



ARTICLES

PUBLIC ORDER AND PUBLIC SECURITY IN EU LAW

edited by Ségolène Barbou des Places

PUBLIC SECURITY AND PUBLIC ORDER IN EU LAW: ADJUDICATIVE CHALLENGES IN THE LAWS OF THE INTERNAL AND DIGITAL MARKETS

XAVIER GROUSSOT* AND GUNNAR THOR PETURSSON**

TABLE OF CONTENTS: I. Introduction. – II. Methodological basis for public policy/security issues in the context of free movement law. – III. Proportionality in free movement law and the EU Charter: a comparison. – IV. The “strictly necessary” test and the “balancing test” in light of the digital case Law of the CJEU. – IV.1. “Strictly necessary” test. – IV.2. Balancing test. – V. National security and national courts in the internal and digital markets. – VI. Conclusions.

ABSTRACT: The digital era has brought about new security challenges. Security in the digital context is neither border centric nor a traditional security threat that can be contained into individual behaviour or which respects traditional borders. It may affect both privacy issues at the individual level and state security. What does this mean for the tools and adjudicative methods of EU law which are used to deal with security issues? Traditionally, national security issues have been state-centric: in the assessment of Member States’ reaction, based on public security/public order issues, the focus has very much been on the *appropriateness* of States’ response. In this context (of mass surveillance and anti-terrorism), there is simultaneously an ongoing battle as to who – the national court or the CJEU – ultimately controls the ambit of core concepts of EU law, namely *national security*, *public security* and *public order*? And where is the “battlefield”: in classic free movement or in secondary legislation? This tension is reflected in number of fundamental rulings of the CJEU that form the core of this *Article*. This *Article* asks whether the traditional adjudicative tests developed under the classic free movement case law are still relevant in the current climate. We focus on the role of proportionality and on the role of the EU Charter of Fundamental Rights (EUCFR) which is both the starting point of any legal analysis under EU law but also brings with it its own methodological framework and a new test of proportionality enshrined in art. 52(1) EUCFR.

KEYWORDS: public security – public order – EU Charter of Fundamental Rights – proportionality – EU free movement – digital market.

* Professor of EU Law, Lund University, xavier.groussot@jur.lu.se.

** Professor of EU/EEA Law, Reykjavik University, gunnarthor@ru.is.



I. INTRODUCTION

The digital era has brought about new security challenges, that we may know too well. What we know by now is that security in the digital context (digi-security) is neither border centric nor a traditional security threat that can be contained into individual behaviour or which respects traditional borders. It may affect both privacy issues at the individual level and, importantly, state security, as demonstrated by the different data attacks which have already occurred.

Digitalization is breaking boundaries in this sense. The digital field is now marked by an influx of EU regulations. What we see with the Digital Single Act (DSA),¹ Digital Market Act (DMA)² and the Artificial Intelligence Act (AIA)³ are frequent references to public policy, public security and the issue of crisis and response, but we also see – especially so within the DSA – frequent references to the EU Charter of Fundamental rights. In this article we will also particularly raise issues related to the e-privacy⁴ and PNR regulations⁵ as well as more recent regulations, such as Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online.⁶

What does this mean for EU law and, more particularly, for the tools and adjudicative methods of EU law which are used to deal with security issues? Arguably, traditionally national security issues, at least in EU law, have been state centric, in the sense that, under EU law and in the assessment of the CJEU of Member States' reaction, based on public security/public order issues, the focus has very much been on the *appropriateness* of the response of the State. In this context (of mass surveillance and anti-terrorism), there is simultaneously an ongoing battle as to who ultimately controls the ambit of core concepts of EU law – namely, *national security*, *public security* and *public order*. Is it the national court or the CJEU which will ultimately call the definition and application of these concept? And where is the "battlefield"? Is it located in classic free movement, or in

¹ Regulation (EU) 2025/2022 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

² Regulation (EU) 1925/2022 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

³ Regulation (EU) 1689/2024 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, (E) 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).

⁴ 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).

⁵ Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

⁶ Regulation (EU) 784/2021 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

secondary EU legislation? This tension is reflected in number of fundamental rulings of the Court of Justice of the European Union (CJEU) that will form the core of this *Article*.

We aim to answer the question of whether the traditional adjudicative tests developed under the classic free movement case law are still relevant in the current climate. Are we able to draw a methodological link between the old and the new, or has everything changed? We will focus on the role of proportionality – which is the common thread – and the role of the EU Charter of Fundamental Rights (EUCFR) – which arguably is both the starting point of any legal analysis under EU law, nowadays, but also brings with it its own methodological framework and a new test of proportionality enshrined in art. 52(1) EUCFR. We will start to briefly revisit the classic approach in free movement up to more recent cases in that field. Thereafter, we will move into the issue of the role of secondary norms in the digital era with a focus on security (digi-security), as they now must be interpreted in the light of the EU Charter. What *similarities* we can draw from the classic logic of free movement and what has *changed*? Is this a visible or invisible change taking place in the context of digitalization and increased regulation at the EU level in this field, or is it much about same methods, but different context?

II. METHODOLOGICAL BASIS FOR PUBLIC POLICY/SECURITY ISSUES IN THE CONTEXT OF FREE MOVEMENT LAW

It is true that the concept of security appears in different contexts of EU law. However, already since the founding of the European Economic Community, the basic provisions on free movement include explicit provisions which allow the Member States to derogate from the fundamental freedoms with reference to public policy and/or public security.⁷ These derogations are interests, fundamental to states, listed also with public health and public morality (for free movement of goods). The conditions for application of these provisions were not spelled out in the founding Treaties, or in subsequent amendments (save some clarifications for the free movement of capital). Therefore, these concepts and their analytical framework have had to be articulated further through interpretation by the CJEU.

⁷ The case law on public policy (public order) and public security and even public interests (public order in that context) is marked by complexity due to overlapping in the use of concept. See for discussion C Kessedjian, 'Public Order in European Law' (2007) Erasmus Law Review 25, who highlighted the conceptual confusion here, and pointed out that in French law there is a conceptual difference between public policy (*loi de police*) and public order (*ordre public*), although admitting it was unclear whether that distinction extended beyond French law, at C Kessedjian, 'Public Order in European Law' cit. 26-27. See also R de Lange 'The European Public Order, Constitutional Principles and Fundamental Rights' (2007) Erasmus Law Review 3, 3-14, who argued that the concept of public order is a multifaceted concept in EU law, but in its narrower sense the concept may be synonymous with the public security concept in EU law. He has also pointed out that it is common in case-law on fundamental rights, in Europe that public policy considerations are "trumped" by fundamental rights, and that in exercise of fundamental rights, they generally feature as a basis for limitations of those rights, rather than the foundation (R de Lange 'The European Public Order, Constitutional Principles and Fundamental Rights' cit. 7-9).

The roots of the public policy/security case law of the CJEU lie in the *Van Duyn* case,⁸ which is the first reference from the UK High Court to the Court of Justice, but also the first time the CJEU had to define the scope of the public policy and public security derogations. The main question was the justification of the refused leave to enter the UK of Ms Van Duyn, a Dutch citizen, due to her relation to the Church of Scientology. The UK had, as of 1968, by the adoption of a Governmental policy, considered the activities of the Church of Scientology to be “socially harmful”. In the case, the CJEU stated that the concept of public policy in the context of Community law should be interpreted *strictly* and that its scope could not be determined *unilaterally* by the Member States without being subject to control by the institutions of the Community, and furthermore that: “[T]he particular circumstances justifying recourse to the concept of public policy may vary from one country to another and from one period to another, and it is therefore necessary in this matter to allow the competent national authorities an area of discretion within the limits imposed by the Treaty”.⁹

Two important elements emerge from this ruling. Firstly, that the concept ‘public policy’ is not a “state” concept, but a concept under the control of the European institutions; its scope could therefore not be “determined unilaterally” by the Member States. This was contrary to the view of AG Mayras, who maintained that it was not possible to deduce from the Treaties “a community concept of public security”.¹⁰ Secondly, the margin of appreciation doctrine was introduced – the role of which remains quintessential in this type of case, and of course, beyond.¹¹

In cases following *Van Duyn*, the CJEU seemingly limited the wide margin that it had allowed the State in that case, and it held that a person who is being expelled on grounds of public policy has to be of “a genuine and sufficiently serious threat to the requirements of public policy affecting one of the fundamental interests of society”.¹² Furthermore, certain consistency requirements were laid down in the case of *Adoui and Cornuaille v Belgian State* (hereinafter *Adoui and Cornuaille*).¹³ In the *Église de scientologie* case,¹⁴ the CJEU elaborated and developed a test of proportionality applicable to evaluate the public

⁸ Case 41/74 *Van Duyn v Home Office* ECLI:EU:C:1974:133.

⁹ *Ibid.*

¹⁰ *Ibid.*

¹¹ Interestingly the result in *Van Duyn* cit. is not that different from the result in *Handyside* (ECtHR *Handyside v. The United Kingdom* App n. 5493/72 [7 December 1976]), a case decided by the Court of Human Rights in Strasbourg shortly after *Van Duyn* cit., and which is generally considered to be the case where the margin of appreciation doctrine emerged, but as it has appeared in the Strasbourg multiple times since.

¹² Case 30/77 *Regina v Bouchereau* ECLI:EU:C:1977:172.

¹³ Joined cases 115/81 and 116/81 *Adoui and Cornuaille v Belgian State* ECLI:EU:C:1982:183. A side-step of a kind is to be found in, case 72/83 *Campus Oil* ECLI:EU:C:1984:256, where the Court for the first time addressed the derogation under art. 36 TFEU based on the grounds of public security. After having established that the level of the existing Community rules was not sufficient for the protection of the stated interest, it concluded that it was possible for a Member State to have recourse to a derogation under art. 36 TFEU, on the basis of public security, even though there were some Community rules on the matter in place (*Campus Oil* cit. para. 31). However, such a derogation is to be subject to the compliance with the principle of proportionality.

¹⁴ Case C-54/99 *Église de scientologie* ECLI:EU:C:2000:124.

order/policy and public security measures adopted by the Member State in the field of free movement. The CJEU made clear that “derogations from the fundamental principle of free movement of capital, be interpreted strictly, so that their scope cannot be determined unilaterally by each Member State without any control by the Community institutions”, a point already found in *Van Duyn*.¹⁵ This is so since even Member States are still, in principle, free to define the conditions of public order/policy and public security in the light of their national needs. The core idea behind this is to secure control of the definition of ‘public security’ at EU level and thus to curtail the powers of the Member States, a line of jurisprudence very similar to the post *Van Duyn* case law in the field of free movement of persons and the definition of public order.

In *Église de scientologie* the CJEU puts its previous case law in the context of an elaborated double test of proportionality that resembles the classical test of proportionality based on the need to evaluate the *suitability* and *necessity* of the Member State measure derogating from EU law. In the first place, because it stems from para. 17, public policy and public security may be relied on only if there is a genuine and sufficiently serious threat to a fundamental interest of society. In other words, the objective of the derogating measure to free movement law must be suitable. In the second place, because it stems from para. 18, measures which restrict the free movement of may be justified on public-policy and public-security grounds only if they are necessary for the protection of the interests which they are intended to guarantee and only in so far as those objectives cannot be attained by less restrictive measures.¹⁶ In that context the CJEU also emphasized that the national measures must also respect procedural requirements (a point further elaborated beyond).¹⁷

This double test of proportionality, which is epitomized by the *Gebhard*¹⁸ case law in the field of free movement of establishment and overriding reasons of public interest in 1994, is the traditional test relied on by the CJEU in assessing derogations in the internal market, such as public policy and public order derogations to free movement law. In very few instances, the CJEU relied on a three-pronged test that includes a balancing test (as a third part of the test) between the public interest (such as public security) and the private interest protected by free movement law. This balancing test was notably used by the CJEU in the *Schmidberger* case in which an EU fundamental right, namely the right to freedom of expression had to be balanced with the free movement of goods.¹⁹ In contrast, and as can be seen in recent free movement cases that concern public policy and public security and also rely on procedural guarantees, such as eg. *Commission v Hungary* (rule of law/public

¹⁵ *Ibid.* para 17.

¹⁶ *Ibid.* para 18.

¹⁷ As may be seen from cases such as case 222/86 *Unectef v Heylens* ECLI:EU:C:1987:442 paras 14 and 15.

¹⁸ Case C-55/94 *Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano* ECLI:EU:C:1995:411.

¹⁹ Case C-112/00 *Schmidberger* ECLI:EU:C:2003:333 this case includes a lot of references to ECtHR case law. See also more recently, case C-128/22 *NORDIC INFO* ECLI:EU:C:2023:951.

security/public policy)²⁰ and *Xella Magyarország* (security of supplies)²¹; it appears that *Église de scientologie* and its double test of proportionality still constitute the chosen methodology for free movement and public policy/security issues.²²

III. PROPORTIONALITY IN FREE MOVEMENT LAW AND THE EU CHARTER: A COMPARISON

The key questions of this contribution are, firstly, whether the traditional methodology used within internal market law is transposable to the new framework created by the entry into force of the EU Charter of Fundamental Rights and, secondly, whether this methodology is also applicable within the harmonized field of EU law when Member States are implementing EU law and are relying on public security and national security to derogate from certain obligations imposed by the EU legislature in the digital market. This situation is for instance illustrated by art. 15 of the e-privacy Directive that allows exceptions to certain obligations of the directive based on public policy, public security or national security.²³

To answer these questions, it is necessary to look at the text of the EU Charter and notably to its art. 52(1) EUCFR, which incorporates a horizontal proportionality test to evaluate the legality of the scope of intervention of a Member States in derogating from a fundamental right falling within the scope of EU law and thus protected by the EU Charter.²⁴ According to art. 52(1) of the Charter: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

²⁰ Case C-66/18 *Commission v Hungary (Enseignement supérieur)* ECLI:EU:C:2020:792.

²¹ Case C-106/22 *Xella Magyarország* ECLI: EU:C:2023:568. See X Grousot, S Michael, and E Mlynarcikova, 'The Screening of Foreign investments in EU Law: When Security and Public Order Become the New Black in Internal Market Laws and Policies' (2024) *Nordic Journal of European Law* 25.

²² What is noteworthy in *Commission v Hungary (Enseignement supérieur)* cit. para. 204) is that the CJEU is relying on the *Église de scientologie* cit. methodology – but is adding the word "present" threat, which is not to be found in *Église de scientologie* cit. case – but is in the 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, 75/35/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, art. 27.

²³ See Directive 2022/58 cit.

²⁴ For an extensive discussion on art. 52(1) EU Charter, see X Grousot and GT Petursson, 'The EU Charter of Fundamental Rights Five Years On: The Emergence of a New Constitutional Framework?' in S de Vries, U Bernitz, S Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing* (Hart 2015) 135; and of the same authors, X Grousot and GT Petursson, 'Je t'Aime...Moi Non Plus: Ten Years of Application of the EU Charter of Fundamental Rights' (2022) *CMLRev* 239.

Art. 52(1) EU Charter provides a methodological framework to test the proportionality of the limitations (derogations) when a state measure falling within the scope of EU law under art. 51 EUCFR is adopted and limits the application of a right enshrined within the Charter:²⁵ (a) the limitation must be provided for by law; (b) the limitation must respect the essence of the fundamental right; and (c) the limitation must be necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. In this article, we focus only on the last part of the framework, since it is the part of the framework that connect the most adequately with the free movement case law of the CJEU concerning public policy, public security and public order. The first sentence of art. 52(1) EUCFR is closely connected to the framework used in the European Convention of Human Rights and in certain Member States such as Belgium and Germany when it comes to the application of the “essence test”.²⁶

If one compares the last sentence of art. 52(1) EU Charter with *Église de scientologie* and the double test of proportionality, it is possible to speck similarities.²⁷ Indeed, the text of the last sentence can clearly be read as providing a double test of proportionality based on necessity and suitability (limitations must genuinely meet objectives of general interest). However, as we shall soon see in detail, the recent case law of the CJEU concerning public security in the harmonized digital field of EU law (unlike the free movement case law) does not provide an analytical framework based on suitability and necessity. And it instead provides a framework based on (a) assessing whether the State measures are “strictly necessary” and (b) relying on a balancing test to be conducted between the public interests and the private interests at issue. This is a different framework from EU free movement; and this new framework should be now studied in detail considering the recent digital case law of the CJEU relating to public security and public policy in this harmonized field.

IV: THE “STRICTLY NECESSARY” TEST AND THE “BALANCING TEST” IN LIGHT OF THE DIGITAL CASE LAW OF THE CJEU

The CJEU has developed in its case law on digital markets a two-pronged test of proportionality that differs from the text of art. 52(1) EUCFR, and which originates from the *Digital Rights*²⁸ and *Tele 2 Sverige* cases.²⁹ On the one hand, the balancing test which is now used by the CJEU does not explicitly mention the text of art. 52(1) EU Charter. On

²⁵ For discussion on art. 51 EU Charter, see X Groussot, L Pech and G T Petursson, “The Reach of EU Fundamental Rights on Member State Action after Lisbon” in S De Vries, U Bernitz, and S Weatherill (eds), *The Protections of Fundamental Rights in the EU after Lisbon* (Hart 2013) 97-118.

²⁶ Only a few Member States in the European Union relied on the essence test at the national level.

²⁷ *Église de scientologie* cit.

²⁸ Joined cases C-293/12 and C-594/13 *Digital Rights Ireland and Seitlinger and Others* ECLI:EU:C:2014:238 para. 51.

²⁹ Joined cases C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C:2016:970.

the other hand, the “strictly necessary test” which bears textual resemblance with the necessary test in EU free movement has been interpreted differently from the free movement case law by incorporating not only elements related to the issue of suitability but also integrating a strong procedural logic (which in fact can sometimes be spotted in the free movement case laws). This mixed approach makes the “strictly necessary” test very difficult to understand if compared with the rather straightforward and two-pronged logic used in the free movement case law based on suitability and necessity.

IV.1. “STRICTLY NECESSARY” TEST

Concerning the “strictly necessary test”, in *Tele 2 Sverige*³⁰ the CJEU has built on *Digital Rights*. It ruled that in the implementation of art. 15(1) of Directive 2002/58, though the effectiveness of the fight against serious crime (in particular organised crime and terrorism), may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.³¹

The CJEU considered that the Swedish legislation permitting the general and indiscriminate retention of all traffic and location data exceeds the limits of what is strictly necessary and cannot be justified, within a democratic society, as required by art. 15(1) of Directive 2002/58 read in the light of arts 7, 8 and 11 and arts 52(1) of the EU Charter.³² The Court clearly stated that this provision of the e-privacy directive “does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary”.³³ In order to fulfil these conditions, the national legislation must, initially, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards.³⁴ These conditions constitute clear procedural requirements.

In *Tele 2 Sverige*,³⁵ the CJEU relied on a procedural safeguard logic to test the proportionality of national legislation implementing EU secondary legislation and to review the national implementing legislation for compliance with substantive norms enshrined in

³⁰ *Ibid.*

³¹ *Ibid.* para. 101. See also *Digital Rights Ireland and Seitlinger and Others* cit. para. 51.

³² *Ibid.* para. 107.

³³ *Ibid.* para. 108.

³⁴ *Ibid.* para. 109. See also *Digital Rights Ireland and Seitlinger and Others* cit. para. 54.

³⁵ See *Tele2 Sverige* cit. and case C-511/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791 para. 132; case C-140/20 *Commissioner of An Garda Síochána* ECLI:EU:C:2022:258; and case C-269/22 *IP and Others (Établissement de la matérialité des faits au principal – II)* ECLI:EU:C:2023:275.

the EU Charter.³⁶ In a similar vein, in *Opinion 1/15*, the Court ruled that procedural requirements in legislation, *in casu* the Passenger Name Record (PNR) Agreement between the EU and Canada must be satisfied in order to pass the so-called strictly-necessary aspect of the proportionality test.³⁷ The PNR agreement was declared incompatible with the art. 7, 8 and 52(1) of the EU Charter, and the CJEU recommended that the EU legislation must determine in a clear and precise manner the PNR data to be transferred from the EU to Canada. As stated by the CJEU, “In order to satisfy that requirement, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse”.³⁸ Importantly, the CJEU after *Opinion 1/15* has confirmed this procedural approach of proportionality to national legislation implementing EU law (thus confirming *Tele 2 Sverige*,³⁹ – e.g. in *La Quadrature du Net*,⁴⁰ *Commissioner of the Garda Síochána*⁴¹ and the more recent *HYA* case.⁴² In all these instances, the CJEU relied on the *Digital Rights* “procedural safeguard logic” to test the proportionality of national legislation implementing EU secondary legislation and to evaluate whether the national legislation was “strictly necessary”.

This evolution in the direction of procedural review within the “Strictly Necessary test” was further developed as exemplified by the judgment in *Commissioner of the Garda Síochána*, in which the CJEU reviewed national legislation for compliance, *inter alia*, with the right to the protection of personal data enshrined in art. 8 of the Charter. The CJEU, in this case, considered that,

“In order to satisfy the requirement of proportionality, the national legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary”.⁴³

³⁶ See *Digital Rights Ireland and Seitlinger and Others* cit. The roots of the procedural logic of the CJEU are to be found in this case which concerns a preliminary ruling on validity.

³⁷ *Opinion 1/15 EU-Canada PNR Agreement* ECLI:EU:C:2017:592 para. 140. *Opinion/15* concerns the validity of the PNR agreement.

³⁸ *Ibid.* para 141.

³⁹ *Tele2 Sverige* cit.

⁴⁰ *La Quadrature du Net and Others* cit. para. 132.

⁴¹ *Commissioner of An Garda Síochána* cit.

⁴² *IP and Others (Établissement de la matérialité des faits au principal – II)* cit.

⁴³ *Commissioner of An Garda Síochána* cit. para. 54. See also *Tele2 Sverige* cit. paras 117 and 118; case C-623/17 *Privacy International* ECLI:EU:C:2020:790 para. 68; and *La Quadrature du Net and Others* cit. para. 32.

This passage clearly echoes the logic used in the free movement case law when it comes to verifying the existence of procedural safeguards before moving to assess whether the national measure complies with the substantive elements of the proportionality principle.⁴⁴

This reading is evident in those digital market cases that specifically concern the enjoyment of the right to privacy and the right to data protection enshrined in arts 7 and 8 of the EU Charter. In case of a lack of procedural safeguards, the CJEU may consider that the substantive EU law rights cannot be properly exercised by an individual, therefore leading to a breach of EU law and to the finding that the national legislation is disproportionate on the basis that the national legislation is too intrusive and therefore is not strictly necessary to ensure the goals of public policy and public security. In the fields of privacy and data protection, the national legislation cannot be constrained to requiring that the domestic authorities' access to such data should relate to the objective pursued by that legislation but must also lay down the substantive and procedural conditions governing that use.⁴⁵

In the recent case law, and besides this procedural approach taken in relation to the "strictly necessary" test and developed since *Digital Rights* and *Tele 2 Sverige*, the CJEU has also clarified what it means when interpreting the limitations in light of the objectives of general interest recognised by the Union as required by the second sentence of Article 52(1) EUCFR. The AG case from 2023, which is a preliminary ruling reference from the Supreme Court of Lithuania, provides an enticing example of this evolution.⁴⁶ Again in this case, the CJEU had to interpret the scope of art. 15(1) of the e-privacy directive in the criminal law context where art. 19(3) of the Law on criminal intelligence provided that the data may be used to investigate not only serious criminal offences, but also disciplinary misconduct or misconduct in office related to acts of corruption.

The CJEU made clear that only action to combat serious crime and measures to prevent serious threats to public security can justify serious interference with the fundamental rights enshrined in arts 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data, whether the retention be general and indiscriminate or targeted. In other words, arts 7 and 8 of the Charter can be justified only for the purposes of combating serious crime and preventing serious threats to public security, thus denying

⁴⁴ See *Église de scientologie* cit. para. 17; Case C-22/18 *TopFit and Biffi* ECLI:EU:C:2019:497 para. 65 and Case C-78/18 *Commission vs Hungary (Transparency of associations)* ECLI:EU:C:2020:476.

⁴⁵ See also case C-146/18 *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* ECLI:EU:C:2021:152 para. 49; *Privacy International* cit. para. 77; *La Quadrature du Net and Others* cit. para. 176. In *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* cit. para. 49, it is stated that "national legislation governing the access of the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use".

⁴⁶ Case C-162/22 *Lietuvos Respublikos generalinė prokuratūra* ECLI:EU:C:2023:631.

the possibility of using the data concerned for the investigation of corruption-related misconduct in office.⁴⁷ In the AG case, the CJEU really went deep into the analysis of the public objectives that are capable of justifying a limitation of the rights and obligations laid down in the e-privacy directive.⁴⁸ As put by the CJEU, “in accordance with the principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entail”.⁴⁹ And the Court also stressed that the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.⁵⁰ It concluded that, while the fight against serious crime and the prevention of serious threats to public security are of lesser importance in the hierarchy of objectives of public interest than the safeguarding of national security, their importance is, however, greater than that of fighting crime generally and of preventing non-serious threats to public security.⁵¹

This special attention given to the types of objectives relied on national authorities to justify a limitation to the fundamental rights to privacy and data protection guaranteed by the Charter shows that the CJEU comes very close to reproducing a suitability test, which is often relied on in the field of free movement law to test the proportionality of national measure derogating from EU law (and this in light of assessing the suitability of the objectives) and the appropriateness of the public objectives. However, in the digital market case law of the CJEU, this test is realized within the framework of the “strictly necessary” test and not within the framework of an explicit suitability test. The approach of the CJEU in the application and interpretation of the “strictly necessary test” reflects thus a mixed and procedural approach. This approach differs from the necessity test used in free movement and internal market laws. Yet, it incorporates methodological elements apparent in the free movement case law that relates to the evaluation of the suitability of the derogating measures and connects to the need to respect specific procedural requirements. It is now important to look at the balancing test used by the CJEU in its digital market case law concerning public security and public policy.

IV.2. BALANCING TEST

It is apparent from the digital market case law of the CJEU related to arts 7 and 8 of the Charter that the core of its proportionality assessment is based on a balancing the test

⁴⁷ *Ibid.*

⁴⁸ *Ibid* para. 34.

⁴⁹ *Ibid.* para. 35. See also *Commissioner of An Garda Síochána* cit. para. 56.

⁵⁰ *Ibid.* *Lietuvos Respublikos generalinė prokuratūra* para. 36; and *Commissioner of An Garda Síochána* cit. para. 57.

⁵¹ *Ibid.* *Lietuvos Respublikos generalinė prokuratūra* para. 38; and *Commissioner of An Garda Síochána* cit. para. 99.

between public and private interests. This balancing test is not explicitly mentioned by art 52(1) EU Charter and, as seen before, is also very limited in the field of free movement law where only a few cases can be found which relates to the use of a balancing test in a preliminary procedure such as the *Sunday trading* cases,⁵² the *Schmidberger* case⁵³ and the recent *Nordic Info* case.⁵⁴ In contrast to free movement law, the balancing test in the digital market constitutes the core of the proportionality test in the case law of the CJEU concerning public security and public order. This is perhaps not a surprise. According to Siofra O'Leary, who is now President of the European Court of Human Rights "both European courts have recently been preoccupied with questions of mass surveillance by State authorities or the use to which the latter put communications and content data transferred by private companies".⁵⁵ Data concerns and data regulations have increased significantly in the last years and this increase in regulation leads to adjudications that relate to the implementation of these regulations by the Member States; and data concerns and data regulations often raise the delicate issue of balancing between public interests, such as public security, public policy and national security; and private interests protected by the EU Charter, in particular rights incorporated in arts 7 and 8 of the EU Charter.

The prominence of the balancing test in EU law was already visible in the early "Digital jurisprudence" on art. 52(1) EUCFR and the principle of proportionality: *Digital Rights* and *Schrems I*.⁵⁶ These early cases are central to understand not only of the balancing test but also its relationship with the "essence test" (and its relationship with proportionality).⁵⁷ These cases also show the vigour of judicial scrutiny at the CJEU by invalidating EU measures contrary to EU fundamental rights based on a proportionality analysis and the EU Charter.⁵⁸ In particular, the case law of the CJEU had to face challenges, related to ambiguity, which still accompanies the judicial balance between the rights to data privacy and conflicting or alternative rights or interests such as freedom of expression and national security. It is hard to refute that the CJEU judges and their "digital jurisprudence"

⁵² Case C-145/88 *Torfaen Borough Council / B & Q PLC* ECLI:EU:C:1989:593.

⁵³ See *Schmidberger* cit.

⁵⁴ See *NORDIC INFO* cit. This case concerns the interpretation of the Citizenship directive and the free movement of persons. It thus also includes a EUs secondary legislation.

⁵⁵ S O'Leary, 'Balancing of Rights in the Digital Age'. (2018) *Irish Jurist* 59, 90.

⁵⁶ Case C-362/14 *Schrems* ECLI:EU:C:2015:650.

⁵⁷ See for more discussion on the essence test, X Groussot and GT Petursson, 'Je t'Aime...Moi Non Plus: Ten Years of Application of the EU Charter of Fundamental Rights' cit.

⁵⁸ In *Digital Rights Ireland and Seitlinger and Others* cit., an "essence test" of a kind is made, separately from the proportionality analysis undertaken in the case. The Court verified that the interference at issue did not adversely affect the essence of the fundamental rights at stake (arts 7 and 8 of the EU Charter). However, this was a rather case-specific exercise, seemingly neither excluding nor impacting on the following comprehensive analysis, which included a detailed proportionality analysis. In *Schrems* cit. the CJEU ruled for the first time a breach of both the essence of the fundamental right to privacy and of the fundamental right to effective judicial protection.

have been crucial in the development of the principle of proportionality and the building of a substantive rule of law in EU law. Moreover, the protection offered by data protection rules is nowadays wider in many respects than that offered by privacy rules. Indeed, “data” has a high value in the market and “personal data” has a potential to become a “personal property”.⁵⁹

In the area of collection of personal data, AG Pitruzzella in *Ligue des droits humains* introduces this high-profile case sent by the Constitutional Court of Belgium by highlighting that “balancing” is at the heart of the relationship between the individual and the society in the age of digitalization. He considers that balancing fundamental rights in digital technologies that assemble, process, and analyse personal data constitutes the “principal dilemmas of contemporary liberal democratic constitutionalism”. In other words, the balancing of fundamental rights is viewed as the core of the digital rule of law understood as a substantive rule of law since it includes EU fundamental rights. Interestingly, the AG stated that the relationship with EU fundamental rights, “on the one hand, calls for delicate balancing acts between the interests of society and the rights of individuals, premised on the paramount importance of the individual in the European constitutional tradition, and, on the other, makes it necessary to establish safeguards against abuse”.⁶⁰ This view is also present in the EU literature. For instance, Giovanni De Gregorio considers that the principle of proportionality is structural to European data protection and central to the reconciliation of fundamental rights necessary in a democratic society.⁶¹ For him, “It is not by chance that the ECJ has relied on the principle of proportionality since the first cases on data protection and this balancing logic is at the core of the GDPR’s structure”.⁶²

The balancing of interests in EU (digital) law is often associated with the application of the principle of proportionality particularly since the ruling in *Promusicae*,⁶³ where the CJEU famously reconciled through balancing the conflicting human rights at issue.⁶⁴ This close relationship is clearly reflected in the digital market case law of the CJEU which often puts in conflicts many types of EU fundamental rights. For instance, in *Youtube and Cyando*, which concerned *inter alia* the e-commerce Directive (Directive 2000/31) and the Copyright Directive, the CJEU decided that the national courts and authorities must strike a balance between the EU Charter provisions at issue in this harmonized field.⁶⁵ One can

⁵⁹ See O Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 46 ff.

⁶⁰ See C-817/19 *Ligue des droits humains* ECLI: EU:C:2022:65, opinion of AG Pitruzzella, para. 2.

⁶¹ See G De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (CUP 2022).

⁶² *Ibid.*

⁶³ See case C-275/06 *Promusicae* ECLI:EU:C:2008:54 para. 68.

⁶⁴ X Groussot, ‘Music Production in Spain (*Promusicae*) vs. Telefonica de Espana SAU - Rock the KaZaA: Another Clash of Fundamental Rights’ (2008) CMLRev 1745.

⁶⁵ See joined cases C-682/18 and C-683/18 *Youtube and Cyando* ECLI:EU:C:2021:503 paras 63, 64 and 138. Art. 52 of the EU Charter is not referred to explicitly in these cases but in case C-265/19 *Recorded Artists Actors Performers* ECLI:EU:C:2020:677, and joined cases C-245/19 and C-246/19 *État luxembourgeois (Droit de recours*

observe that the case law of the CJEU is subject to an expansion of this type of litigations based on balancing of rights and balancing of interests in the harmonized field of the Digital Single Market.⁶⁶

Importantly, the balancing test is systematically used by the CJEU in its digital case law to examine the proportionality of public policy and public/national security measures that conflicts with EU fundamental rights as derogations from EU secondary law. This evolution constitutes a sequel of the “conflict of rights” case law (such as *Promusicae*) into the CJEU jurisprudence concerning specifically the balancing of public and private interests. Furthermore, this evolution differs from the free movement case law which from a historical perspective has been enormously limited when it comes to the use of the balancing test in relation to the interpretation of the derogations in EU internal market law. The third part of a proportionality test⁶⁷ when conducted in EU free movement, follows the application of the suitability and necessity tests. In the digital market case law of the CJEU, it appears that the balancing test always follows the application of the “strictly necessary” test and is (the balancing test) undertaken in a systematic basis to determine which of the public or private interests take priority over the other. This systematic balancing of interests in the digital field is comprehensible due to the very nature of the situations/cases that concern implementation of EU legislation. This also explains its difference with EU free movement case law (which rarely uses the balancing test) since the field of the internal market constitutes a non-harmonized area of EU law. However, as we shall see soon in more detail in the next section, even if the application of the balancing test in a harmonised area of EU law is logical; it may also lead to conflicts and tensions with the national courts. This is particularly so when the national public interests concern matters of national security.

Today, considering the recent case law of the CJEU on the EU Charter, it is worth noting that there is no need to engage in a “balancing of interests” where the EU measure in question breaches the essence of an EU fundamental right and is thus declared invalid before reaching the balancing test. This absence of balancing may be viewed sometimes as problematic if one considers the “act of balancing” as part of a constitutional exercise of authority by the judiciary.⁶⁸ In any case, this discussion on the framework of art. 52(1) EU Charter and its balancing test shows the significance of the principle of proportionality and its crucial role in the development of judicial review of national legislation

contre une demande d'information en matière fiscale ECLI:EU:C:2020:795, the CJEU affirmed the importance of the conditions of art. 52(1) EUCFR. These cases concerned application at the national level of EU secondary norms, and how they should be applied and implemented, in compliance with the EU Charter.

⁶⁶ See generally on balancing, A Engel and X Groussot, “The EU’s Digital Package: Striking a Balance for Fundamental Rights in the Proposed DSA and DMA Regulations” in M Bergström, V Mitsilegas (eds), *EU Law in the Digital Age* (Hart 2024) 71.

⁶⁷ See Section II for the discussion in light of the free movement case law.

⁶⁸ *Ibid.*

implementing EU secondary legislation adopted in the digital field.⁶⁹ We also believe that the balancing test in the digital market field may arguably spill-over into the free movement area and may lead to a potential increased application of the balancing test in the free movement area - and thus may lead to its methodological evolution. In fact, this (r)evolution can be triggered both by the newest digital market case law of the CJEU⁷⁰ and by the general increasing regulatory surge of internal and digital markets secondary laws in the last years.⁷¹ This methodological evolution may, however, be slow to occur considering the likely essential need for EU courts to establish a distinction between harmonized (bringing less discretion to the State, thus justifying a three-pronged test) and non-harmonized (bringing more discretion to the State and thus justifying a two-pronged test) areas in adjudicating discretionary powers in EU law matters.

V. NATIONAL SECURITY AND NATIONAL COURTS IN THE INTERNAL AND DIGITAL MARKETS

In approaching the conclusion of this contribution, it is impossible not to say a few words on the concept of national security and the role of national courts regarding its interpretation and application.⁷² The concept of national security (*i.e.* state security) is the ultimate and potentially strongest limitation to the implementation of EU legislation in the digital field and can differ from the concept of public security.⁷³ National security is both encrypted within the texts of the EU legislation in the digital field, *e.g.* art. 15(1) of

⁶⁹ A Engel and X Groussot, 'Making the Rule of Law Great Again: The Building of the Digital Rule of Law in the European Union' in M Bungenberg, M Frölich, T Giegerich, N Zdraveva (eds), *New Directions in Digitalisation. European Union and its Neighbours in a Globalized World* (Springer 2024) 273.

⁷⁰ See *NORDIC INFO* cit.

⁷¹ Such as *eg* the adoption of the citizenship directive that has codified the free movement of persons case law. See also Regulation 1925/2022 cit., the Regulation 2065/2022 cit. and the Regulation 1689/2024 cit.

⁷² The concept of public security within the meaning of the Articles, in which the Treaty provides for derogations applicable in situations, which may affect public security, covers both a Member State's internal security and its external security. See the concept reserved, at first, for the meaning of art. 36 TFEU *eg* cases such as C-367/89 *Richardt* ECLI:EU:C:1991:376 para. 22; case C-83/94 *Leifer and Others* ECLI:EU:C:1995:329 para. 26; C-273/97 *Sirdar* ECLI:EU:C:1999:523 para. 17; C-285/98 *Krell* ECLI:EU:C:2000:2 para. 17; C-423/98 *Albore* ECLI:EU:C:2000:401 para. 18, where the CJEU extended the meaning of the concept to the Treaty; case C-186/01 *Dory* ECLI:EU:C:2003:146 para. 32, where the CJEU extended the meaning of the concept to Articles "in which the Treaty provides for derogations applicable in situations which may affect public security".

⁷³ See the distinction in art. 15(1) of Directive 2002/58 cit. However, the distinction between national security and public security is not always clear-cut. See also in general R Wodak and S Boukala, 'Talking about Solidarity and Security in the Age of Crisis: The Revival of Nationalism and Protectionism in the European Union – A Discourse-Historical Approach' in C Carta and J-F Morin (eds.) *EU Foreign Policy through the Lens of Discourse Analysis: Making Sense of Diversity* (Routledge 2014) 179.

the e-privacy directive; and in EU primary law, e.g. art. 4(2) TEU⁷⁴ and art. 346 TFEU.⁷⁵ The interpretation of EU secondary legislation in the digital single market⁷⁶ by the CJEU may enter conflict with the national vision of national security in relation to the use of data at the domestic level. Such a tension comes to its peak when the CJEU conducts a balancing test between national security interests and private interests. In this instance, the national courts may react to a balancing of interests that it deems incorrect. This is precisely the situation that occurred in *Quadrature du Net*.⁷⁷

Indeed, the CJEU ruled in *Quadrature du Net* that art. 15(1) of the e-privacy directive read in light of arts 7, 8 and 11 and art. 52(1) of the EU Charter must be interpreted as precluding legislative measures which, for the purposes laid down in art. 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data.⁷⁸ The French *Conseil d'État* refused to apply the balancing test conducted by the CJEU based on national security concerns. As lucidly put by Araceli Turmo,

"The French court has established a new exception to the primacy of EU law, justified by national security concerns: whenever the French judges are not satisfied that EU standards are compatible with these concerns, as defined by French authorities, they reserve the right not to implement them and thus to set aside the balance established by the ECJ between fundamental rights and the need to fight against crime and ensure security and public order".⁷⁹

⁷⁴ The protection of national security constitutes one of the sovereign functions of any State. The EU is not an exception and explicitly provides in art. 4(2) TEU that it respects the essential State functions, among which safeguarding national security is incorporated. In addition, under art. 4(2) TEU national security is the area of the sole responsibility of each Member State. The CJEU has emphasized in case C-300/11 ZZ ECLI:EU:C:2013:363 para. 35 that art. 4(2) TEU and art. 346(1)(a) TFEU states that State security remains the responsibility of solely the Member States. Besides, art. 72 TFEU states that the existence of the area of freedom, security and justice does not affect the responsibilities of the Member States regarding maintenance of law and order and the safeguarding of internal security (that is an integral part of national security).

⁷⁵ The derogations provided for in arts 346 TFEU must, in accordance with settled case-law in respect of derogations from fundamental freedoms, be interpreted strictly. In case C-474/12 *Schiebel Aircraft* ECLI:EU:C:2014:2139 para. 33. The CJEU has ruled that the derogation, allowed under art. 346 TFEU must, in accordance with settled case-law concerning derogations from fundamental freedoms, be narrowly construed. Moreover, although art. 346 TFEU refers to measures which a Member State may consider necessary for the protection of the essential interests of its security, that article cannot, however, be read in such a way as to confer on Member States a power to depart from the provisions of the EU Treaty based on no more than reliance on those interests.

⁷⁶ See SA de Vries, 'The Resilience of the EU Single Market's Building Blocks in the Face of Digitalization' in S de Vries, U Bernitz, X Groussot, and J Paaju (eds) *General Principles of EU Law and the EU Digital Order* (Kluwer 2020) 3.

⁷⁷ *Quadrature du Net and Others* cit.

⁷⁸ *Ibid.*

⁷⁹ A Turmo, 'National Security Concerns as an Exception to EU Standards on Data Protection' (2021) *Nordic Journal of European Law* 86, 87.

Here, the national court stays away from the direct conflict of an *ultra vires* judgement and decides, as an alternative, to disregard the CJEU's exercise of EU competences in the area which it deems to be outside their scope.⁸⁰ This signifies

"[...] ignoring the balance chosen by the ECJ between privacy and the protection of public security and holding that, by nature, the ECJ was unable to determine the contents of the latter. Instead of complying with a balance established at the European level, according to the *Conseil d'État*, national authorities must be capable of establishing their own balance between the (fundamental rights) standards set at the EU level and the security concerns defined within the Member State".⁸¹

National security is an area where the national courts are under high political pressure. The *Quadrature du Net* case provides an enticing illustration of such mantra, where the French government, which is usually overtly pro-European, took a very assertive position to the control of the meaning of national security which accordingly should remain solely in the hands of the Member State and not the European Union. This assertive position is certainly common to many EU Member States and may lead to further problems in the implementation of the legislation related to the digital market. It is thus certainly not a surprise that the CJEU in *AG* recently interpreted the scope of national security and art. 4(2) TEU in the context of the digital market. In this case, the CJEU made clear that there is a hierarchy to be respected between the various public interest that a Member State can rely in derogating from the implementation of EU legislation and that importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails.⁸² The Court stated in that regard,

"[...]the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, according to which national security remains the sole responsibility of each Member State, exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives".⁸³

This statement is extremely important and shows the importance given by the CJEU to the interpretation of the national security derogation considering art. 4(2) TEU. It is also worth remarking that the CJEU underlined that objective of safeguarding national

⁸⁰ *Ibid.* 88.

⁸¹ *Ibid.*

⁸² See *Lietuvos Respublikos generalinė prokuratūra* cit. para. 35. See also *Commissioner of An Garda Síochána* cit. para. 56.

⁸³ *Lietuvos Respublikos generalinė prokuratūra* cit. para 36. This also similar to the reasoning used in the free movement case law (see section 2).

security is constrained by the other requirements laid down in art. 52(1) of the Charter, such as the need to have a measure which is “strictly necessary” and “balanced” as discussed in the previous section.⁸⁴ In other words, the application of the concept of national security and its wide discretion is limited by the principle of proportionality enshrined in art. 52(1) EU Charter.⁸⁵ Having in mind the CJEU case law on national identity and art. 4(2) TEU,⁸⁶ one should be aware that it is not only art. 52(1) of the EU Charter that constitutes a constraint to the application of national security but also the principle of loyalty which is enshrined in art. 4(3) TEU.⁸⁷ These constraints are essential to keep in mind in the digital market which constitutes an integral part of a broader political context where some of the EU Member States have a tendency to backslide in terms of rule of law protection. The digital (single) market is a field of law where special attention must be given to avoid situations where national security concerns are used by a Member State as a façade to circumvent the application of the rule of law. The internal market case law already provides numerous examples where Member States used national security concerns to avoid the application of the rule of law.

But even outside the politically loaded area of the backsliding of the rule of law, it appears that national security and public security can act as an effective brake on the implementation of EU secondary legislation and to the application of EU fundamental rights falling within the scope of EU law, and this is so even beyond the field of the Digital Single Market. Suffice it to look here at the *EncroChat*⁸⁸ litigations in many countries of Europe, which concern the interpretation of art. 14(1) of the EIO Directive and e-evidence/data. In one of these cases, the Frankfurt Public Prosecutor’s Office requested, by way of an EIO, authorization from the French authorities to use the *EncroChat* data for criminal proceedings.⁸⁹ Will EU fundamental rights be taken into consideration by the CJEU? This is not so certain after the Opinion of the Advocate General in the case which provides a narrow reading of the *Prokuratuur* case – a preliminary reference sent by the Supreme Court of Estonia.⁹⁰ Furthermore, the *EncroChat* litigations reflect the core

⁸⁴ See in general on art. 4(2) TEU, E Cloots, *National Identity in EU Law* (OUP 2015).

⁸⁵ A parallel can be drawn here with Free Movement case law on public security. In *Campus Oil* cit. (note 13), the Court for the first time addressed the derogation under art. 36 TFEU based on the grounds of public security. After having established that the level of the existing Community rules was not sufficient for the protection of the stated interest, it concluded that it was possible for a Member State to have recourse to a derogation under art. 36 TFEU, on the basis of public security, even though there were some Community rules on the matter in place (*Campus Oil* cit. para. 31). However, such a derogation is to be subject to the compliance with the principle of proportionality.

⁸⁶ X Groussot, ‘Constitutional Dialogues, Pluralism and Conflicting Identities’ in M Avbelj and J Komárek (eds), *Constitutional Pluralism in the European Union and Beyond* (Hart 2012) 319.

⁸⁷ See *Prokuratuur* (*Conditions d’accès aux données relatives aux communications électroniques*) cit. for the link between rule of law and digitalization.

⁸⁸ C-670/22 *M.N. (EncroChat)* ECLI:EU:C:2023:372.

⁸⁹ See case C-670/22 *M.N. (EncroChat)* ECLI:EU:C:2023:817, opinion of AG Capeta.

⁹⁰ *Ibid.*

problematic beyond national security and public security in the sense that the national courts are often very reluctant to make use of art. 267 TFEU and ask for an interpretation of EU law to the CJEU. For instance, in Sweden, no national court has referred to the CJEU in the many litigations occurring all over the country. This is not surprising given the explosive context in terms of public (in)security and the war against the gangs waged by the Swedish government. Yet, the *EncroChat* litigations raise central issues as to the scope of public security and public order measures limiting the application of the EU fundamental rights. Similarly, to this harmonized field, national security constitutes a brake for the national court in the non-harmonized areas. The *Huawei*⁹¹ litigations throughout the EU Member States that concern national security derogations in the free movement context also exemplify the reluctance of national courts to use a preliminary reference under art. 267 TFEU to ask for an interpretation of EU law, which is often necessary. In other words, national security concerns in EU law too often come under the radar of the CJEU due to the silence of the national courts. This silence has consequences for the adjudicative framework of the test of proportionality since it is difficult to develop a solid framework where only a few cases appear in front of the CJEU. The evolution of concepts in EU law and the associated adjudicative tests depend on a symbiosis between the national courts and the CJEU. National security matters constitute sensitive matters; and therefore are not the most appropriate matters to keep the flame of EU law alive between the EU courts – *i.e.* the national courts and the CJEU, in the interpretation of internal and digital market laws.

VI. CONCLUSIONS

In this *Article* we have analysed the impact of the increasing digitalization of our times and the development of EU regulation in this field on the methodological framework used by the CJEU when dealing with national security issues. Do the traditional methods developed in the *Van Duyn* and *Église scientologie* era still hold true, or does the nature of current security challenges, for example being less border centric, mean that there is a methodological, and even conceptual, shift in the case law?

In the *classic* free movement type of cases, the concepts of public policy and public security remain under the strict control of CJEU. However, the principle of proportionality plays a key role in assessing the restrictive measures – as is also the case in the context of fundamental rights, as protected by the EU Charter, and laid down in art. 52(1) of the EU Charter. Furthermore, in the context of the proportionality principle, the *appropriateness* of the national public policy/security measures are also limited, in the sense that they may be relied upon only if there is *a genuine (present) and sufficiently serious threat to a fundamental interest of society* – which is a narrow path, based on the

⁹¹ Court of Appeal of Stockholm of 22 June 2022 *Swedish Post and Telecom Authority (PTS) v Huawei*, joint case 5222-21 and 5223-21.

CJEU case law. Additionally, procedural guarantees have gradually been introduced in this same context, and these guarantees need to be complied with when it is being assessed whether a restriction to free movement can be justified. All in all, this means that the margin of appreciation, the origins of which can be traced back to these types of cases before the CJEU, is more often appearing as a myth than reality.

Nevertheless, what is revealed in this article is that the recent case law of the CJEU concerning public security in the harmonized digital field of EU law, does not rely on an analytical framework based on suitability and necessity in the same way as it is the situation in the classic free movement case law. Instead, it provides a framework based on (a) assessing whether the State measures are ‘strictly necessary’ and (b) on a balancing test to be conducted between the public interests and the private interests at issue.

The “strictly necessary” approach which is now apparent in the recent digital market case law of the CJEU, especially in the context of fundamental rights guaranteed by the EU Charter, focuses on a strong procedural safeguard logic, which is also found in the free movement case law. The interference at issue is to be limited to what is “strictly necessary”, but to fulfil these conditions, the national legislation must, initially, lay down clear and precise rules governing the scope and application of such rules, which fulfil procedural safeguards. At the same time, the CJEU focuses on the nature of the objectives at issue – the public interests relied on by the national authorities – especially in the context of the EU Charter rights, such as the right to privacy and data protection. This comes very close to reproducing a suitability test, which is often relied on in the field of free movement law to test the proportionality of national measure derogating from EU law and the appropriateness of the public interests. However, in the digital market case law of the CJEU, this test is realized within the framework of the “strictly necessary” test and not within the framework of an explicit suitability test. In addition, the CJEU has explicitly recognized a specific hierarchy of these objectives – where, for example, national security objectives are of greater importance in the hierarchy of objectives than the fight against serious crime or the prevention of serious threats to public security, even if the latter objectives’ importance is greater than that of fighting crime generally and of preventing non-serious threats to public security. This methodological approach of the CJEU in the application and interpretation of the “strictly necessary test” reflects thus a mixed and procedural approach which differs somewhat from the proportionality assessment used in free movement and internal market laws, even if incorporating some of the same elements. The proportionality assessment in the digital market case law is based on a balancing the test between public and private interests and is seemingly often of different nature from what we see in classic free movement cases. Here we are of course dealing with secondary norms, often in a fully or at least partially harmonized field of law. Importantly, the balancing test systematically used by the CJEU in its digital case law is to examine the proportionality of public policy and public/national security measures that conflict with EU fundamental rights as derogations from EU secondary

law. Furthermore, this evolution differs from the free movement case law since, here, proportionality assessment in the strict sense (*stricto sensu*), seems rather to be the rule than the exception.

Finally, this article, reflects upon the concept of national security and the role of national courts regarding its interpretation an application this digital field. National courts are sensitive towards the application of the term national security in EU law – but also towards CJEU’s balancing of national security and private interests. This has led to both reluctances to refer cases to the CJEU through the preliminary ruling procedure, but also to national courts not respecting the outcome of that process, even if using the procedure in the first place. That shows the highly political and sensitive nature of this field of law. Proportionality has always been used as a tool to allow great flexibility in the hands of the judges at the CJEU. In that sense it has the potential to control the delicate balance exercise that needs to take place when national security issues are at issue. Nonetheless, there are real challenges in the digital field of EU law. It is currently a field of law which is dominated by EU secondary regulation. Even if the principle of proportionality plays a key role here, when the line between public and private interests is drawn, there are clearly methodological implications that come with this new field of law. We have tried to lift these elements to the fore and compare the “new” to the “old”. Somehow, one is left with the impression that we are just in the early phase of the substantive and methodological evolution of this digital sphere of EU law.

