an increase in coordination of intelligence operations in pursuit of overarching goals has been reported especially following 9/11, with networks of public and private agencies sharing data at different scales [1]. As response to heightened risk environment, intelligence, law enforcement and defence agencies have consolidated and enhanced their defence posture, making some assert the weaponization of data for surveillance purposes. The advent of AI systems has exacerbated these concerns on the side of the civilian society. Researchers and advocates of fundamental human rights have expressed unease about potential top down AI misuse given its use in the law enforcement and national security areas, mostly streaming from surveillance activities. In their view, surveillance of the public space done in the name of short term safety leads to the dangers of a surveillance state or what researchers have called digital authoritarianism [2].

Both the Artificial Intelligence Act and the GDPR have exceptions in the areas of law enforcement, national security and defence. The adoption and implementation of the General Data Protection Regulation (GDPR) across the European Union reflects the values of the EU, having at its hart the protection of fundamental rights and freedoms. As such, the GDPR represents a high threshold in comparison with other data protection legislations around the globe, granting data subjects a high level of protection. Numerous arguments stand witness to this fact, from the activity of the courts, the numbers and levels of complaints, the number of professionals working in the privacy field in EU contexts, to more mediatized aspects, such as the intense debated Schrems cases and the time it took to negotiate the EU-US data framework agreement. The protection given by the regulation is granted to the data subjects in front of other individuals, companies and the state, when conducting a data processing activity. In the case of the data processing conducted by government organisations, the state has greater powers when it comes to conducting activities in line with national and public safety, therefore limiting the protection given to the data subjects, as reflected under article 23 of the GDPR. The GDPR stipulates in article 23 that rights may be restricted "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: national security; defence; public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security etc." Whenever surveillance technologies are being deployed in the public space, a necessity and proportionality test is conducted in balancing these factors. Lawyers and advocates of human rights see this as a risk within the EU law, given that governments can exploit these exceptions. It has been even argued that in the long term, the prioritization of national security can become a danger to national security itself, in the case when governments change to less democratic regimes where political repression is high and can make use of enhanced surveillance capabilities previously strengthen by practice and legislation [2]. However, one should not forget that laws, state interest and priorities have to be considered in a symbiotic dynamic relation, and just as the current law cannot be applied retroactively nor should it be applied anticipatory. As governments change, state interest changes and whether it is a positive or negative development it still represents the position of a sovereign state and the its laws have a time-stamp applicability. This is not to deny the need for healthy expert debate about how laws and jurisprudence develop in an organic manner, but rather to caution on the arguments used for the way legislation is being shaped and constructed. Noteworthy also is the fact that that while prioritization of national security vis-a-vis privacy and human rights is considerably different in geopolitical regions. If prioritization of national security appears normalized in the US, the EU narrative adheres to an initial balancing test between public and private interests, in relation with the principle of proportionality of article 52 of the EU Charter of Fundamental Rights. An additional challenge in the EU case is that areas of public and national security remain in the realm of member states control. Despite harmonizing legislation such as the GDPR and AI Act, the exceptions that fall under member state authority and the diverse digital, socio - political and security posture make for a diverse implementation landscape. An additional risk raised by lawyers and privacy professionals comes form the fact that AI systems deployed in the areas of law enforcement, intelligence and defence are exempted from being registered in the open national or EU level databases for high risk AI systems, and are included in sector

dedicated closed systems, which makes professional outside scrutiny challenging. This becomes a higher risk in less democratic states where oversight of high risk systems is only determined at national level.

The privacy – security relation has often been characterized as a tug of war in democratic societies who need to balance individual or private interests and rights with collective or public interests. This balancing act is reflected in the text of the GDPR and also comes into play when it intersects with other lex specialis that touch upon personal data, especially when it comes to the area of public and national safety and law enforcement. As a result of evolving threat landscape, increased complexity of technological and data deployment models, complex supply chains, and the concrete difficulties experienced in daily practices by different institutions when balancing public and individual interests, new legislation is being proposed and debated in member states regarding the means by which personal data can be processed and by whom with the purpose of defending the population against different threat and actors. Most debates and public media attention related to restrictions on the protection of personal data falling under article 23 of the GDPR are related to the risks coming from measures taken to counter threats to public and national security, weather online of offline, measures including mass surveillance, the use of AI in predictive policing, ethnic profiling. These risks have been extensively addressed by national supervisory authorities, for example the Dutch Supervisory Authority authority in relation to the European Commission's evaluation of the LED [3] and the European level data protection authorities such as the European Data Protection Board and the European Data Protection Supervisor. The court of Justice of the European Union (CJEU) has issued several specifications on the interpretation of the exceptions that fall under the remit of national security purposes, and also indicated that where secret surveillance techniques fall outside the scope of EU law, they should comply with the corresponding requirements of the European Convention on Human Rights [200]. Of importance to this determination is whether the data collection is done via service providers or not.

From the civil society side then, there has always been the fear that state surveillance capabilities can be deployed in an un-targeted manner, leading to mass surveillance. Current technological developments will only deepen these debates, as technology will be means for both offensive and defensive objectives. This might not just be a matter of unilateral perception, as researchers have even argued that "wherever people are watching other people there will be embedded biases and power hierarchies going on between the watchers and the watched" [5]. Examples are the deployment of AI on a street in Eindhoven for early signalling of street parties going out of hand and the most recent highly mediatized case: the Paris 2024 Olympic Games. Such large events attracting large crowds of people and world media attention, posing increased security risks as they make attractive targets (take the Munich Olympics massacre or the Boston bomb attacks). In response to these threats, Olympic Games become "security spectacles" [6] and give law enforcement and security agencies the possibility to lawfully deploy and test advanced surveillance systems in the public space. In the case of the 2024 Olympic Games this led to the threat level in France being raised for the risks of terrorist attacks. It has also been argued that once these intelligent surveillance systems are put in place for a certain large event, they most often remain in place afterwards, with the permanent residents of the city remaining subject to

higher surveillance methods that were initially deployed due to an increased number of visitors attending a large event considered a security risk. Surveillance thus becomes an urban matter and this initially event specific deployment becomes an "Olympic legacy" and leading to the normalisation of surveillance [7] or surveillance creep. In the case of the AI enabled video-processing the law will stay in place until March '25. Most debated was article 7 of the law regulating the use of video surveillance, allowing deployment of AI enabled surveillance. Any biases inherited from the training data have an exacerbated impact in the case of systems used for predictive policing or smart cameras, or algorithmic surveillance, where cases of individuals serving time in prison due to wrongly identification of AI systems, criticised as not being compliant with the provisions of the GDPR.

With surveillance slowly creeping into daily lives by the standard settings embedded in everyday technology, such as the location function on smartphones, it may seem that the acceptance of individual forms of surveillance is growing, given the assumption that use of the technology implies acceptance of its terms of use. When it comes to the case of surveillance in the public space, the possibility of consenting to being subjected to surveillance is limited. Entering the public space means acceptance of being subjected to intelligent surveillance (including facial or gait recognition, crowd detection forming, detection of possible aggressive behaviour just to name a few) and potentially also to predictive policing.

Also, with many of these intelligent surveillance systems being developed by commercial companies, the role and power that the commercial sector receives must be addressed. Some consider that control over the public space is being given away to corporations or private entities and as a result the role of the state, as exclusive controller of lawful use of violent means is being questioned. A concrete example is the placement in Belgrage of over 1000 Huawei cameras in the public space, against security concerns expressed by experts, something that was chareacterized as an example of security influenced by economics. In addition to this, law enforcement and security agencies being held accountable to political oversight (for example parliamentary or presidential oversight) raising concerns about the impact that change in political agendas have on the way surveillance technology will being used in the future. Civil society have expressed the fear that democracies can thus easier be turned into authoritarian regimes.

3. Prioritizing safety and security concerns

In the area or law enforcement, the Law Enforcement Data Protection Directive - LED, unlike the GDPR, which is directly applicable to the Member States once it entered into force, leaves more flexibility to the Member States regarding its implementation, which was necessary given the complexity of MS legislations in the areas of law enforcement and security [204]. Due to the fact that public and national security fall in the responsibility of Member States according to Article 4(2) of the Treaty of European Union, the complexity of national contexts regarding the areas where the GDPR is not applicable gives rise to the additional laws restricting, clarifying or complementing the applicability of the regulation. National profiles in the area of security also influence the need for additional legislation. Such is the case of a piece of legislation currently debated in the Netherlands regarding the processing of personal data for the purpose of conducting a personalized approach to

combating radicalisation and terrorist activities, law 36225 [9] - Processing of personal data [for] personalized approach of radicalisation and terrorist activities. This shows the tension points of the balancing act between the protection of individual rights and the public interest, and how a multi-party approach to data sharing is transposed at legislative level in public programmes for prevention of radicalisation, extremism, terrorism, fighting crime and the protection of national security. For the purpose of combating radicalisation and terrorist activities, different authorities process personal data in a tripartite (in its simplest form) structure, composed of branches of the public authorities that fall either under or at the intersection of the application of the GDPR and the national implementation of the LED. In some cases the personal data in question belongs to data subjects that are considered vulnerable under the GDPR (such as minors) of falls in the category of sensitive personal data (such as health status, political affiliation or religious beliefs). The challenge that arises in this case is reflected by the fact that in order to handle a case, exchange of personal data needs to be conducted by authorities having different status when it comes to the applicability of the exceptions under the GDPR or who do not fall under the LED. The case is of interest due to several factors: the exchange between different institutions or institutional representatives of data that potentially falls under different regimes, the technical means by which such processing is facilitated, the privacy audits in place and, when retrospective is possible, the impact that the exchange has had on the success rates of the intervention focusing on prevention of radicalisation. The details of the case are explained in the following.

The legislative case in question steams out of a particular national context of combating terrorism threats in the Netherlands. While terrorism remains a threat to the internal security of the entire EU [10] there are substantial differences between member states regarding threat levels, occurrences of attacks and arrests. Based on reports of EUROPOL [10] for 2022, given the number of attacks and arrests on suspicion of terrorism, there is a visible EU west – east differentiation, with occurrences being predominant in West and South of Europe, specifically France, Germany, Spain, Italy, Belgium, the Netherlands. Looking at the official threat levels, in the case of France this is at its maximum, while for the Netherlands it is “substantial”. In the latter case, threats are coming from jihadism, right wing extremism, online radicalisation and anti-institutional extremism [11]. On this background, at national level, different government structures are responsible with the identification of possible threats. It is in the conducting of these activities that the intersection with the personal data protection legislation comes into discussion, with questions regarding who has access to what data, how the data is collected and shared between authorities and wheatear such processing gives way to discrimination against certain population groups. These initiatives carry technical challenges in matter of IT provisions and legislative sway, and are also politically sensitive. Processing under the aforementioned purpose is evidently stated as a limitation in the GDPR, as these processing activities do fall under article 23 – Restrictions.

In the activity for fighting radicalisation and terrorist activities, a person-centred approach to radicalisation and terrorism is used at local authority level, the so called case-consultation, where different parties come to the table and share case data from their own entry points. The is an already well established practice, but the proposed law (36225) sets

the legal bases for the personal data exchange between the different institution representatives coming at the table. Since this is personalized approach, the individual in question (who is registered in a certain municipality and for whom there have been registered signals of risk for radicalisation) is at the centre of the case consultation. In this individual level approach, the degree of intrusion in the personal life of the individual very high. Some of the personal data being exchanged falls into the special category of sensitive data, such as mental health or political affiliation, but also other indications of radicalisation coming from police sources [12]. According to the proposed law, the personal data can be used only for the purpose of the prevention, reducing and combat of radicalisation and terroristic activities (purpose limitation principle).

The trio of parties coming together to discuss the case are the municipality (with a coordinating role) and public safety partners – police and public prosecutor. Depending on the case, care workers (representatives of health care facilities) could also join. One challenging point of the legislation is determining if processing for the purpose of the case-consultation is in line with the original purpose for which the data was collected [12]. Given the purpose of the law, it has been argued that the processing falls in the category of ART 23 of the GDPR.

Noteworthy is that the proposed law revolves around prevention, meaning the individuals to whom the data belong have not actually conducted extremist or terrorist activities but have shown indications of such inclinations. Prevention does fall under the exemptions mentioned in article 23 of the GDPR. One of the risks mentioned during the law debate in the House of Representatives was the unjustly registration of an individual in the group of people presenting the potential for radicalisation and extremism. Similar debates have been conducted around the topic of predicting policing. The above mentioned proposed law for prevention and early signalling of radicalisation reflects upon data subjects who have not committed a terrorist act. Newer legislations are not exempted from similar challenges.

This proposed legislation on combating terrorism and radicalisation reflects the Dutch culture of the polder model, where consultations, debates and consensus are at the heart of society. Bringing different parties at the table also has the advantage of offering multiple views to the case (such as is the contribution of health care workers). On the other hand, the more parties are involved, the higher the risk of a data breach, either due to IT failure or to human error. An additional risk for the concerned data subject is that once details on their case have entered the system it might be difficult to be erased or data to be corrected. As it was mentioned in a debate of the Dutch House of Representatives, the 5 years deletion term might be an impediment to future investigations in the case of individuals coming back from areas of radicalisation, of minors being registered as representing a risk. A similar situation is found during the prosecution of criminal investigations where personal data of the individual under trial is exchanged between different parties, data which might fall under different jurisdictions. In this case, data from police sources reaches the other parties involved in the handling of the case, from the prosecution, the defence lawyer, or social services that might be needed for the social of psychological support of the individual on trial.

In such cases, several data protection principles and elements come into play: the security of the system into which the data is logged, the channel by which data is transmitted, the policies in place regarding the transfer and terms of retention for all parties involved. This implies having a cohesive approach along the entire process chain of the data, regardless of the different institutions that might be involved and therefore requiring the same training/awareness programme for all parties involved.

The anonymization/pseudonymisation steps that should take place in the first phase if possible, for example, in the case of data from law enforcement sources, should also be done before the data is sent to the other parties involved in the case. Conducting a DPIA is most often required in such cases under the GDPR, the law on police data and the law on justice and criminal data. An additional aspect to be considered is the compatibility between the initial purpose of the data collection for the investigation itself and possible secondary purposes. In certain settings and under certain limitations, data coming from police sources is used for different purposes in addition to the primary ones of law enforcement, such as research (in collaboration with research institutions), the development of redress programmes for individuals having gone through the penal system or at risk of doing so, training of AI systems for the automation of processes within LEAs, prevention of crime. It is in this secondary usage that both compatibility with the initial purpose and compatibility of data processor's status need close consideration.

4. Concluding remarks

Between the visible constructed boundaries of the public space, visibily void space is filled by the deployment of digital technologies. This digitally field space, either vertically or horizontally, can represent a resilience enabler factor if enhancing public and national security but can also become a threat if not secured against malicious interference. How this digital filled space is regulated is a matter of legal and political will. The protection given to individuals in advanced rule of law democracies brings with itself challenges when state authorities need to take action for protecting public safety and national security. As a result of these concrete difficulties experienced in daily practices by different institutions when balancing public and individual interests, new legislation and regulations are being proposed and debated in EU member states regarding the means by which personal data can be processed and by whom with the ultimate purpose of defending the population against different threat actors.

The article has explored instances of data processing activities falling under the exception of article 23, current legislative interpretations, case law and new proposed legislative initiatives under this exemption. The European Court of Human Rights [209] gives an overview of how case law on the topic of mass surveillance evolved and how the courts interpreted the claims of violations to the Convention.

The laws covering data processing in intelligence and law enforcement work will evolve, together with the evolving threat landscape and practices required in the field. Development and deployment of novel technologies, such as AI, will bring an additional practical and legislative challenge to the table, given the novelty and complexity of the technology itself, the currently unaccounted for effects of its deployment, especially in a field that cannot follow full disclosure and transparency principles. Concerns about these exceptions have

been expressed in relation to the deployment of AI systems in law enforcement, border control management, given that these uses are exempted from being registered in the open for public scrutiny EU level data base for high risk systems, making external inquiry difficult if not impossible.

Cooperation between data protection authorities and state structures in the area of intelligence and law enforcement with broader complimentary powers in line with the protection of national interests are a necessary strategy for countering opposition or scepticism on the part of the population in relation to the measures needed to ensure public and national security. This enables wide democratic support and cohesion between different state entities, and builds resilience towards threat actors who might use the argument of an mass surveillance conducted by the state in order to undermine state legitimacy and weaken stability and make room for foreign interference. It is for countering the threats of foreign interference, terrorism and hybrid threats that actions for reassuring the public that they are not targeted by surveillance arbitrarily is essential, doubled by the principles of purpose limitation, lawfulness and redress mechanisms.

With the EU landscape being fragmented in terms of the activity of privacy protection institutions and law enforcement and security agencies, the balancing act between the two values will have to be embedded in national contexts. In this regard, security interests receive the upper hand since they are legislated at national level, and are provisioned as exceptions in the European Data Protection regulation. Additionally, national security landscapes are very different across the EU, requiring considerable investments in developing initiatives and organisations addressing the specific threats. It is also in these cases - France, Germany, the Netherlands - that privacy maturity levels are most advanced in terms of budgets, activities of legislators, oversight agencies with sanctioning powers and privacy literacy levels within the population, leading therefore to strong debates, up to the point of tensions around prioritization of one set of values or the other. It is also where media outlets are most active that these debates receive wider public attention.

The case of introducing smart surveillance on the occasion of large events, due to the potential threat posed by large numbers of people coming into a city, and afterwards leaving those systems in place thus placing the permanent residents under higher surveillance is of interest for the privacy – security balancing act. On the one side it can be argued that once the temporary threat no longer exists, the solutions deployed to counter it are also no longer needed. On the other side it can be argued that with the (theoretical) initial acceptance of the surveillance of the public space, the permanent residents should not be further impacted by its remaining in place, since its initial purpose (or target) was not the permanent residents anyways. While the democratic debate over the limits of surveillance, conducted – perhaps paradoxically – within the limits of the public-security relationship, seems to have led to the publics acceptance of the role of surveillance and the role that professional agencies play in this regard, it has also been argued that this acceptance is based on ignorance, since the public is unaware of the real volume of (secret) information that is being circulated [14].

The remaining in place of the surveillance would then continue to serve the protection of the permanent residents. This would then lead to the so called “surveillance creep” or “permanentization of surveillance”. Privacy is a right protected in rule of law democracies, that also pride themselves in providing security to their population while abiding to the principles of the rule of law. Smart states can capitalize on the accumulation of information from the deployment of technology in the public space in order to better meet their core objectives – the protection of state interests. In doing so, the constant interrogation of the right balance between public and private interests rests on the collective intelligence. It is a multiple loop exercise tha allows for both internal and external adaptation.

References

[1] H. Wilson, O. Samuel and D. Plesch, Open Source Investigations in the age of Google, World Scientific, 2024.

[2] F. Fedorczyk, "The transformative power of top-down AI misuse: threats to individual freedom and risk of digital authoritarianism," *Lawtomation conference*, 2024.

[3] EDPB, "Individual replies from data protection supervisory authorities to the European Commission's evaluation of the LED," 2022. [Online]. Available: https://www.edpb.europa.eu/individual-replies-data-protection-supervisory-authorities-european-commissions-evaluation-led_en.

[4] European Union Agency for Fundamental Rights, "Surveillance by Intelligence Services. Fundamental Rights Safeguards and Remedies in the EU- 2023 Update," 2023.

[5] H. Wilson, Interviewee, *The power of open-source intelligence. War studies podcast.* [Interview]. 2024.

[6] P. Boyle, "Securing the Olympic Games: Exemplifications of Global Governance," in *The Palgrave Handbook of Olympic Studies*, London, Palgrave Macmillan, 2012.

[7] M. Ferrari, "Test, swarm, normalize: how surveillance technologies have infiltrated Paris 2024 Olympic Games," *Cad. Metrop., São Paulo*, vol. 25, no. 56, pp. 75-96, 2023.

[8] European Commission, "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (‘LED’)," 2022.

[9] "Wet gegevensverwerking persoonsgerichte aanpak radicalisering en terroristische activiteiten".

[10] Europol, "European Union Terrorism Situation and Trend Report," Publications Office of the European Union, Luxembourg, 2023.

[11] NCTV, "Terrorist Threat Assessment for the Netherlands," 2023.

[12] Tweede Kamer der Staten-Generaal, "Dossier- en ondernummer 36225 nr. 3," 2022.

[13] The European Court of Human Rights, "Factsheet – Mass surveillance," 2024.

[14] D. Bigo, "Shared secrecy in a digital age and a transnational world," *Intelligence and National Security*, vol. 34, no. 3, pp. 379-394, 2019.