EJLT European Journal of Law and Technology

EU Law, Artificial Intelligence and National Security Policing: Where Concept Creep meets Competence Creep

Markus Naarttijärvi[*]

Abstract:

This article examines the use of the 'national security argument' in Swedish efforts to expand artificial intelligence (AI) use in law enforcement and its legal implications under EU law. Swedish authorities have invoked national security to justify the inapplicability of EU regulations, in a process of potential 'concept creep'. However, the European Court of Justice (CJEU) has rejected similar broad interpretations of national security when such measures affect obligations under EU law. The article analyses the CJEU's insistence on jurisdiction over measures undertaken in the national security context, and how its case law can be explained and characterized as a potential 'competence creep' challenging Member States' attempts to bypass EU safeguards. It argues that national security-based exemptions are more viable when used by specialized intelligence agencies acting independently, but generally likely to fail when applied to broader or overlapping police functions subject to EU data protection law. Ultimately, the CJEU's stance could potentially support EU legal protections by preventing Member States from expanding police use of AI under the guise of national security in the future, but it also reflects a broader struggle of competence between national governments and EU institutions which is likely to intensify.

Keywords: AI, National Security, Policing, Concept Creep, Competence Creep

[*] Professor of Law, Department of Law, Umeå University, Sweden. This research was supported by the Swedish Research Council, grant no. 2020-02278.

1. 'Couldn't look you in the eye' – Avoidance of EU law in the context of police implementation of AI

In line with many other public actors in the European Union, the Swedish police authority has begun to actively develop and pursue the deployment of artificial intelligence (AI) technologies. These initiatives are simultaneously a response to national governmental priorities,[1] internal police priorities,[2] and European initiatives.[3] This includes introducing systems of biometric identification such as facial recognition technology,[4] and the processing of large unstructured datasets to identify threats or patterns, or to predict crime developments.[5] These systems could, under the present definition in Article 3(1) of the EU AI-Act (AIA), be construed as AI systems.[6]

These national developments take place against a backdrop of legal developments on the EU level that impact the deployment of AI in the police setting in different ways. First, there is the AIA, which includes limits relating to certain deployments of, for instance, live facial recognition systems,[7] or certain safeguards and risk mitigation procedures for high-risk AI systems such as biometric identification systems.[8] Second, there are developments in the case law of the Court of Justice of the European Union (CJEU) relating to the interpretation of *necessity* under the Law Enforcement Directive

[1] Justitiedepartementet, Biometri i brottsbekämpningen [Dir. 2021:34].
[2] Polismyndigheten, 'Hemställan om översyn av polisens brottsdatalag' (2024) Hemställan A593.896/2024.
[3] See 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 2019 (OJ L); Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy 2020.
[4] Datainspektionen, 'Förhandssamråd Om Polismyndighetens Planerade Användning Av Programvara För Ansiktsigenkänning Mot Signalementsregistret' <https://www.imy.se/globalassets/dokument/ovrigt/2019-10-23-polisen-forhandssamrad.pdf>; Polismyndigheten, 'Ansiktsigenkänning får användas för att utreda Brott' (polisen.se, 24 October 2019) <https://polisen.se/aktuellt/pressmeddelanden/2019/oktober/ansiktsigenkanning-far-anvandas-for-att-utreda-brott/>.
[5] Polismyndigheten (n 2).
[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) 2024.
[7] Article 5(1)(h) AIA.
[8] Annex III, p. 1 AIA.

(LED),[9] where the court has applied a stricter test for the processing of special category data, including biometric data.[10]

Taken together, these developments imply that as national ambitions relating to the use of AI in law enforcement increase, they run the risk of bumping up against legal requirements and interpretations flowing from EU law and the court in Luxembourg. This potential friction with EU law on data protection and AI is interesting in its own right, but one facet of it also highlights an ongoing 'struggle for competence' taking place between Member States and EU institutions regarding the significance of EU law and the role of the CJEU in the intersection of policing and national security.[11] This struggle primarily revolves around two articles in EU primary law: Article 4(2) TEU and Article 72 TFEU.

Article 4(2) TEU holds that the Union 'shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State'. Article 72 TFEU relates to the Area of Freedom, Security and Justice, and states that EU competences in this area shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

These two articles have been a point of contestation in recent cases on bulk surveillance of telecommunication data, *La Quadrature du Net* and *Privacy International*, where Member States have argued that the interception and surveillance of such data in the context of national security is one which falls outside the scope of EU law, and thus outside of the jurisdiction of the CJEU.[12] In response, the CJEU has held that 'the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law'.[13] This contested space is further complicated by the increased blurring of the lines between

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA 2016.

[10] Criminal proceedings against VS [2023] ECJ Case C-205/21; Markus Naarttijärvi, 'AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity' in Eduardo Gill-Pedro and Andreas Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions 2023: Law and the Governance of Artificial Intelligence* (Springer Nature Switzerland 2024).

[11] Monika Zalnieriute, 'A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union' (2022) 85 The Modern Law Review 198.

[12] *La Quadrature du Net and Others v Premier ministre and Others* [2020] ECJ Joined Cases C-511/18, C-512/18, C-520/18 89; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECJ Case C-623/17.

[13] *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 99. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 44.

'regular' policing and national security policing, through the changing dynamics of phenomena such as terrorism, hybrid warfare, and organized crime.[14] In any case, the claim of the CJEU that Member State measures taken within the context of national security may fall within the scope of EU law is not without controversy. Cameron notes that 'the Court has left very little outside the scope of EU law (and its own jurisdiction)',[15] and that there are 'good reasons for Member States to be skeptical towards the Court's assertions of competence over this area'.[16] Meanwhile, the wide approach to the scope of application of EU law by the CJEU has been described as having spill-over effects where EU law may preempt Member State action in areas that are formally theirs to regulate.[17] This has been described as resulting in a type of 'competence creep' whereby the competences of the Union are expanded gradually and in a surreptitious manner without support in the Treaties.[18]

Currently, there are signs that national ambitions relating to the implementation and use of artificial intelligence (AI) in law enforcement may open a new front in this struggle for competence. The Swedish government recently tasked an inquiry with proposing reformed rules on data processing for the Swedish Security Service to allow for further use of AI in the processing of large amounts of unstructured data from open internet sources, including social media.[19] As a point of context, the Swedish Security Service serves as both a law enforcement agency in charge of internal (national) security and a national security intelligence service. As such it has police functions in fields such as investigating terrorist offences and espionage, while predominantly functioning as an internal intelligence agency, with functions comparable to civilian agencies in England or Canada.[20] In the directives to the inquiry tasked with developing a proposal for the data protection reform, the government held that EU law did not apply to the data processing by the agency, which meant that ensuring compliance with EU data protection rules and the (then) upcoming AI act was not part of the remit of the inquiry.[21] While this is a question open to debate, and one which ultimately may be decided by the CJEU, the position of the government seems to have inspired connected arguments within the regular Swedish police authority.

---

[14] See Colin Atkinson, 'Where Were You While We Were Getting High Policing? The Consequences of Co-Location for Broader Partnership Working in Tackling Organised Crime and Terrorism' (2019) 29 Policing and Society 922; James Sheptycki, 'The Police Intelligence Division-of-Labour' (2017) 27 Policing and Society 620.

[15] Iain Cameron, 'A. Court of Justice Metadata Retention and National Security: Privacy International and La Quadrature Du Net' (2021) 58 Common Market Law Review 1433, 1458.

[16] Cameron (n 15) 1471.

[17] FX Millet, 'In the Name of Analogy: Judicial Copy-Pasting and Competence Creep in the Connection Data Case Law' (2024) 61 Common Market Law Review 1289, 1290–1291.

[18] See Millet (n 17) 1290.

[19] Swedish Government, Säkerhetspolisens informationshantering 2023 [Dir. 2023:64].

[20] Markus Naarttijärvi, *För Din Och Andras Säkerhet – Konstitutionella Proportionalitetskrav Och Säkerhetspolisens Preventiva Tvångsmedel* (Iustus förlag 2013).

[21] Swedish Government Säkerhetspolisens informationshantering (n 19).

In a recent formal request to the government from the Swedish police authority for a reform of the police data protection act (Brottsdatalagen, a national transposition of the Law Enforcement Directive), the police authority argued that much of what it does, in particular the work against organized crime, serves to protect national security. According to the Police authority, this meant that further exceptions from the EU data protection rules were both warranted and allowed.[22] These arguments were explicitly tied to the need for increased AI use within the authority and connected to the ongoing reforms in the national security context. In parallel, the authority argued that data protection principles could be interpreted in a less stringent manner and petitioned the government to remove 'any obstacles not required by EU law'.[23]

Both Swedish developments highlight how EU law seems to be perceived by relevant authorities as an impediment for the increased implementation of AI in the law enforcement setting. They also highlight how the debated scope and relevance of EU law in the context of national security opens a field of contestation and at least potential legal maneuverability in relation to EU law for both government and agency policy making. This is not a phenomenon exclusive to Sweden. Following the *La Quadrature du Net* ruling, the French Conseil d'État declined to apply the same balancing that the CJEU had established in their ruling, claiming that national security was a domestic concept under the Treaty and in need of national interpretation. While falling short of claiming that the CJEU acted *ultra vires*, the French court still ended up asserting a different interpretation and balancing of interests than the CJEU.[24] By reinterpreting or asserting a national definition of the concept of national security, national actors can thus engage in what I would like to call a type of 'concept creep' – a gradual and surreptitious reinterpretation of a concept that the CJEU has claimed jurisdiction over, but which belongs to a contested space of competence. The Swedish development shows that the ambitions relating to the use of AI has the potential of opening a new front in the overall struggle for competence which is likely to influence not only the debate surrounding the scope of EU law, but by extension the legal boundaries for the implementation of AI in the law enforcement setting and the overall relevance of EU data protection laws and the AIA as a safeguard for individual rights in relation to such implementation. As such, it is an issue that warrants further investigation.

2. 'What the hell am I doin' here?' - Aim, research questions, and method

This article will analyze two developments moving in opposite directions. First, what I will label as 'the national security argument' in the context of law enforcement and AI policymaking in Sweden – more specifically the legal argument that data processing

[22] Polismyndigheten (n 2).
[23] Polismyndigheten (n 2).
[24] CE Ass., 21 April 2021, Req. no. 393099; for a discussion on this case, see Araceli Turmo, 'B. National Courts National Security as an Exception to EU Data Protection Standards: The Judgment of the Conseil d'État in *French Data Network and Others*' (2022) 59 Common Market Law Review 203, 87.

relating to national security falls outside the scope (and limits) of EU law and that the CJEU lacks jurisdiction to review national legislation enabling such processing. The concept creep displayed in the shape of this argument and the reforms and policy ambitions it has unlocked in the Swedish context will be used as a point of departure to analyze the legal viability of these arguments in the light of the second development. This is the gradual development of case law from the CJEU interpreting the scope of EU law in the national security context and the competence creep displayed within this case law context. The claim that the CJEU has contributed to competence creep in this context is not new. Millet has criticized the Court for engaging in copy-paste jurisprudence in the data retention context leading to competence creep.[25] Zalnieriute, while not characterizing it as competence creep, points to how the CJEU has asserted its authority over national security in the surveillance cases while being increasingly receptive to Member States national security concerns in its rulings.[26] What my study contributes here is tying together these discussions in the area of data protection with a longer trend in relation to earlier case law in the free movement and non-discrimination contexts as well as situating the development in a wider explanatory framework.

Both strands of my analysis, the national and the European, will serve the overarching aim of extrapolating and understanding the underlying tension and struggle for competence within the national security and law enforcement sector in general and the legal implications thereof, in particular for the implementation of AI in the context of policing. While the policymaking examples are drawn from the Swedish context, the analysis of EU law is more general, so the findings are likely to be relevant for understanding developments in policing and data protection across other EU Member States and to further our understanding of competence creep within EU law.

As a point of delimitation, it is worth noting that the article thus focuses on questions relating to the potential *scope* of EU law and the implications this has for national policymaking on the use of AI in the law enforcement context. It is not my ambition to make a full accounting of the more detailed rules and principles relating to EU data protection law or the AIA. Some notes will however be made regarding what exceptions from rules and principles otherwise established by EU law the national security argument may or may not unlock.

The analysis of Swedish policymaking is mainly based on a close reading of official government inquiries and the remits for such inquiries, in addition to departmental inquiries, policy papers, missives and written communication between the police authority and the government. Comments on legislative proposals from consultative bodies are included to provide context to the analysis made by the government. For my analysis of EU law, a legal doctrinal method is deployed. Here I will primarily focus on identifying current key cases and trace the gradual development of EU law through

[25] Millet (n 17).
[26] Zalnieriute (n 11).

CJEU case law in reverse chronological order, reference by reference until no further references can be found. After building this network of cases and extrapolating the legal argumentation in it, as well as the legal basis for these arguments, the reasoning of the CJEU will be interpreted in line with established concepts and principles developed in relevant legal scholarship commenting on and interpreting EU law. The cut off point of relevant case law has been May 1, 2025, while legal research commenting on that case law may be of a later date.

This paper is structured in the following manner. Following the introductory section 1, and this section 2 on aim and methods, I will begin in section 3 with establishing a timeline of the national security argument in Swedish policymaking relating to the intersection of EU law and policing. In section 4, I will first establish current explications on the scope of EU law in the context of national security (section 4.1) and then trace it back to highlight its development over time. This timeline of cases will then be analyzed in relation to the delineation of national security against similar concepts such as public security or internal and external security and the way the CJEU has responded to possible concept creep (section 4.2). In section 4.3 I will analyze the identified developments as expressions of the doctrine of pre-emption, and to what extent this can be seen as an example of competence creep. Finally in section 5 I will draw conclusions and discuss possible implications thereof.

3. 'I wish I was special' - The National Security Argument in the context of Swedish police policymaking

In November of 2024, the Swedish Police Authority made the previously mentioned formal written request (‘hemställan’) to the government for a complete reform of the data processing rules in Brottsdatalagen (the Crime Data Act)[27] and the associated rules in Polisens brottsdatalag (the Police Crime Data Act),[28] both of which govern different aspects of the police authority’s processing of personal data. Throughout their request, the police authority stresses the need to further implement AI in their work.

> The police authority must be able to process personal data within large information sets with modern technology. To quickly manage large amounts of unstructured material the authority needs to use different AI-abilities.[29]

The authority clearly ties this need for AI to a connected need to collect large amounts of data from the open internet and other sources. Here the authority relies on the Swedish government’s strategy against organized crime where the government has highlighted how artificial intelligence ‘will be of great importance for authorities' ability to combat organized crime’ as well as highlighting the need ‘to identify,

[27] Brottsdatalag (2018:1177).
[28] Lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.
[29] Polismyndigheten (n 2) 2.

manage, sort, and draw conclusions from datasets in all types of information processing, both for crime prevention and criminal investigations'.[30] To further the ability to use AI, the authority asked for a loosening of national data protection rules implementing the LED towards the minimum level required by EU law. More importantly, the authority also argued for *exceptions* to be made from the application of EU law data protection requirements. In the view of the Police authority, much of the work the police does in relation to organized crime furthers the interest of national security, as serious organized crime is, according to the police authority, system-threatening ('systemhotande').[31] This view of organized crime and criminal networks is not unique to the police authority, but one which the Swedish government has itself made a centerpiece of its strategy against organized crime. The argument of the Swedish government has been that organized crime does not only threaten the safety and security of citizens, but by extension basic values such as democracy, rule of law, trust between citizens and towards the government.[32] The Swedish minister of justice has referred to network criminals involved in the surge of violent shootings and bombings in Sweden as 'domestic terrorists' and called for additional measures to combat this threat.[33]

This line of reasoning by the government effectively opened the door to the national security argument, whereby the Swedish Police Authority could point to the exceptions from data protection standards enjoyed by the Swedish Security Service to ask for similar exceptions. Indeed, in relation to the data processing of the Security Service, the Government has both recently, and for some time, argued that EU law is inapplicable, and that the data protection frameworks impacting national security policing only need to meet the requirements of the Swedish constitution and the European Convention on Human Rights.[34] The police authority now asked the government to carve out similar exceptions for their data processing in the fight against organized crime. It is worth noting that the request by the Swedish Police Authority actually took this line of argumentation one step further, as the authority claimed that much of everyday crime – from fraud to thefts and burglaries – could form a part of the chain of organized crime and thus underpin criminal networks.[35] While not stating it outright, it seems the exceptions the Police authority would like

[30] Swedish government, 'Regeringens Skrivelse 2023/24:67 – Motståndskraft Och Handlings-Kraft – En Nationell Strategi Mot Organiserad Brottslighet' <https://www.regeringen.se/contentassets/1ae2655654ab479d8e4210d12f44e816/motstandskraft-och-handlingskraft---en-nationell-strategi-mot-organiserad-brottslighet-skr.-20232467>.
[31] Polismyndigheten (n 2).
[32] Swedish government (n 30) 3.
[33] Swedish government, 'Anförande av justitieminister Gunnar Strömmer vid Folk och Försvars Rikskonferens 2024' (*Regeringskansliet*, 7 January 2024) <https://www.regeringen.se/tal/2024/01/anforande-av-justitieminister-gunnar-strommer-vid-folk-och-forsvars-rikskonferens-2024/> accessed 10 June 2025.
[34] Swedish government Säkerhetspolisens informationshantering (n 19).
[35] Polismyndigheten (n 2).

to see could potentially extend quite far into everyday policing in what can be described as a form of concept creep.

To understand the background to this request we need to go back to the first foray of EU data protection rules into the specific context of law enforcement – the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. As this precursor to the LED was implemented into Swedish law, the government had to assess the alignment of existing rules with the new EU requirements. One of the aspects considered was how the exceptions in the decision relating to national security was to be understood in the Swedish legislative context. The government noted that what the European Commission had defined as national security was the protection of national sovereignty against internal and external threats.[36] This aligned with what had traditionally been discussed in Sweden as 'rikets säkerhet' or the 'security of the realm'. This led the government to draw a functional and institutional boundary of the concept; as the function of ensuring the security of the realm belonged to the Swedish Security Service, the national security exception would apply to the activities performed (and the data processed) by that authority. In this context, the government noted that the tasks of the Swedish Security Service only partly related to the protection of national sovereignty and included a wider set of threats to important societal functions or democratic values.[37] Still, the view of the government was that the overall task of the security service related to national security, so the exceptions to the framework decision should apply to their activities as a whole as well.[38]

This institutional delineation of national security mostly carried over as the framework decision was replaced by the LED in 2018. In the legislative work implementing the LED the government maintained that most of what the Swedish Security Service was responsible for fell within the ambit of national security.[39] The institutional borders were not, however, kept as clean as before. First, the regular Swedish Police Authority would fall under the exception carved out for the Swedish Security Service when rendering assistance to the security service. Secondly, when the security service rendered assistance to the regular police, they would not be subject to the exception.[40]

The implementation of the LED did shed some light on the government's view on both the definitional importance of national security and the power to define the concept.

[36] Swedish Government, Godkännande av Dataskyddsrambeslutet 2008 [prop. 2008/09:16] 32; Swedish Government Official Inquiry, Dataskydd vid europeiskt polisiärt och straffrättsligt samarbete [SOU 2011:20] 222.
[37] The Swedish Security Service itself used an effect-based definition, i.e., if an actor engaging in unlawful influence had the capacity to have an actual effect on important societal functions, this constituted a threat to national security.
[38] Swedish Government Godkännande av Dataskyddsrambeslutet (n 36) 32–33.
[39] Swedish Government, Brottsdatalag 2018 [Prop. 2017/18:232] 102.
[40] Swedish Government, Brottsdatalag (n 39) 105.

In the legislative proposal for the Swedish Crime Data Act, the government pointed out that, as a concept, the term had implications for delineating the scope of EU law, yet despite calls from consultative bodies – including the Police Authority – to more closely define the term national security,[41] the government refrained from doing so. Instead, it stated that:

> At the same time, it is a concept rooted in EU law, which delineates the competencies of the EU in relation to the Member States. Ultimately, it is for the Court of Justice of the European Union to determine the precise meaning of the concept. Against this background, the Government considers it inappropriate to define the term 'national security' within the framework of this legislative matter.[42]

In other words, at this point in time (in 2018), we can see an explicit acknowledgement of the role and jurisdiction of the CJEU over the concept, at least as it relates to the boundaries of possible exceptions from data protection rules targeting regular law enforcement.

Three years later, in 2021, a Swedish government inquiry was tasked with proposing new adaptations to the Swedish rules on communications data retention.[43] It was the third attempt at making rules that properly took EU law into account after failures to fully acknowledge the implications of the rulings of the CJEU in *Digital Rights Ireland*, and *Tele2 Sweden*.[44] In these cases, the CJEU opened the door for certain limited exceptions to the prohibition against general and undifferentiated retention of telecommunications data in the context of clear and present threats against national security. The government had tasked the inquiry to take advantage of those exceptions to establish rules on national security retention, which meant that the inquiry had to approach the concept of national security.[45] In its report, the 2021 inquiry noted that national security was technically the sole responsibility of Member States. It also noted that there was no clear definition of the term national security in the treaties or in the case law of the CJEU,[46] though no accounting of relevant CJEU case law was presented and, as we will see, this statement is arguably at least partially incorrect.[47] It further noted that, from a national Swedish perspective, the term was

[41] Swedish Government, Brottsdatalag (n 39) 102.
[42] Swedish Government, Brottsdatalag (n 39) 104.
[43] Swedish Government, Datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering 2021 [Dir. 2021:58].
[44] Previous attempts had been made in 2014, 2015 and 2017 which all failed to recognize the key parts of the rulings from the CJEU, see Datalagring, EU-rätten och svensk rätt 2014 [Ds 2014:23]; Swedish Government Official Inquiry, Datalagring och integritet 2015 [SOU 2015:31]; Swedish Government Official Inquiry, Datalagring – brottsbekämpning och integritet 2017 [SOU 2017:75].
[45] Swedish Government Datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering (n 43).
[46] Swedish Government Official Inquiry, Datalagring och åtkomst till elektronisk information 2023 [SOU 2023:22] 182.
[47] See section 4 below.

not legally defined either, but the inquiry pointed to the Swedish national security strategy and noted that '[t]he actors that are important for the security of society are not only more numerous than before, but also more diversified. Influence over central areas and societal functions, which previously lay to a greater extent with the state, can today be shared by many. As a consequence of globalization, the connection between internal and external security is more direct than before'.[48]

Later, in 2025, the most explicit discussion on the relationship between national security and EU data protection legislation arose in the inquiry proposing a reformed legal framework for data protection within the Swedish Security Service, mentioned at the outset of this article. As already mentioned, the government had indicated in the tasking of the inquiry that EU law did not apply to the security service. The inquiry followed this instruction and asserted that EU law should not serve as the point of departure for the new act, given that Article 4(2) TEU places national security under the exclusive competence of Member States. As a result, the inquiry held that EU data protection rules are not binding when Sweden enacts legislation governing data protection solely in relation to national security.[49] The 2025 inquiry acknowledged that the rules it sought to reform closely mirrored EU data protection standards. This alignment had been intended to simplify the application of the rules and support Sweden's commitments under the Data Protection Convention. Beyond this, certain arguments remained valid for maintaining proximity to EU rules – for example the benefit of synergy when oversight bodies apply similar standards to monitor both the Swedish Security Service and the Police Authority. Such alignment also permitted EU legal concepts and terminology to inform the implementation of the Swedish Security Service's data protection rules.[50]

However, the 2025 inquiry went on to present several arguments *against* allowing EU law to serve as a guiding framework for the proposed reform. First, it noted that the interests involved in safeguarding national security, and the expectations placed on responsible agencies, are not comparable to those in general law enforcement. In this regard, the inquiry cited the CJEU's reasoning in *La Quadrature du Net*,[51] which held that national security concerns can justify more far-reaching interferences with fundamental rights.[52]

Second, the inquiry argued that the EU legal framework had not fully balanced privacy and data protection interests against national security considerations. This balancing is, according to the inquiry, expected to occur at the national level – taking into

[48] Swedish Government Official Inquiry, Datalagring och åtkomst till elektronisk information (n 46) 184.
[49] Swedish Government Official Inquiry, Säkerhetspolisens behandling av personuppgifter 2025 [SOU 2025:49] 272.
[50] Swedish Government Official Inquiry, Säkerhetspolisens behandling av personuppgifter (n 49) 272.
[51] See further section 4.1 below.
[52] Swedish Government Official Inquiry, Säkerhetspolisens behandling av personuppgifter (n 49) 273.

account the specific threats facing each Member State. In this context, the inquiry found that the current legislation failed to strike a reasonable balance between the needs of the security service and the rights it was expected to safeguard.[53]

Third, the inquiry warned that allowing EU law to influence the core functions of the security service would risk applying judgments related to general law enforcement to the more sensitive domain of national security. It maintained that Member States, pursuant to Article 4(2) of the Treaty, are best positioned to assess and respond to national security threats. Moreover, the inquiry argued that it is practically impossible for the CJEU to fully evaluate a data protection issue in the context of national security, given that Member States are unlikely to publicly disclose all the justifications behind specific data processing activities.[54] This argument mirrors the position of the French Conseil d'État discussed in section 1 above, asserting national competency (in both senses of the word) over the balancing of national security against opposing data protection interests.

Fourth, the inquiry suggested that, if the legislation remained closely aligned with EU law, interpretations developed under EU law would inevitably shape the interpretation of the Swedish Security Service Data Act. In light of these considerations, the inquiry concluded that there were 'good arguments in favor of more clearly separating this area from the one where EU law has a deciding influence' and allowing the Swedish legislator to independently balance national security interests against other competing concerns.[55]

The 2025 inquiry's position on the relationship to EU law resulted in a proposed new set of data protection rules that marked significant departures from existing standards on adequacy, relevance, and data minimization. It recommended lower thresholds for the initial processing of data, longer and more flexible retention periods, and the removal of the prohibition on processing sensitive data. At the same time, it introduced a general proportionality requirement for further processing, with stricter safeguards for sensitive data.[56]

Additionally, the 2025 inquiry proposed a separate law governing the processing of personal data in 'special data collections' – that is, bulk data collected from open sources such as social media. This framework was explicitly designed to enable the use of artificial intelligence tools to detect risks and threats to national security. The legal model for this law was based on the framework for bulk surveillance, which had

[53] Swedish Government Official Inquiry, Säkerhetspolisens behandling av personuppgifter (n 49) 274.
[54] ibid.
[55] ibid.
[56] See Swedish Government Official Inquiry, Säkerhetspolisens behandling av personuppgifter (n 49) 23–35.

previously been reviewed by the European Court of Human Rights and found to be in compliance with the European Convention on Human Rights (ECHR).[57]

In essence, the 2025 inquiry's view that EU law does not apply to the Swedish Security Service's data processing activities directly enabled the inquiry to propose an expanded use of AI-assisted analysis within the agency and increased the overall flexibility of its data processing practices. The proposal has, at the time of writing, not yet been implemented but is currently being processed within the Ministry of Justice.

Under Swedish legislative procedure, government authorities, universities, and civil society organizations are invited to comment on the reports of legislative inquiries. Interestingly, almost no expert bodies mentioned the potential relevance of EU law in their consultation reports.[58] Neither the privacy and data protection authority (Integritetsskyddsmyndigheten) nor the ombudsman for discrimination (Diskrimineringsombudsmannen) commented on the EU law aspect of the inquiry's report, despite the centrality of EU law for their respective tasks.[59] The Parliamentary Ombudsmen (Justitieombudsmannen), one of the most important consultative bodies in matters of protecting fundamental rights, wrote in their report:

> The inquiry notes that the protection of national security is a national matter and that activities concerning national security are not covered by Union law. The legislation should therefore not be based on an EU-law foundation. I have based my review on that position. I therefore also assume that the inquiry's proposal does not entail any breach of Sweden's obligations under EU law.[60]

From this overview, it is clear that the national security argument has played an important part in the Swedish government's policymaking in the area of data protection, and more recently been at the heart of new measures implementing AI into the Swedish security police. Lately, a significant shift can be identified in the position on the jurisdiction of the CJEU over the definitional boundaries of national security. Whereas the government has previously indicated that the CJEU is the final arbiter of what constitutes national security under EU law, the 2025 inquiry instead

---

[57] See Swedish Government Official Inquiry, Säkerhetspolisens behandling av personuppgifter (n 49) 563–572.

[58] One exception being the comment by Umeå University, prepared by the author of this article.

[59] Integritetsskyddsmyndigheten, 'Yttrande över Säkerhetspolisens hantering av personuppgifter (SOU 2025:49)' (22 August 2025) <https://regeringen.se/contentassets/2c996b613dfe49328375529fee691d5b/integritetsskyddsmyndigheten.pdf> accessed 1 January 2026; Diskrimineringsombudsmannen, 'Yttrande Över SOU 2025:49 Säkerhetspolisens Behandling Av Personuppgifter' (20 August 2025) <https://regeringen.se/contentassets/2c996b613dfe49328375529fee691d5b/diskrimineringsombudsmannen.pdf> accessed 1 January 2026.

[60] Justitieombudsmannen, 'Yttrande över betänkandet Säkerhetspolisens behandling av personuppgifter (SOU 2025:49)' (19 August 2025) <https://regeringen.se/contentassets/2c996b613dfe49328375529fee691d5b/riksdagens-ombudsman.pdf> accessed 1 January 2026.

argues that the definitional boundaries and balancing of interests must be made on the national level due to the nature of national security concerns.

In the next section, I will trace the response from the CJEU to similar arguments made by Member States in the context of national and public security under EU law.

4. 'I Wanna Have Control' - Outlining the contested space of national security under EU law

4.1 'When you were here before' – Tracing the evolution of national security case law before the CJEU

In this section, I will trace the most recent responses by the CJEU to the national security argument backwards in time to its conceptual and interpretive origin. This reverse timeline serves two purposes. It allows for a clear view of the gradual interpretive development of EU law in relation to national security as well as the identification of distinct generations of case law and the contested concepts under EU law. As such, it serves to highlight how, and where, the CJEU has seen fit to respond to the national security argument and how this has impacted the struggle for competences in this area.

The most recent cases relating to the question of EU jurisdiction in the national security context presents, on the surface, a rather clear picture. In Case C-623/17, *Privacy International*,[61] a challenge had been made by the NGO Privacy International before the UK Investigatory Powers Tribunal on whether the national UK legislation requiring providers of electronic communication to forward traffic data and location data to national intelligence agencies complied with the ePrivacy directive.[62] This resulted in a request for a preliminary ruling to the CJEU on whether the ePrivacy directive read in light of Article 4(2) TEU applied to such transfers.[63] The CJEU was faced with arguments made by intervening Member State governments relating to Article 4(2) TEU, where they argued that EU-law should not apply to such transfers when they were made for the purpose of safeguarding national security.[64] The CJEU found that the directive applied to such transfers given that the telecommunication providers were subject to the requirements under the directive.[65] Part of this finding rested on the technicality that the ePrivacy directive included specific exceptions for

[61] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 16).
[62] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2009.
[63] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 30.
[64] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 32. The argument was made by nine Member States: Czech Republic, Estonia, Ireland, France, Cyprus, Hungary, Poland, Sweden and the United Kingdom.
[65] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 46.

the adoption of laws restricting the confidentiality of electronic communications for national and public security purposes – indicating to the Court that the directive as such is applicable to national security measures.[66] However, the Court also made a more general pronouncement on the point of Article 4(2) TEU:

> [A]ccording to the settled case-law of the Court, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.[67]

The case of *La Quadrature du Net*, delivered on the same day, revolved around the question of whether national rules on data retention were acceptable under the ePrivacy directive. Similar questions arose here regarding the applicability of the directive, and EU law more generally, to measures taken that at least in part aimed to safeguard national security.[68] Here too, national governments intervening in the case had referred to Article 4(2) TEU.[69] Finding that EU law, and the ePrivacy directive, applied to the retention given the obligations targeting telecommunication providers, the CJEU repeated the same locution as in *Privacy International*, holding that measures taken for the purpose of safeguarding national security cannot render EU law inapplicable or exempt Member States from their obligations under EU law.[70]

In both *Privacy International* and *La Quadrature du Net*, the CJEU refers to the same three cases as support for their statement on the relevance of EU law in the context of national security as a part of the 'settled case-law of the court'.[71] These three cases can thus be seen to represent a second layer of the CJEU case law on the national security argument. Given the rather definitive formulation made by the CJEU in *Privacy International* and *La Quadrature du Net*, it is interesting to note that none of the cases cited explicitly mentions *national* security.

The first cited case, C-187/16, *Commission v Austria*,[72] deals with the connected but different concept of *public security*. In the case, the Austrian government had made exceptions to the public procurement process to award the state printing office

---

[66] *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 97; see also Maria Tzanou and Spyridoula Karyda, '*Privacy International and Quadrature Du Net:* One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28 European Public Law 128.
[67] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 44.
[68] *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 85.
[69] *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 89.
[70] *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 99.
[71] *ZZ v Secretary of State for the Home Department* [2013] ECJ Case C-300/11; *European Commission v Republic of Austria* [2018] ECJ Case C-187/16; *European Commission v Republic of Poland and Others* [2020] ECJ Joined Cases C-715/17, C-718/17, C-719/17.
[72] *European Commission v Republic of Austria* (n 71).

contracts to produce identity documents and other official documents. The Austrian government argued essentially that these measures were necessary for the protection of public security due to the sensitivity of these documents.[73] The CJEU in its judgment recognized that it was indeed a matter for Member States to define their essential security interests, and more specifically security measures necessary for the protection of the public security. Nevertheless, the court continued by concluding that 'measures adopted by the Member States in connection with the legitimate requirements of national interest are not excluded in their entirety from the application of EU law solely because they are taken, inter alia, in the interests of public security'.[74]

The second, Case C-300/11, *ZZ v Secretary of State of the Home Department*, concerned the refusal of entry into the United Kingdom of an EU citizen, ZZ, on the basis of public security. At the heart of the case was whether the state, on appeal, was obliged to provide a full account of the evidence that underpinned a decision by a court to not grant his entry, and whether a failure to do so would violate EU law and in particular the requirement to state reasons for limitation to the freedom of movement under Directive 2004/38/EC,[75] and the right to an effective remedy under Article 47 of the Charter. The Italian government had intervened in the case, arguing that the CJEU lacked jurisdiction as the question related to issues which under Article 4(2) TEU and Article 346(1)(a) TFEU remained the responsibility of solely the Member States and outside the competence of the EU.[76] Here too, the CJEU asserted that it had jurisdiction and that 'the mere fact that a decision concerns State security cannot result in European Union law being inapplicable'.[77] There is, however, a notable shift in the language used in the preliminary ruling, compared to the language used in the national court context. In the UK court, the term 'national security' appeared 27 times, including in the question referred by the national court for a preliminary ruling.[78] The CJEU appears to carefully avoid the term and even when quoting (within quotation marks) the question put to the CJEU by the UK court of appeals, exchanging the word 'national security' for 'state security'.[79] A possible explanation for this exchange is that the court uses French as the language of deliberation, which could translate the language of the national court's request from 'national security' to the

[73] *European Commission v Republic of Austria* (n 71) 58.
[74] *European Commission v Republic of Austria* (n 71) 76.
[75] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (Text with EEA relevance)Text with EEA relevance 2011.
[76] *ZZ v Secretary of State for the Home Department* (n 71) 35.
[77] *ZZ v Secretary of State for the Home Department* (n 71) 38.
[78] *ZZ v Secretary of State for the Home Department* [2014] Court of Appeal (Civil division) [2014] EWCA Civ 7 9.
[79] *ZZ v Secretary of State for the Home Department* (n 78) 34. A similar exchange was done by the Advocate General, see *Opinion of Advocate General Bot delivered on 12 September 2012 ZZ v Secretary of State for the Home Department Case C-300/11* (ECJ).

French 'sûreté de l'État', which could then be translated back to English as 'state security'. However, given that the CJEU uses the term 'sécurité nationale' in the French language version of the more recent cases of *La Quadrature du Net* and *Privacy international*, it remains possible that the avoidance of the term 'national security' in the ruling was intentional by the court.

The third ruling in this generation of cases is *Commission v Poland, Hungary and Czech Republic*. This case is somewhat different in that it revolves around the failure of the respondent governments to fulfil their obligations under a temporary mechanism for the relocation of applicants for international protection. One of the arguments provided in defense of the actions (or inactions) of the respondent states was that failures in the temporary relocation mechanism brought 'risks posed by the possible relocation on their territory of dangerous and extremist persons who might carry out violent acts or acts of a terrorist nature'.[80] As the temporary relocation mechanism was enacted under Title V of the TEU, Poland and Hungary argued that the obligations had to be subject to the limitation under article 72 TFEU, which holds that Title V should not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security. Furthermore, they argued that this provision should be read in light of Article 4(2) FEU, allowing them to disapply secondary and lower-ranking obligations in the relocation mechanism.[81] The CJEU disagreed, holding that 'although it is for the Member States to adopt appropriate measures to ensure law and order on their territory and their internal and external security, it does not follow that such measures fall entirely outside the scope of European Union law'.[82] In this case, the court went further, stating '[t]he scope of the requirements relating to the maintenance of law and order or national security cannot therefore be determined unilaterally by each Member State, without any control by the institutions of the European Union'.[83] This is a rare mention of national security in the generation of cases preceding *Privacy International* and *La Quadrature du Net*. The statement is however not specifically targeting the implications of Article 4(2) TEU but instead mentioned in the context of Article 72 TFEU and the possibility to derogate from specific EU instruments, but the implications appear wider, as a general claim of jurisdiction of EU institutions to review measures taken in the national security context. The case, however, does not extend to the question of the possibility for Member States to legislate within their exclusive competence in the area of national security in a way that impacts on EU law in other areas, only that the CJEU reserves the right to review derogations within that context.[84]

---

[80] *European Commission v Republic of Poland and Others* (n 71) 134.
[81] *European Commission v Republic of Poland and Others* (n 71) 134–137.
[82] *European Commission v Republic of Poland and Others* (n 71) 143.
[83] *European Commission v Republic of Poland and Others* (n 71) 146.
[84] This is apparent from the references the court made to previous case law specifically discussing derogations, such as *K v Staatssecretaris van Veiligheid en Justitie and HF v Belgische Staat* [2018] ECJ Case C-331/16 40; *Z Zh v Staatssecretaris van Veiligheid en Justitie and Staatssecretaris van Veiligheid en Justitie v I O* [2015] ECJ Case C-554/13 48.

As support for its reasoning in these three cases the CJEU refer to an earlier generation of cases, where the CJEU used a slightly different locution to maintain the relevance of EU law. This generation of cases all relate to contexts where Member States had argued on public security grounds for derogations from fundamental freedoms in the shape of duty-free imports of military equipment.[85] The court begins with the now familiar locution on the responsibility of Member States to take appropriate measures to safeguard their security, while holding that this does not place such measures 'entirely outside the scope of Community law'.[86] Here however, the CJEU also stresses the binding and uniform nature and application of EU law, by adding:

> It cannot be inferred that the Treaty contains an inherent general exception excluding all measures taken for reasons of public security from the scope of Community law. The recognition of the existence of such an exception, regardless of the specific requirements laid down by the Treaty, would be liable to impair the binding nature of Community law and its uniform application.[87]

This line of cases can in turn be traced back, through non-discrimination cases relating to recruitment in the armed forces where the similar locutions are used,[88] to a single case from 1986: Case 222/84, *Johnston*.[89] In this case, the court held that only the specific derogations for *public safety* provided for in the treaties could be relied on to avoid EU law requirements, continuing; 'If every provision of community law were held to be subject to a general proviso, regardless of the specific requirements laid down by the provisions of the treaty, this might impair the binding nature of community law and its uniform application'.[90]

Having traced the line of argumentation of the CJEU in *Privacy International* and *La Quadrature du Net* back to its beginnings, we can tell that the insistence of the EU court to maintain jurisdiction over matters connected to various permutations of the national security argument is clear. Current scholarship has indeed largely engaged with the outcomes of these two important cases as a matter of *who defines* the boundaries of the contested concept of national security, where the CJEU is seen as

---

[85] *European Commission v Kingdom of Denmark* [2009] ECJ Case C-461/05; *European Commission v Hellenic Republic* [2009] ECJ Case C-409/05; *European Commission v Portuguese Republic* [2010] ECJ Case C-38/06.
[86] *European Commission v Kingdom of Denmark* (n 92) 51; *European Commission v Hellenic Republic* (n 92) 50; *European Commission v Portuguese Republic* (n 85) 62.
[87] *European Commission v Kingdom of Denmark* (n 92) 51; *European Commission v Hellenic Republic* (n 92) 50; *European Commission v Portuguese Republic* (n 85) 62.
[88] *Angela Maria Sirdar v The Army Board and Secretary of State for Defence* [1999] ECJ Case C-273/97 15; *Tanja Kreil v Bundesrepublik Deutschland* [2000] ECJ Case C-285/98 16; *Alexander Dory v Bundesrepublik Deutschland* [2003] ECJ Case C-186/01 31.
[89] *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary* [1986] ECJ Case 222/84.
[90] *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary* (n 89) 26.

expanding review powers further into Member State territory.[91] The ruling by the Conseil d'Etat following *La Quadrature du Net* suggests that the contest surrounding this definitional power remains unresolved.[92]

I would suggest, however, that there are two additional components helpful in understanding the outcome of the CJEU's historical assertion of jurisdiction in cases involving the national security argument.

The first is the relative importance of the delineation between *national security* (arguably outside the scope of EU law under Article 4(2) TEU) and other similar concepts such as *public security*, *internal and external security*, *state security*, *and public safety*, where the CJEU has maintained a longer, and more direct, claim of jurisdiction.

The second is whether the claim of jurisdiction by the CJEU carries further implications relating to our understanding of the *scope* of EU law and whether Member States taking national legislative or operational measures within the field of national security have a responsibility to respect EU law enacted *outside* the field of national security impacted by such legislative or operational measures. In other words, should Article 4(2) be construed to create an area where EU law in its entirety does not apply? In one sense, the approach of the CJEU can be explained as a matter of claiming the right to determine – as guardians of the treaties – when matters do, or do not, fall within national security. I would argue, however, that the way the court has structured its argumentation may also carry implications for our understanding of the scope of EU law and the freedom of Member States to legislate within their exclusive areas of competence.

In the following sections I will analyze these questions, beginning with the matter of delineating different notions of security, before proceeding with the matter of the scope of EU law.

4.2 'You float like a feather' – The difficult delineation between national and public security

The previous outline of the contested space of national security may give the impression that the CJEU would be inclined to maintain a certain ambiguity regarding the concept of national security. This would allow the court to argue that a certain action by Member States may be deemed to belong under a concept (public security, for instance) where the court has a more arguable case of competence as it would not touch explicitly upon Article 4(2) TEU. However, the CJEU has in specific cases proven keen to draw a clear line between national security and neighboring concepts. In the recent Grand Chamber case of *Telekom Deutschland*, also dealing with data retention, the European Commission had argued in an observation to the court that

[91] See Sarah Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature Du Net and Others and Privacy International' (2022) 8 European Data Protection Law Review 143; Zalnieriute (n 11); Tzanou and Karyda (n 66).
[92] Turmo (n 24).

particularly serious crime could be treated in the same way as a threat to national security.[93] The CJEU however repeated the stance it has held in the *Garda* and *La Quadrature du Net cases*,[94] that:

> [T]he objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.[95]

The court continued by arguing that to treat national security and even particularly serious crime alike would create an intermediary category between the two and cause an intermingling of applicable requirements.[96] When national security *is* at stake, the CJEU has held that the importance of this objective goes beyond objectives such as 'combating crime in general, even serious crime, and of safeguarding public security'.[97] From a proportionality standpoint, it can therefore justify more serious interferences with fundamental rights as long as the other requirements in Article 52(1) of the Charter are fulfilled.[98] At the proportionality stage, the CJEU is thus keen to ensure that the proper security concept ends up on the scale in the balancing exercise. However, the delineation does not appear as interesting to the court in other respects.

In the case of *Commission v Poland (State printing office)*, the Advocate General had attempted to draw the boundaries of the concept of the state's *essential security interests*, included in the possibility of derogating from procurement rules established by Directive 2014/24. The AG noted that 'defining "security" in a precise and exhaustive manner is an impossible task'.[99] It was, according to the AG, dependent on a multitude of factors which could vary between Member States and over time, and the notion of 'essential security interests' was subject to inevitable subjectiveness where 'much depends on historical, political and geopolitical considerations which may vary from one State to the other'.[100] The recognition of this assessment, including

---

[93] *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* [2022] ECJ Joined Cases C-793/19 and C-794/19 92.
[94] *GD v The Commissioner of the Garda Síochána and Others* [2022] ECJ Case C-140/20 61; *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 135.
[95] *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* (n 93) 92; see also *GD v The Commissioner of the Garda Síochána and Others* (n 94) 61; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 74.
[96] *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH* (n 93) 94.
[97] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 74; *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 136.
[98] ibid.
[99] *Opinion of Advocate General Emiliou in European Commission v Republic of Poland* [2021] ECJ Case C-601/21 46.
[100] ibid.

significant discretionary aspects that Member States are likely more suited to assess, did not, however, carry over to the conclusion of the AG or the decision by the CJEU. The AG concluded that the term 'security' included in *essential security interests* corresponded to *national* security and *public security*, expressed in the various instruments and provisions of the treaties.[101] While referring to the previously mentioned definition of national security provided in *Garda,* the AG appears to accept a certain overlap, but one which has to be subject to strict review by the CJEU.[102] This reasoning was largely endorsed in the judgment by the CJEU.[103] Ølykke has argued that this reasoning makes it interesting to distinguish not so much which security term is used in a specific provision, but rather what type of security threats Member States are attempting to guard against and the conditions for and scope of the relevant derogations.[104] Ølykke notes that, while Poland did not rely on Article 4(2) TEU in the case, the CJEU still brought up national security as a term on its own accord – as did the AG – with one possible explanation being the lack of conceptual stringency by the court.[105] Like Ølykke, I would argue that there is a lack of stringency by the court, but one which may have developed gradually through what Millet has described as *copy-paste jurisprudence.*[106] Millet defines this as a type of analogy-reasoning and as a 'long-standing practice of the Court of Justice that consists in copying large amount of the text, irrespective of its legal status or normativity, of earlier judgments and pasting it, verbatim or with some alterations, into later judgments'.[107] Millet's analysis of this practice in the data protection context suggests that the copy-pasting technique of the CJEU in the name of analogy 'may foster competence creep to the detriment of both the Member States and the Union legislature'.[108] Millet's examples are primarily relating to how statements about the proportionality implications of the EU data retention directive made in Digital Rights Ireland have been copy-pasted by the CJEU into cases concerning different legislative frameworks and moving step by step from the context of EU-directives to review of national legislative measures and from the question of retention to questions of access to data.[109] However, Millet also makes the point that the CJEU 'opened up the scope of application of EU law, with the result of limiting Member States' competence […]'.[110]

As we have seen in the chronology presented in section 4.1, the CJEU has indeed more or less applied the same locution in settings varying from non-discrimination to public procurement, and, more recently, data protection. Whereas the court long stayed

[101] *Opinion of Advocate General Emiliou in European Commission v Republic of Poland* (n 99) 48.
[102] *Opinion of Advocate General Emiliou in European Commission v Republic of Poland* (n 99) 49–52.
[103] *European Commission v Republic of Poland* [2023] ECJ Case C-601/21 78.
[104] Grith Skovgaard Ølykke, 'Safeguarding "National Security" In a Public Procurement Context' (2025) 62 Common Market Law Review 1121, 1125.
[105] Ølykke (n 104) 1141.
[106] Millet (n 17).
[107] Millet (n 17) 1291.
[108] Millet (n 17) 1293.
[109] Millet (n 17).
[110] Millet (n 17) 1314.

clear of referring to national security, even when Member States used the term, it took the step in *La Quadrature du Net* and *Privacy International* to use the term explicitly in the otherwise repeated locution. This is in line with the understanding of copy-paste jurisprudence as defined by Millet. It also signifies that the CJEU no longer considers it necessary to base its competence on Member States acting outside the scope of Article 4(2) TEU. Having circled so many other concepts like public security, state security, and internal and external security, perhaps the CJEU eventually found that the sum of all these cases allowed it to explicitly take a step into the outright review of measures the court itself places under the term *national* security.

Future case law will likely shed more light on the implications of this step and whether the court now expressly sees itself having a more overall competency to review national measures within the context of national security. The effect of this approach, however, can potentially be that the CJEU will make its evaluation not only dependent on the specific term used, or the threat faced – as Ølykke argues – but also the *impact* of national measures on the effectiveness of EU law, a matter which we will now turn to.

4.3 'I don't belong here' – Pre-emption as competence creep in the context of national security

The second component I would argue warrants further discussion is whether the claim of jurisdiction by the CJEU carries further implications relating to our understanding of the *scope* of EU law. This implies a further question as to what extent Member States' national legislative or operational measures within the field of national security need to respect EU law enacted *outside* the field of national security impacted by such legislative or operational measures. This distinction between competence and impact can be explained through *pre-emption*. Despite rarely figuring in the case law of the CJEU, the concept of pre-emption has long been a subject of discussion in legal research. These discussions have focused on whether the concept, originating in United States federal law, is viable in the EU setting, if it adds anything beyond the concept of supremacy, and, if so, how these additions can be understood.[111] It is not my ambition to give a complete picture of the concept here, but as I will show, the national security argument provides a new context to illustrate the potential explanatory power of this concept under EU law.

At a general level, pre-emption can be understood as the question of *where*, and to *what degree* – rather than *if* – EU law should have primacy over Member State law. Pre-emption is dependent on the primacy of EU law, and while primacy in case of a conflict is clear from the treaties, pre-emption helps elucidate *where* primacy will come into play. Schütze has divided the concept of pre-emption in EU law into three

[111] See Marcus Klamert, 'Supremacy, Pre-Emption, and the Union Interest' in Marcus Klamert (ed), *The Principle of Loyalty in EU Law* (Oxford University Press 2014).

somewhat overlapping categories: field pre-emption, obstacle pre-emption, and rule pre-emption.[112]

The first of these – field pre-emption – is the most far-reaching. It occurs when the EU has created exhaustive legislation within a field, creating a situation where any national legislation within that field would interfere with Union law. As Schütze puts it, this can effectively turn an area of shared competence to one of *de facto* exclusive competence.[113] The second type – obstacle pre-emption – occurs when there is a material conflict between EU and national law. It is not, however, dependent on national law conflicting with a specific EU rule, but rather with the proper functioning of EU law or impeding the objectives of Union legislation.[114] It can be contrasted with the third type – rule pre-emption – which occurs when national legislation literally contradicts a specific EU rule, making compliance with both sets of rules '(physically) impossible'.[115]

Much of the existing discussion on pre-emption has focused on areas of *shared* competences – in particular EU external relations – as the concept is helpful to understand the friction that can occur when both parties exercise their legislative competence.[116] It has not, however, been explored as thoroughly in terms of EU action within an area of EU competence pre-empting Member State law in an area where the EU explicitly lacks competence. In this context, supremacy as a question becomes converted into the extent and significance of reserved areas of national sovereignty under the treaties. Despite this conceptual difference, some lessons can still be drawn from the external relations context, where Reuter as early as 2013 identified a shift away from the notion of *powers* towards the *scope of EU law*, 'in that questions of competence no longer determine the extent to which national action may be restrained',[117] resulting in significant compliance restraints characterized by two key features:

> Firstly, the scope of the restraints is no longer circumscribed by the limits of Union competence. Rather, the notably broader notion of 'scope of EU law' increasingly forms the basis for determining whether and to what extent Member States' freedom of action should be constrained in a given case. […] Secondly, the Member States are increasingly subject

[112] See Robert Schütze, 'Supremacy without Pre-Emption? The Very Slowly Emergent Doctrine of Community Pre-Emption' (2006) 43 Common market law review 1023, 1047.
[113] Schütze (n 112) 1040.
[114] Schütze (n 112) 1041.
[115] Schütze (n 112) 1042.
[116] See Schütze (n 112); Klamert (n 111); Amedeo Arena, 'Exercise of EU Competences and Pre-Emption of Member States' Powers in the Internal and the External Sphere: Towards "Grand Unification"?' (2016) 35 Yearbook of European Law 28; Paul Luif, 'The Division of Powers/Competences Between the EU and the Member States: What Can We Learn from Pre-Emption in the United States?' in Lucia Serena Rossi and Federico Casolari (eds), *The EU after Lisbon: Amending or Coping with the Existing Treaties?* (Springer International Publishing 2014).
[117] Kristin Reuter, 'Competence Creep via the Duty of Loyalty? : Article 4 (3) TEU and Its Changing Role in EU External Relations' (Thesis, European University Institute 2013) 252.

> to obligations of result. Such restraints range from the obligation to eliminate existing incompatibilities with EU law to the avoidance of future conflicts by precluding Member State action altogether through the imposition of a duty to abstain from acting unilaterally.[118]

Reuter has characterized this as a form of *competence creep*, and similar points have been made by Prechal, who has shown how general principles of EU law have limited Member State action through their application by the CJEU in areas where the scope of EU law is unclear. One of her conclusions is that '[a]s soon as Member State action or, in more neutral terms, "a situation" can be situated within the scope of EU law, various limits have to be observed, including those imposed by general principles of law. These limits are often perceived as a loss of sovereign powers and for that matter creeping competences of the EU'.[119] It is likely that similar dynamics have come to play out in the context of national security.

Taken together, this highlights the need to consider not only whether something is (solely) a Member State competence, but whether that competence can be exercised in light of existing EU law commitments.

At this point in the evolution of CJEU case law, it can be challenging to identify whether any pre-emption in play in the previously covered case law would be expressions of obstacle pre-emption or rule pre-emption, but given the exclusive competence of Member States in national security concerns, it remains unlikely to extend as far as field pre-emption.

In *La Quadrature du Net*, the CJEU applied the requirements of the ePrivacy directive, read in light of the Charter, to the French retention legislation. This application of the directive hinged on the fact that retention obligations extended to private companies, which implied exceptions to their obligations of preserving confidentiality for electronic communication under the ePrivacy directive.[120] Similarly in *Privacy International*, the obligations placed on private companies to transfer data to national security agencies interfered with their competing obligations under the directive.[121] This was despite those requirements being implemented on national security grounds. As put by Mitsilegas et al, '[t]he source of the obligation imposed on the private sector is thus immaterial. What matters in order for EU law to apply is the actual activity performed by the private sector'.[122] Consequently, the implementation of such requirements interfered with requirements under EU law and needed to comply with the possibilities to make legitimate derogations from those instruments,

---

[118] Reuter (n 117) 252.
[119] Sacha Prechal, 'Competence Creep and General Principles of Law' (2010) 3 Review of European Administrative Law 5, 6.
[120] See *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 101–102.
[121] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 12) 46.
[122] Valsamis Mitsilegas and others, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2023) 29 European Law Journal 176, 180–181.

including the requirements of the Charter. Importantly, the ePrivacy directive includes in Article 15.1 a possibility for Member States to adopt legislative measures that restrict, among other provisions, the scope of the confidentiality of communications, when such a restriction 'constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security'. This derogation clause implied in the eyes of the CJEU that the directive was applicable in relation to legal requirements placed on private parties in the national security context, as there had otherwise been no need to include an explicit derogation. However, the question which both cases hinged on was whether the derogations made had been proportional, taking into account responsibilities under the Charter.

However, the CJEU differentiated their conclusion against measures that would interfere with confidentiality *without* imposing processing obligations on providers of electronic communications services. In that situation the protections of confidentiality under the ePrivacy regulation would not apply. Instead, the processing would have to 'comply to national law only, subject to the application of [the Law Enforcement Directive], with the result that the measures in question must comply with, *inter alia*, national constitutional law and the requirements of the ECHR'.[123] This has been taken as implying that the CJEU sees the Law Enforcement Directive as applying to public agencies when processing data for national security purposes.[124] This is however not entirely clear from the wording 'subject to'.[125] Instead, I would argue that the CJEU simply states that, if not governed by the GDPR/ePrivacy due to the involvement of private parties subject to those instruments, public bodies would operate under national rules and the ECHR, and possibly the LED – depending on whether the processing falls under its area of application. It is indeed likely that the CJEU was hesitant to exclude the possibility of the LED being applicable, given that the French retention law straddled the line between national security and public security policing. With this caveat in mind, I would argue that the rulings in *La Quadrature du Net* and *Privacy International* exhibit characteristics of rule pre-emption, where the involvement of private telecommunications providers in legislation enacted within the exclusive Member State domain of national security made it impossible for those providers to preserve anonymity in line with requirements in the ePrivacy directive and disproportionately undermined the protection of fundamental rights as a consequence. In other words, Article 4(2) TEU does not create a legislative *carte blanche* if measures taken to further national security impacts the effectiveness of EU law.

---

[123] *La Quadrature du Net and Others v Premier ministre and Others* (n 12) 103.

[124] Zalnieriute (n 11) 212.

[125] While the phrase 'subject to' may imply a requirement, most plain language definitions of the term include a conditional element, that something is possibly affected (by something). 'What Does "Subject to" Mean? | Britannica Dictionary' <https://www.britannica.com/dictionary/eb/qa/What-Does-Subject-to-Mean-how-to-use> accessed 27 February 2025; 'Definition of SUBJECT TO' (16 February 2025) <https://www.merriam-webster.com/dictionary/subject+to> accessed 27 February 2025.

If we look back to the earlier generations of cases, there are signs of the CJEU applying something akin to obstacle pre-emption through the recognition of how a general exception to EU law, regardless of the specific requirements laid down by the Treaty, would be liable to impair the binding nature of Community law and its uniform application. It suggests a notion that whatever the Member States do within their own competence, it better not interfere with the functioning of EU law in those fields where the EU *has* competence. This shifts the discussion from what states are trying to achieve (safeguarding national security for instance) to how the measures taken impact EU law more generally. This could have important implications for the ambitions of Member States in the context of artificial intelligence, given the extensive EU regulation relating to data protection and more recently AI as such. A matter we will now turn to.

5. 'I don't care if it hurts' – AI as a new frontier in the struggle for competence

In this article, I have endeavored to show how the national security argument, more specifically the argument that national security measures fall outside the scope of EU law, has been discussed in and impacted Swedish national policy and legislation in the context of implementing AI in policing. Furthermore, I have analyzed to what extent such arguments have historically held up to scrutiny before the CJEU. I have found that the case law emanating from the CJEU in this context has developed through copy-paste jurisprudence in a way where measures taken within the context of national security are not necessarily exempt from EU law requirements. Indeed, measures taken by Member States within the national security context will need to carefully avoid impacting the effectiveness of EU law even if the scope of EU law formally does not extend into that domain. In this final section, I will attempt to outline some of the possible implications of these developments in relation to the ambitions of Member States in relation to the implementation of AI in policing.

As a first point, Member States have historically had little luck in arguing for a wholesale lack of competence of the CJEU over measures they have taken in the national interest, whether that is for national security, public security, internal or external security, or similar aims. It remains, however, a reoccurring argument from Member States before the CJEU, given the treaty provisions making national security a matter of their exclusive competence. Despite these provisions, we can see that in practice the CJEU has chosen to intervene when measures Member States have taken in the national security domain impact the effective implementation of EU law. While this can be viewed as an expression of *competence creep*, the cases where this practice has developed also show that what the court has primarily been cautious of is accepting Member States' use of the national security argument as a wholesale 'get out of jail card' when their measures impact EU law obligations. However, once the matter of applicability of EU law has been settled and the CJEU continues into the substantive legal issues, the security interests of the state have indeed often played a significant role in the overall proportionality assessment of the court. The significance and weight of these state interests have likely played a role in why the CJEU has been keen to guard against concept creep. I would argue that the risk of

undermining fundamental rights protections established in legal frameworks such as the ePrivacy directive and the LED by excluding significant aspects of modern policing from their ambit speaks in favour of this strict review by the CJEU.

Another key implication follows from the way the CJEU appears to use something akin to rule or obstacle pre-emption. It implies that Member States may be more successful in using the national security argument where measures do not impact actors or sectors subject to competing EU law obligations. In *La Quadrature du Net* for instance, this included the obligations of telecommunications providers to safeguard the secrecy of communications and the privacy of their customers. In other words, where Member States implement more *direct* and *discreet* measures used directly by national security agencies, the risk of interfering with the proper application of EU law decreases.[126] This potentially includes measures such as the bulk collection of data from the open internet directly by national security agencies (such as the Swedish Security Service) to facilitate AI training and analysis by these agencies, like the mandates Sweden has recently proposed. In these proposals, private actors are not involved and not subject to obligations to cooperate or undermine confidentiality requirements. Similarly, the direct and discrete use of hacking by national security agencies, with no corresponding requirement for other private or public entities to cooperate, may have a better chance of arguing for compliance with EU law obligations under the current interpretation of the CJEU than measures that would, for instance, force private actors to undermine encryption protocols or provide backdoors.

The viability of the national security argument is likely to decrease significantly when claimed by actors subject to conflicting EU law obligations, regardless of whether these actors may have tasks that support national security efforts. This includes actors subject to the LED like the Swedish Police Authority. Given the stringent and narrow interpretation of measures that are to be seen as pursuing national security, in combination with the willingness of the CJEU to review measures impacting competing EU law obligations, it is very likely that attempting to extend the exceptions from EU law carved out for national security agencies to the regular police are poised to fail. Given that the CJEU has gradually begun leaning more on fundamental rights than specific provisions of the LED in their review of the necessity and proportionality of measures in the law enforcement context, this would likely hold true even in the face of potential reforms of the LED.

Finally, while the jurisdiction of the CJEU on measures taken to promote what Member States perceive of as national security interests is likely to remain a point of contestation in the interpretation of EU law and its scope, it should be said that the approach taken by the CJEU is not without merit. The narrow interpretation of national security, along with the application of pre-emption-like considerations, have served to prevent Member States from implementing measures that would indeed

[126] See also Plixavra Vogiatzoglou and Stefano Fantin, 'National and Public Security Within and Beyond the Police Directive' 29 <https://papers.ssrn.com/abstract=3466821> accessed 1 January 2026.

likely undermine not only the effective implementation of EU law, but important fundamental rights as well. Indeed, if the CJEU's approach continues, it is likely to play an important role in helping other instruments, like the recently adopted AI Act, to fulfil its potential in relation to the use of AI in the policing context. While the Act includes several exceptions and accommodations for law enforcement use of AI, it also includes some red lines relating to the use cases the EU legislator has found to be associated with unacceptable risks for society and fundamental rights. The limited chance of success in carving out substantial exceptions to the overall application of EU law in areas closely related to national security reduces the risk of national ambitions expanding the police use of AI beyond the restrictions of the AI Act under the guise of national security. In this sense, the approach of the CJEU in national security case law holds the door open for a strict review of AI technologies implemented in the law enforcement context going forward. However, it would come at the cost of continued clashes with Member State policies in areas they now more forcefully defend as their exclusive domain under the treaties.