



Constitutionalising the Security Union

Effectiveness, rule of law and rights
in countering terrorism and crime



Edited by **Sergio Carrera**
and **Valsamis Mitsilegas**

Foreword by **Julian King**

CONSTITUTIONALISING THE SECURITY UNION

*EFFECTIVENESS, RULE OF LAW AND RIGHTS
IN COUNTERING TERRORISM AND CRIME*

EDITED BY

SERGIO CARRERA

AND

VALSAMIS MITSILEGAS

FOREWORD BY

JULIAN KING

CENTRE FOR EUROPEAN POLICY STUDIES (CEPS)

BRUSSELS

The Centre for European Policy Studies (CEPS) is an independent policy research institute in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe. The views expressed in this book are entirely those of the authors and should not be attributed to CEPS or any other institution with which they are associated or to the European Union.

This paperback book falls within the framework of SOURCE Network of Excellence, which is financed by the EU FP7 programme with the aim of creating a robust and sustainable virtual centre of excellence capable of exploring and advancing societal issues in security research and development. For more information about the project, please visit <http://societalsecurity.net/>



Societal
Security
Network



ISBN 978-94-6138-643-4

© Copyright 2017, Centre for European Policy Studies and the authors.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the prior permission of the Centre for European Policy Studies.

Centre for European Policy Studies
Place du Congrès 1, B-1000 Brussels
Tel: (32.2) 229.39.11
E-mail: info@ceps.eu
Internet: www.ceps.eu

CONTENTS

Foreword

Julian King i

Introduction

Sergio Carrera and Valsamis Mitsilegas 1

Part I. Cross-Border Criminal Investigations and Preventive Justice 4

1. The Security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law
Valsamis Mitsilegas 5
2. Two crucial challenges in cross-border criminal investigations
Anne Weyembergh 21
3. Old and new challenges to European criminal justice
Petra Bárd 33
4. Reviewing the effectiveness of EU counter-terrorism policies
Fiona de Londras 45
5. The Radicalisation Awareness Network: Producing the EU counter-radicalisation discourse
Diana Davila Gordillo and Francesco Ragazzi 54

Part II. EU Information Access and Exchange, and International Cooperation 64

6. Security of the interstice and interoperable data sharing: A first cut
Deirdre Curtin 65
7. International cooperation and the exchange of personal data: Safeguarding trust and fundamental rights
Evelien Brouwer 73

8.	A Security Union in full respect of fundamental rights: But how effectively respectful? <i>Gloria González Fuster</i>	87
9.	Will more data bring more security? Remarks on the Security Union approach to interoperability <i>Reinhard Kreissl</i>	93
10.	Cross-border access to electronic evidence: Policy and legislative challenges <i>Katalin Ligeti and Gavin Robinson</i>	99
Part III. Conclusions.....		112
11.	Constitutionalising the Security Union <i>Sergio Carrera and Valsamis Mitsilegas</i>	113
List of Abbreviations.....		144
List of Contributors		145
Annex. Programme of the Policy Workshop co-organised by CEPS and DG HOME.....		147

FOREWORD

This book is the result of a policy meeting organised by CEPS on 12 May 2017 under the title “Reappraising EU Security Policy: Effectiveness, rule of law and rights in countering terrorism and crime”. Bringing together EU policy-makers and academics, it provided an opportunity to exchange perspectives that proved useful to the Comprehensive Assessment that the European Commission has recently concluded in the field of security policy and which I promised to conduct upon becoming the first Commissioner for the Security Union in September 2016.

The interconnected and cross-border threats that we collectively face mean that the security of one Member State is the security of all Member States. The case for EU action to support Member States in the daily challenges they face in fighting terrorism, countering radicalisation and violent extremism, combating organised crime and responding to the growing threats posed by cybercrime, is unanswerable. This was what was in President Jean-Claude Juncker’s mind when he created the post I have the privilege to occupy – the urgent need to build an effective and sustainable Security Union.

The Juncker Commission is structured in a way that breaks down traditional silos between different EU policy areas, and the Security Union is no exception to this approach. I draw on a cross-cutting Task Force covering more than 30 Commission Directorates-General and the European External Action Service.

The Commission’s action essentially takes place on two fronts: First, it is closing down the space in which terrorists and criminals operate and denying them the means – money, munitions and movement. That includes working on the prevention of terrorism, and working to counter radicalisation. Second is building our resilience, strengthening our information systems by closing information gaps and making them more joined up, and strengthening critical infrastructure, particularly our transport, energy and cyber security, which are too often targeted by terrorists and criminals.

To increase the transparency of EU action on security, a progress report on the implementation of the Security Union is published every month. Earlier this year, the Commission published a Comprehensive Assessment of EU Security Policy. The assessment was carried out after a thorough dialogue with think tanks, industry, academics, the European Parliament and others. I thank those who were able to contribute, and those like CEPS who continue to contribute with independent research to the debate on EU security policy.

Overall, the review showed that Member States now clearly recognise that the EU can and should play an active role in security, with a step change in Member States' engagement at the European level; it also identified some challenges and gaps.

Since early 2015 the terrorist threat has increased markedly in Europe and the EU has responded by adapting its priorities and increasing the pace of work. Interoperability is at the top of the list of priorities of this Commission. Improving the access to and sharing of information is at the heart of our efforts to strengthen security in the EU. Identity fraud is a growing problem – particularly with returning terrorist fighters. We have several EU databases that contain valuable information but which were developed separately and do not communicate with each other.

We need to ensure that our border guards and police, our immigration officers, our customs and judicial authorities have the necessary information at their disposal to protect our external borders, lead the fight against terrorism and organised crime and better protect our citizens. It is essential to ensure that individuals can only be registered under one identity and that law enforcement and border staff on the ground have the ability to search across all databases biometrically as well as alphanumerically.

The Commission set up a High-Level Expert Group on Information Systems and Interoperability to identify and propose solutions to addressing shortcomings and information gaps caused by the complexity and fragmentation of our information systems at the European level. The group produced its final report in May 2017 and the Commission moved rapidly to present proposals to amend the information systems concerned, and to introduce the three operational dimensions of interoperability:

- a European search portal,
- a shared biometric matching service, and
- a common identity repository.

The conclusions adopted by the Council on 9 June 2017 on the way forward to improve this information exchange and ensure interoperability of EU information systems prove that this is a shared priority at the highest political level.

London Bridge, Manchester, Westminster, Stockholm, Berlin, Nice and Brussels: What these terrorist attacks all have in common, apart from the often crude methods used, is the alarming speed at which some of the individuals involved became radicalised.

There is a clear and urgent need to act and do more to counter radicalisation. Fortunately, we have laid a solid foundation in our work over the last two years. The Commission launched the EU Internet Forum in 2015, to bring together EU interior ministers, high-level representatives of major Internet companies, Europol, the EU Counter-Terrorism Coordinator and the European Parliament.

In July 2016, an EU Internet Referral Unit was set up at Europol to ensure the swift removal of violent content online. It plays an important role in reducing accessibility to terrorist content online and it has referred over 24,000 pieces of content to Internet companies and enjoys an over 90% take-down rate. It directly supports the goals of the Forum, because we believe that a public and private partnership, which is voluntary and based on mutual trust, is the best way forward in this fight.

Through these cooperative platforms, Internet companies have agreed to step up their action against terrorist content online. For instance, a 'database of hashes', a platform to flag terrorist online content in order to ensure its irreversible removal, was developed by the Internet industry in close cooperation with the Commission. It was launched in March 2017.

There is a great deal more to do, with Internet companies needing to shoulder a greater share of the responsibility for keeping the Internet safe and free of hate speech and terrorist propaganda. The Commission also announced its new Civil Society Empowerment Programme, which, with support from the Internet companies, will enable credible voices across the EU to be amplified online.

In the Radicalisation Awareness Network, we have created an operational network of grassroots actors, civil society and researchers. The Commission has established a High-Level Expert Group on Radicalisation to build stronger links between this work and policy-makers in national administrations. The group will provide advice and expertise on counter-radicalisation work at the EU level, including priority areas such as prison radicalisation, returning foreign terrorist fighters and the Internet.

As our economies become more interconnected and digitalised, they are also more vulnerable and exposed to cyber threats. Attacks – whether state-sponsored, from a terrorist background or resulting from the exploitation of vulnerabilities due to human error – have the potential to result in the disruption of the supply of essential services. The Wannacry and NotPetya cyberattacks were only reminders of this. British hospitals, German railways and Spanish telecoms were among the victims. Cybercrime is a threat that no Member State can tackle on its own, which has an economic and fundamental rights impact that we cannot afford to neglect.

Fighting cybercrime effectively requires more active cooperation across communities, from law enforcement to cybersecurity authorities and particularly from the private sector, which owns and operates more than 90% of the infrastructure. Europol's European Cybercrime Centre plays a key role in supporting cross-sectorial and international cooperation.

We need to improve criminal justice in cyberspace, focusing on cross-border access to electronic evidence. We also need to reflect on the role of encryption in criminal investigations.

Instruments and tools like the Schengen Information System, the European Arrest Warrant or mutual legal assistance support national authorities in collecting and exchanging information and evidence, allowing coordinated operational action, and help them to bring offenders to justice. Frameworks for cooperation, such as the EU Policy Cycle for organised and serious international crime, help national authorities define common operational priorities. EU agencies in justice and home affairs have become central actors in their fields – such as Europol or Eurojust and their roles with the European Arrest Warrant and the European Investigation Order (EIO).

On 8 June 2017 the Council supported the swift implementation of a number of practical measures to improve cooperation among judicial authorities and with service providers. These include the creation of an electronic and user-friendly version of the EIO, the creation of single points of contact within the authorities of Member States and service providers to facilitate cooperation, the streamlining of service providers' policies on procedures and conditions to request access, and the standardisation of forms used by Member States to request access to e-Evidence, among others.

Security, freedom and rights continue to be intimately intertwined. Compliance with fundamental rights is a key characteristic of EU security policy, in line with our Treaty obligations, and the overall EU set-up makes fundamental rights compliance an inherent aspect of our collective policy-making. The challenge is to address the security threat without stoking the

fear, which is exactly what the terrorists want, and without compromising the values we are here to defend: openness, tolerance and freedom.

These are all elements of the foundations of a genuine and effective Security Union. This should be the framework within which we cooperate closely on the basis of solidarity, mutual assistance and in full respect of each other's national competences, while also acknowledging that in today's more connected and more global world, the security of one Member State is the security of all.

Julian King

Commissioner for the Security Union
European Commission

INTRODUCTION

SERGIO CARRERA AND VALSAMIS MITSILEGAS

This collective book is the result of a policy workshop co-organised by CEPS and the Task Force on Security Union at the Directorate-General for Migration and Home Affairs (DG Home) of the European Commission on 12 May 2017 in Brussels. The event aimed at bringing together a selection of EU policy-makers and academics, and contributions to an evidence-based and informed assessment of EU security policy. It gathered a group of leading scholars who have played a key role in EU- and nationally-funded research projects in the social sciences and humanities covering themes of relevance to the Security Union.

The closed-door event provided a unique opportunity for the exchange of perspectives and interdisciplinary knowledge with Commission officials. It fed into the “Comprehensive Assessment of EU Security Policy” that DG Home (the Task Force on the Security Union) conducted in the field of security policy, which was published on 26 July 2017.¹

The Comprehensive Assessment is one of the main outputs of the creation, in 2016, of a specific European Commission portfolio for the Security Union supported by a task force drawing on the expertise of all relevant Commission services as well as the European External Action Service, and led by Commissioner Julian King.

Engaging in participative roundtable panels, the attendants of the policy workshop were invited to identify key issues and gaps in existing EU security policy instruments in relation to the following three issues or ‘challenges’:

- cross-border criminal and judicial investigations and judicial cooperation in criminal matters;

¹ See European Commission, *Comprehensive Assessment of EU Security Policy*, Commission Staff Working Document, SWD(2017) 278 final, Brussels, 26.7.2017. The Comprehensive Assessment was published together with the Commission Communication, “Ninth Progress Report towards an Effective and Genuine Security Union, COM(2017) 407 final, Brussels, 26.7.2017.

- the use of information systems, including the issue of interoperability of EU databases; and
- international cooperation.

The detailed programme of the event is presented in the annex of this book. The event was structured around the above-mentioned three challenges, which dealt with the specific issues and questions outlined below.

Challenge 1. Cross-border criminal investigations

Coordinated actions in cross-border criminal and judicial investigations and proceedings constitute a central component of the EU security agenda. EU cooperation on extradition and the gathering of evidence (through European Investigation Orders), as well as joint investigation teams coordinated by EU agencies represent illustrative examples. To what extent have these tools been used and have they been 'effective'? What should be improved? Also, the expansive use of electronic communications and an intelligence-driven ('preventive justice') policing approach to law enforcement raise issues related to criminal justice systems and to the fundamental rights of defence and fair trial.

Challenge 2. Information exchange

The effectiveness of information tools for law enforcement purposes is a priority of the EU security agenda and a key challenge, provoking questions not only about access, but also about their actual use by law enforcement agencies. As part of this priority, the goal of full interoperability of EU databases or information exchange systems (e.g. the Schengen Information System II, Visa Information System, Eurodac and Prüm Treaty) is another concern. However, is 'more data' the most efficient answer in view of current experience and future trends? What are the issues raised by the increasing use of EU information systems, and the development of biometric technologies, for law enforcement purposes in light of the principles of proportionality, necessity and the fundamental rights of data protection and privacy?

Challenge 3. International cooperation

International cooperation is an additional component of growing relevance for the EU Security Union. Cooperation with third countries through information exchange aims at reinforcing EU security. In the area of criminal investigations and judicial proceedings, the EU relies on specific agreements with countries covering access, tools for the exchange of information (e.g.

passenger name records and the Terrorist Finance Tracking Programme) and treaties on mutual legal assistance. Yet, in an era of increasingly dematerialised exchanges and reliance on electronic information and IT communication, access to data and evidence entails a number of dilemmas related to such issues as conflict of laws, jurisdiction and EU data protection legislation.

In discussing these matters, particular attention was paid to the effectiveness, proportionality, fundamental rights and societal implications of EU security policies and instruments based on independent academic research and knowledge in social sciences and humanities. The contribution of the policy workshop was expressly acknowledged by the European Commission Staff Working Document (Part 2) accompanying the Comprehensive Assessment, which also included a short transcript of the minutes of the meeting.²

The policy workshop fell within the scope of the SOURCE research project, a network of excellence funded by the Seventh Framework Research Programme (FP7) of the European Commission with the aim of creating a robust and sustainable virtual centre of excellence capable of exploring and advancing societal issues in security research and development.³

The structure of the book follows the main themes and questions covered during the policy workshop. **Part I** deals with cross-border criminal investigations and the notion of 'preventive justice' in the context of the Security Union. **Part II** continues the journey with a set of contributions addressing EU information exchange and international cooperation. **Part III** presents a synthesis of the main findings emerging across the various contributions making up the volume and advances suggestions aimed at constitutionalising the Security Union.

² See Part 2/2 in European Commission, SWD(2017) 278 final (2017), op. cit. Refer to p. 5 and pp. 164-167 of the document.

³ For more information about the SOURCE project, refer to <http://societalsecurity.net/>.

PART I

CROSS-BORDER CRIMINAL INVESTIGATIONS AND PREVENTIVE JUSTICE

1. THE SECURITY UNION AS A PARADIGM OF PREVENTIVE JUSTICE: CHALLENGES FOR CITIZENSHIP, FUNDAMENTAL RIGHTS AND THE RULE OF LAW

VALSAMIS MITSILEGAS

1.1 Introduction

Security has been at the heart of European integration, in one way or another, since the entry into force of the Maastricht Treaty. A series of terrorist attacks in the 2000s, including 9/11, 7/7 and the Madrid bombings, have been followed by a plethora of responses by the EU legislator, with EU intervention being justified as emergency law and pushing boundaries in criminal law and the constitutional systems of the Union and its Member States. This pattern of EU response has been replicated after successive terrorist incidents, resulting in a patchwork of measures adopted swiftly, without detailed justification or impact assessment and resembling at times kneejerk reactions or quick fixes to complex issues, while presenting significant challenges to fundamental rights and the rule of law in Europe.

In recent years, the development of a European security strategy and the publication of regular reports on the Security Union could be framed as an attempt to present a more strategic response. However, the way in which Security Union reports are presented entails the risk of the Union pursuing relentlessly and uncritically a security agenda without due consideration for the protection of fundamental rights and the rule of law. The aim of this contribution is to distil the main features of the emergence of the EU security agenda in recent years, and to outline the issues for fundamental rights and the rule of law. A central element of the argument will be that the EU has embraced a paradigmatic change from repression to prevention, with the Security Union being viewed essentially as a Union of preventive justice.

This chapter will highlight that in this process, a number of boundaries have been blurred:

- the boundaries between migration and security, security and foreign policy, and internal security and militarisation;
- the boundaries between internal and external security, and EU criminal law and external relations;
- the boundaries between public and private prevention, and the increasing role of the private sector in the EU security model; and
- the boundaries between suspicion and generalised surveillance, embracing surveillance of everyday, perfectly legitimate activities by all of us.

By highlighting these parameters of the EU preventive justice paradigm, the chapter will conclude by flagging up the profound challenges this paradigm poses for fundamental rights and the rule of law. The contribution will urge a rethink of the Security Union to place fundamental values of the Union at the heart of the European security strategy.

1.2 The EU and preventive justice

Preventive justice is understood here as the exercise of state power in order to prevent future acts that are deemed to constitute security threats. There are three main shifts in the preventive justice paradigm: a shift from an investigation of acts that have taken place to an emphasis on suspicion; a shift from targeted action to generalised surveillance; and, underpinning both, a temporal shift from the past to the future. Preventive justice is thus forward rather than backward looking – it aims to prevent potential threats rather than punish past acts, and in this manner it introduces a system of justice based on the creation of suspect individuals through ongoing risk assessment.¹

This model of preventive justice has been a key post-9/11 response by the US, linked with the evolution of a highly securitised, emergency agenda² and has been largely transposed into EU law since. Preventive justice can take the form of the state's intervention in the field of criminal law, by

¹ See V. Mitsilegas, *EU Criminal Law After Lisbon*, Oxford: Hart Publishing, 2016, ch. 9.

² See inter alia D. Cole, "The Difference Prevention Makes: Regulating Preventive Justice", *Criminal Law and Philosophy*, Vol. 9, No. 3, 2014; B. Ackerman, *Before the Next Attack*, New Haven, CT: Yale University Press, 2006; and J. Waldron, *Torture, Terror and Trade-Offs*, Oxford: Oxford University Press, 2010.

extending the scope of criminal law to gradually remove the link between criminalisation and prosecution on the one hand, and the commission of concrete acts on the other,³ thus leading to what scholars have called the “criminal law of the enemy”⁴ and placing criminal justice within the framework of the “preventive state”,⁵ transforming criminal law into “security law”.⁶ The considerable extension in the criminalisation of terrorism – as evidenced clearly in the recent amendment of the EU substantive criminal law on terrorism to address the phenomenon of ‘foreign fighters’ – is a key example. But preventive justice can also extend – under the guise of the term ‘border security’ – to extensive monitoring of mobility via the use of immigration control for security purposes⁷ and can also take the form of generalised, pre-emptive surveillance.⁸

The development of a number of EU databases, the widening of access to these databases (including immigration databases) to security authorities, and the introduction of systems of generalised surveillance under data retention and regulatory frameworks on passenger name records (PNR) are

³ See A. Ashworth and L. Zedner, *Preventive Justice*, Oxford: Oxford University Press, 2014.

⁴ Also referred to as ‘*Feindstrafrecht*’ – see inter alia G. Jakobs, “Feindstrafrecht? – Eine Untersuchung zu den Bedingungen von Rechtlichkeit”, *HRRS* 8/9, 2006, p. 289 et seq.

⁵ See inter alia P.-A. Albrecht, “La Politique Criminelle dans L’État de Prévention”, *Déviance et Société*, Vol. 21, 1997, p. 123 et seq.

⁶ See U. Sieber, “Der Paradigmenwechsel vom Strafrecht zum Sicherheitrecht”, Max-Planck-Institut für ausländisches und internationales Strafrecht, which also appeared in K. Tiedemann, U. Sieber, H. Satzger, C. Burchard and D. Brodowski (eds), *Die Verfassung moderner Strafrechtspflege Erinnerung an Joachim Vogel*, Baden-Baden: Nomos Verlagsgesellschaft, 2016, pp. 351-372.

⁷ D. Bigo and E. Guild (eds), *Controlling Frontiers*, Farnham: Ashgate, 2005; V. Mitsilegas, “Human Rights, Terrorism and the Quest for ‘Border Security’”, in M. Pedrazzi, I. Viarengo and A. Lang (eds), *Individual Guarantees in the European Judicial Area in Criminal Matters*, Brussels: Bruylant, 2011, pp. 85-112; and V. Mitsilegas, “Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens Strengthening the State”, *Indiana Journal of Global Legal Studies*, Vol. 19, No. 1, 2012, pp. 3-60.

⁸ D. Lyon, *Surveillance Society: Monitoring Everyday Life*, Maidenhead: Open University Press, 2001; K.D. Haggerty and R.V. Ericson, “The Surveillant Assemblage”, *British Journal of Sociology*, Vol. 51, No. 4, 2000, p. 605 et seq.; L. Amoore and M. de Goede (eds), *Risk and the War on Terror*, London: Routledge, 2008; V. Mitsilegas, “The Transformation of Privacy in an Era of Pre-Emptive Surveillance”, *Tilburg Law Review*, Vol. 20, No. 1, 2015, pp. 35-57.

examples of EU action in this context. Critical to the development of preventive justice in this context is the collection, processing and exchange of a wide range of personal data. All these features of the preventive justice paradigm can be found in the emergence of the Union's security strategy building the Security Union.

1.3 The Security Union as a multi-purpose and cross-sectoral endeavour: Blurring the boundaries between migration, crime, security and foreign policy

The Commission's Communication on the "European Agenda for Security" emphasised the need for a joined-up interagency and cross-sectoral approach.⁹ This approach reflects a blurring of the boundaries between different areas of EU law and policy, ranging from immigration to criminal justice to foreign policy to defence. A laboratory in this field has been the development of EU policies aiming at controlling borders and mobility, where the traditional paradigm of immigration control has been replaced by an emphasis on border security.¹⁰

These developments mirror the US approach, where a notable recommendation of the 9/11 National Commission Report was to target what was termed "terrorist travel",¹¹ resulting in the development of systems of generalised surveillance of mobility such as the establishment of PNR systems aimed at intervening pre-departure and preventing movement if necessary. In this paradigm, border control measures have thus been adopted and developed as security measures and data obtained in the context of immigration and border control (e.g. data on visa applications or passenger information) are also viewed as security data, which must be

⁹ European Commission, "The European Agenda on Security", COM(2015) 185 final, Strasbourg, 28.4.2015.

¹⁰ V. Mitsilegas, "Border Security in the European Union. Towards Centralised Controls and Maximum Surveillance", in E. Guild, H. Toner and A. Baldaccini (eds), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Oxford: Hart Publishing, 2007, pp. 359-394.

¹¹ See the National Commission on Terrorist Attacks, 2004, p. 385.

accessible not only by immigration authorities, but also by intelligence and law enforcement authorities for security purposes.¹²

Recent developments on the use of Security Council resolutions to boost EU action on border security, through the Common Foreign and Security Policy (CFSP) under the banner of operation EUNAVFOR Med, confirm the further blurring of boundaries between immigration, security and defence, and result in the militarisation of the border.¹³ This cross-policy and interagency approach is based on maximum collection and exchange of personal data and access to EU databases irrespective of their main purpose or rationale. A constant theme in the seventh and eighth Commission progress reports towards the Security Union is the prioritisation of the interoperability of databases.¹⁴ A High-Level Expert Group on Information Systems and Interoperability was established and reported in May 2017,¹⁵ while the mandate of the EU's IT-management system is currently being revised to include the specific task of enabling interoperability.¹⁶ The most recent report on the Security Union at the time of writing emphasises yet again the need for enhancing information exchange and operational cooperation.¹⁷

This blurring of boundaries between the use of various databases has significant consequences for fundamental rights and citizenship. Enabling

¹² V. Mitsilegas, "The Law of the Border and the Borders of Law: Rethinking Border Control from the Perspective of the Individual", in L. Weber (ed.), *Rethinking Border Control for a Globalizing World*, London: Routledge, 2015, pp. 15-32.

¹³ D. Bigo, "The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts", *Security Dialogue*, Vol. 45, No. 2, 2014, pp. 209-225.

¹⁴ See European Commission, "Seventh progress report towards an effective and genuine Security Union", COM(2017) 261 final, Strasbourg, 16.5.2017 and "Eighth progress report towards an effective and genuine Security Union", COM(2017) 354 final, Brussels, 29.6.2017.

¹⁵ See High-Level Expert Group on Information Systems and Interoperability, "Final report", European Commission, DG for Migration and Home Affairs, May 2017 (<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>).

¹⁶ See the European Commission's "Proposal for a new Regulation on eu-LISA", COM(2017) 352 final, Brussels, 29.6.2017, Art. 9.

¹⁷ European Commission, "Ninth Progress Report towards an effective and genuine Security Union", COM(2017) 407 final, Brussels, 26.7.2017, p. 3.

access to immigration databases such as the Visa Information System (VIS) and Eurodac to law enforcement and security authorities overlooks the purpose of immigration law and poses significant challenges to privacy, data protection and non-discrimination.¹⁸ The shift from border control to the generalised surveillance of mobility further serves to extend control and surveillance to *all* travellers, including EU citizens – thus undermining fundamental principles of free movement and citizenship within the EU.¹⁹ Blurring boundaries in this manner results in an all-encompassing, yet at the same time amorphous concept of security, which is continually prioritised but may serve to undermine key distinctions and limits to the reach of the state in the lives of individuals.

1.4 Blurring the boundaries between internal and external security

Another element in the emergence of the preventive justice paradigm in the Security Union, linked inextricably with calls for a multi-purpose and cross-cutting approach outlined above, is the merging of internal and external security. This trend is acknowledged by the European Agenda on Security, stating expressly that

we need to bring together all internal and external dimensions of security. Security threats are not confined by the borders of the EU. EU internal security and global security are mutually dependent and interlinked. The EU response must therefore be comprehensive and based on a coherent set of actions combining the internal and external dimensions, to further reinforce links between Justice and Home Affairs and Common Security and Defence Policy. Its success is highly dependent on cooperation with international partners. Preventive engagement with third countries is needed to address the root causes of security issues.²⁰

¹⁸ N. Vavoula, “Immigration and Privacy in the Law of the European Union: The Case of Databases”, PhD thesis, Queen Mary University of London, 2017.

¹⁹ See V. Mitsilegas, “The Borders Paradox: The Surveillance of Movement in a Union without Internal Frontiers”, in H. Lindahl (ed.), *A Right to Inclusion and Exclusion? Normative Fault Lines of the EU’s Area of Freedom, Security and Justice*, Oxford: Hart Publishing, 2009, pp. 33-64.

²⁰ See European Commission, “The European Agenda on Security”, COM(2015) 185 (2015), op. cit.

The emergence of the EU as a global security actor is not a novel phenomenon. The EU has played a leading role in negotiating major international and regional conventions on transnational crime and security and its institutions and certain Member States participate in non-traditional, global security norm-setters such as the Financial Action Task Force (FATF) and the UN Security Council, both key actors in developing a paradigm of preventive justice in the field of terrorist sanctions.²¹ The EU then revises its internal *acquis* to comply with the international standards it has contributed to shaping, claiming that it is essential for the EU legal order to align with global norms.²²

There is thus a process of synergy, which can result in the introduction of far-reaching norms into the EU legal order that may challenge fundamental legal principles. The evolution of criminal law on 'foreign fighters' is a characteristic example in this context: norms first developed by the UN Security Council have been transplanted into the legal orders of EU Member States, first via the revision of the Council of Europe Counter-terrorism Convention and subsequently via the revision of EU substantive criminal law on terrorism.²³ As with the regular revisions of internal EU anti-money laundering and terrorist finance law (justified as essential to align the EU *acquis* with the new standards by the FATF),²⁴ the extension of EU substantive criminal law on terrorism has followed a paradigm developed initially by the Security Council.

This internalisation of external norms has also occurred through transatlantic security cooperation. A key example in this regard is the

²¹ V. Mitsilegas, "The European Union and the Globalisation of Criminal Law", in C. Barnard and O. Odudu, *Cambridge Yearbook of European Legal Studies 2009-2010*, Vol. 12, Oxford: Hart Publishing, 2010, pp. 337-407.

²² V. Mitsilegas, "The EU and the Implementation of International Norms in Criminal Matters", in M. Cremona, J. Monar and S. Poli (eds), *The External Dimension of the Area of Freedom, Security and Justice*, Bern: Peter Lang, 2011.

²³ V. Mitsilegas, "The European Union and the Global Governance of Crime", in V. Mitsilegas, P. Alldridge and L. Cheliotis (eds), *Globalisation, Criminal Law and Criminal Justice: Theoretical, Comparative and Transnational Perspectives*, Oxford: Hart Publishing, 2015, pp. 153-198.

²⁴ For more on the latest EU directive, see V. Mitsilegas and N. Vavoula, "The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law", *Maastricht Journal of European and Comparative Law*, Vol. 23, No. 2, 2016, pp. 261-293.

emergence of preventive legislation on PNR data. The conclusion of a series of EU-US international agreements enabling the transfer of PNR data to US authorities has been the outcome of the need for the EU to comply with unilateral US legal requirements and has been controversial in challenging fundamental rights in the EU legal order.²⁵ However, and notwithstanding these concerns, recent terrorist incidents in Europe have provided political justification for the internalisation of this model of preventive surveillance in the EU, through the adoption of an 'internal' PNR Directive. The challenges to EU values that this internalisation of external standards in the field of security can pose should not be underestimated. The recent Opinion of the Court of Justice of the European Union (CJEU) on the EU-Canada PNR Agreement²⁶ confirms that PNR systems as currently devised fall foul of fundamental rights in the EU.

1.5 Blurring the boundaries between the public and the private: Everyday data and dangerousness

The model of preventive justice focuses increasingly on the collection by the state of personal data and the co-option of the private sector in the fight against crime. The collection of personal data involves data generated by ordinary, everyday life activities. This includes records of financial transactions,²⁷ airline travel (PNR) reservations²⁸ mobile phone telecommunications,²⁹ and digital evidence.³⁰ The focus on monitoring

²⁵ V. Mitsilegas, "Transatlantic Counter-terrorism Cooperation and European Values: The Elusive Quest for Coherence", in D. Curtin and E. Fahey (eds), *A Transatlantic Community of Law*, Cambridge, MA: Cambridge University Press, 2014, pp. 289-315.

²⁶ See Opinion 1/15 of the Court (Grand Chamber) on the EU-Canada PNR Agreement, 26 July 2017.

²⁷ See V. Mitsilegas, *Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance versus Fundamental Legal Principles*, The Hague: Kluwer Law International, 2003; M. de Goede, *Speculative Security*, Minneapolis: University of Minnesota Press, 2012.

²⁸ V. Mitsilegas, "Contrôle des étrangers, des passagers, des citoyens: Surveillance et anti-terrorisme", *Cultures et Conflits*, No. 58, 2005, pp. 155-182.

²⁹ V. Mitsilegas, *EU Criminal Law*, Oxford: Hart Publishing, 2009.

³⁰ S. Carrera, G. Gonzalez-Fuster, E. Guild and V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Centre for European Policy Studies, Brussels, July 2015.

everyday life may thus result in mass surveillance, marked by the collection and storage of personal data in bulk.

Inextricably linked with the focus on the monitoring of everyday life for preventive purposes is the privatisation of surveillance under a model of what has been referred to as a 'responsibilisation strategy' aiming to co-opt the private sector in the fight against crime:³¹ banks and other financial and non-financial institutions (as well as lawyers), airlines, mobile phone and Internet providers among others are legally obliged to collect, store and reactively or proactively transfer personal data to state authorities. The privatisation of preventive justice in this manner expands considerably the reach of the state and poses grave challenges to fundamental rights.

Everyday and sensitive personal data are now being collected *en masse* and legislation imposes growing demands for this data to be transferred from the private sector to state authorities in a generalised manner. This has led to what has been called "the 'disappearance of disappearance' – a process whereby it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions".³² State authorities thus have access to a wealth of personal data, enabling practices such as profiling and data mining. As the Court of Justice noted in *Tele2* regarding retention of metadata,

[t]hat data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them ... In particular, that data provides the means ... of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.³³

The impact of state intervention on the individual is intensified when one considers the potential of combining personal data from different databases

³¹ D. Garland, "The Limits of the Sovereign State", *British Journal of Criminology*, Vol. 36, No. 4, 1996, pp. 445-471.

³² Haggerty and Ericson (2000), *op. cit.*, pp. 605-622.

³³ See CJEU, Judgment of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and 698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others*, para. 99.

collected for different purposes in a landscape of blurring boundaries and interoperability described above in order to create a profile of risk or dangerousness. Mass surveillance is linked closely with ongoing risk assessment in the preventive justice model. As noted by a number of governments intervening in the CJEU EU-Canada litigation, the use of PNR data

is intended to identify persons hitherto unknown to the competent services who present a potential risk to security, while persons already known to present such a risk can be identified on the basis of advance passenger information data. If solely the transfer of PNR data concerning persons already reported as presenting a risk to security were authorised, *the objective of prevention could consequently not be attained.* (Emphasis added)³⁴

1.6 Caught between the public-private and internal-external divides: Digital evidence as a Trojan horse?

In addition to existing statutory mechanisms requiring the collection and transfer of everyday information from the private sector to the state, a broader issue has arisen with regard to access by the state to personal data held by private companies in the context of cross-border investigations. The issue has been framed by EU institutions as one concerning ‘digital evidence’ in the context of the fight against ‘cybercrime’, although in reality it concerns judicial cooperation in criminal matters. The Commission has recently published a so-called non-paper on improving cross-border access to electronic evidence.³⁵ The non-paper reiterates the Commission’s commitment in the Communication on a European Agenda on Security to reviewing obstacles to criminal investigations on cybercrime, notably on issues of access to electronic evidence, and set out the issues as follows:

For most forms of crimes, in particular cybercrimes as witnessed recently, electronic evidence – such as account subscriber information, traffic or metadata, or content data – can provide significant leads for investigators, often the only ones. The electronic evidence connected to these crimes is often cross-

³⁴ See Opinion 1/15 on the EU-Canada PNR Agreement (op. cit.), para. 58.

³⁵ See the non-paper from the Commission services, “Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward” (undated) (https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf).

jurisdictional, for example because the data is stored outside the investigating country or by providers of electronic communications services and platforms – whose main seat is located outside the investigating country, resulting in investigating authorities not being able to use domestic investigative tools.

The Commission's non-paper summarises work undertaken by the Commission's services and states that cross-border access to electronic evidence may be obtained in three ways:

- through formal cooperation channels between the relevant authorities of two countries, usually through mutual legal assistance (MLA) or a European Investigation Order (EIO) (where applicable), or police-to-police cooperation;
- through direct cooperation between law enforcement authorities of one country and service providers whose main seat is in another country, either on a voluntary or mandatory basis. Notably service providers established in the US and Ireland reply directly to requests from foreign law enforcement authorities on a voluntary basis, as far as the requests concern non-content data; and
- through *direct access* from a computer, as allowed by a number of Member States' national laws.

The Commission claims that the current legal frameworks reflecting traditional concepts of territoriality are challenged by the cross-jurisdictional nature of electronic services and data flows, adding that a number of Member States and third countries have developed or are developing national solutions that might result in conflicting obligations and fragmentation and create legal uncertainty for both authorities and service providers. It also claims that owing to the fact that the concept of territoriality is still based largely on the place where data is stored, any cross-border access to electronic evidence that is not based on cooperation between authorities may raise issues in terms of territoriality, with this applying both within the EU and where data is stored in a third (non-EU) country.

The different scenarios for future action set out in the Commission's non-paper must be scrutinised fully and approached with caution at this stage. All three scenarios put forward – direct cooperation between law enforcement authorities, direct cooperation between law enforcement authorities and the private sector and most importantly, direct access to private databases – challenge fundamental principles of judicial cooperation in criminal matters in the EU and serve to bypass recently adopted EU law containing a high level of fundamental rights protection, namely the

Directive on the European Investigation Order. The Commission is pushing for broader availability of and accessibility to personal data under a model of prevention by framing an issue of judicial cooperation in criminal matters, requiring judicial authorisation, as an issue pertaining to ‘cybercrime’. It thus seems to adopt an agenda privileging police efficiency at the expense of a number of safeguards for the individual.

The Commission claims in this respect that the problem is territoriality, when in reality solutions can be found under the current EIO and externally through the MLA systems to endeavour to provide information in a speedy manner – one of the key aims of mutual recognition in criminal matters under the EIO is in fact to secure this speed. The Commission also seems keen to blur the boundaries between internal and external action in the field, disregarding the important and critical case law of the CJEU regarding the data protection and privacy benchmarks required by third countries – and in particular the US – for data exchanges to take place. Direct cooperation between law enforcement authorities and the private sector and direct access to private databases cause a number of concerns in this regard, in an era in which the adequacy of US requirements is continually being questioned in courts on both sides of the Atlantic.

In view of the significant challenges that the proposed models pose to fundamental rights and the integrity of the EU *acquis*, the justification for these new ideas seems to be limited. It is striking that the Commission seems to adopt as a justification piecemeal practices in a number of jurisdictions, whose compatibility with EU law is questionable. This follows a similar pattern as the justification for adopting an internal EU PNR system, which was justified – notwithstanding the controversy regarding the transatlantic PNR agreements – on the basis that a small number of EU Member States operated internal PNR systems. The legality of the EU PNR Directive is currently questionable following the CJEU Opinion on the EU-Canada PNR Agreement.

1.7 Challenges of preventive justice to fundamental rights, citizenship and the rule of law

The evolution of Europe’s Security Union within a paradigm of preventive justice poses significant dilemmas for the rule of law, the protection of fundamental rights and citizenship in the EU. In terms of the rule of law, preventive justice entails serious challenges *ex ante* (at the stage of the adoption of EU rules in terms of the existence and exercise of EU competence

to legislate and in terms of justification of EU action, transparency and democratic control) and *ex post* (in terms of setting limits to the arbitrariness of state action and ensuring full and effective judicial scrutiny and control).³⁶

In terms of challenges to the rule of law *ex ante*, a key example is the recent introduction into EU law of the criminalisation of conduct related to ‘foreign fighters’ – with UN Security Council standards being transposed into EU law via the vehicle of amending the Council of Europe Convention, in a 9/11-style emergency framing with no impact assessment or full scrutiny of the constitutional implications of these proposals.

Challenges to the rule of law *ex ante* are also posed by shifts in legality and the use of legal bases (with the legal bases of the Area of Freedom, Security and Justice (AFSJ) being replaced by CFSP legal bases on terrorist sanctions and border security) and by the shift from the adoption of legal standards as such to an emphasis on unregulated operational action and cooperation. The rule of law *ex post* is challenged by limits to effective judicial protection and state arbitrariness, as evidenced in relation to preventive terrorist sanctions by the extensive *Kadi* litigation in the CJEU. Rule of law *ex post* concerns are inextricably linked with fundamental rights issues.

A paradigm of security based upon preventive justice additionally challenges a number of fundamental rights, including the principle of legality in criminal offences and sanctions, the presumption of innocence (through the preventive criminalisation of terrorism and organised crime), the right to an effective remedy and effective judicial protection. It gives rise to concerns, in particular in cases of generalised pre-emptive surveillance outlined in this chapter, about the principle of non-discrimination and the rights to privacy and data protection.

In a series of landmark rulings, the CJEU has upheld the importance of the rights to data protection and privacy and found generalised pre-emptive surveillance contrary to EU law.³⁷ The Court has further confirmed that the

³⁶ On the distinction between rule of law *ex ante* and *ex post*, see V. Mitsilegas, “Rule of Law: Theorising EU Internal Security Cooperation from a Legal Perspective”, in M. Rhinard and D. Bossong (eds), *Theorising European Internal Security*, Oxford: Oxford University Press, 2016, pp. 113-114.

³⁷ CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*; see also *Tele2 Sverige* and *Watson* (op. cit.); and Opinion 1/15 on the EU–Canada PNR Agreement (op. cit.).

EU fundamental rights benchmark is also applicable in the Union's external action, in the fields of both judicial cooperation in criminal matters³⁸ and data exchange.³⁹

Judicial interventions are important in this context in highlighting the close link between protecting the right to privacy and upholding citizenship ties by safeguarding trust in the relationship between the individual and the state.⁴⁰ This link between privacy and citizenship has been underscored by constitutional courts in EU Member States in litigation over the constitutionality of preventive data retention measures. According to the German Constitutional Court,⁴¹

a preventive general retention of all telecommunications traffic data ... is, among other reasons, also to be considered as such heavy infringement because it can evoke a sense of being watched permanently ... The individual does not know which state official knows what about him or her, but the individual does know that it is very possible that the official does know a lot, possibly also highly intimate matters about him or her.

The Romanian Constitutional Court has noted on the other hand that data retention addresses all of the law's subjects, regardless of whether they have committed criminal offences or whether they are the subject of a criminal investigation, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes.

Also according to the Romanian Court, continuous data retention is sufficient to generate, in the mind of the persons, legitimate suspicions regarding the respect of their privacy and the perpetration of abuses (by the state).⁴² These concerns have been reflected in the case law of the CJEU,

³⁸ CJEU, Judgment of Court (Grand Chamber) of 6 September 2016 in Case C-182/15 *Petruhhin v Latvijas Republikas Ģenerālprokuratūra*.

³⁹ CJEU, Judgment of the Court (Grand Chamber) of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*.

⁴⁰ V. Mitsilegas, "The Value of Privacy in an Era of Security", *International Political Sociology*, Vol. 8, No. 1, 2014, pp. 104-108.

⁴¹ Judgment of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1BvR 586/08, para. 24..

⁴² Romanian Constitutional Court, Decision No. 1258 of 8 October 2009.

where the adverse impact of generalised preventive surveillance without an explicit link to a specific suspicion has been pointed out.⁴³

In its recent ruling in *Tele2 Sverige and Watson*, which built upon the Court's ruling in *Digital Rights Ireland*, the CJEU noted that the interference of systematic and continuous data retention with the rights to privacy and data protection is very far-reaching and must be considered to be particularly serious, as the fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance.⁴⁴

The Court noted that the legislation in question, which was found to be contrary to EU law, affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings; therefore, it applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences.⁴⁵ Protecting the right to privacy is essential to uphold citizenship ties more broadly in this context.

1.8 The way forward: Constitutionalising the Security Union

The above analysis has cast light on the challenges that the evolution of the European security strategy and a Security Union relying increasingly on a paradigm of preventive justice poses for the rule of law, the protection of fundamental rights and citizenship in Europe. The management of Union security responses has in recent months taken the form of regular reports on

⁴³ For an overview and on the specific link between surveillance and suspicion, see V. Mitsilegas, "Surveillance and Digital Privacy in the Transatlantic 'War on Terror': The Case for a Global Privacy Regime", *Columbia Human Rights Law Review*, Vol. 47, No.3, 2016, pp. 1-77.

⁴⁴ See *Tele2 Sverige and Watson* (op. cit.), para. 100.

⁴⁵ *Ibid.*, para. 105; see also Opinion 1/15 on the EU-Canada PNR Agreement, para. 205 (op. cit.), where the Court noted that

as regards air passengers in respect of whom no such risk has been identified on their arrival in Canada and up to their departure from that non-member country, there would not appear to be, once they have left, a connection – even a merely indirect connection – between their PNR data and the objective pursued by the envisaged agreement which would justify that data being retained.

the Security Union, combined – also in response to repeated terrorist incidents in major European cities – with separate communications by the European Council and the Commission. The ongoing emphasis on the Security Union and the publication of Commission reports almost on a monthly basis serve to produce timely reactions to events, but risk continually promoting *new* EU action and the adoption of new legislation in the field of security, thus replicating earlier security responses post-9/11 and post-7/7.

Calls for new measures and initiatives may present the political and symbolic advantage of being seen to be doing something, and of responding urgently to terrorism. However, prior to the Security Union resulting in yet more EU law in the field, detailed and serious thought should be given to three matters: the adequacy of the existing – and quite extensive – Union legal framework on security, the effectiveness of proposed new initiatives, and the compatibility of Union security measures with the European constitution and its key values, including fundamental rights and the rule of law.

Overreacting on security and disregarding fundamental rights in the process poses a direct challenge to the very values upon which the Union is based, values that the Union is constitutionally bound to uphold and promote in its external action after Lisbon. With the Security Union based increasingly upon operational cooperation, interoperability and the generalised collection and exchange of personal data under a model of pre-emptive surveillance, the risks posed to fundamental rights, but also essential bonds of trust and citizenship across the Union are acute.

The CJEU's rejection of generalised surveillance, in a series of landmark and consistent cases, should be taken fully into account by the other Union institutions in developing the Security Union and making it rights-compliant. In times of upheaval, it is the judiciary that has reminded us of the importance of fundamental rights guarantees in the process of constitutionalising the Security Union and setting limits to an uncritical move towards prevention.

2. TWO CRUCIAL CHALLENGES IN CROSS-BORDER CRIMINAL INVESTIGATIONS

ANNE WEYEMBERGH

Considerable progress has been made in terms of cooperation within the EU in the area of cross-border criminal investigations. However, the area is still facing many challenges. This contribution does not intend to be exhaustive but to highlight two main themes for the future of cooperation in this field, namely the need for greater consistency and complementarity among the various aspects of criminal justice (section 2.1) and the need to learn all the lessons from the current achievements and complete the EU integration process in this area (section 2.2).

2.1 A need for greater consistency and complementarity in criminal justice matters

The EU's criminal justice area should be designed and established as a coherent system with weights and counterweights. Complementarity among its different instruments is essential. It is evident in the case of the relationship between mutual recognition and the approximation of laws: the link between the two aspects is expressly enshrined in Art. 82(2) of the Treaty on the Functioning of the European Union (TFEU), which subordinates approximation in procedural matters to the condition that it is necessary in order to facilitate mutual recognition and cooperation. Such a link is, for instance, clear with respect to evidence. As happened with the European Arrest Warrant (EAW),¹ the practical application of the Directive on the

¹ Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002, pp. 1-20.

European Investigation Order (EIO)² will most probably reveal the need to adopt complementary harmonising measures.³

There is also a need to achieve greater consistency and complementarity among the different mutual recognition instruments and among these and other tools aimed at enhancing cooperation in cross-border investigations (section 2.1.1). Another aim should be to achieve better consistency and complementarity among the different EU actors competent in the field (section 2.2.2). Finally, enhanced cooperation and variable geometry is particularly challenging for the coherence of the EU area of criminal justice (section 2.2.3).

2.1.1 *Mutual recognition instruments*

As we had the chance to write elsewhere,⁴ there is an obvious need for more consistency and complementarity among the mutual recognition instruments.

Currently, there is a lack of consistency among these instruments, which affects their legitimacy and credibility. When comparing the various framework decisions and directives applicable, some differences are striking, for instance as to the grounds permitted for refusal, including those based on fundamental rights, or as to the proportionality test to be conducted by the competent authorities before issuing or executing a decision, order or warrant.

The interaction between these mutual recognition instruments should also be developed, for instance the relationship between the EAW and the EIO calls for reflection. The same is true for the relationship between the EAW and the European Supervision Order.⁵ “Organising” their interactions

² Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1-36 (see recital 43).

³ See for instance, C. Janssens, *The Principle of Mutual Recognition in EU Law*, Oxford: Oxford University Press, 2013, p. 261.

⁴ See A. Weyembergh, I. Armada and C. Brière, “Critical assessment of the existing European Arrest Warrant Framework Decision”, Research paper for the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (IPOL-JOIN_ET(2013)510979_EN), 2014.

⁵ Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view

would especially contribute towards solving the issue of overuse of the EAW for prosecution purposes and the resulting issue of overuse of pre-trial detention.⁶

The same is also true for the interaction/relationship between mutual recognition instruments and other available tools intended to strengthen cooperation in cross-border investigations. This is especially the case for the relationship between the joint investigation teams (JITs)⁷ and the EIO. The question arises as to whether there is some kind of overuse of JITs in the sense that they are increasingly used without any 'cross-border physical move' of the national authorities involved, the latter staying in their own territory where they perform their investigations on their own but using the JIT tool to exchange, smoothly and rapidly, the information they obtain from their counterparts. Is such a use of JITs in line with the objective pursued by the EU legislator? It would, in any case, be necessary to improve the way in which JITs interact with the EIO.

Whereas a few elements show that there is some awareness in this regard,⁸ deeper reflection is needed as to how to optimise recourse to and the interactions between the various elements offered by the 'EU toolbox'. Among the recommendations that we have made elsewhere in this regard⁹ is to provide for a clear duty for the practitioners, when they intend to resort to one of the EU tools, to pay due consideration to available alternative measures. This implies having knowledge of the overall picture of the EU area of criminal justice and thus particular efforts in terms of training the competent authorities.

to the supervision of probation measures and alternative sanctions, OJ L 337, 16.12.2008, pp. 102-122.

⁶ See Weyembergh, Armada and Brière (2014), *op. cit.*

⁷ Council Framework Decision 2002/465/JHA on joint investigation teams, OJ L 162, 20.6.2002, pp. 1-3.

⁸ See for instance the EIO Directive, where the interaction with the EAW and EIO is explicitly tackled in recital 26. Indeed, it states:

With a view to the proportionate use of an EAW, the issuing authority should consider whether an EIO would be an effective and proportionate means of pursuing criminal proceedings. The issuing authority should consider, in particular, whether issuing an EIO for the hearing of a suspected or accused person by videoconference could serve as an effective alternative.

⁹ Weyembergh, Armada and Brière (2014), *op. cit.*

2.1.2 *EU specialised agencies and bodies*

The increase in the number of EU specialised agencies and bodies in justice and home affairs (JHA) is well known. Such ‘abundance’ means that good articulation between them is required, especially if the purpose is to establish a consistent Area of Freedom, Security and Justice in which its three interrelated components – freedom, security and justice – are effectively implemented. Sound articulation between the EU bodies is also crucial in order to develop a multidisciplinary approach in the fight against serious cross-border crime. This need for articulation has been repeatedly underlined, particularly by EU institutions, for which there must be complementarity, which implies working hand-in-hand to achieve common goals, the respect of specific mandates and expertise, as well as good communication and coordination in case of overlaps.

However, establishing such complementarity is proving a difficult task for a number of reasons. Among these, one can mention the structural differences traceable to the time when they were established and to the modalities of their establishment by the EU legislator (e.g. first or third pillar), the differences in professional cultures (e.g. police and justice), the silo approach taken by both the Commission and the Council, in which the EU agencies/bodies are dealt with by different directorates-general within the Commission (which do not always entertain the best relations) and by different units in the General Secretariat of the Council.¹⁰

Against this background, the legislative instruments governing each EU agency/body remain vague with regard to cooperation with counterparts. Interagency relations are mostly left to the EU agencies and bodies themselves. This reflects the need for flexibility, which is indeed important. Nonetheless, and particularly where there are clear overlaps between their respective mandates or difficulties in collaboration, more concrete legislative provisions regulating bilateral cooperation might well need to be added to the relevant instruments of EU secondary law.

A general improvement in relations between the EU agencies and bodies has been witnessed, due to the conclusion or revision of bilateral agreements and memoranda of understanding, to the passage of time and the resulting gains in terms of experience. Such improvement also stems

¹⁰ This resulted from the division of the ex-Directorate-General 2 devoted to judicial cooperation in civil and criminal matters, police and customs cooperation.

from other factors, such as the creation of coordination and monitoring mechanisms and the encouragement of interagency cooperation in JHA. It has especially taken the form of meetings of the JHA contact group and of the JHA heads of agencies. They annually report to the Standing Committee on Operational Cooperation on Internal Security,¹¹ notably through a scorecard on cooperation, which is annexed to the common annual report they present. Recently adopted legislative texts, such as the Europol Regulation,¹² and the proposals under negotiation, such as the Eurojust Regulation,¹³ show that this effort has already been made in part, for instance with the establishment of the 'hit/no hit' system in the information sharing regime between Eurojust and Europol.¹⁴

Still, and in spite of a lot of quite positive official declarations, there are difficulties to resolve. Among the 'worrying' elements is the growing imbalance of powers and resources between Europol and Eurojust: the former especially benefits from more resources and has been conferred an essential role in the internal security strategy, whereas the latter has far less in terms of resources and is weakened by the current fragmentation of the EU's judicial actors, which will become even more pronounced with the arrival of a new judicial actor, namely the European Public Prosecutor's Office (EPPO).¹⁵

¹¹ This Standing Committee was set up within the Council by the Council Decision of 25 February 2010 and has met regularly since March 2010.

¹² Regulation (EU) No. 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), OJ L 135, 24.5.2016, pp. 53-114.

¹³ Council of the European Union, Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) – General approach, 6643/15, Brussels, 27 February 2015.

¹⁴ See Art. 40 of the proposal for a Eurojust Regulation and Art. 21 of the Europol Regulation.

¹⁵ See I. Armada, C. Brière and A. Weyembergh, "Competition or cooperation? State of play and future perspectives on the relations between Europol, Eurojust and the European Judicial network", *New Journal of European Criminal Law*, Vol. 6, No. 2, 2015, pp. 258-287; I. Armada, C. Brière and A. Weyembergh, "The interagency cooperation and future architecture of the EU criminal justice and law enforcement area", Research paper for the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (IPOL_STU(2014)510000), November 2014.

The establishment of the latter creates new complexity. As a new EU judicial body, the EPPO will have to integrate itself into the landscape of existing EU agencies/bodies that are also active in protecting the EU's financial interests. Its relations with the EU's Anti-Fraud Office (OLAF), Eurojust and Europol will be of crucial importance to ensure that the EPPO contributes effectively to fighting offences against the EU's financial interests. These relations will be set out in specific provisions in the future EPPO and Eurojust regulations but they suffer from several weaknesses.¹⁶ They will also be further developed when Regulation 883/2013 on OLAF¹⁷ is being revised.

2.1.3 *Management of variable geometry*

There is a need for deep reflection on the management of variable geometry and the imbalances that it creates. The role of enhanced cooperation in both police and judicial cooperation in criminal matters has clearly increased over time. It has acquired a growing place with the Treaty of Lisbon and has become more topical with the advent of the EPPO, which will be established via enhanced cooperation as permitted by Art. 86(1) TFEU¹⁸ and as set out in the Commission's White Paper of 1 March 2017 on the future of Europe.

¹⁶ See C. Brière and A. Weyembergh, "Relations between the EPPO and Eurojust – Still a privileged partnership?", in P. Geelhoed, A. Meij and L. Erkelens (eds), *Shifting Perspectives on the European Public Prosecutor's Office*, The Hague: Asser Press, Springer Verlag, 2017, forthcoming; C. Brière and A. Weyembergh, "The future cooperation between OLAF and the European Public Prosecutor's Office", Study for the Committee on Budgetary Control of the European Parliament (PE 603.789), June 2017 and by the same authors, "Towards a European Public Prosecutor's Office (EPPO)", Study for the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (PE 571.399), November 2016 ([http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571399/IPOL_STU\(2016\)571399_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571399/IPOL_STU(2016)571399_EN.pdf)).

¹⁷ Regulation (EU, Euratom) No. 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No. 1073/1999 and Council Regulation (Euratom) No. 1074/1999, OJ L 248, 18.9.2013, pp. 1-22.

¹⁸ For the final version of the regulation, resulting from the negotiations within the Council before the launch of enhanced cooperation as provided for by Art. 86(1), see Council of the European Union, Proposal for a Regulation on the establishment of the European Public Prosecutor's Office, 5766/17, 31 January 2017.

Enhanced cooperation procedures are among the ways forward set out in that latter document and particularly so in the areas of justice and security.¹⁹

Whereas enhanced cooperation presents advantages, it threatens the coherence of the European criminal justice area. Indeed, allowing some Member States to avoid or to escape part of the *acquis* brings with it the risk of ending up with serious imbalances. Two examples can be given in this respect. First, as regards the aforementioned complementarity among mutual recognition instruments, the UK has so far been bound by the EAW but not by the European Supervision Order, although it strongly denounced what it perceived as overuse of the EAW in the pre-trial phase. Second, as in the case of Denmark, Ireland is bound by the EAW but not by the EIO.²⁰ In terms of the relationship between mutual recognition and approximation of laws, neither the UK, Ireland nor Denmark are bound by Directive 2013/48 on the right of access to a lawyer,²¹ which ensures that the person subject to an EAW has access to a lawyer in the executing state and is informed of his/her right to appoint a lawyer in the issuing state.²² Such examples raise a question as to the limits of the ‘pick and choose’ possibility. Limits aimed at ensuring consistency do exist and should be taken into due consideration. However, they are not systematically provided for and seem rather randomly applied.²³

A solid effort in this field should be made. The role of the Court of Justice of the European Union (CJEU) in this regard is also notable, as shown by its two interesting decisions in *UK v Council* where it limited the ‘cherry-

¹⁹ See particularly the third scenario of the European Commission’s White Paper on the Future of Europe, Reflections and Scenarios for the EU27 by 2025, COM(2017) 2025, Brussels, 1.3.2017.

²⁰ See Houses of the Oireachtas, Joint Committee on European Scrutiny, *Sixth Report: Special Report on New EU Legislation, 1 January to 30 June 2010*, November 2010, p. 225.

²¹ Directive 2013/48/EU of the European Parliament and of the Council 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, pp. 1-12.

²² *Ibid.*, Art. 10.

²³ About these limits, see A. Weyembergh, “Enhanced cooperation in criminal matters: Past, present and future”, in R. Kert and A. Lehner (eds), *Liber Amicorum für Frank Höpfel*, Vienna, 2017, forthcoming.

picking' approach to the Schengen Protocol.²⁴ Indeed, the Court insisted on the importance of maintaining the coherence of the *acquis*²⁵ and concluded that Member States legitimately refused to authorise the participation of the UK in the relevant measures (i.e. the Frontex Regulation²⁶ and the Decision concerning access to the Visa Information System²⁷). These are two important precedents but it remains to be seen whether the Court will be given and will seize the opportunity to defend the consistency of the EU *acquis* as it did in both of these respects.

2.2 A need to learn lessons from current achievements and complete the EU integration process

On some points, the EU integration process in the penal domain is incomplete and this entails the risk of resulting in an unbalanced EU area of criminal justice or an area missing some of its objectives or not being efficient enough in reaching them. Four illustrations of such incompleteness follow.

First, there is a certain level of incompleteness resulting from the poor level of transposition by the Member States. There is an obvious need to monitor this closely, to check for correct transposition in the Member States and to launch infringement procedures if necessary. Since 1 December 2014, i.e. the end of the transitional period, such infringement procedures can also be launched for the absence of or bad transposition of 'old instruments' of the ex-third pillar of the Treaty on European Union. Such a possibility does not seem to have been fully exploited so far. Furthermore, it should be exploited in all the domains of criminal justice – not only in those sectors seeking to develop security, but also in the approximation of procedural

²⁴ See the decisions of the CJEU in Case C-77/05, *UK v Council* (Frontex Regulation) [2007] and Case C-482/08, *UK v Council* (Decision concerning access to the Visa Information System) [2010].

²⁵ Case C-482/08 (*supra*), para 48.

²⁶ Council Regulation (EC) No. 2007/2004 of 26 Oct. 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25.11.2004, p. 1.

²⁷ Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.8.2008, p. 129.

guarantees for suspects and accused persons, for instance. Indeed, it is the effectiveness of the whole area of criminal justice that is to be guaranteed.

Second, mutual recognition is not complete in the sense that it does not cover the entire landscape of judicial cooperation. We refer here to the transfer of proceedings, where a proposal was negotiated before the entry into force of the Lisbon Treaty but was abandoned,²⁸ and to the quite complex field of disqualification decisions.²⁹ There is also a need to accompany mutual recognition with other measures, without which it can be detrimental to individuals. Two examples are worth recalling here. On the one hand, more ambitious rules to prevent and solve conflicts of jurisdiction but also to modernise and reinforce the *ne bis in idem* principle should be on the EU's legislator's agenda.³⁰ Indeed, on several points, the existing ones are not sufficiently ambitious. On the other hand, the EU should also address the issue of compensation for unjustified arrest, detention and surrender or transfer on the basis of EAWs or other relevant instruments of mutual recognition. Indeed, practice shows that cases of unjustified detention for the purpose of executing an EAW, for instance, do take place. Unjustified detentions may be the consequence of different circumstances, i.e. clear mistakes by the issuing or executing states (or both), or errors by the person, for example following the theft or selling of identity cards.

The concerned persons sometimes receive compensation but sometimes they do not. The question is extremely complex: situations that should give rise to compensation are very different, the difficulties the persons may face, and the way responsibility may shift between the issuing and executing states may vary considerably. EU intervention in this field is urgently needed. The differences among national compensation mechanisms may be regarded as impairing the achievement of an EU area of criminal justice where EU citizens can equally enjoy their rights. The EU should ensure that reinforced judicial cooperation is not detrimental to individuals' fundamental rights. It follows that in order to counterbalance the

²⁸ Council of the European Union, Proposal for a Council Framework Decision on the transfer of proceedings in criminal matters, 11119/09, 30 June 2009.

²⁹ See the Programme of measures to implement the principle of mutual recognition of decisions in criminal matters, OJ C 12, 15.1.2001, pp. 10-22.

³⁰ See potential derogations to the *ne bis in idem* principle as provided in Art. 55 of the Convention on Implementing the Schengen Agreement.

‘prosecutorial effect’ of the EAW and other mutual recognition instruments, the EU has a responsibility to ensure that the individual who suffers from unjustified detention receives fair compensation, as provided for by Art. 6 of the Charter read together with Art. 53, para. 2. This EU obligation would mirror the one provided for in Art. 5, para. 5 of the European Convention on Human Rights³¹ as interpreted by the European Court of Human Rights.³²

Third, on a series of points, the defence position and cooperation should be strengthened. In recent years and particularly since the entry into force of the Lisbon Treaty, a lot of initiatives have been launched and several new, important instruments have been adopted, as illustrated by the six directives approximating procedural guarantees for suspects and accused persons.³³ Yet, much is still to be done, concerning for instance the training of defence lawyers, EU handbooks specifically designed for them, the

³¹ The European Convention on Human Rights provides in its Art. 5(5) as follows: “Everyone who has been the victim of arrest or detention in contravention of the provisions of this Article shall have an enforceable right to compensation.” Under EU law a right to compensation may be deduced from Art. 6 of the Charter read together with Art. 53(2).

³² For more details, see “Compensation” in Council of Europe, A guide to the implementation of Art. 5 of the ECHR, Human Rights Handbook No. 5, Strasbourg, pp. 67-68.

³³ See the following directives of the European Parliament and of the Council: Directive 2010/64/EU of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ L 280, 26.10.2010, pp. 1-7; Directive 2012/13/EU of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, pp. 1-10; Directive 2013/48/EU (op. cit.), pp. 1-12; Directive (EU) 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, pp. 1-11; Directive (EU) 2016/800 of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132, 21.5.2016, pp. 1-20; and Directive (EU) 2016/1919 of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, pp. 1-8.

creation of an institutionalised network of defence lawyers^{34, 35} or the set-up of a secure system for exchanging information in cross-border cases.³⁶

Fourth, the integration process is incomplete because it does not go far enough in some respects, in the sense that it does not push EU integration as far as needed to achieve its objectives. This is, for instance, clear in protecting the EU's financial interests if one takes a look at the current version of the EPPO Regulation: the question is whether it goes far enough to be able to attain the objectives of effectively preventing and fighting fraud related to the EU budget and of protecting individuals' rights. Indeed, during the negotiations, Member States tended to renationalise – or re-horizontalise – the EPPO as much as possible.³⁷

2.3 Concluding remarks

The aforementioned observations do not intend to 'condemn' the numerous EU achievements in the field. They aim at highlighting and raising awareness of some of the main challenges ahead. In this context, one should keep in mind that it is a work in progress. In line with the dynamic or step-by-step approach dear to the founding fathers of the EU, much is still to come and to be done. In order for the EU and its Member States to reach their destination, there is a final, essential point to highlight, which is the need to keep a high level of expertise and objectivity in the field, particularly when it comes to *ex ante* evaluations or impact assessments. Some impact

³⁴ See for instance, G. Vernimmen-Van Tiggelen and L. Surano, "Analyse transversale", in G. Vernimmen-Van Tiggelen, L. Surano and A. Weyembergh (eds), *The future of mutual recognition in criminal matters in the European Union*, Université Libre de Bruxelles, 2009, p. 560; see also European Criminal Policy Initiative, "A Manifesto on European Criminal Procedure Law", *ZIS*, 11/2013, p. 435.

³⁵ Ambitious proposals have been put forward in the past, i.e. the Eurodefensor – see especially S. Schüneman (ed.), *Ein Gesamtkonzept für die europäische Strafrechtspflege* [A European Programme of Criminal Law and Procedure], 2006, p. 93.

³⁶ In this regard, see the lack of continuity of the pilot project "PenalNet – Secure E-Communications in Criminal Law Practice", which was an initiative developed from 2007 to 2013, supported and co-financed by the European Commission, and involving the Spanish, French, Hungarian, Italian and Romanian bar associations.

³⁷ See Brière and Weyembergh (2016), *op. cit.*

assessments have been neglected³⁸ while others have been criticised.³⁹ In this respect, a considerable effort is needed because, if EU intervention in the field lacks credible justification, then it will face a real problem of legitimacy.

³⁸ See the proposal for a directive on combating terrorism and replacing Council Framework Decision 2002/475/JHA, COM(2015) 625 final, 2.12.2015, which justifies quite briefly the absence of an impact assessment in spite of its sensitivity: “Given the urgent need to improve the EU framework to increase security in the light of recent terrorist attacks including by incorporating international obligations and standards, this proposal is exceptionally presented without an impact assessment.”

³⁹ See for instance European Commission, Regulatory Scrutiny Board, opinion on the DG JUST - Proposal for a Regulation on Mutual Recognition of Freezing and Confiscation Orders (Ref. Ares(2016)6635351 - 25/11/2016), Brussels, 2016.

3. OLD AND NEW CHALLENGES TO EUROPEAN CRIMINAL JUSTICE

PETRA BÁRD

Criminal justice in the EU Member States poses multiple challenges to the rule of law and human rights, and vice versa: deterioration of the latter values jeopardises the effective operation of crime prevention and prosecution. The first part of this chapter will look at three of these challenges and show how EU criminal cooperation between the Member States takes the problems to a new level. The second part considers the difficulties of existing mechanisms in tackling the three problems.

3.1 Three challenges for criminal justice

3.1.1 *Everyday science fiction and the quest for absolute security*

The quest for absolute security dates back to postmodernism, making societies victims of their own structures and generating risk factors of various sorts: health, environmental, criminal, etc. The primary objective became the identification of insecurities and their prevention.¹ The fight against terrorism vividly illustrates politics and law-making based on the worst-case scenario, striving at maximum security.²

The point of departure of the proponents of the security model is that security and human rights are competing aspects that might mutually exclude each other. They insist that the global threat to security necessitates an entirely new equilibrium. Threat creates emergency, and emergency situations call for a different allocation of liberties than what we are used to in normal times. New technologies in crime prevention – such as CCTV

¹ See U. Beck, *Risikogesellschaft: auf dem Weg in eine andere Moderne*, Frankfurt am Main: Suhrkamp, 1986; A. Giddens, *The consequences of modernity*, Cambridge: Polity Press, 1991.

² G.T. Marx, “La Société de Sécurité Maximale”, *Déviance et Société*, Vol. 12, No. 2, 1988, pp. 147-166.

cameras, DNA fingerprinting for ever-more types of crimes or even misdemeanours, the extensive use of wiretapping, data fishing, sales of security in the private sphere to victims (e.g. camera use or chips placed on or in their loved ones, including dogs and kids) – result in a so-called surveillance assemblage³ that is typical of postmodern societies. New attempts to formulate the quest for security in the rights language make these claims stronger than ever.⁴

Those wary of the security-versus-liberty balance metaphor emphasise that the two notions do not constitute a zero-sum game, not least because they are not comparable concepts.⁵ An alleged new equilibrium would constitute numerous problems: those concerned insist that some fundamental rights cannot be abandoned, that giving them up is a slippery slope and that it will be extremely difficult to regain liberties once we have abandoned them. They voice their worries about the growing tendencies of negative attitudes towards religious organisations, ethnic minorities, foreigners and asylum seekers. In relation to new technologies, they emphasise privacy and data protection considerations.⁶

The stress placed on the security side of the balance has some further, less direct and more subtle drawbacks from the point of view of the rule of law. Actual rights have to be given up for the sake of a perceived, future danger, whereas it is extremely difficult to determine the probability of the danger occurring. The ‘risk society’ prepares for the worst case, the ‘what if’ scenario, placing everything and everyone under surveillance and control so as not to overlook any type of risk and new technologies serve as ideal tools in this exercise. From a technological viewpoint, the possibilities are limitless. The question is whether a certain morality could be enforced and

³ See, e.g. R. Lippert, “Signs of the surveillant assemblage: Urban CCTV, privacy regulation and governmentality”, *Social and Legal Studies*, Vol. 18, No. 4, 2009, pp. 505-522.

⁴ L. Lazarus, “The right to security – Securing rights or securitising rights?”, in R. Dickinson, E. Katselli, C. Murray and O.W. Pedersen, *Examining critical perspectives on human rights*, Cambridge and New York, NY: Cambridge University Press, 2012, pp. 87-106.

⁵ E. Guild, S. Carrera and T. Balzacq, “The Changing Dynamics of Security in an Enlarged European Union”, Challenge Research Paper No. 12, Centre for European Policy Studies, Brussels, 2008, pp. 8-9 (<https://www.ceps.eu/system/files/book/1746.pdf>).

⁶ C. Sunstein, *Laws of fear: Beyond the precautionary principle*, Cambridge, MA: Cambridge University Press, 2005.

rationality could be reintroduced into decision-making through legal means to prevent abuses called into life by risk hysteria.

Problems at the national level are multiplied in the EU context, not least with the principle of availability introduced by The Hague programme, where “the methods of exchange of information should make full use of new technology”.⁷ The Council Presidency further clarified that “the aim is obviously that as large a list of information categories as possible is exchangeable with as little effort as possible (i.e. requiring a minimum of formalities, permissions, procedures, if any)”.⁸ Interoperability became the magic word for databases in the EU. Beyond the problems related to the creation of a panoptic society, this also means that information kept in violation of privacy rights in one Member State⁹ could easily end up being used in a criminal procedure in another EU member country, thereby proliferating potential infringements of human rights.¹⁰

3.1.2 *Cruelty of the Middle Ages in contemporary criminal justice*

We also face an opposite problem. While science fiction-like high-tech solutions employed in the fight against crime pose new problems, we still face centuries-old challenges we thought to have abandoned towards the end of the Middle Ages with the Enlightenment infiltrating into the criminal justice systems of the day. Cesare Beccaria spoke out against cruel and barbaric criminal sanctions already in 1764,¹¹ but we still have cases where

⁷ See The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, OJ C 53/1, 3.3.2005.

⁸ Presidency of the Council of the European Union, “Approach for enhancing the effective and efficient information exchange among EU law enforcement authorities”, 7416/05, Brussels, 17 March 2005, point 5.

⁹ Cf. European Court of Human Rights, *S and Marper v United Kingdom*, Application nos. 30562/04 and 30566/04, 4 December 2008.

¹⁰ See Council of the European Union, Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210/1, 6.8.2008 and Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210/2, 6.8.2008.

¹¹ Cesare marchese di Beccaria, *On crimes and punishments*, trans. by H. Paolucci, Indianapolis, IN: Bobbs-Merrill, 1963.

states violate the absolute prohibition of torture, inhuman and degrading treatment or punishment.

More specifically, when such problems in the domestic setting are systemic,¹² abuses are “exported” and multiplied in the EU criminal cooperation setting, especially with the help of the principle of mutual recognition.¹³ The principle was labelled by the Tampere Programme in 1999 as a “cornerstone” of judicial cooperation contributing to the Union becoming an Area of Freedom, Security and Justice.¹⁴ In 2000 the Commission further defined the concept as meaning that a judicial decision, once taken in one Member State, should automatically be accepted in all other Member States, and have the same or at least similar effects there.¹⁵ Meanwhile, both the EU legislative and the judiciary refined the principle in an attempt to make sure that the principle does not lead to the multiplication of human rights abuses.

European co-legislators have introduced a proportionality check, a consultation process between the executing and issuing judicial authority and explicit grounds for non-execution based on fundamental rights in the 2014 Directive on the European Investigation Order.¹⁶ In the same year the European Parliament, in a resolution based on a “legislative initiative report”, called for similar grounds to be introduced in the framework decision on the European Arrest Warrant¹⁷ and more generally, in respect of

¹² See e.g. European Court of Human Rights, *Varga and Others v Hungary*, Application nos. 14097/12, 45135/12, 73712/12, 34001/13, 44055/13, and 64586/13, 10 March 2015.

¹³ Art. 82(1) TFEU states: “Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83.”

¹⁴ Presidency Conclusions of the Tampere European Council of 15 and 16 October 1999, Bull. 10/1999, point 33.

¹⁵ European Commission, Communication on “Mutual recognition of Final Decisions in criminal matters”, COM(2000) 0495 final, Brussels, 27.6.2000, p. 2.

¹⁶ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130/1, 1.5.2014.

¹⁷ Council of the European Union, Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial, OJ L 81/24, 27.3.2009.

other measures implementing mutual recognition in the area of judicial cooperation in criminal matters.¹⁸ This latter suggestion has not yet been taken up by the Commission; however, another branch of government, the EU judiciary, came to rescue. In April 2016,¹⁹ for the first time in the history of EU criminal cooperation, the Court of Justice of the European Union (CJEU) held that mutual trust in the mechanisms for fundamental rights protection of all Member States cannot be taken for granted; even if an EU instrument does not contain a fundamental rights exception for refusing enforcement, the executing judicial authority must not blindly trust the issuing Member State. Rather, it has to assess the fundamental rights situation in that country. Even though the Court left a number of issues open,²⁰ the judgment can be seen as a milestone in putting a halt to the proliferation of human rights abuses.

3.1.3 *An all-encompassing problem: Rule of law backsliding*

Rule of law backsliding should also be mentioned in this context.²¹ In a country based on the rule of law, built-in correction mechanisms compensate for the deficiencies of a majoritarian government: the doctrines of separation of powers, checks and balances, constitutional scrutiny, judicial oversight and media pluralism all make sure that those in power do not abuse power.

¹⁸ See European Parliament, Resolution of 27 February 2014 with recommendations to the Commission on the review of the European Arrest Warrant (2013/2109 (INL)), P7_TA-PROV(2014)0174. See also M. del Monte, "Revising the European Arrest Warrant", European Added Value Assessment accompanying the European Parliament's Legislative Own-Initiative Report (Rapporteur: Baroness Ludford MEP), European Parliamentary Research Service, PE 510.979, March 2014, along with Annex I to that assessment by A. Weyembergh with the assistance of I. Armada and C. Brière, "Critical Assessment of the Existing European Arrest Warrant Framework Decision" and Annex II by A. Doobay, "Assessing the Need for Intervention at EU level to Revise the European Arrest Warrant Framework Decision".

¹⁹ CJEU, Judgment of the Court (Grand Chamber) of 5 April 2016, *Pál Aranyosi and Robert Căldăraru v Generalstaatsanwaltschaft Bremen*, Requests for a preliminary ruling from the Hanseatisches Oberlandesgericht in Bremen, Joined Cases C-404/15 and C-659/15 PPU.

²⁰ For details, see W. van Ballegooij and P. Bárd, "Mutual Recognition and Individual Rights: Did the Court get it Right?", *New Journal of European Criminal Law*, Vol. 7, No. 4, 2016, pp. 439-464.

²¹ The term has been coined by J.-W. Müller in "Safeguarding Democracy inside the EU: Brussels and the Future of Liberal Order", Working Paper No. 3, Transatlantic Academy, Washington, D.C., 2013.

These institutions and procedures operate along the paranoid logics of constitutional law introducing precautionary measures into democratic systems to protect them against a future potential government acquiring and retaining powers at all costs, i.e. superseding constitutional government with emotional government.

In contrast, in a country making a U-turn on the path of the rule of law, the government will systematically eliminate the channels for any kind of internal dissent, i.e. diminishing the potentialities for criticism, for example by modifying election laws through gerrymandering, weakening the powers of the constitutional court, influencing the judiciary, eliminating ombudsman's offices, weakening media pluralism and attacking civil society. This is what academic literature denotes as constitutional capture²² and what the Lisbon Treaty calls a "serious and persistent breach" of EU values.²³ At the time of writing, Member States illustrating such systemic threats include Hungary²⁴ and Poland,²⁵ but established democracies are not immune to rule of law challenges either.

For the first time in EU treaty history, the Lisbon Treaty expressly refers to Union values. Art. 2 of the Treaty on European Union (TEU) makes clear that the EU is a *Wertegemeinschaft*,²⁶ a community based on common values. Nevertheless, the EU is lacking an enforcement mechanism for these foundational values. The challenge underlying enforcement lies in the debate about conferral of powers and national sovereignty, subsidiarity and proportionality, i.e. about the vertical separation of powers between the EU and its constitutive elements. With special regard to purely internal

²² J.-W. Müller, *Constitutional Patriotism*, Princeton, NJ: Princeton University Press, 2007.

²³ See Art. 7 of the Treaty on European Union.

²⁴ See e.g. the European Parliament Resolution of 3 July 2013 on the situation of fundamental rights: Standards and practices in Hungary (pursuant to the European Parliament Resolution of 16 February 2012) (2012/2130(INI)), which is commonly referred to by the name of its rapporteur, the (Rui) 'Tavares Report', or more recently European Parliament Resolution of 17 May 2017 on the situation in Hungary (2017/2656(RSP)).

²⁵ See the European Commission's College Orientation Debate on recent developments in Poland and the Rule of Law Framework, Brussels, 13 January 2016 (http://europa.eu/rapid/press-release_MEMO-16-62_en.htm).

²⁶ See for example Konrad Adenauer's address at the Foreign Press Association in London on 7 December 1951, in *Bulletin des Presse- und Informationsamtes der Bundesregierung*, Nr. 19/51, 314.

situations, the legitimacy of EU interference is repeatedly questioned by Member States. But a Member State's breach of fundamental values should be regarded as a European issue. It is likely to undermine the very foundations of the Union and the trust between its members, whatever field the breach occurs in.²⁷ Beyond harming nationals of a Member State, Union citizens residing in that state will also be detrimentally affected. A lack of limits to illiberal practices²⁸ may encourage other Member State governments to follow suit. In other words, rule of law violations – if no consequences occur – may become contagious.²⁹

Moreover, all EU citizens will to some extent suffer due to the given state's participation in the EU's decision-making mechanisms, and to say the least, the legitimacy of decision-making of the Union will be affected. Therefore, a state's departure from the rule of law standards and the European consensus will ultimately hamper the exercise of rights of individuals EU-wide.³⁰ Rule of law backsliding does not leave any legal domain intact and also jeopardises the criminal justice system. Acceptance of criminal court judgments, for example, will be legitimately questioned by other Member States, if the issuing country's judiciary lacks independence, if its constitutional tribunal was incapable of exercising meaningful constitutional review or if there was institutional discrimination against certain minorities.

²⁷ European Commission, Communication on "Article 7 of the Treaty on European Union – Respect for and promotion of the values on which the Union is based", COM(2003) 606 final, Brussels, 15.10.2003, p. 5.

²⁸ The term was coined long ago, but it gained practical relevance in the EU after Hungarian Prime Minister Viktor Orbán praised such state approaches in his speech given in Tusnádfürdő on 25 July 2014. The original speech is accessible in video format (<https://www.youtube.com/watch?v=PXP-6n1G8ls>). Cf. the speech by Frans Timmermans: "there is no such thing as an illiberal democracy" (see F. Timmermans, "EU framework for democracy, rule of law and fundamental rights", Speech to the European Parliament, Strasbourg, Speech/15/4402, 12 February 2015).

²⁹ See L. Waller, "Viktor Orbán: The conservative subversive", in "Class of 2017", *Politico* 28, 2017.

³⁰ For further effects on the EU, see P. Bárd, S. Carrera, E. Guild and D. Kochenov, "An EU Mechanism on Democracy, the Rule of Law and Fundamental Rights", CEPS Paper in Liberty and Security, No. 91, Centre for European Policy Studies, Brussels, 2016, pp. 62-68.

3.2 Remedies to tackle the three problems and their challenges

Whereas there are a number of mechanisms addressing the above problems, they suffer from fundamental flaws.

First, European mechanisms to tackle the above problems – at least those with an effective enforcement mechanism – are mainly human rights-oriented. They might remedy problems in the first and second scenarios mentioned – science fiction-like violations of privacy on the one hand, and more traditional human rights abuses on the other. The third type of rule of law problems, however, are not effectively tackled. Future Member States are filtered for their compliance with these values before they accede to the Union,³¹ but no similar method exists to supervise adherence to these foundational principles after accession. History and recent events have proven that this so-called ‘Copenhagen dilemma’ is currently a very vivid one in the EU.

Although there are several EU-level instruments for evaluating and monitoring EU values at the Member State level,³² these mechanisms constitute a scattered and patchwork set of Member States’ EU surveillance systems overseeing their obligations with regard to the rule of law and fundamental rights.³³ The only ‘hard law’ with a Treaty basis is Art. 7 TEU. Yet Art. 7 has never been activated in practice because of a number of political and legal obstacles. In response to these deficiencies, in 2014 the European Commission launched a new EU framework to strengthen the rule of law,³⁴ commonly known as the pre-Art. 7 procedure. The pre-Art. 7

³¹ See European Parliament, Plenary debate on the political situation in Romania, statement by Viviane Reding, 12 September 2012. See also V. Reding, “The EU and the Rule of Law: What Next?”, speech delivered at the Centre for European Policy Studies, Brussels, 4 September 2013.

³² These include, for instance, the Cooperation and Verification Mechanism for Bulgaria and Romania, the EU Justice Scoreboard, the EU Anti-Corruption Report, as well as the European semester, annual reports on fundamental rights published periodically by the European Commission, the European Parliament and the Fundamental Rights Agency, Commission infringement procedures (Arts 258 and 259 of the Treaty on the Functioning of the European Union, TFEU), peer reviews in accordance with Art. 70 TFEU, and European Parliament resolutions.

³³ Bárd et al. (2016), op. cit.

³⁴ European Commission, Communication, “A New EU Framework to Strengthen the Rule of Law”, COM(2014) 158, Strasbourg, 11.3.2014.

procedure, however, does not remedy the problem. Its monitoring dimension is weak in nature; the launch of a ‘rule of law opinion’ or a ‘rule of law recommendation’ in the frame of a pre-Art. 7 process is rather discretionary; the assessment is not carried out by entirely independent academic experts who would ensure the full impartiality of the findings; and finally, it has also failed on the efficiency test at its debut vis-à-vis Poland.³⁵ Academics and policy-makers caught up with the issue of rule of law backsliding and constitutional capture in the EU soon after it happened in some Central and Eastern European Member States, and formulated an array of proposals for how to deal with the outstanding problems,³⁶ but the EU branches of government have not yet taken up the early suggestions.

Second, the main entities responsible for the enforcement of EU values are the courts, which are well suited to solve human rights-related problems, especially if minorities’ rights are at stake. Minorities are often misrepresented or lacking any representation. Some are simply not part of the electorate (typically certain groups of detainees are affected, but in the UK, none of them have voting rights), while others simply constitute an unpopular minority and as a consequence fall victim to majoritarianism. Members of minority groups who have been excluded from ‘we the people’

³⁵ For the initial recommendation, see the Commission recommendation regarding the rule of law in Poland, C(2016) 5703 final, Brussels, 27.7.2016 (http://ec.europa.eu/justice/effective-justice/files/recommendation-rule-of-law-poland-20160727_en.pdf). For later developments and their criticism, see e.g. L. Pech and K. Lane Scheppele, “Poland and the European Commission, Part III: Requiem for the Rule of Law”, *VerfBlog*, 3 March 2017 (<http://verfassungsblog.de/poland-and-the-european-commission-part-iii-requiem-for-the-rule-of-law/>); P. Bárd and S. Carrera, “The Commission’s Decision on ‘Less EU’ in Safeguarding the Rule of Law: A play in four acts”, CEPS Policy Insights, No. 2017/08, Centre for European Policy Studies, Brussels, March 2017, pp. 1-11 (<https://www.ceps.eu/publications/commission’s-decision-‘less-eu’-safeguarding-rule-law-play-four-acts>).

³⁶ For brief overviews, see C. Closa, D. Kochenov and J.H.H. Weiler, “Reinforcing the Rule of Law Oversight in the European Union”, RSCAS Working Paper 2014/25, European University Institute, Florence, 2014; E.-M. Poptcheva, “Member States and the rule of law: Dealing with a breach of EU values”, Briefing, European Parliament Research Service (PE 554.167), March 2015 ([http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/554167/EPRS_BRI\(2015\)554167_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/554167/EPRS_BRI(2015)554167_EN.pdf)). For more in-depth analyses, see the contributions in C. Closa and D. Kochenov (eds), *Reinforcing Rule of Law Oversight in the European Union*, Cambridge, MA: Cambridge University Press, 2016; and A. Jakab and D. Kochenov (eds), *The Enforcement of EU Law and Values*, Oxford: Oxford University Press, 2016.

may be granted participation in democratic processes by courts and ombudspersons – entities anyway better equipped with tools of human rights protection than other branches of power. Whereas courts are the ideal branch of power to deal with human rights infringements, they are less equipped to address rule of law challenges, especially in a state of constitutional capture.

Third, the weakness of external apex courts – such as the European Court of Human Rights (ECtHR), still the main human rights defender in Europe – should be mentioned. The Strasbourg Court is not exposed to the above problem, i.e. to being captured, but it is relatively insensitive to the specificities of the EU legal system, such as the principles of loyalty, mutual trust or mutual recognition – or at least this was the criticism of the Luxembourg Court in Opinion 2/13 vetoing EU accession to the European Convention on Human Rights.³⁷ Such a problem could only be overcome if the CJEU has a chance to scrutinise all EU cases with a human rights element before the ECtHR does so. Should it establish a judicial review for human rights cases that corresponds to Strasbourg tests, the fears over the ECtHR disrespecting or indeed violating the EU law principles, such as the primacy, unity and effectiveness of EU law, would recede.

The ECtHR has already paved the way for such a mechanism by establishing the *Bosphorus* presumption and making sure that only cases that the CJEU has had a say on end up in Strasbourg.³⁸ The ECtHR still keeps this option open, even after Opinion 2/13 was delivered and even though that Opinion was fairly hostile to human rights and the Strasbourg Court in particular.³⁹ However, for the *Bosphorus* presumption to survive, and so as to grant individuals meaningful rights equivalent to the protection afforded by the Strasbourg mechanism, the EU's legislative and judicial powers will have to clarify how they wish to reconcile the protection of fundamental rights with EU values, such as mutual trust, mutual recognition,⁴⁰ respect for national identities and the primacy of EU law, and how they wish to share

³⁷ CJEU, Opinion 2/13 of 18 December 2014.

³⁸ ECtHR, *Bosphorus v Ireland*, Application no. 45036/98, 20 June 2005; *Michaud v France*, Application no. 12323/11, 6 December 2012.

³⁹ ECtHR, *Avotiņš v Latvia*, Application no. 17502/07, 23 May 2016.

⁴⁰ Van Ballegooij and Bárd (2016), op. cit.

responsibility among the Member States, and between the Member States and the EU when ensuring liberty and security.⁴¹

Finally, as things currently stand in the EU, all enforcement mechanisms – including those addressing human rights violations and those tackling rule of law problems – are unresponsive. They can neither prevent deterioration nor culmination into systemic breaches of human rights and rule of law violations, nor can they serve as the basis of mutual trust and recognition.

It seems that the establishment of an *ex ante* rule of law mechanism, including human rights monitoring based on equality, scientific rigour and sound methodology, is inevitable. The mechanism should entail a prompt response to rule of law backsliders, and should include effective, dissuasive and proportionate sanctions.⁴² This would be vital for the EU, since deterioration of the rule of law at the domestic level is ultimately also a European matter. A state's departure from the European consensus on rule of law standards will eventually hamper the exercise of individuals' rights EU-wide. As long as the Member States – with or without good reason – have no faith in one another's mechanisms for human rights protection, the administration of EU criminal justice will also remain cumbersome.

Apart from these substantive problems, the principle of primacy would also be jeopardised. Member States would invoke the human rights argument in order to permit exemptions from the principle of primacy of EU law. The German Federal Constitutional Court is most illustrative for retaining the right to be the ultimate reviewer of EU law in the form of fundamental rights, *ultra vires* or constitutional identity review.⁴³ Whereas the German Constitutional Court takes a firm stance on protecting its own

⁴¹ "If used lightly and carelessly, the national security exception can be a much stronger centrifugal force in Europe than cries of constitutional identity could ever be." See R. Uitz, "The Return of the Sovereign: A Look at the Rule of Law in Hungary – and in Europe", *VerfBlog*, 5 April 2017 (<http://verfassungsblog.de/the-return-of-the-sovereign-a-look-at-the-rule-of-law-in-hungary-and-in-europe>).

⁴² See the European Parliament Resolution of 25 October 2016 with recommendations to the Commission on the establishment of an EU mechanism on democracy, the rule of law and fundamental rights (2015/2254(INL)), P8_TA-PROV(2016)0409.

⁴³ For such attempts, see e.g. BVerfGE 37, 271 – Solange I, 7 BVerfGE 73, 339 – Solange II, BVerfGE 102, 147 – Bananenmarktordnung, BVerfGE 89, 155 – Maastricht, BVerfGE 123, 267 – Lissabon, BVerfG, 21.06.2016 – 2 BvR 2728/13; 2 BvR 2728/13; 2 BvR 2729/13; 2 BvR 2730/13.

review powers on the constitutional permissibility of EU law, it only does so in order to grant EU values a higher level of protection; moreover, in the overall assessment it almost always comes to EU law-friendly conclusions. But its firm stance on being the final arbiter of EU law may encourage other domestic apex courts to follow suit, and to opt out from the principle of primacy, and these latter fora may use the same claims for a less friendly interpretation of EU law or even for lowering the level of human rights protection. Not remedying the problems addressed in the present chapter may therefore potentially have fatal consequences for EU criminal cooperation and the whole of the EU legal system.⁴⁴

⁴⁴ G. Vermeulen, W. De Bondt and C. Ryckman (eds), *Rethinking international cooperation in criminal matters in the EU: Moving beyond actors, bringing logic back, footed in reality*, Antwerp, Apeldoorn and Portland: Maklu, 2012, pp. 269–270.

4. REVIEWING THE EFFECTIVENESS OF EU COUNTER-TERRORISM POLICIES

FIONA DE LONDRAS

A comprehensive review of the effectiveness of EU counter-terrorism policies is welcome. I have previously written that there is a clear need for the effectiveness of the wide range of EU laws and policies on counter-terrorism to be reviewed, not least so as to properly understand their impacts (including on rights) and their legitimacy (beyond legality).¹ The need for such a review is clear when one considers, first, the basic principles of good public administration and the role therein of assessing whether policy decisions actually ‘work’; second, the impact in domestic legal systems across the EU Member States of measures introduced in Brussels; and third, the demands of democratic legitimacy within a multi-level structure such as the European Union.

However, having accepted the need for a comprehensive review of EU counter-terrorism policies, the Union – and particularly Commissioner Julian King – is faced with the question of how to go about that review. That is the focus of this contribution, which makes three connected but discrete arguments. These are i) that asking the right questions is key to the success of an effectiveness review, ii) that understanding context is vital to assessing effectiveness and framing potential recommendations, and iii) that such a review must take into account the limitations of the EU and the implications thereof for counter-terrorism. This chapter addresses each of these points in turn.

¹ See F. de Londras, “Governance Gaps in EU counter-terrorism: Implications for democracy and constitutionalism”, in F. de Londras and J. Doody (eds), *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism*, London: Routledge, 2015, p. 204.

4.1 Asking the right questions

An effectiveness review is clearly challenging, not least because it requires an analysis of whether the materials, laws and policies under review actually ‘work’ in a meaningful sense. This is the essence of the concept of effectiveness: for something to be effective it should achieve what it was designed to do.² In the context of counter-terrorism, as in other contexts, this is perhaps more difficult than it sounds, for it requires analysis of both meta-objectives and specific objectives.

Meta-objectives here are the broader objectives of counter-terrorism within a rights-based, liberal constitutionalist milieu *per se*, i.e. to enhance security, to maintain the rule of law and to maintain the constitutionalist character of the polity, state or supra-state institution (in this case the EU). The specific objectives are those that have been articulated for a specific instrument or policy, for example the disruption of terrorist financing or the sharing of passenger name data between aviation corporations and state or supra-state authorities.

While we might imagine that specific objectives should be relatively easy to analyse, in fact challenges can arise from the fact that they are sometimes not clearly articulated, and that questions of scale can arise. So, if an instrument assists in the disruption of some terrorist finance but terrorist organisations have adapted and found other financing mechanisms to evade this regulation, or much conventional financing activity continues undisrupted, is the instrument effective? And is it sufficiently effective to justify any interference with fundamental rights that might be occasioned by its use? These are the kinds of questions that an effectiveness review should be able to answer in a way that, for example, a judicial review ordinarily cannot.

The purpose of judicial review is to check legality and proportionality, but not to enquire definitively into effectiveness *per se*.³ In this way, judicial

² See F. de Londras, “Evaluation and Effectiveness in Counter-Terrorism”, in W. Hardyns, K. Ponnet, G. Reniers, W. Smit, L. Braeckmans and B. Segaert (eds), *Socially Responsible Innovation in Security: Critical Reflection*, London: Routledge, 2018, forthcoming.

³ On the limitations of judicial review in the context of counter-terrorism effectiveness assessment, see F. de Londras, “Accounting for Rights in EU Counter-Terrorism:

review is an important but ultimately limited tool in attempts to review counter-terrorism.⁴ An effectiveness review must, then, ask questions that relate to *both* legality and proportionality (in a classical, quasi-legalistic mode) but *also* to effectiveness. Otherwise, there is no new or added value from the effectiveness review compared with a pre-existing judicial or legal review, and the really difficult questions of the relationship and pay-offs between legal acceptability and practical effectiveness, with connected concerns about legitimacy, cannot be grasped.

4.2 The challenge of context

Getting to these important questions in such a review is anything but simple. This is not least because of three important elements of context: the predetermination of key antecedent questions through the process of compaction, the predetermination of key questions about worthy goals and rationality by the political process, and the pragmatic need for compromise that underpins all law- and policy-making at the EU level.

4.2.1 Compaction

It has long been noted that there is a tendency for domestic counter-terrorism law to be normalised.⁵ That is, that measures introduced as ‘exceptional’ to address difficult counter-terrorism challenges lose their exceptional status, and their innovations begin to ‘creep’ across the legal system. For example, jury-free trials introduced to tackle paramilitary violence begin to be used for organised crime, and the like.⁶ The standard that was considered exceptional when the law was first introduced becomes normalised, and becomes the starting point the next time an extraordinary challenge presents itself. In this way, the starting point for human rights protection is

Towards Effective Review”, *Columbia Journal of European Law*, Vol. 22, No. 2, 2016, pp. 237, 264-267.

⁴ Ibid; see also F. Davis and F. de Londras (eds), *Critical Debates on Counter-Terrorism Judicial Review*, Cambridge, MA: Cambridge University Press, 2014.

⁵ For a comprehensive and illustrative account see, e.g. A. Neal, “Normalization and Legislative Exceptionalism: Counterterrorist Lawmaking and Changing Times of Security Emergencies”, *International Political Sociology*, Vol. 6, No. 3, 2012, p. 260.

⁶ This is what happened with Ireland’s Special Criminal Court; see A. Greene, “Shielding the State of Emergency: Organised Crime in Ireland, the State’s Response”, *Northern Ireland Legal Quarterly*, Vol. 62, No. 3, 2011, p. 249.

consistently renegotiated 'downwards' and our conceptualisation of standard policing (compared with extraordinary security activities) becomes blurred.⁷

The same phenomenon can be observed in the context of EU counter-terrorism, in which the content of a pre-existing measure is taken as a starting point, the necessity, effectiveness, rationality and impact of which does not need to be assessed; its mere existence as part of the *acquis* appears essentially to predetermine its effectiveness. This can be observed in the context of the EU Directive on Combating Terrorism. The explanatory memorandum in which the Directive was proposed by the Commission suggested that the fact that many of the (then-proposed) measures already existed in the 2002 and 2008 Framework Decisions⁸ was sufficient to effectively foreclose debate as to their appropriateness.⁹

This suggestion was notwithstanding the continuing concern on the part of much of civil society about, for example, the expansive nature of the definition of terrorism in the 2002 Framework Decision.¹⁰ Thus, the provisions of the 2002 and 2008 Framework Decisions were 'compacted' (i.e. became hardened and acted as the foundational stones on which the next advancement in the *acquis* would take place), so that at the time the 2017 Directive was proposed, no root and branch assessment of its necessity, rationality and likely impact was actually undertaken.

⁷ On 'downwards recalibration' in human rights and counter-terrorism, see F. de Londras, *Detention in the 'War on Terror': Can Human Rights Fight Back?* Cambridge, MA: Cambridge University Press, 2011; H. Fenwick, "Recalibrating Human Rights and the role of the Human Rights Act post 9/11: Reasserting international human rights norms in the 'war on terror'", *Current Legal Problems*, Vol. 63, No. 1, 2010, p. 153.

⁸ Council of the European Union, Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, p. 3, amended by Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, OJ L 330, 9.12.2008, p. 31.

⁹ European Commission, Proposal for a Directive of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism, COM(2015), 625 final, Brussels, 25.12.2015.

¹⁰ See for example the Joint Submission by Amnesty International, the International Commission of Jurists, the Open Society Justice Initiative and the Open Society European Policy Institute of 6 February 2016 (<https://www.opensocietyfoundations.org/sites/default/files/submission-ec-terrorism-directive-20160219.PDF>).

Taking this tendency towards compaction into account has an important implication for an effectiveness review. It points to the need to strip back these layers of normalisation for the purposes of truly ‘seeing’ and assessing the impacts of counter-terrorism law on the legal system as a whole, in order then to feed that into a consideration of effectiveness.

4.2.2 *Political predetermination*

Any assessment of the proportionality of a measure (in both legal and practical terms) requires a clear scoping of the problem to be addressed, a convincing case that the measure proposed is necessary to address that problem, and establishment that the measures proposed are rationally connected to that aim.¹¹ These are not only expected steps in legalistic proportionality analysis, but also very basic principles of public administration – a process that is fundamentally about problem-solving.

Once again, it has long been observed that security generally (including counter-terrorism) is a field in which these basic principles are sometimes neglected,¹² not least because political decisions that ‘something must be done’ sometimes overtake the administrative (and perhaps bureau-technocratic) processes of problem-scoping and problem-solving. Thus, in domestic jurisdictions the temporal connection between an attack and an (often repressive) counter-terrorism law has been remarked upon,¹³ sometimes with the attack being presented as proof of both the problem and the necessity for the measure in question. Something similar can be seen in the EU context, although perhaps not quite as blatantly. However, where the Council determines that ‘something must be done’, often in the wake of an attack within the Union, the Commission and other agencies of the Union have very little option but to make something happen. Once again, using the recent Directive on Combating Terrorism as an example may be instructive.

The momentum for the 2017 Directive originated in October 2014 with EU Council Conclusions that referenced emerging concerns around foreign terrorist fighters and the need to review the effectiveness of existing legislation to respond to this phenomenon, in particular. The European

¹¹ See, for example, R. Sulitzeanu-Kenan, M. Kremnitzer and S. Alon, “Facts, Preferences, and Doctrine: An Empirical Analysis of Proportionality Judgment”, *Law & Policy Review*, Vol. 50, No. 2, 2016, p. 348.

¹² See for example F. de Londras (2015), *op. cit.*, p. 204.

¹³ For an account see, for example, C. Pantazis and S. Pemberton, “Reconfiguring Security and Liberty”, *British Journal of Criminology*, Vol. 52, No. 3, 2011, p. 1.

Commission in January 2015 and the European Parliament in February 2015 subsequently supported the Council's recommendations, and on 2 December 2015, shortly after the terrorist attacks in Paris, the European Council and the European Parliament adopted the European Commission's proposal for a Directive on Combating Terrorism. The evidence underpinning the proposal was scarce, to say the least.

Although the then-most-recent Europol EU Terrorism Situation and Trend Report at the time indicated that the scale of the problem of foreign terrorist fighters was increasing, there was remarkably little empirical evidence on which to ground the claim that a specific legal instrument to tackle foreign terrorist fighters was needed, or that it should be introduced at the EU level. A similarly vague approach to the scale of the problem and question of necessity preceded the passage of UN Security Resolution 2178 (November 2015) and the Additional Protocol to the Council of Europe Convention on Combating Terrorism (May 2015), giving effect to that Resolution. Here we see also the multi-level nature of compaction, with the content of international instruments to which the EU instrument was giving effect predetermining much of the approach taken in the policy and design phase of the 2017 Directive. Within that context, little or no space was left for critical discussions of necessity, scale and rationality; much of the Union's approach was effectively predetermined by politico-legal decisions taken elsewhere.

4.2.3 *Compromise*

Of course, it is not always the case that counter-terrorism measures emerge from such a process, or have predetermined by politics these key questions of necessity and rationality by reference to the scale of the problem. However, in some cases it is, and in these cases effective review is difficult to undertake as it may require calling into question some decisions that are, ultimately, political decisions as to what role the Union should play in countering terrorism across its Member States.

The nature of the Union as both an entity in itself and a collection of 28 Member States (at least for now) adds a further level of context and complexity to the task of asking the right questions. It is in the nature of all EU laws that they are, fundamentally, a compromise (or a set of compromises) and that the legal instrument (perhaps particularly a directive) that is settled on at the Union level will lay out a minimum level of agreement between the participating states. The obligation on the Member States will then be to implement that minimum standard. Yet, there is no

preclusion on using the legal obligation to implement the Directive on Combating Terrorism as an opportunity to go beyond what it requires and introduce more repressive measures.

The fact that the Directive must be implemented as a matter of law closes out opportunities to challenge the necessity and rationality of the law *per se* at the domestic level, while the information monopolies that exist across the security sphere make it difficult to challenge the claims that country x needs to go even further than the Directive requires in order to tackle the particular dynamics of terrorism in the jurisdiction in question. Combined with the regrettable fact that civil society space and the political purchase of rights are declining in a number of EU Member States (such as Hungary and Poland), this means that the obligation to legislate for European law may well become a licence to legislate for repression.

Any comprehensive review of the effectiveness of EU counter-terrorism – to be meaningful – must also look at what happens to EU law and policy when it ‘leaves’ the European space and ‘enters’ the domestic space: What are its (direct and indirect) impacts on domestic legal standards, human rights, operational protocols and civil liberties? How is the obligation to implement used as an opportunity to advance repressive political priorities and positions? What is the practical effect, in the domestic sphere, of the European instrument? This must be more than a simple implementation review (i.e. a ‘check’ as to whether Member States have fulfilled their legal obligation to implement directives) and instead go into the substance of implementation. That, however, is clearly challenging, and brings us to difficulties arising from the limitations of the EU.

4.3 Dealing with the limitations of the EU

When the attacks of 9/11 took place, the EU did not have a body of counter-terrorism law and policy; now it has an emerging Security Union and a substantial *acquis* in the field. Security-oriented institutions and agencies have been developed, from coordination agencies such as Europol and Eurojust to dedicated institutional offices such as the EU’s Counter-Terrorism Coordinator. All of this has happened without a comprehensive review of EU counter-terrorism policies having taken place: the system has grown and mushroomed, reacting to attacks and risks, innovating for efficiency and circumstance, and becoming increasingly embedded across multiple areas of the workings of the EU.

In that context – when a vast infrastructure and doctrinal *acquis* has developed in a certain area – it can be almost insurmountably difficult to take into account the possibility that the system in itself may be insufficient, ineffective or inappropriate. Nevertheless, for a comprehensive review to be meaningful, surely it must be conducted with an openness to the possibility of such an outcome. The review must, to borrow from Susan Marks,¹⁴ be willing to consider the roots of a problem and then to assess the system’s structures, institutions, laws, policies, assumptions and working practices against the extent to which it enables Member States to tackle those root causes.

In this context, it means that the review must be conducted with a willingness fundamentally to question whether EU law is the appropriate mechanism for achieving the meta-objectives and specific objectives of counter-terrorism. We must be willing to consider critically the implications of a body of law and policy that creates minimum standards and thus licenses *but does not constrain* domestic law-making, in a law and policy field that is notoriously susceptible to overreaching, cognitive bias, false positives and human rights abuses.

As a body of law and policy, EU counter-terrorism does nothing to constrain overreach at the domestic level while creating irresistible imperatives towards domestic legislation – imperatives that can be used to justify processes of making law and policy in national parliaments that are difficult for civil society to penetrate and influence. This is all the more worrying when one considers that it is precisely the *ex ante* processes of impact assessment through which civil society is structurally engaged in the policy-making process that may be ‘bypassed’ by the EU institutions in order speedily to design and implement measures.¹⁵

4.4 Concluding remarks

There is a great danger – with a process limited by time, human resources and budget – that what is billed as a comprehensive review of EU counter-terrorism policies will not have the ability to get to the truly knotty questions

¹⁴ See S. Marks, “Human Rights and Root Causes”, *Modern Law Review*, Vol. 74, No. 1, 2011, p. 57.

¹⁵ On the role of *ex ante* impact assessment in EU counter-terrorism see F. de Londras (2016), *op. cit.*, p. 237. For reasons of ‘urgency’, no *ex ante* impact assessment was carried out for the Directive on Combating Terrorism. See the Explanatory Memorandum to the Directive, European Commission, COM(2015), 625 final (2015), *op. cit.*

suggested here that are vital to a true effectiveness analysis. Without doubt, those questions are difficult, and may well lead to some uncomfortable conclusions. However, the stakes are high, for the EU, for security, for fundamental rights, and for the domestic laws and policies throughout the Member States that are inevitably impacted by the EU *acquis*. In such a context, and with so much at stake, difficult questions are best addressed. Whether the comprehensive review is the vehicle that can and will address them remains to be seen.

5. THE RADICALISATION AWARENESS NETWORK: PRODUCING THE EU COUNTER-RADICALISATION DISCOURSE

DIANA DAVILA GORDILLO AND FRANCESCO RAGAZZI

Radicalisation and counter-radicalisation have been part of the political debate in Europe since 2005, when in the aftermath of the London bombings of that year the EU launched its counter-terrorism strategy under the British presidency of the Council. The strategy was organised around four ‘pillars’:¹ prevent, protect, pursue and respond. Simultaneously, the European Council adopted the “European Union Strategy for Combating Radicalisation and Recruitment to Terrorism”, updated in 2014.² In November 2010, the European Commission presented the “EU Internal Security Strategy”.³ Subsequently, in January 2014, the Commission presented the Communication on “Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU’s Response”.⁴

The EU’s primary role is to support national initiatives to fight terrorism by creating a legal framework for cooperation, providing funding

¹ See Council of the European Union, “The European Union Counter-Terrorism Strategy”, 14469/4/05, Brussels, 30.11.2005.

² Council of the European Union, “The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism”, 14781/4/05, Brussels, 24.11.2005; “Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism”, 15175/08, Brussels, 14.11.2008; “Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism”, 9956/14, Brussels, 15.1.2014.

³ See the “EU Internal Security Strategy” (COM(2010) 673 final, Brussels, 22.11.2010), endorsed by the Council of the European Union.

⁴ European Commission, Communication on “Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU’s Response”, COM(2013) 941 final, Brussels, 15.1.2014.

for internal security and developing common abilities.⁵ As part of these support strategies, in 2011 the European Commission set up the Radicalisation Awareness Network (RAN, Directorate-General for Migration and Home Affairs) as an ‘umbrella network’ to pool expertise, knowledge and good practices, with the collaboration of civil society members (including victims), local authorities, academics and field experts. The RAN is an assistance body for Member States that provides input into national policies through policy recommendations. The RAN policy recommendations, for instance, were considered in the drafting of the 2014 “Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism” and the 2014 Commission Communication on preventing radicalisation mentioned above.

In this chapter, we show that the RAN is one of the core institutions producing a new European discourse on security, in which terrorism is to be governed “through society”.⁶ The policy recommendations of the RAN emphasise that strategies should go beyond traditional law enforcement techniques, promoting the empowerment of communities. They require the involvement of a wide array of actors, including non-governmental organisations (NGOs), experts and front-line practitioners, as well as civil society and communities. Furthermore, they call for training for those acting ‘on the ground’ closer to communities.

In this chapter, we analyse five aspects of these recommendations and how they shape the EU counter-radicalisation response. The chapter examines how i) the discourse of the RAN conceives of policy recommendations that put communities at the centre of counter-radicalisation policies; ii) it conceptualises the development of ‘tailor-made’ strategies; and iii) it reformulates grievances as mere ‘perceptions’, avoiding engagement with factual data. Finally, the chapter shows how the RAN relies on the engagement of iv) key individuals and v) front-line practitioners tasked with propagating the state-sanctioned narrative about radicalisation, with the concomitant exclusion of alternative voices. In conclusion, we show how these recommendations promote a state that ‘rules at a distance’,

⁵ European Commission, “Fighting terrorism at EU level – Fact sheet”, Brussels, 11.1.2015.

⁶ N.S. Rose, *Powers of freedom: Reframing political thought*, Cambridge, UK and New York, NY: Cambridge University Press, 1999.

through proxies but which nonetheless is more in control of the situation within the communities by having people on the ground.

5.1 Shifting responsibility from the state to the community

The RAN policy recommendations justify a shift of responsibilities from the state to the communities, a trend characteristic of advanced liberalism.⁷ At the core of this project lies the objective of empowering communities and key individuals.⁸ Communities are construed as the units based upon which strategies on counter-radicalisation will be devised.

Most importantly, from this perspective, communities are defined as sources of vulnerability, as sources of possible actors and as the spaces within which counter-radicalisation will take place. Locating communities at the centre of counter-radicalisation ensures that actions will take place “at a level closest to the most susceptible individuals in the most affected communities”.⁹

As part of the process of putting communities at the centre of counter-radicalisation, the RAN policy recommendations define radicalisation as a local issue that requires local solutions and active communities. Most importantly, the RAN asserts that this ‘local issue’ can be contained within those communities.

5.2 “Emotions are more important than evidence”

To do so, the policy recommendations stress that the grievances considered to be root causes of radicalisation are not necessarily factual but only perceived or felt by communities. This framing is crucial, because felt or perceived grievances can be managed by communities, whereas factual grievances require at the very least some action from the state. The policy recommendations thus propose strategies that avoid privileging factual or cognitive engagement. For instance, the RAN Working Group on Prison and Probation (P&P) explains: “Emotions are more important than evidence ... success is not achieved in counter-narrative terms through evidence, which

⁷ Ibid.

⁸ RAN, Charter of Principles Governing the Activities of the RAN Center of Excellence, Brussels, 2011.

⁹ Ibid.

can always be refuted and countered. Instead, they need to appeal to human emotions.”¹⁰

Likewise, the RAN Working Group on Deradicalisation and Exit Interventions (RAN DERAD) provides another illustration of this:

The methodological emphasis is put on emotional learning and emotional intelligence rather than cognitive learning and debate skills ... [G]ood-practice interventions don't overstress educational 'topics' or 'historical issues' as such but instead look for the subjective investments placed on them by each participating individual. (Emphasis added)¹¹

Building along the lines of grievances as perceived, the policy recommendations emphasise appealing to human emotions and subjective investment. Evidence and “historical issues” are downplayed. This type of strategy supports the idea of a state that is released from responsibility for the grievances faced by communities. At the same time, individuals and communities are made responsible for their own grievances. In short, communities are increasingly invested with the responsibility of managing and containing radicalisation.

Communities are thus the objects of these policy recommendations, as well as the source of subjects who will be engaged and eventually work as part of the counter-radicalisation policies. This builds on the notion that ‘earlier and closer interventions’ are best. Acting at the ‘closest’ level is one of the crucial arguments the RAN presents to refocus attention on communities. This type of action requires the engagement of local actors. The RAN policy recommendations assert that interventions are only possible through local actions and the involvement, participation and support of these local actors. They are defined as individuals with the ability to stop radicalisation within the boundaries of the communities. To do so, however, grievances need to be framed as non-factual. Following this line of reasoning, the RAN Working Group on Early Intervention and Prevention of Radicalisation (RAN PREVENT) states:

Some of the key drivers for radicalisation are the lack of identity, belonging, role models and a sense of participation for the

¹⁰ RAN P&P Working Group, “Proposed Policy Recommendations for the High Level Conference”, Brussels, December 2012.

¹¹ RAN DERAD Working Group, “Proposed Policy Recommendations for the High Level Conference”, Brussels, December 2012.

individual at risk and therefore *a consistent, local actor can be key in providing for some of those needs and filling those gaps.* (Emphasis added)¹²

According to the working group, a perceived grievance can be addressed or a gap “filled” by a community’s actions. This can be done, for instance, through the provision of role models, a sense of belonging and participation. The RAN policy recommendations hence assert that communities should be able to provide for and ‘fill the gaps’ that have caused radicalisation through their own actors.

5.3 Tailor-made strategies

The RAN policy recommendations insist on the need for ‘tailor-made’ strategies that speak to each community in culturally specific ways. This approach comprises the inclusion of local actors and communities as responsible subjects and implementers of counter-radicalisation strategies. An active advocate of tailor-made strategies is the RAN Working Group on Voices of Victims of Terrorism (VVT). This group, in one of its policy recommendations, stresses the need for culturally specific interventions.¹³

The RAN policy recommendations have thus shifted the focus of the counter-radicalisation discourse towards communities and the local level. However, this focus has not been equally divided among all members of communities. In fact, the policy recommendations differentiate between members of communities, defining some as “key individuals” or “key groups”, while others are defined only as members of communities, or even as vulnerable individuals.

5.4 Key individuals as “trusted Muslims”

Whereas a reference to local actors seems to imply a widespread opening for all members of the community to be engaged, the RAN policy recommendations ascertain that the local voices will only be few. The policy recommendations have outlined this differentiation since the launch of the

¹² RAN PREVENT Working Group, “Proposed Policy Recommendations for the High Level Conference”, Brussels, December, 2012.

¹³ RAN VVT Working Group, “Proposed Policy Recommendations for the High Level Conference”, Brussels, December, 2012.

network in 2011, through calls to empower “key groups in vulnerable communities”.¹⁴ Similarly, the policy recommendations of the RAN INT/EXT Working Group on Internal and External Factors stress the importance of key individuals in the definition of counter-radicalisation strategies. This group asserts that “knowledgeable local actors can reconstruct identity and provide a more humanistic point of view to counter the individual or group mentality of the radicalised extremist”.¹⁵ This illustrates how, within communities, a limited number of individuals will be treated differently in the process of implementing counter-radicalisation policies. Some individuals will be objects of the policies, while others, the key groups, will be empowered and more directly engaged. In other words, while the majority of the community is regarded as “suspect” some “key individuals” will be regarded as “trusted Muslims”.¹⁶

According to the policy recommendations, key individuals are those members of the communities who are able to help bridge the connection between the greater society and the self-reliant community. Nevertheless, it is unclear how these individuals are chosen. The RAN INT/EXT Working Group is the only one that advances a definition of who these key individuals are and what is expected of them. The working group asserts its duty as regards local actors as follows:

Identify and engage ... actors (including spiritual leaders and mass organisations such as the Nahdlatul Ulama) that have the legitimacy, credibility and expertise necessary to: a) marginalise and discredit the narratives associated with violent extremism; and b) generate a positive paradigm, which facilitates social harmony and cohesion within EU Member States and abroad.¹⁷

Whereas the work that these individuals should do is fairly clear, it is unclear how the “legitimacy, credibility and expertise” required of key individuals is evaluated. Other working groups, such as RAN PREVENT, limit their policy recommendations to stress that key individuals should be aware of

¹⁴ See the RAN Charter (2011), op. cit.

¹⁵ RAN INT/EXT Working Group, “Proposed Policy Recommendations for the High Level Conference”, Brussels, December 2012.

¹⁶ F. Ragazzi, “Suspect community or suspect category? The impact of counter-terrorism as ‘policed multiculturalism’”, *Journal of Ethnic and Migration Studies*, Vol. 42, No. 5, 2016, pp. 1-18.

¹⁷ RAN INT/EXT Working Group (2012), op. cit.

“wider issues in communities”¹⁸ – which is again vague and hard to operationalise in practice. The first hint about how key individuals’ legitimacy is construed comes from the RAN Police and Law Enforcement Working Group (POL). Their document, contrary to what could be expected, makes no reference to legitimacy within the community but rather to the external recognition these subjects should achieve. The policy recommendation states: “Local professionals and communities, in addition to better understanding, and acceptance that the phenomenon [radicalisation] exists, must also gain sufficient confidence in the police or security services.”¹⁹ This document thus illustrates that the legitimacy is based on the willingness of these individuals to work with the state and that their position is dependent on acquiescence to the official discourse about radicalisation. It therefore seems that sharing the views of the state is a precondition to be considered a key individual.

The acceptance of the state narrative implies a connection on the part of the key individuals with the state. However, as has been argued, the fact that communities have been brought to the centre of counter-radicalisation policies implies the state taking a step back. Therefore, this connection takes place at the community level with front-line practitioners. According to the 2014 RAN policy recommendations,

[l]ocal practitioners can make a difference, as they know their citizens and communities best and thus have the opportunity to detect worrying signs and act upon them. They can also develop tailor-made de-radicalisation or re-socialization programmes ... We identified relevant practitioners from the following different sectors: legal and law enforcement (community/local police officers), local governments, youth work, the educational sector, (mental) health care and NGOs.²⁰

5.5 Front-line practitioners to access vulnerable communities

Front-line, or local, practitioners can be defined as the counterparts of key individuals. Key individuals and front-line practitioners have direct access to the vulnerable communities and as such are able to develop a certain

¹⁸ RAN PREVENT Working Group (2012), op. cit.

¹⁹ RAN POL Working Group, “Proposed Policy Recommendations for the High Level Conference”, Brussels, December 2012.

²⁰ RAN, *Report, Cities Conference on Foreign Fighters to Syria*, The Hague, 30 January 2014.

degree of legitimacy and credibility within communities while at the same time being considered legitimate interlocutors by the state. They work within the communities, are critical contributors to the tailor-made strategies and most importantly are expected to provide insights about the communities. As the RAN PREVENT Working Group puts it, “the ones who are best positioned are practitioners and volunteers that work ‘on the ground’”.²¹

The choice of words seems particularly important here. The reference to “on the ground” is part of the differentiation the RAN policy recommendations make between being part of the community and being “outside” it. That is, of being a key individual and being a front-line practitioner. This differentiation illustrates the deep and clear division the RAN policy recommendations are making between vulnerable communities and other communities.

Front-line practitioners are also the connection between vulnerable communities and the state. As with key individuals, a prerequisite for their engagement is their acceptance of the state-sanctioned narrative about radicalisation and concomitant policies. It follows that the discourse articulated within the communities must be unified and standardised. Nevertheless, this requires a certain presence of the state, as outlined by the RAN DERAD Working Group:

The deradicalisation intervention delivered by outside non-governmental practitioners [needs] to be securely embedded in the governmental institution and supported through the informed assistance of the institution’s statutory employees. Since good-practice deradicalisation is systemic by nature ... the intervention needs to be systemically grounded in and complemented by the everyday procedures of the institution.²²

Consequently, the vision of the RAN is one in which front-line practitioners are directly overseen by the state in order to present a unified and standardised discourse. Indeed, front-line practitioners are thus the ones making sure that key individuals convey the same discourse carried by the state and translated by front-line practitioners for the communities. Furthermore, this document from the RAN DERAD Working Group establishes a ‘two-tiered’ approach through which counter-radicalisation policies are delivered, thereby differentiating between front-liners and

²¹ RAN PREVENT Working Group (2012), op. cit.

²² RAN DERAD Working Group (2012), op. cit.

governmental institutions. The latter are clearly not directly engaging with communities but employing front-liners to carry out their policies.

Interestingly, the RAN policy recommendations underscore the importance of a two-tiered approach based on two arguments. First, that it would be counter-productive to introduce into communities an ‘expert’ with no rapport or engagement with the communities. The RAN refers to “parachuting” an expert into communities and insists on its negative effects.²³ The reference to “parachuting” has the same effect as the reference to “on the ground” previously addressed. It is employed to differentiate the actual public spaces of the communities and the state. In addition, the RAN also argues that a direct state presence might limit trust and rapport on the part of communities towards practitioners. A case in point is the following statement: “People feeling marginalized and sometimes alienated by state structures will rather accept to work with non-governmental practitioners than with authorities.”²⁴

The second argument of the policy recommendations in favour of the two-tiered approach is that direct state intervention may complicate matters because of bureaucratic constraints. The following points illustrate this:

Too much statutory control and regulation ... leads to the inhibition of creativity and responsiveness of those specialist non-statutory organisations ... In addition, these organisations [civil society and NGOs] are often specifically set up to deliver ‘this’ [build trust, delivering intervention and prevention] work. They are therefore able to be flexible and responsive in their approach whereas larger, more bureaucratic organisations may face greater challenges due to the ‘broader’ nature of their function/ role e.g. social workers whose remit it is to safeguard – not to provide counter narrative.²⁵

Clearly the RAN presents arguments to disengage the state from direct action. Yet total disengagement does not occur, for, as argued previously, those executing policies will have to accept the official discourse and reiterate it. Consequently, it is possible to assert that by promoting the employment of front-line practitioners the RAN policy recommendations legitimise the state taking a step back and implementing a system of governance by ‘indirect rule’.

²³ RAN PREVENT Working Group (2012), op. cit.

²⁴ RAN, “Empowering Local Actors to Prevent Violent Extremism”, Discussion Paper for the High Level Conference in Brussels, 29 January 2013.

²⁵ RAN PREVENT Working Group (2012), op. cit.

5.6 Concluding remarks: Trusted Muslims and suspect communities

One of the main critiques of counter-radicalisation policies is that they produce “suspect communities”.²⁶ According to much of the critical literature, ‘suspicion’ under these types of policies is not directly linked to a possible wrongdoing but to membership of a particular community. As this chapter has shown, however, communities are both the objects and the subjects of security practices.²⁷ Counter-radicalisation policies function as much through suspicion as they do through trust relations: key figures and trusted Muslims are an essential part of the strategy.²⁸ As such, counter-radicalisation works through more engrained notions of self-management and societal involvement in the procurement of security, which has direct political effects.

RAN policy recommendations exemplify the blueprint of counter-radicalisation as a societal discourse, which locates communities at the centre, develops tailor-made strategies, reframes grievances as perceived and non-factual, and engages co-opted key individuals and front-line practitioners to relay the state-sanctioned narrative about radicalisation, with the concomitant exclusion of alternative voices. These processes engage communities and disengage the state. In the RAN policy recommendations, the state is no longer a visible actor, whereas communities are in turn expected to become active, responsive and responsible. Most importantly, key individuals function in such a way as to silence voices within the communities. The RAN policy recommendations thus promote a state that ‘rules at a distance’ through proxies but which nonetheless remains more in control of the situation within the communities by having people on the ground.

²⁶ See S. Body-Gendrot, “Muslims: Citizenship, security and social justice in France”, *International Journal of Law, Crime and Justice*, Vol. 36, No. 4, 2008, pp. 247–256; A. Kundnani, *Spooked! How not to Prevent Violent Extremism*, Institute of Race Relations, London, 2009; L. Nouri and A. Whiting, “Prevent and the Internet”, in C. Baker-Beall, C. Heath-Kelly and L. Jarvis (eds), *Counter-Radicalisation Critical Perspectives*, Abingdon: Routledge, 2015; and C. Pantazis, and S. Pemberton, “From the ‘old’ to the ‘new’ suspect community”, *British Journal of Criminology*, Vol. 49, No. 5, 2009, pp. 646–666.

²⁷ C. Heath-Kelly, “Counter-terrorism and the counterfactual: Producing the ‘radicalisation’ discourse and the UK prevent strategy”, *British Journal of Politics and International Relations*, Vol. 15, No. 3, 2013, pp. 394–415.

²⁸ Ragazzi (2016), op. cit.

PART II

EU INFORMATION ACCESS AND EXCHANGE, AND INTERNATIONAL COOPERATION

6. SECURITY OF THE INTERSTICE AND INTEROPERABLE DATA SHARING: A FIRST CUT

DEIRDRE CURTIN

Information exchange in the EU constitutes an essential part of various different policies. In many policy fields, information sharing is crucial for decision-making but this does not necessarily include the exchange of personal information. In certain fields, however, information exchange contains vast troves of personal data and therefore affects the rights of individuals. The Area of Freedom, Security and Justice (AFSJ), as it was renamed in the Amsterdam Treaty, has seen significant policy developments since the late 1990s.

There has arguably been no other example of a policy area making its way so quickly and comprehensively to the centre of the Treaties and to the top of the EU's policy-making agenda.¹ In areas related to law enforcement and judicial cooperation, such as the AFSJ, horizontal information sharing (including the exchange of personal data) has become an essential tool in the internal security policy of the EU.² It is also an essential tool of external security. This has helped the creation of a common administrative space and

¹ See J. Monar, "Justice and Home Affairs in a Wider Europe: The Dynamics of Inclusion and Exclusion", ESRC 'One Europe or Several?' Programme Working Paper 07/00, Economic and Social Research Council, Swindon, 2000 (<http://www.mcrit.com/scenarios/visionsofeurope/documents/one%20Europe%20or%20Several/J%20Monar%20.pdf>).

² F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonized Data Protection Principles for Information Exchange at EU-level*, Berlin and Heidelberg: Springer Verlag, 2012, p. 1.

effective policy implementation while avoiding the creation of a large, centralised EU government.³

Data sharing is the opposite of ‘stove piping’ and implies that existing data are shared among multiple users for efficiency reasons and the desire to achieve more effective decision-making. It is closely associated with intelligence reform in response to changing and often accentuated security threats or apparent failures of intelligence, regarding collection, sharing or analysis. Interoperability implies not only full availability but also inter-connections between different systems and actors. It refers to the ability of information systems to exchange (personal) data and to enable the sharing of information.⁴

The interoperability-based mechanisms of data exchange in the AFSJ share many of the traits of what is usually termed as Europe’s composite administration. Composite administration is a concept that seeks to bring into balance “autonomy, mutual considerateness and the ability to undertake common action”.⁵

The term is usually employed to describe the networked character of relations between the various regional, national and supranational levels of administration in the EU. Some versions of the concept of composite administration have convincingly demonstrated that Europe’s multilevel administrative system is also increasingly connected to international levels

³ D.-U. Galetta, H. Hofmann and J.-P. Schneider, “Information Exchange in the European Administrative Union: An Introduction”, *European Public Law*, Vol. 20, No. 65, 2014, p. 68.

⁴ European Commission, High-Level Expert Group on Information Systems and Interoperability, “First Meeting – 20 June 2016, Report”, Brussels, 27 June 2016, p. 6 (<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24078&no=1>); European Commission, High-Level Expert Group on Information Systems and Interoperability, “Scoping Paper”, Brussels, June 2016 (<http://statewatch.org/news/2016/sep/eu-com-hleg-interoperability-info-systems-scoping-paper-6-16.pdf>).

⁵ E. Schmidt-Aßmann, “Einleitung: Der Europäische Verwaltungsverbund und die Rolle des Europäischen Verwaltungsrechts”, in E. Schmidt-Aßmann and B. Schöndorf-Haubold (eds), *Der Europäische Verwaltungsverbund*, Heidelberg: Mohr Siebeck Verlag, 2005, p. 7.

of governance.⁶ As the possibilities for transnational security mechanisms have expanded in recent decades, it is unsurprising that composite administration, in interoperable networks, has come to include also cooperation with third states.

The acceleration and intensification of databases at the EU level goes hand in glove with the concern to preserve the states' control over what occurs in their territories while maintaining a European space without internal borders. The EU's powers in security are exercised by a wide array of institutions and a growing number of agencies and administrative bodies. The Hague programme of 2004 placed greater emphasis on the exchange of information between EU agencies and the interoperability of databases,⁷ particularly in the context of migration management.⁸ Intelligence networks in the AFSJ result from the policy of interoperability. They are composed of quite different types of EU legal entities: independent EU agencies (Europol, Frontex), large police and immigration databases (Schengen and the Visa Information System, VIS). The various nodes are multi-level, multi-actor and can span both the public and private sectors. Ballaschk has helpfully distilled two different levels of networks: vertical (basically the EU agencies and bodies) and horizontal (Prüm Treaty and passenger name records) as well as the 'intermediate' information systems (eu-LISA, Schengen, VIS, Eurodac and Customs).⁹

The question of interoperability has been most sensitive regarding access to the VIS and Eurodac. Both databases were primarily designed as instruments of migration control. Law enforcement agencies at the national and EU levels have attempted to utilise migration control practices to abet counter-terrorism activities. In particular, there is evidence that systems for monitoring and gathering data on migrants have been harnessed as part of

⁶ A. von Bogdandy and P. Dann, "International Composite Administration: Conceptualizing Multi-Level and Network Aspects in the Exercise of International Public Authority", *German Law Journal*, Vol. 9, 2008, pp. 2013, 2015.

⁷ Boehm (2012), op. cit., p. 7.

⁸ V. Mitsilegas, "The Borders Paradox: The Surveillance of Movement in a Union without Internal Frontiers", in H. Lindahl (ed.), *A Right to Inclusion and Exclusion? Normative Fault Lines of the EU's Area of Freedom, Security and Justice*, Oxford: Hart Publishing, 2009, p. 55.

⁹ J. Ballaschk, "Interoperability of Intelligence Networks in the European Union: An analysis of the policy of Interoperability in the EU's Area of Freedom, Security and Justice and its compatibility with the right to data protection", PhD thesis, University of Copenhagen, 2015.

the EU's anti-terrorism strategy. Migration data was long declared essential for law enforcement and counterterrorism purposes and national security agencies were granted access to pre-existing databases as well as to a growing number of new databases and data collection schemes in this area.

6.1 Interoperable EU databases: Security of the interstice

The use of new information and communication technologies in the AFSJ in the form of *information systems* has spiralled in recent decades, as witnessed by the recent creation of a new EU agency specifically to manage these information systems: eu-LISA, the European agency for the operational management of large-scale IT systems in the AFSJ. In its own words, it “strives to support and facilitate European policies in the area of justice, security and freedom. It proactively supports and promotes effective cooperation and information exchange between relevant EU law enforcement bodies by ensuring the uninterrupted operation of large-scale IT systems”.¹⁰ These information systems vary greatly in their degree of complexity and formality. In the EU, a layered approach has been followed. New or enhanced EU bodies (or specific databases) intended to promote information sharing among the law enforcement and security agencies of its Member States (through Europol, Eurodac and Schengen) have seen their powers boosted considerably (for example, Europol and Eurojust). More recently, new agencies have been set up (the European Border and Coast Guard) or discussed (an EU intelligence agency).

The EU has actively attempted to facilitate and encourage information sharing among the Member States by developing the principle of availability.¹¹ According to this principle, information needed for law enforcement purposes by the authorities of one EU Member State should be made available by the authorities of another Member State, subject to certain conditions. The Hague programme of 2004 placed greater emphasis on the

¹⁰ See the eu-LISA website, “Mandate and Activities” (<http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/Pages/default.asp>).

¹¹ J.D. Occhipinti, “Availability by Stealth? EU Information-sharing in Transatlantic Perspective”, in C. Kaunert and S. Léonard (eds), *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe*, Basingstoke: Palgrave Macmillan, 2013, pp. 143, 144.

exchange of information between EU agencies and the interoperability of databases,¹² particularly in the context of migration management.¹³

Mitsilegas commented that the emphasis on enabling the flow of data between EU databases or EU agencies and bodies in order to enhance the exchange of personal data is often justified on the basis of the ‘war on terror’.¹⁴ As Ballaschk puts it, “[t]he history of the development of a supranational EU justice and home affairs policy is a history of institutional and political interoperability”.¹⁵ Interoperability is a more general and less passive term than availability that implies not only full availability but also interconnections between different systems and actors. It refers to the ability of information systems to exchange data and to enable the sharing of information.¹⁶ It fits within an accentuated trend in recent years towards more institutional and organisational interoperability in law enforcement and intelligence in the EU and globally.

In a recent Commission Communication on “Stronger and Smarter Information Systems for Borders and Security”, for example, the Commission highlighted the recent terrorist attacks in Paris and Brussels and the need to improve the interoperability of information systems as a long-term objective.¹⁷ To achieve these objectives, the Commission set up a High-Level Expert Group on Information Systems and Interoperability, which has been given the task of assessing different options for achieving interoperability and of identifying any gaps and shortcomings of information systems at the European level.¹⁸ The expert group recently published a report of its first meeting and the challenges that lie ahead, but no mention was made of the legal framework applicable to data protection

¹² See European Council, “The Hague Programme: Strengthening freedom, security and justice in the European Union”, OJ C 53/1, 3.3.2005; see also Boehm (2012), *op. cit.*, p. 7.

¹³ Mitsilegas (2009), *op. cit.*, p. 55.

¹⁴ *Ibid.* p. 54.

¹⁵ Ballaschk (2015), *op. cit.*, pp. 38-39.

¹⁶ European Commission, High-Level Expert Group on Information Systems and Interoperability, “Scoping Paper” (2016), *op. cit.*

¹⁷ European Commission, “Stronger and Smarter Information Systems for Borders and Security”, COM(2016) 205 final, Brussels, 6.4.2016, p. 2.

¹⁸ *Ibid.*, p. 15.

in information exchanges between EU agencies.¹⁹ The expert group appears to be more centred on enhancing interoperability, further cooperation and the technical requirements.²⁰

The Commission nonetheless emphasised the importance of the Charter of Fundamental Rights and in particular the new data-protection reform instruments in addressing current gaps and shortcomings in the EU as regards data management for border control and security. The Commission holds that the principles of the Charter and EU data protection legislation will “guide the Commission” and ensure that the “further development of information systems in these areas will be in line with the highest standards of data protection”.²¹ For now such words are mere pious aspirations that have no grounding in concrete data protection requirements nor in any readily comprehensible way for data subjects to challenge the exchange of their personal data and the use to which it is subsequently put.

6.2 In search of transparency and accountability: Pie in the sky?

The visible part of the EU pushes for “a strong Europe in a world of uncertainties”.²² One of the key challenges facing Europe is “to ensure the security of our citizens confronted with growing external and internal threats”. In the EU, the ‘dignified’ institutions (the European Council, Council of the EU, European Parliament and national parliaments) will all have a visible role to play should a European defence union of sorts come to pass with military headquarters and joint defence forces.

Yet the focus of this chapter is on concealed security governance. In a policy area like the AFSJ, the need for a careful balance between EU-wide security interests and the demands of national sovereignty, might recommend not giving public opinion the impression that the EU is extensively involved in security matters. The area of security and law enforcement is where information gathering, mining and interoperable

¹⁹ European Commission, High-Level Expert Group on Information Systems and Interoperability, “First Meeting – 20 June 2016, Report” (2016), *op. cit.*

²⁰ See for example the High-Level Expert Group on Information Systems and Interoperability, “Scoping Paper” (2016), *op. cit.*

²¹ European Commission, COM(2016) 205 final (2016), *op. cit.*, p. 5.

²² This is the core joint ambition of the French and German foreign ministries for the post-Brexit EU, in a joint paper with this title by Jean-Marc Ayrault and Frank-Walter Steinmeier of September 2016.

sharing is very largely invisible but at the same time subject to accelerated and intensified cooperation. It makes use of vast networks of ‘data cops’ to do its ‘efficient’ work. The problem is, how do we make the invisible transparent? And how do we make informal, unseen and multijurisdictional arrangements accountable?

A network that straddles multiple organisations and jurisdictions gives rise to specific problems that are not the same as those for formal institutions. The boundaries of networks are inevitably amorphous with fluctuating membership and relationships, and they will generally not have their own formal powers or even necessarily formal routines. In one specific respect security networks are like an organisation: “its members are all members of organizations, and the behaviour of network members is conditioned by the patterns of behaviour common to their organizations”.²³ Informal expectations are powerful within the network. In the words of Glennon, “members are thus counted on, for example, to exhibit loyalty to existing decisions, avoid publicly embarrassing other members of the network, and demonstrate fidelity to commonly shared values and assumptions”.²⁴

What can, if anything, be done to improve visibility and accountability? There are different layers to consider in thinking further about possible directions for improvements. One approach is to tone up the ‘dignatarian’ muscles, for example by deleting or amending the national security exception (Art. 4(1) TEU), or by narrowing the scope of or limiting formal secrecy requirements in security (adopting an EU secrets law as earlier proposed).²⁵ But such stopgap measures are unlikely to be widely adopted or fruitful even if they were more likely to happen in practice.

Another approach in thinking further about ways of challenging the lack of transparency and accountability is through the principle of legality and the rule of law. As Kaarlo Tuori points out, one of the normative problems of the EU’s “security constitution” is that AFSJ provisions treat individuals as “passive recipients of collective security goods rather than active citizens or bearers of rights” who “enter the focus of security measures

²³ M.J. Glennon, *National Security and Double Government*, Oxford: Oxford University Press, 2015, pp. 86-87.

²⁴ *Ibid.*, p. 87.

²⁵ For example, in my inaugural address at the University of Amsterdam in 2011: “Top Secret Europe” (Inaugural Lecture 415, University of Amsterdam, 2011).

primarily as security risks whose characteristics, propensities and actions must be surveyed and recorded". In this sense, Tuori concludes, the EU's security constitution treats individuals as objects of surveillance, as replaceable members of a group rather than citizens, and therefore risks leading to their "de-individualization".²⁶ In this light, the need to ensure that fundamental rights are observed becomes even more pressing.

What can the affected individuals do themselves? Despite the fact that it is their personal data that is concerned, there is very little that affected individuals can do. They will very rarely know that information about them is entered into a database or of any causal link with any subsequent action or decision in their regard. There is hardly access to justice in the sense of an ability to bring a case. Of course, law enforcement is always a special case to some extent when it comes to data gathering and data sharing. The need for confidentiality, even of secrecy, is clear certainly when it comes to ongoing or planned prosecutions. Still, when not only national cops, but also national border guards and intelligence officers access personal data that was entered for a concise and different purpose we need to recall the "forgotten purpose" of purpose limitation.²⁷ The reason this matters is that data cops "do not regulate truck widths or set train schedules. They have the capability of radically and permanently altering the political and legal contours of our society."²⁸

²⁶ K. Tuori, *European Constitutionalism*, Cambridge, MA: Cambridge University Press, 2015, p. 317.

²⁷ E. Brouwer, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation", in L.F.M. Besselink, F. Pennings and S. Prechal (eds), *The Eclipse of the Legality Principle in the European Union*, Alphen aan de Rijn: Kluwer Law International, 2011.

²⁸ M.J. Glennon, "Investigating Intelligence Activities: The Process of Getting Information for Congress", in T.M. Franck (ed.), *The Tethered Presidency: Congressional Restraints on Executive Power*, New York, NY: New York University Press, 1981, p. 52.

7. INTERNATIONAL COOPERATION AND THE EXCHANGE OF PERSONAL DATA: SAFEGUARDING TRUST AND FUNDAMENTAL RIGHTS

EVELIEN BROUWER

7.1 Introduction

Recurring terrorist attacks in cities in Europe, but also elsewhere, establish the necessity of timely and effective cooperation among the different authorities involved in preventing terrorism and serious crimes. This cooperation requires, first of all, mutual knowledge about the competent organisations or agencies in other states and the existing networks and contact channels between the states involved, to allow swift and reliable exchange of information. Second, in order to ensure the willingness to cooperate and to share information, international cooperation can only be based on mutual trust between these states. This trust concerns the reliability and accuracy of the information to be shared, but also the lawfulness of data processing and the protection of fundamental rights in the different states involved.

When dealing with the cooperation between EU states, mutual trust is considered a fundamental principle underlying such cooperation in the Area of Freedom, Security and Justice (AFSJ). Yet the case law of the Court of Justice of the European Union (CJEU) has underlined that even if trust with regard to the protection of fundamental rights and EU law can be assumed, there is no such principle of “blind trust”.¹ In the case of evidence concerning

¹ See E. Brouwer and D. Gerard (eds), “Mapping Mutual Trust: Understanding and Framing the Role of Mutual Trust in EU Law”, EUI Working Paper MWP 2016/13, European University Institute, Florence (<http://cadmus.eui.eu/>). See also the different contributions to the special section on “Mutual Recognition and Mutual Trust -

a breach in the protection of fundamental rights in another EU state, such evidence may rebut trust, and thus block cooperation, also with regard to the exchange of personal information.²

Whereas there is ongoing discussion about the threshold to apply for the evidence necessary to substantiate the ‘rebuttable presumption’ of mutual trust between EU states, it seems clear that when dealing with cooperation between the EU and third states, this threshold must certainly be lower. Unlike within the EU, the cooperation between the EU and third states is not built upon shared values and fundamental principles, the harmonisation of law and procedural guarantees, or mechanisms for cooperation and supervision. Therefore, as underlined by the CJEU in the case law described below, the adoption of agreements with third countries, and more specifically agreements on data sharing, must include further and more detailed rules on the protection of fundamental rights.

Since the terrorist attacks in the US in September 2001, many instruments have been adopted within the legal framework of the EU dealing with the collection and exchange of personal information. Aside from those resulting in large-scale data collection on third-country nationals (such as the Schengen Information System (SIS) II, Visa Information System (VIS) and Eurodac), these measures also involve the exchange of information between judicial and law enforcement authorities (through Europol, Eurojust and the Prüm Treaty) and the adoption of agreements on data transfers between the EU and third states. The cooperation between the EU and third states involves among others the exchange of passenger data with the US, Canada and Australia, and cooperation between the US government and Europol for the purpose of the Terrorist Financing Tracking Program (TFTP).³ During the negotiations preceding the adoption of these

Reinforcing EU Integration?”, in *European Papers – A Journal on Law and Integration*, Vol. 1, No. 3, 2016, and Vol. 2, No. 1, 2017.

² Already in 2006, the CJEU found that with regard to entry bans reported in the Schengen Information System (SIS), the refusal of entry to third-country nationals who were spouses of EU citizens could not automatically be based on the SIS information, but required the further exchange of information between the reporting and the executing state. See CJEU, Judgment of the Court (Grand Chamber) of 31 January 2006 in Case C-503/03, *Commission v Kingdom of Spain*.

³ An analysis of many of these measures is provided in D. Bigo, E. Brouwer, S. Carrera, E. Guild, E.-P. Guittet, J. Jeandesboz, F. Ragazzi and A. Scherrer, “The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty

agreements, concerns were raised by the European Parliament, different non-governmental organisations, and the national and EU supervisory data-protection authorities, addressing the level of data protection in the third state and the scope of legal protection of the data subjects involved. Because of these concerns, together with the scrutinising role of the CJEU (on the basis of which, for example, the EU-US Agreement on Passenger Name Records (PNR) of 2004 was annulled), the negotiations on these agreements were painstakingly long, requiring both a diplomatic and a stringent position by the European Commission.⁴ The adoption in December 2016 of the EU-US Umbrella Agreement, entering into force in February 2017, was presented by Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, as a “common transatlantic privacy framework based on high standards with the USA”, supporting and facilitating “law enforcement cooperation by building trust and legal certainty for data transfers”.⁵

In case law dealing with the mass collection of personal data and data transfer to third states, the CJEU has defined important criteria that, as argued above, at least should be taken into account when dealing with agreements on the transfer of personal data between third states and the EU.⁶ On the basis of this case law and the new EU data protection rules entering into force in 2018, this chapter will address the following standards: necessity and proportionality, transparency or the principle of purpose limitation, and the right to legal remedies. It will submit that these standards

Agenda”, CEPS Policy Brief No. 81, Centre for European Policy Studies, Brussels, February 2015.

⁴ See CJEU, Judgment of the Court (Grand Chamber) of 30 May 2006 in Joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission*, annulling Decision 2004/496/EC – Agreement between the European Community and the United States of America – Passenger Name Records of air passengers transferred to the United States Bureau of Customs and Border Protection (adopted on the wrong legal basis, Art. 95 EC, on the internal market). See also the new Agreement of 14 December 2011, published in OJ L 215/5, 11.8.2012.

⁵ See V. Jourová, “EU-US data flows and data protection: Opportunities and challenges in the digital era”, speech delivered in Washington, D.C. on 31 March 2017 (SPEECH/17/826), Press Release, European Commission, Brussels.

⁶ See also on the implications of the CJEU’s case law in I. Nesterova, “Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards”, ESIL Conference Paper No. 11/2016, European Society of International Law Annual Conference in Riga, 8–10 September 2016 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2911999&download=yes).

should be the among the guiding principles during, but also before starting negotiations with a third state for the purpose of sharing personal information. Furthermore, the chapter will address some lack of clarity and possible gaps in protection under the Umbrella Agreement, also taking into account the risks of onward transfers by the third state to other non-EU states.

7.2 Necessity and proportionality

In early case law, the European Court of Human Rights (ECtHR) made clear that the collection, storage and processing of personal information falls within the scope of the right to privacy as protected in Art. 8 of the European Convention on Human Rights (ECHR), irrespective of whether this information is subsequently used or not.⁷ Art. 8(2) ECHR prescribes that every limitation to the right to privacy should be in accordance with the law and necessary in a democratic society for one of the goals specified in Art. 8(2). In EU law, the right to privacy has been included in Art. 7 of the EU Charter of Fundamental Rights, and read together with Art. 52(1) of the Charter, these provisions further require that each limitation should be in accordance with the principle of proportionality.

According to the General Data Protection Regulation (GDPR) of 2016, which will be applicable from 2018, the processing of personal data shall only be lawful for the grounds specified in its Art. 6.⁸ Dealing with the execution of public tasks, this provision entails that the processing must be “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”. Except for the situations described in para. 2, Art. 9 prohibits the processing of special categories of personal data, such as racial or ethnic origin, religious or philosophical belief and biometric data. Furthermore, the Data Protection Directive 2016/680 dealing with the processing of data for law enforcement purposes and which was to be implemented in 2016, provides in Arts 35-40

⁷ ECtHR, *Amann v Switzerland*, Application no. 27798/95, 16 February 2000.

⁸ Regulation (EU) 2016/679 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 and on the free movement of such data, OJ L 119, 4.5.2016.

further requirements specifically dealing with the transfer of personal data to third states.⁹

The aforementioned conditions on data transfers to third states must be read and applied in conformity with the fundamental rights of privacy and data protection and the criteria defined on the basis of these rights by the ECtHR and the CJEU. More specifically, the conclusions formulated by the CJEU in the cases of *Digital Rights Ireland* in 2014 and *Schrems* in 2015 should be considered basic criteria to be fulfilled by the EU legislator whenever negotiating agreements with third states.¹⁰ In the judgment in *Digital Rights Ireland*, the CJEU annulled the Data Retention Directive 2006/24, because its implementation would risk violating the rights in Arts 7 and 8 of the Charter. In its case law, the CJEU referred explicitly to the case law of the ECtHR, dealing with Art. 8 ECHR.¹¹

In its judgment in *Digital Rights Ireland*, the reasons the CJEU gave for finding the Data Retention Directive in violation of Arts 7 and 8 of the Charter were related to the following grounds.¹² First, the Directive was not considered in compliance with the principle of proportionality, as it would entail processing the data of practically the entire European population, involving persons without any link to criminal prosecution. Second, the Directive did not include prior review by a court or independent body to determine whether access is strictly necessary. Third, the CJEU found that the Directive established a “general absence of limits” with regard to authorities having access to data and subsequent use, or abuse. Fourth, the time limits as provided in the Directive would not be circumscribed to what is strictly necessary.

Applying these standards to third-country agreements, such as the Umbrella Agreement, but also to future agreements, this means that at the least the following criteria must be met, taking into account the principle of

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, OJ L 119/89, 4.5.2016.

¹⁰ See CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014 in Case C-293/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*; see also CJEU, Judgment of the Court (Grand Chamber) of 6 October 2015 in C-362/14, *Maximillian Schrems v Data Protection Commissioner*.

¹¹ See Case C-293/12 (*supra*), paras 35 and 55.

¹² *Ibid.*, paras 57-68.

necessity and proportionality. They should not include provisions allowing for the blanket and unspecified processing or transfer of personal information, involving large groups of citizens without any link to an individual suspicion or criminal investigation. Prior to the adoption of the agreement, the national and European data protection supervisors must be involved, assessing the necessity of the measure at stake. Furthermore, the agreement must provide specified and clear rules, limiting both the data retention of processed data, as well as the access and use by authorities, to what is strictly necessary. This latter requirement is closely related to the principle of purpose limitation, which is developed further in the next section.

7.3 Purpose limitation – Transparency

The requirement of transparency when dealing with data collection and data sharing follows not only from the right to privacy as included in Art. 8 ECHR and Art. 7 of the Charter, but is also to be considered one of the central principles of data protection law: the principle of purpose limitation.¹³ Within the context of EU law, the right to data protection has been recognised as a separate fundamental right in Art. 8 of the Charter. The explicit inclusion of the principle of purpose limitation in Art. 8(2) of the Charter underlines that this is to be regarded as an intrinsic part of the right of data protection.

The principle of purpose limitation is included in Arts 5(1)(b) and 6 of the GDPR. According to Art. 5(1)(b), personal data may only be collected for “specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes”. Furthermore, Art. 5(1)(c) of the GDPR explicitly refers to the principle of data minimisation, providing that personal data should be “adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed”.

Elsewhere, we have described the different layers of the principle of purpose limitation, including the ban on “aimless data collection” and the obligation of purpose specification.¹⁴ The first entails a material limitation of

¹³ See Art. 5 of the Data Protection Convention of the Council of Europe of 28 January 1981, ETS, No. 108.

¹⁴ E. Brouwer, “Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation”, in L.F.M. Besselink, F. Pennings and S. Prechal (eds), *The Eclipse of Legality Principle in the European Union*, Alphen aan de Rijn: Kluwer Law International, 2011, pp. 273-294.

the power to collect and process personal information, the second is an obligation to lay down in clear and transparent rules which data are to be collected or processed for which purposes. In different judgments, the ECtHR has clarified that “in accordance with the law”, as stipulated as a condition in Art. 8(2) ECHR, means that the law allowing the use or collection of personal information must be accessible to the individual concerned and its consequences predictable.¹⁵

Dealing with the use of secret police files by the Swedish special police service in the famous *Leander* case, the ECtHR recognised that in cases of national security, the requirement of predictability cannot be the same as that applied to general cases.¹⁶ However, the ECtHR made clear that “the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which, and the conditions on which, the public authorities are empowered to this secret and potentially dangerous interference to private life”.

In 2008, assessing the UK’s Interception of Communication Act in the *Liberty v UK* judgment, the ECtHR explicitly rejected the government’s submission that when considering the requirement of a specific and clear legal basis, there would be a difference between intercepting the communication of targeted individuals and general surveillance schemes. More specifically, “[t]he Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other”.¹⁷

Unlike its predecessor, Directive 95/46/EC, the GDPR does not refer explicitly to the right to privacy, nor to Art. 8 ECHR. However, Art. 1(2) specifies that this Regulation “protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”. In different decisions, the CJEU has underlined the close relationship between the right to privacy and data protection.¹⁸ The necessary condition

¹⁵ See ECtHR, *Huwig and Kruslin v France*, Application nos 11801/85 and 11105/84, 24 April 1990, and *Malone v UK*, Application no. 8691/79, 2 August 1984.

¹⁶ ECtHR, *Leander v Sweden*, 26 March 1987, paras 50-51.

¹⁷ ECtHR, *Liberty v UK*, Application no. 58243/00, 1 July 2008, para. 61-63.

¹⁸ CJEU, Judgment of the Court of 20 May 2003 in Cases C-465/00, *Rechnungshof v Österreichischer Rundfunk and Others*, and *Christa Neukomm (C-138/01)* and *Joseph Lauerermann (C-139/01)*, paras 68-71.

of transparent and specified rules, following from the protection of Arts 7 and 8 of the Charter, was underlined by the CJEU in its judgment in *Digital Rights Ireland*, in which the CJEU invalidated the Data Retention Directive.¹⁹ According to the CJEU,

the EU legislation in question 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 have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.

Referring to earlier case law of the ECtHR applying Art. 8 ECHR, the CJEU stressed that the “need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data”.

The aforementioned principles, and interpretation by the CJEU, imply that new instruments for data processing and data sharing, including agreements with third states, must provide clear rules defining the scope and content of the powers at stake. Furthermore, purpose limitation prohibits the blanket and unspecified sharing of data between authorities in the EU, and between the EU and third states. This also requires using precise definitions, and ensuring a harmonised interpretation and implementation of mutual agreements. For example, when including definitions for terms such as ‘terrorist events’ or ‘serious crimes’, if not further defined, these terms may be considered too vague and too open for a different interpretation to provide a sufficient and reliable basis for mutual exchange of information. Even if lower standards with regard to predictability may apply when it comes to internal security measures, the ECtHR made clear that both the circumstances and the conditions on the basis of which personal information may be processed for these purposes should be ‘sufficiently clear’. Dealing with third-country agreements where the risk of unlawful access might be larger, further safeguards are necessary.

Finally, EU agreements with third states must be adopted on a clear legal basis and published in official journals, and substantive information

¹⁹ See *Digital Rights Ireland* (Case C-293/12), op. cit., paras 54-55, where the CJEU also refers to the judgments of the ECtHR dealing with Art. 8 ECHR, including the *Liberty v UK* judgment.

with regard to the scope and implementation of third-country agreements should be submitted to the European Parliament and national parliaments. Only this allows parliaments and individuals to assess the legality of an agreement and prevents a lack of clarity about which state or organisation is to be held accountable for the implementation of the agreement.²⁰

7.4 Access to effective legal remedies

The right to an effective judicial remedy is protected in Art. 47 of the Charter and more specifically with regard to data processing in Art. 79 of the GDPR.²¹ In addition, dealing with data relating to criminal convictions and offences “or related security measures”, Art. 10 of the GDPR provides that this data processing may only be carried out “under the control of official authority” or when the processing is authorised by EU or national law providing for “appropriate safeguards for the rights and freedoms of data subjects”. The GDPR provides for a more extended role of national supervisory authorities and the European Data Protection Supervisory Board (replacing the current European Data Protection Supervisor).

In the *Schrems* judgment, the CJEU emphasised the importance of the right to effective judicial protection:

legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very

²⁰ That is to avoid a gap of legal protection as recently established in view of the EU-Turkey deal on the relocation of asylum seekers from the EU to Turkey and vice versa. Here, the General Court declared itself not competent to assess the human rights implications of this agreement, considering it was not an EU treaty – see the Order of the General Court of 28 February 2017 in Case T-192/16, *NF v European Council*.

²¹ Art. 79 of the GDPR states that “each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation”.

existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.²²

Furthermore, in *Digital Rights Ireland*, when annulling the Data Retention Directive because of violation of Arts 7 and 8 of the Charter, the CJEU scrutinised the lack of access to any independent review. According to the CJEU,

the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.²³

Moreover, the CJEU found that

it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security ... is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.²⁴

In other words, the CJEU regarded the lack of independent control and safeguards ensuring the security and compliance with data protection rules in a third state to which personal data would be transferred from controllers or authorities within the EU, as a violation of Art. 8 of the Charter.

Considering the EU-US Umbrella Agreement, it is questionable whether the individual right of access to legal remedies and the supervisory role of data protection authorities is sufficiently and effectively safeguarded. In the first place, the scope of protection provided by the Umbrella Agreement seems to be limited. This Agreement has been approved by EU negotiators under the condition of the US legislator adopting the Judicial

²² See *Schrems* (Case C-362/14), op. cit., para. 95.

²³ See *Digital Rights Ireland* (Case C-293/12), op. cit., para. 62.

²⁴ *Ibid.*, para. 68.

Redress Act, as this would ensure that data subjects whose data would be transferred from the EU to the US would have access to legal remedies.

However, the text of the Judicial Redress Act, adopted in February 2016 by the US Congress, only offers citizens of designated countries access to civil remedies, in accordance with the US Privacy Act of 1974, and this list just includes EU states (with the exception of Denmark and the UK).²⁵ Therefore, third-country nationals resident in the EU, or third-country nationals whose data have been collected by EU authorities (e.g. in SIS II, Eurodac or the VIS) and subsequently transferred to US authorities, are not covered by this right to judicial remedies.

Second, the US Privacy Act and the Judicial Redress Act provide access to civil law procedures, but not legal redress actions in the field of criminal or administrative law. This means that formally, whenever measures are taken in immigration or criminal law procedures against EU citizens whose data have been transferred under the Umbrella Agreement, these individuals may be excluded from access to legal remedies, or their procedural rights may be limited by US law. In this regard, the rules in the Umbrella Agreement differ from the specific provisions included in the EU-US TFTP Agreement of 2010, which provides for “all persons regardless of nationality or residence, access to judicial redress from adverse administrative action”. Also, the EU-US PNR Agreement includes a wider scope of legal protection in Art. 13(1), providing that “any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with US law”. Furthermore, Art. 13(2) provides that “any individual is entitled to seek to administratively challenge the Department of Homeland Security (DHS) decisions related to the use and processing of PNR”. Where these provisions seem to bridge the aforementioned gap of the Judicial Redress Act, the relationship between the general rules of the Umbrella Agreement and the rules in the specific transfer agreements should be made clearer, also when adopting future agreements.

Finally, the effect of the executive order under the Trump administration of 25 January 2017 (“Enhancing Public Safety in the Interior

²⁵ The Judicial Redress Act requires the adoption of a separate list of ‘designated countries’, to be found on the US Department of Justice website (<http://www.justice.gov/opcl/judicial-redress-act-2015>). This list excludes Denmark and the UK, awaiting the formal notification that these countries shall apply the Umbrella Agreement.

of the United States”) requires further investigation. According to section 14 of the Privacy Act, as amended by this executive order, “[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information”.²⁶ Although the phrase “to the extent consistent with applicable law” may limit the practical outcome of this executive order, the text itself seems to imply that the former extension of rights in the US Privacy Act to EU citizens by the adoption of the Judicial Redress Act should be considered void.

7.5 Adequacy decision, appropriate level of data protection and onward transfer to third states

In *Schrems v Data Protection Commissioner*, the CJEU annulled the Safe Harbour Decision 2000/520, in which the Commission had found that US law provided an adequate level of data protection in accordance with Directive 95/46, allowing the transfer of personal data from the EU to organisations within the US. In this judgment, the CJEU defined “an adequate level of data protection” as a level of protection that is “essentially equivalent protection to that guaranteed within the European Union”.²⁷ Even if the means chosen by a third state to ensure an adequate level of protection might differ from those employed in the EU, the CJEU found that those means must nevertheless “prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union”.

Therefore, “essentially equivalent” would mean that the essential elements of data protection included in Art. 8 of the Charter are to be complied with. This, according to the CJEU, also implies that, “as the level of protection ensured by a third state is liable to change”, the Commission should periodically assess the content of those rules to ensure that the

²⁶ See “Executive Order: Enhancing Public Safety in the Interior of the United States”, Office of the Press Secretary, White House, Washington, D.C., 25 January 2017 (<https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>).

²⁷ See *Schrems* (Case C-362/14), op. cit., para. 74.

decision with regard to the adequate level of data protection is still factually and legally justified.²⁸

In accordance with Art. 45 of the GDPR (and Art. 36 of Directive 2016/680), the transfer of personal data to a third country or an international organisation requires a prior adequacy decision by the Commission. This decision can only be based on an assessment of the adequacy of protection in that third state or organisation with regard to, among others, the rule of law, respect for human rights and fundamental freedoms, as well as “effective and enforceable data subject rights and effective administrative and judicial redress for the data subject at stake”. In the absence of such a decision, Art. 46 of the GDPR (and Art. 37 of Directive 2016/680) allows personal data to be transferred to a third country or international organisation, but only if the processor or controller provides “appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available”.

Considering this general requirement of either an adequacy decision or the provision of an appropriate level of protection necessary for the transfer of data from the EU to third states, it seems odd that the Umbrella Agreement allows in Art. 7 the onward transfer of personal data, acquired on the basis of this Agreement between the EU and the US, to other third states, only if the prior consent of the state originally transferring this data has been obtained. The Umbrella Agreement does not provide, through a decision on the adequate level of data protection in the US, for this onward transfer, but refers in Art. 7(2) to “an appropriate level of protection of personal information”, which should be ensured in the third state.²⁹ Furthermore, Art. 7(2) provides that the transfer “may” be subjected to specific conditions. In other words, the onward transfer of data to third states on the basis of the Umbrella Agreement is bound by fewer guarantees and safeguards than those provided in the GDPR and Directive 2016/680 for the transfer of personal data from the EU to third states in general.

7.6 Concluding remarks

The negotiation of agreements with third states allowing the transfer of personal data should be based on evidence sustaining the necessity and

²⁸ Ibid., para. 76.

²⁹ See also the Note on the EU-US Umbrella Agreement by the Meijers Committee, CM1613, Utrecht, 2016 (www.commissie-meijers.nl).

proportionality of any systematic and general data transfers. In this regard, it should be taken into account that the GDPR and Directive 2016/680 already provide a basis for the exchange of personal data in individual and specific situations, under conditions and supervision by data protection authorities. The adoption of any new agreements with a third state allowing for the further and more general exchange of personal data requires a prior and in-depth examination of the law, practice and judicial redress systems in that state.

Furthermore, the level of protection should be in accordance with the criteria developed in the aforementioned case law of the CJEU and “essentially equivalent” to the protection offered by the GDPR and the Directive. Any future agreement must have a clear legal basis and be officially published to ensure its transparency and the accountability of the powers and actors involved. Finally, in dealing with the Umbrella Agreement, the EU legislator should address the current gap in protection for non-EU citizens with regard to the right to- judicial remedies and the lack of specific safeguards for the onward transfer of data to third states.

8. A SECURITY UNION IN FULL RESPECT OF FUNDAMENTAL RIGHTS: BUT HOW EFFECTIVELY RESPECTFUL?

GLORIA GONZÁLEZ FUSTER

The EU's security policy must be designed, and unfold, in full respect of fundamental rights. This imperative emanates directly from the EU's Treaties, and obliges EU institutions to keep in mind compliance with EU fundamental rights at all stages of policy-making, as well as beyond. This, however, does not always appear to be an easy task – especially insofar as compliance with the fundamental rights to privacy and personal data protection are concerned.

The Union's security policy has indeed been decidedly built upon extensive reliance on the use of information, and most crucially personal information. By virtue of EU security-related policies and instruments, the personal data of both EU citizens and third-country nationals are nowadays massively retained, vastly shared, often copied and increasingly made available both internally and externally.

These practices and their underpinning policy choices, leaning towards 'security' through widespread data processing, put pressure on critical, basic privacy and data protection, such as proportionality and necessity. In light of these principles, measures involving personal data processing should only be supported after strictly considering the need for each data processing operation, which calls for a careful prior evaluation of their potential, as well as assessing and balancing other possible, less invasive, alternatives.

EU institutions and Member States have not systematically carried out these assessments with clear success. Over the last few years, they have more than once visibly failed to duly grasp the relevance and implications of the rights to privacy and personal data protection as enshrined by the EU Charter of Fundamental Rights. And, as a result, the Court of Justice of the European Union (CJEU) has repeatedly ruled against both EU institutions and national authorities in matters related to privacy and personal data

protection. A few particularly well-known judgments and opinions illustrate this recurrent problem.

In April 2014, the CJEU declared the Data Retention Directive to be invalid,¹ which imposed, in the name of the fight against serious crime, obligations to retain and make available the communications data of all users across EU Member States.² Examining the instrument's validity from the viewpoint of the EU Charter of Fundamental Rights, the Court notably criticised the way in which the obligations to retain communications data covered the data of "all persons ... in a generalised manner",³ and the "general absence of limits" governing access to such data.⁴

Less than a year later, in October 2015, the Court of Justice annulled⁵ a decision by the European Commission aimed at facilitating flows of personal data from the EU to organisations established in the US.⁶ The Commission's decision was declared invalid on the grounds of its failure to comply with EU legal requirements, read in the light of the EU Charter of Fundamental Rights. The Court emphasised that interference with the rights to privacy and personal data protection is only permissible insofar as "strictly necessary". The Court noted that legislation can never be regarded as such if it authorises, "on a generalised basis", the storage of anyone's personal data "without any differentiation, limitation or exception being made in the light of the objective pursued", and without objective criteria limiting access to the data by public authorities or their use, for specific purposes that are

¹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54–63.

² CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*.

³ *Ibid.*, § 57.

⁴ *Ibid.*, § 60.

⁵ CJEU, Judgment of the Court (Grand Chamber) of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*.

⁶ See Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 2015, 25.8.2000.

“strictly restricted and capable of justifying” the interference with the fundamental rights entailed.⁷

More recently, in July 2017, the Court of Justice similarly declared that the proposed EU-Canada Agreement on the transfer and processing of passenger name records for air passengers flying between the EU and Canada was not compatible with the Treaties.⁸ The Agreement had been prepared in 2014, and when the Council requested approval by the European Parliament, the latter decided to refer the matter to the CJEU. Looking into it from the prism of the EU Charter, the Court decries the fact that the envisaged Agreement permitted the “systematic and continuous transfer”⁹ of categories of data not defined with enough precision,¹⁰ as well as the lack of sufficient clarity concerning criteria to limit disclosure of the data.¹¹

These pronouncements represent major steps in the progressive assertion of fundamental rights requirements of EU law. They strongly affirm the relevance of the right to privacy, and consolidate the progressive emergence of the EU right to personal data protection, which was a key novelty brought forward by the entry into force of the EU Charter of Fundamental Rights in 2009. They can also be read as an explicit warning against the temptation of routinely pursuing security through an indeterminate reinforcing of the processing of personal data, calling instead for only adopting measures that circumscribe such processing to the greatest extent possible. Interference with the fundamental rights to privacy and data protection are only permissible *when* strictly necessary, and *on condition* that any data processing measures are designed in a manner that curtails the extent of the interference to strict necessity.

Despite such a clear and repeated message addressed at the EU legislator and policy-makers, reactions have not been particularly vigorous. After each of these pronouncements, EU institutions have generally expressed that they have taken note of them, typically announcing their intention to take their time to analyse their impact, and ponder the issue at stake. In this sense, for instance, the judicial invalidation of the Data

⁷ *Ibid.*, § 93.

⁸ CJEU, Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017 on the EU-Canada PNR Agreement.

⁹ *Ibid.*, § 127.

¹⁰ *Ibid.*, § 163.

¹¹ *Ibid.*, § 217.

Retention Directive did not lead to any immediate strong reaction against the generalised retention of communications data across the EU.

Data subjects in the EU actually had to wait for another judgment by the Court of Justice to further amplify the message that the general and indiscriminate retention of everybody's communications data is incompatible with EU law, also when implemented at the national level.¹² The timidity of reactions by the EU's institutions is growing increasingly problematic as this message is repeated again and again, thus becoming ever-less unexpected news that would need special time to digest. It certainly does not emanate from any sudden, unpredictable or variable set of standards, but follows directly from the text of the EU Charter (most notably, but not only, Arts 7 and 8), on the interpretation of which further guidance is in the meantime widely available.¹³

The recent Comprehensive Assessment of the Union's action in the area of internal security gave the European Commission an excellent opportunity to engage in a critical reflection on these issues – in relation to both the substance (that is, the question of how compliant the Union's security policy is with fundamental rights requirements) and the procedures in place (the question of how such compliance is guaranteed). The assessment aimed at exhaustively reviewing the Union's action in the area of internal security, as developed and crystallised over the last 15 years.¹⁴

Despite identifying some gaps and room for improvement in certain areas of EU security policy, the European Commission draws from the assessment the conclusion that, specifically in relation to fundamental rights, everything is globally fine.¹⁵ It interprets the exercise as confirming that “compliance with fundamental rights is a key characteristic of EU security

¹² See CJEU, Judgment of the Court (Grand Chamber) of 21 December 2016 in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*.

¹³ See, for instance, European Data Protection Supervisor (EDPS), “Developing a ‘toolkit’ for assessing the necessity of measures that interfere with fundamental rights (Background paper for consultation)”, Brussels, 16 June 2016.

¹⁴ European Commission, “Comprehensive Assessment of EU Security Policy” Commission Staff Working Document, SWD(2017) 278 final, part 1, 26.7.2017, Brussels, p. 4, which accompanied the Communication on the “Ninth progress report towards an effective and genuine Security Union”, COM(2017) 407 final, Brussels, 26.7.2017.

¹⁵ European Commission, COM(2017) 407 final (*supra*), p. 12.

policy, in line with the legal obligation under the Treaties”,¹⁶ and celebrates two concrete aspects: first, that the CJEU is seemingly fulfilling its role in terms of judicial control; and second, that the European Commission has been working on trying to mainstream fundamental rights in the formulation of legislative and policy proposals.¹⁷

No particular link is established by the European Commission between the fact that the observed regular need for the Court of Justice to intervene and invalidate EU legal instruments might be indicative of the persistent shortcomings of such celebrated fundamental-rights mainstreaming. And this can only be deplored. Indeed, the European Commission’s objective should not be to support an EU security policy that *eventually* complies with fundamental rights, but a security policy that complies with such requirements *from the very start* (or, in words more in line with privacy and data protection parlance, *by design* and *by default*).

Any really ‘comprehensive’ assessment of the Union’s action in the area of internal security should thus aim at evaluating not only the effectiveness of EU policies and instruments to support and attain security objectives, but also the effectiveness of the measures in place to guarantee their full compatibility with fundamental rights. Such an evaluation should include a substantive review (addressing the question of whether the measures in place and those in the pipeline are compliant with fundamental rights requirements). It should also involve a detailed and in-depth review of the manner in which compliance is guaranteed (including the point at which such compliance is achieved – after how many years of implementing unlawful pieces of legislation, after how much data is unduly retained and made available, after how many instances of illegal interference with data subjects’ fundamental rights to privacy and data protection).

A careful assessment of this kind would reveal the intrinsic limitations of designing a security policy that is primarily based on the processing of (most of the time personal) data, but fails to firmly give privacy and data protection the same level of priority. Taking seriously the idea that “protecting and fostering citizens’ security and complying with fundamental rights are complementary and mutually reinforcing” requires applying the same demands for effectiveness to both concomitant objectives;¹⁸ more efforts are thus required to make sure not only that the Security Union is

¹⁶ Ibid., p. 3.

¹⁷ Ibid.

¹⁸ Ibid. p. 6.

effective and in full respect of fundamental rights *in the end*, but also that such respect is guaranteed from inception as effectively and efficiently as possible.

If policy choices like further promoting information exchange and ‘fully exploiting’ the potential of information systems,¹⁹ boosting data access and calling for ever-smarter systems are (still) deemed the way forward for EU security, these choices urgently need to be better framed, channelled and construed in line with the strict necessity and proportionality requirements emanating from EU fundamental rights. In other words, and in spite of the European Commission’s optimistic reading of the EU’s Comprehensive Assessment of EU Security Policy, the time has certainly come to devise a security policy that is effectively value-driven,²⁰ as opposed to occasionally, abruptly stopped by surviving EU values.

¹⁹ See, for instance, European Commission, “Commissioner Julian King’s exchange of views at the first LIBE security dialogue at the European Parliament”, Speech, Brussels, 23 March 2017.

²⁰ See for example, in relation to cybersecurity, the work of the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity), co-funded by the EU (<https://canvas-project.eu/>).

9. WILL MORE DATA BRING MORE SECURITY? REMARKS ON THE SECURITY UNION APPROACH TO INTEROPERABILITY *REINHARD KREISSL*

This chapter elaborates on the input and discussion at the CEPS Policy Workshop on “Reappraising EU Security Policy: Effectiveness, rule of law and rights in countering terrorism and crime”, addressing in particular questions raised about information sharing: Is ‘more data’ the most efficient answer in view of current experience and future trends? What are the issues raised by the increasing use of EU information systems, and the development of biometric technologies, for law enforcement purposes in light of the principles of proportionality, necessity and fundamental rights of data protection and privacy?

To better identify and assess the problems emerging with regard to the use of data in the operations of the European Security Union, some conceptual clarifications and practical considerations can be helpful to better understand the processes underlying data-driven security work.

First, it could be helpful to have a more precise definition and clearer understanding of the problems to be addressed. European policy documents discussing the issues emerging in the progress towards an effective and genuine Security Union link migration and security as similar and interconnected problems. This tends to blur important differences between problems to be solved separately when discussing policies governing the collection and use of data, information and intelligence. Starting from an explicit, precise and actionable concept of security, a number of important problems with regard to data, information and intelligence can be identified, requiring close scrutiny.

However, whether these problems have anything to do with migration per se or the governance of individual mobility and travel into or within the Schengen area is an open question. Taking a look at recent terrorist crimes in Europe, many of the attackers would fall under the category of home-grown

terrorists, i.e. while having a non-European ethnic background, mostly from the Middle East and North Africa, they were born and raised in the country where they launched their attacks and also held European passports.

The migration–security link, while taken for granted in most policy discussions, should be disentangled to better understand and more effectively address the problems of data-driven intelligence strategies when it comes to assessing data-driven approaches to govern mobility and identify individuals, using categories of threat and risk.

The High-Level Expert Group on Information Systems and Interoperability, in its final report of May 2017, supports (within the existing legal framework) a policy of lowering thresholds for seamless access to data in order to enhance control of migration, the mobility of persons and security, and to combat undefined terrorist threats.

Practical considerations of how such a policy might affect the daily routine work of operatives, law enforcement authorities and border personnel are not taken into account. Nor are the systemic problems of a data-driven approach to border control and security adequately addressed. Again, a brief look at terrorist attacks shows that data and intelligence about the attackers had been collected, but had not triggered any action preventing the attacks. This situation reflects the irony of comprehensive data collection by intelligence, border and law enforcement authorities. The more persons are registered in any of the databases the higher the probability of finding a file on an attacker in one of these data collections *after* a crime has been committed.

The collection of data and their seamless exchange among relevant authorities within Europe (and beyond) per se is no adequate strategy to address security problems. The equation of more data equals more security ignores the practical and conceptual problems of data analysis.

A critique of EU policies in the security and migration areas by data protection and privacy experts focuses on rule of law issues. A number of relevant points can be raised here. While such an analysis centred on the rule of law has its merits, it leaves aside the problems emerging in the practical implementation of regulations governing the collection and use of data by European authorities.

Taking into account the practical problems at the end-user level is important to assess the feasibility and effectiveness of any new data-driven strategy. Asking for more and seamless access to data/information from a wide variety of sources immediately translates into more efforts and more resources spent. This is echoed by recurrent requests to increase the numbers

of personnel within the law enforcement, intelligence and border control authorities. However, the problem here is not primarily one of quantity but also of quality, organisation, and strategies for information and intelligence processing.

Again, one should distinguish here between three different operational contexts, e.g. mass border control, targeted law enforcement investigations and data-driven intelligence operations.

- i) When using data to check the identity of a person, a standard scenario here might look like this: person x applies for a visa, requests entry into EU territory or is checked at a checkpoint within this territory. Border guards or any other official representative of EU/Member State authorities check the 'identity claims' of the applicant against existing databases. This may require time-consuming procedures, such as taking fingerprints or processing other biometrical identification markers. Operating on the basis of a hit/no hit approach, as suggested by the High-Level Expert Group, further action may be taken or access may be granted. Such a procedure, when applied as a standard routine for border checks, will have substantial impact, most probably seriously disrupting the flow of traffic. In the case of a 'hit situation' there may be a number of causes, not all of them related to security problems. As Molotch¹ points out, the schematised categories of a normal person ignore a multitude of idiosyncratic variations that have no relevance for security, but can trigger a security alert. As a result of such an alert based on a data check, entry into European territory may be refused. This approach may not only disrupt the flow of movement but also create a substantial number of false positives, while not significantly reducing the number of false negatives.²
- ii) A more refined version of this approach could use early warning signs, e.g. performing in-depth identity checks only when a member of a defined group is involved. Here other problems have to be solved, relating to categories of profiling: How can and should a risk profile be

¹ H. Molotch, *Against security: How we go wrong at airports, subways, and other sites of ambiguous danger*, Princeton, NJ: Princeton University Press, 2014, p. 87 *passim*.

² The problem of false positives/negatives may be aggravated by the mechanism of base rate fallacy, based on flawed mundane calculations of the type "[a]ll terrorists are Muslims, so all Muslims should be considered potential terrorists" (see A. Locksley, C. Hepburn and V. Ortiz, "Social stereotypes and judgments of individuals: An instance of the base-rate fallacy", *Journal of Experimental Social Psychology*, Vol. 18, No. 1, 1982, pp. 23-42).

designed and used? How can an individual be identified as a member of such a risk group? Informed decisions at the level of individual border guards and law enforcement officers on duty have to be made to single out individuals for identity checks. Very little is known about these decisions and there are no quality-tested, standardised procedures in place to assure the quality, uniformity and effectiveness of such a risk-based approach. Critical observers, based on in-depth studies of security work on the ground, have coined the term “security theatre” (e.g. Schneier in 2009)³ to describe the practical limits of such a strategy (e.g. Mueller and Stewart; Schneier in 2006).⁴

- iii) There may be situations where more data about an individual suspect can help to improve and facilitate law enforcement operations. Data and information in most cases provide useful evidence to investigate a criminal event. Data from CCTV or intelligence operations, for example, in many cases contribute to criminal investigations, although the final apprehension of the suspect always requires the work of experienced police officers, drawing on what could be called the detective’s tool kit. Still, this constellation is different from the two other scenarios described in (i) and (ii) above, both representing the needle in the haystack dilemma, whereas in (iii) a specific individual has already been identified and data queries are applied to learn more about this person, her social media use, mobility pattern or local social networks, etc.

As shown by this brief discussion of different constellations, where data are used for security purposes, an extensive use of data is not a silver bullet for security work or security-related migration control. The overall policy approach should not be to ask for more data, but rather to direct efforts towards improving targeted forms of data analysis.

When investigating the use of data for security purposes we have distinguished different approaches: huge datasets can be used to identify specific individuals for special treatment, e.g. during border checks or visa applications, as discussed above. A different approach, developed in

³ B. Schneier, “Beyond security theatre”, *New Internationalist*, No. 427, 2009, pp. 10-12.

⁴ J.E. Mueller and M.G. Stewart, *Chasing ghosts: The policing of terrorism*, Oxford: Oxford University Press, 2016; B. Schneier, *Beyond fear: Thinking sensibly about security in an uncertain world*, Berlin: Springer Science & Business Media, 2006.

commercial marketing, applies the strategy of social sorting (see Lyon).⁵ Social sorting or customer relations management puts individuals into different categories of taste, purchasing power, credit scores, etc., based on mass data produced in consumer research. According to this categorisation, consumers receive differential treatment or targeted advertisement. In the realm of security, the equivalent would be the dragnet operation, using mass data to construe categories for social sorting along the lines of security threats. The problem here is that although massive datasets about a huge number of individuals may be available, it is difficult to define valid categorisations because the number of individuals who could reliably be qualified as security risks, since they for instance committed a terrorist attack, is extremely low, as noted by Brooks.⁶

To limit the use of data-driven approaches in security, privacy and data protection, regulations have been introduced. The unconditional collection and storage of person-related data is limited by legal regulations, restricting the range of data to be collected, stored, exchanged and processed. However, recent developments in data science and algorithm-based machine learning have opened new venues for data-driven intelligence work not yet comprehensively addressed by data protection laws. As Kosinski et al.⁷ have demonstrated, private traits and personal information can be predicted from an analysis using trivial and publicly available data of a person from social media. In the age of electronic consumerism, citizens have been transformed into leaking data containers, and with the emergence of sophisticated algorithms new “weapons of math destruction” (as O’Neil puts it)⁸ are being applied as tools for the governance of different segments of the population. While these ‘weapons’ may not yet have developed their full potential, any policy addressing the use of data should consider the effects of lowering the threshold for linking different databases.

⁵ D. Lyon, *Surveillance as social sorting: Privacy, risk, and digital discrimination*, Hove: Psychology Press, 2003.

⁶ R.A. Brooks, “Muslim ‘homegrown’ terrorism in the United States: How serious is the threat?”, *International Security*, Vol. 36, No. 2, 2011, pp. 7-47.

⁷ M. Kosinski, S. Stillwell and T. Graepel, “Private traits and attributes are predictable from digital records of human behaviour”, *Proceedings of the National Academy of Sciences*, Vol. 110, No. 15, 2013, pp. 5802-5805.

⁸ C. O’Neil, *Weapons of Math destruction: How big data increases*, New York, NY: Crown Publishing Group, 2016.

Apart from conceptual, logical and legal concerns, the growth of a multi-agency security regime based on the low-threshold exchange among different data-collecting bodies may have detrimental effects stemming from intricate problems of inter-organisational coordination and communication emerging in such large social-cognitive ecosystems (see e.g. Grijpink).⁹ A simple approach of a linear growth in data collection within ever-wider legal limits producing more of the same does not automatically produce a linear increase in the performance of data-driven intelligence and security work.

Finally, any policy option advertised to increase security and improve border management not only has to be weighed against the legal, financial, social and other costs it entails, but also has to stand comparison with alternative solutions, starting from alternative assumptions. This involves a critical view of existing programmes and strategies from an outside perspective, as Atran et al.¹⁰ write with a view of the situation in the US:

The U.S. government (USG) has relied almost exclusively on the intelligence community, which monitors individuals and groups that threaten national security and specializes in clandestinely gathering and analysing pertinent information. Problems with data collection and interpretation have limited this effort to understand terrorist groups' motivations, recruitment, and capabilities. The intelligence community initially had nearly all existing data on actual, possible, and potential terrorists; however, such information has not necessarily been constrained by scientifically testable theories and methods or systematically cross-examined for accuracy and completeness. The pressing need to protect people's lives and assets justifies use of partial information, sometimes to good effect in capturing dangerous terrorists and preventing terrorist actions; but policy-makers tend to fit such information to prevailing paradigms in foreign policy, military doctrine, and criminal justice, each with serious drawbacks when applied to terrorism.

⁹ J.H.A.M Grijpink, "Chain Communication Systems", *Journal of Chain-computerisation*, Vol. 5, No. 2, 2014.

¹⁰ See S. Atran, R. Axelrod, R. Davis and B. Fischhoff, "Challenges in researching terrorism from the field", *Science*, Vol. 355, No. 6323, 2017, p. 352.

10. CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE: POLICY AND LEGISLATIVE CHALLENGES

KATALIN LIGETI AND GAVIN ROBINSON

The intense growth of information and communications technology (ICT) in recent decades now means that almost any kind of routine, everyday activity – whether licit or illicit – leaves a digital trace. Access to the increasingly vast volumes of data thereby generated is becoming essential to law enforcement charged with the detection and investigation not only of cybercrimes, but also any offline criminal offence to which electronic evidence¹ may pertain. The information that users generate by means of new ICT is, however, typically under the control of private companies. Without their cooperation, law enforcement authorities (LEAs)² would often simply be unable to detect, investigate and/or prosecute a large number of offences.³

¹ Although the precise contours and limits of the notion of electronic evidence remain elusive, for the purpose of this contribution the term shall be used to mean any probative information stored or transmitted in digital form. Since EU law and ongoing policy debates at the EU level divide electronic data of relevance to law enforcement authorities' activities into subscriber data (e.g. the individual behind a webmail account used to coordinate drug deals), metadata (e.g. WhatsApp call logs of suspected terrorist cells; geolocation of smartphones) and content data (e.g. threatening messages sent from one spouse to another on Facebook), this contribution will accordingly use these categories throughout.

² 'LEAs' is a term that, for the purposes of this contribution, refers to police and judicial authorities.

³ Ranging from typical 'target cybercrimes' (e.g. hacking) and 'content-related cybercrimes' (e.g. child pornography) to fraud, organised crime, drug trafficking and terrorism, which are either committed by means of a computer or other electronic device, or otherwise leave electronic traces that could be used as evidence.

Cooperation between LEAs and companies providing information and communications services is, of course, nothing new. It can be voluntary, but very often it is based on rules laid down in national criminal procedures. In practice, there are often situations where obtaining electronic evidence necessitates transnational enforcement efforts; this is the case, for instance, where data is stored outside the investigating country or where the service provider on whose systems data is held is established in another jurisdiction. Whereas transnational investigations are traditionally governed by the applicable instruments on mutual legal assistance (MLA), within the EU there has been a shift since the late 1990s away from MLA towards the mutual recognition of judgments and judicial decisions, implying their free circulation within the Area of Freedom, Security and Justice.⁴ A prime recent example is the Directive on the European Investigation Order (EIO), a judicial decision issued by one Member State to have one or several specific investigative measure(s) carried out in another Member State to obtain, *inter alia*, electronic evidence.⁵

Yet as the ink has been drying on national implementation of the EIO Directive, we have witnessed a further shift away from MLA in the shape of informal, so-called direct cooperation between LEAs seeking to obtain electronic evidence and the foreign service providers in (exclusive) control of it. Citing the doubtless lengthy and allegedly problematic nature of MLA mechanisms, LEAs are increasingly disregarding them in order to address requests for information directly to foreign service providers, in the process excising the role of the judicial authority where service providers are established or targets are habitually resident. In practice, this often entails the issuing of a domestic investigative measure by the LEA directly to the foreign service provider. Where granted – since doing so is in principle voluntary – such cooperation thus represents both the *de facto* extraterritorial reach of national investigative powers, and an extension of the ‘sword’ function of criminal law enforcement through private actors. What is especially novel in the current debate on electronic evidence, however, is that those same actors may choose to shield individuals from the reach of law enforcement, and challenge orders to hand over data in the

⁴ At the Tampere European Council, it was decided that mutual recognition should become the cornerstone of judicial cooperation in criminal matters. The principle of mutual recognition was then confirmed in The Hague and Stockholm programmes.

⁵ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014.

place of the target and data subject: their customer. Performing this shield function on behalf of customers (targets of LEA activity) may often feature prominently in the business model. Moreover, it can be regarded as an expression of the accessory or secondary obligation, under private law, to safeguard the counterparty's legitimate interests;⁶ failure to comply with such secondary obligations may even result in damages.⁷ There might, thus, be a legal motive alongside the commercial one to refrain from voluntarily disclosing customer data.

The overall picture is one of fragmentation and an acute lack of legal certainty for all stakeholders vis-à-vis the enforceability of such cross-border requests, the classification of service providers as domestic or foreign, the potential illegality (in some jurisdictions) of granting cooperation, differences in types of data it is possible to request, divergent definitions of those types of data, varying procedures for submitting requests, unreliable responses and unpredictable response times.⁸ It is against this background that the European Commission is currently exploring options for the formalisation of such 'direct' cooperation through EU legislation, following an exceedingly rare request from the Council – acknowledgment in and of itself that any national solutions are unlikely to be enforceable, workable and sufficient. To meet its stated goals, however, any common Union approach will have to confront a host of technical and practical complexities as well as legal and policy challenges posed by the direct involvement of private actors in the cross-border gathering of electronic evidence.

This chapter focuses on the deficiencies of the existing European and international legal framework applicable to cross-border access to electronic evidence and offers a brief overview and critical discussion of competing instruments and mooted options for reform.

⁶ Under German law, e.g. such so-called *Nebenpflichten* are explicitly dealt with in section 241, para. 2 of the Civil Code, *Bürgerliches Gesetzbuch*. Cf. G. Bachmann in F.-J. Säcker, R. Rixecker and H. Oetker (eds), "Münchener Kommentar zum Bürgerlichen Gesetzbuch", in Vol. 2 of *Schuldrecht – Allgemeiner Teil*, 7th edition, Munich: CH Beck, 2016, §241, margin numbers 46 et seq.

⁷ *Ibid.*, margin number 61.

⁸ See European Commission, Non-paper, "Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace", (hereafter 'Commission non-paper 1'), para. 1.2.1, accompanying Council of the European Union, 15072/1/16 REV, Brussels, 7 December 2016.

10.1 Disregard for mutual legal assistance: The emergence of informal cooperation between LEAs and foreign service providers

In practice, informal cooperation between LEAs and foreign service providers has become the main channel for LEAs to obtain non-content data. Compliance with direct requests from law enforcement authorities of one country to a service provider headquartered in another country is in general voluntary; service providers usually do not have a legal obligation to provide data to foreign LEAs.⁹ Moreover, the national legislation in a majority of EU countries either does not cover or explicitly prohibits service providers established within their jurisdictions from responding to direct requests from foreign LEAs.¹⁰ Whereas all US-based service providers are able to provide non-content data directly to foreign law enforcement authorities under US law,¹¹ within the EU only Ireland-based service providers may do so.¹² The principal reason for the upsurge in informal cooperation in these countries is that they account for a large proportion of the total volume of requests (both informal and MLA) due to the fact that major service providers are headquartered there.¹³

As the example of Ireland and the US indicates, the type of data solicited plays an important role in informal cooperation. In this context, responses to a recent Commission questionnaire revealed that the definitions of types of data vary significantly among Member States, with only a handful

⁹ Of the 24 Member States that responded to a questionnaire issued by the Commission services, 14 Member States considered compliance with direct requests sent from national authorities directly to a service provider in another country to be voluntary, while 7 Member States considered these requests mandatory; see Commission non-paper 1, *ibid.*, para. 1.2.1.

¹⁰ *Ibid.*, para. 1.2.1.

¹¹ See 18 U.S. Code Chapter 121 Section 2702 ('Stored Communications Act') on voluntary disclosure of customer communications or records.

¹² See section 8 of the Irish Data Protection Acts 1988 and 2003. See also A. Hogan, "The Interception of Communications in Ireland - Time for a Re-Think", *Data Protection Ireland*, Vol. 7, No. 5, 2014, p. 9.

¹³ See the non-paper of the Commission services of June 2017 on "Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward" (hereafter 'Commission non-paper 2'), p. 3.

allowing the disclosure of content data and “other data”.¹⁴ A divergence in practices was also identified in relation to the procedures for making direct requests.¹⁵ There is no common approach among Member States as to the competent authority to initiate the process, the modalities of a request or the means to transmit the information.¹⁶ Again not only do the legal regimes or practices of Member States diverge, but also the responses of service providers vary (in time and extent), at times depending on the requesting country. LEAs also report that responses by service providers vary depending on where requests come from.¹⁷ For instance, Google responded recently to 75% of requests from Finland¹⁸ and 71% from the UK,¹⁹ but to none from Hungarian LEAs.²⁰

LEAs also reported problems in identifying and reaching the contact point of the relevant service provider, and even where this is achieved, matters are complicated further due to the lack of a common line among providers regarding the use of platforms, forms, required content of a request, language or communication channels.²¹ LEAs must therefore tailor their approach to each individual company, but complain of a lack of transparency on the providers’ side in relation to why a given request is granted or refused.²² Service providers, meanwhile, complain of difficulties in assessing the legitimacy and authenticity of requests since national provisions differ widely even among Member States,²³ generating significant costs for providers.²⁴ Also, where cooperation is voluntary, service providers create their own internal policies of handling requests or decide on a case-

¹⁴ Commission non-paper 1 (op. cit.), para. 1.2.1.

¹⁵ Ibid., para. 1.2.1.

¹⁶ Ibid., para. 1.2.1.

¹⁷ Ibid., para. 2.1.6.

¹⁸ See Google, “Transparency Report” ([https:// www.google.com/transparencyreport/userdatarequests/FI/](https://www.google.com/transparencyreport/userdatarequests/FI/)).

¹⁹ Ibid.

²⁰ Ibid.

²¹ Commission non-paper 1 (op. cit.), para. 2.1.4.

²² Ibid., para. 1.2.1.

²³ Ibid., para. 2.1.5.

²⁴ Ibid.

by-case basis whether and how to cooperate.²⁵ Service providers face conflicting interests: they have to protect their users' privacy while being expected to cooperate with LEAs. They have, *inter alia*, data protection obligations towards their customers and thus may wish to release information about requests received (and cooperation granted) in their regular transparency reports – at the risk of compromising an investigation.²⁶

Closely linked to a lack of transparency and reliability, the Commission reported problems deriving from a lack of accountability. Not knowing which crimes are being investigated renders it difficult for service providers to be accountable to their users.²⁷ US-based providers are also not accountable to LEAs for submitting no/incomplete/false information since there is no legal obligation under US law to submit any data.²⁸ Furthermore, criminal procedure laws usually do not regulate direct cooperation across borders, which may not only lead to problems in terms of accountability or a lack thereof, but also to problems with the admissibility as evidence in a later criminal trial.²⁹

10.2 Towards formulating legal responses

In the aftermath of the March 2016 terrorist attacks in Brussels and under pressure from LEAs, several Member States pushed the Council of the European Union to request that the Commission explore possibilities for a common EU approach to improving criminal justice in cyberspace.³⁰ The Council set the Commission to work in three areas: enhancing cooperation with service providers, streamlining MLA (and mutual recognition) proceedings, and reviewing rules on enforcement jurisdiction in

²⁵ *Ibid.*, para. 2.1.

²⁶ *Ibid.*, para. 2.1.1.

²⁷ *Ibid.*, para. 2.1.3.

²⁸ *Ibid.*

²⁹ *Ibid.* and para. 2.1.7.

³⁰ Council of the European Union, "Council Conclusions on improving criminal justice in cyberspace", Press Office, Brussels, 9 June 2016 (https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf) (hereafter 'Council Conclusions').

cyberspace.³¹ Within a month, the Commission had launched an expert consultation process to explore possible solutions and work towards a common EU position, and in December 2016 a first progress report was provided to the Justice and Home Affairs (JHA) Council³² detailing the Commission's activities and describing the problems identified in each of the three areas. A second non-paper³³ based on the results of the expert consultation process was presented at the JHA Council meeting in June 2017, with a greater emphasis on the way forward, through legislative action among others. The ministers gave the green light to the Commission to table a concrete legislative proposal, prompting an announcement by Commissioner Věra Jourová that one will be put forward in early 2018.³⁴ On 4 August 2017, an "Inception Impact Assessment" was published to inform stakeholders of the Commission's work, to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities.³⁵ A first public consultation on improving cross-border access to electronic evidence was launched on the same day.³⁶

In its recent non-papers, the Commission has outlined in the first place possible practical improvements within the existing rules, as regards cooperation between competent authorities on the one hand and between LEAs and service providers on the other.³⁷ For instance, creating an electronic version of the EIO form and setting up a secure platform for the exchange of EIOs, requests and responses between competent authorities

³¹ Ibid., I-III.

³² Commission non-paper 1 (op. cit.).

³³ Commission non-paper 2 (op. cit.), p. 2.

³⁴ See the statement by Commissioner Věra Jourová at the "Justice and Home Affairs Council, 3546th meeting: Joint press conference by Marlene Bonnici, Maltese Permanent Representative to the EU, and Věra Jourová, Member of the EC", 2017 (<http://ec.europa.eu/avservices/video/player.cfm?ref=I139501&videolang=INT&start time=347&devurl=http://ec.europa.eu/avservices/video/player/config.cfm>).

³⁵ See European Commission, "Inception Impact Assessment", Ref. Ares(2017)3896097, 3.8.2017.

³⁶ See European Commission, Public consultation on improving cross-border access to electronic evidence in criminal matters, 2017 (https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en).

³⁷ Commission non-paper 2 (op. cit.), para. 3.1.

was considered.³⁸ Concerning cooperation between Member States' authorities and service providers within the existing framework, suggested improvements include the creation of a single point of contact on the law enforcement/judiciary side for law enforcement requests issued to service providers established abroad, the creation of a single point of entry on the service provider side for dealing with such requests, training on either side on providers' different policies and procedures, standardisation and reduction of forms used by LEAs, streamlining of providers' policies and the establishment of an online platform to provide comprehensive guidance to LEAs on current policies, forms, channels, and so on.³⁹

The Commission, however, acknowledges that the proposed practical solutions can only partly address the existing problems as "they cannot provide solutions for fragmented legal frameworks among Member States".⁴⁰ Hence, in its most recent non-paper from June 2017, the Commission reflects not only on practical measures within the existing framework, but also on regulatory approaches. To provide legal certainty for cross-border requests and reduce the level of complexity and fragmentation outlined above, one proposed regulatory solution is a legislative measure enabling LEAs to request ("production request") or compel ("production order") a third party, i.e. a service provider, in another Member State to disclose information about a user.⁴¹ Where the location of data, infrastructure or the relevant provider cannot be established or where there is a risk of losing data, "direct access" – often referred to as 'legal hacking' – might also be considered, in light of the fact that a number of Member States already provide for this measure in domestic law.⁴² In this case, common conditions and minimum safeguards should be defined as well as mitigating measures, such as notifications to possibly affected countries.⁴³ The Commission has also been mandated to pursue work on facilitating access to electronic evidence in third countries, in particular the US⁴⁴

³⁸ Commission non-paper 1 (op. cit.), para. 3.1.1.

³⁹ Commission non-paper 2 (op. cit.), p. 2 et seq; in detail see also Commission non-paper 1 (*supra*), para. 3.1.2.

⁴⁰ Commission non-paper 2 (*supra*), p. 4.

⁴¹ *Ibid.*

⁴² *Ibid.*, p. 5.

⁴³ *Ibid.*

⁴⁴ Commission non-paper 1 (op. cit.), para. 3.2.

With regard to a comprehensive, single EU instrument, a central question is whether to request or compel a service provider, whose main seat is in another Member State, to provide access to data. An EU instrument may establish a legal basis for authorities to act and service providers to respond voluntarily (production request), or provide for a mandatory production order with a sanctioning system to enforce the order in case of non-compliance (subpoena).⁴⁵ Both measures would mean that service providers can be addressed directly without the request or order having to go through a law enforcement or judicial intermediary in the other Member State. Obviously, the least intrusive option would be to rely on voluntary cooperation, but considering the dependence on cooperation of providers it would also be the least effective option if there is no strong incentive for providers to comply.

As envisaged by the Commission, the production request and production order raise a number of complex legal questions. First of all, any future EU legislation would need to define the notion of electronic evidence, establish what kind of electronic evidence is covered and precisely circumscribe those entities to which a production order or production request may be addressed. Electronic evidence commonly refers to data of value to an investigation that is stored on, received or transmitted by an electronic device. As technology advances, the amount and types of data that can be found on electronic devices are constantly increasing. Various types of data exist that can be of value for an investigation: data that are visible to end users, such as subscriber data and content data; and data that are not readily visible to end users, such as metadata,⁴⁶ which consist, inter alia, of information on file designation, creation and edit history data, location data or traffic data. In different EU legal instruments, definitions of certain types of data exist, e.g. the notion of “personal data” now has identical definitions under Art. 3 of the Directive on Police and Criminal Justice Authorities⁴⁷ and

⁴⁵ Commission non-paper 2 (op. cit.), p. 4.

⁴⁶ Some metadata, for instance file date and size, can easily be accessed by the end user, while other metadata is embedded in file locations requiring special tools or knowledge to be revealed.

⁴⁷ See 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

the General Data Protection Regulation.⁴⁸ The notions of “traffic data” and “location data” are defined in Art. 2 of the E-Privacy Directive. The Budapest Convention, in contrast, only provides technical definitions of the notions of “computer data” and “traffic data”.

Considering that the E-Privacy Directive sets forth elaborated categories of data and abolishes the differentiation between data in transition and stored data, one may ask whether a new instrument should rely on these data categories or go beyond them. One may also ask whether a definition of subscriber data is necessary in this context. None of the directives, nor the General Data Protection Regulation, nor the Budapest Convention contains a definition of ‘subscriber data’. The information sought under the heading ‘subscriber data’ is information similar to a reverse directory check – it is information that links an individual to an account. As there is no binding definition of subscriber data, the notion could also be read as covering all sorts of data that social networks and other services keep on their customers, which can be highly personal and is not traditionally thought of as communications data.⁴⁹ Therefore, it is inevitable that the proposed instrument will have to define those data which constitute electronic evidence. Alongside the type of data, the volume of data to be accessed is also relevant for assessing the intensity of any interference with rights to data protection and respect for private and family life under the EU Charter Fundamental Rights.⁵⁰

The issue of which categories of data in relation to which a production request or production order may be issued is intertwined with the personal scope of the measure: in other words, which service providers ought to be covered. One approach would be to use an open-ended, relatively technologically-neutral definition, such as ‘digital service provider’. The flexibility offered by such an approach, however, comes with the risk of

movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

⁴⁸ A similar but not identical definition of ‘personal data’ can be found in Art. 2 of Directive 95/46/EC on Data Protection, to which Art. 2 of the E-Privacy Directive used to refer (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, OJ L 201, 31.7.2002, p. 37).

⁴⁹ See House of Lords/House of Commons, “Joint Committee on the Draft Communications Data Bill”, Report from Session 2012-2013, p. 47 et seq.

⁵⁰ Commission non-paper 2 (op. cit.), p. 6.

burdening service providers that are not priority targets for law enforcement, to the detriment of smaller enterprises. One way to temper this danger might be to provide for limits such as those in the recent German *Netzwerkdurchsetzungsgesetz* (NetzDG),⁵¹ which foresees an obligation to disclose data within 48 hours only for social media providers with more than 2 million registered users in Germany.⁵² Alternatively, rather than using an open definition, affected service providers could be categorised depending on the service they provide, similar to the technical distinctions made in terms of liability in the E-Commerce Directive⁵³ or by including definitions capable of covering not only major ‘information society services’ such as Twitter and Facebook, but also providers of cloud services and digital marketplaces, for example.

Considering that a single regime for cross-border access to evidence in general is already in place in the form of the EIO framework, the relationship between the EIO framework and any such production order for electronic evidence would also require clarification as a matter of priority. The same applies to the question of how the production order would relate to other legal instruments and agreements, such as MLA treaties and the Budapest Convention. The EIO Directive, for instance, foresees that where reference is made to MLA in relevant international instruments, such as the Budapest Convention, it should be understood that between the Member States bound by the Directive it takes precedence over those conventions.⁵⁴ From a policy perspective, too, given the coexistence of the EIO framework and the envisaged production order, their interrelationship would have to be clearly articulated in order to ensure that the production order constitutes sufficient added value to justify a separate legislative effort. This might be achieved, by way of example, by limiting the production order to serious crime – meaning that the EIO would be the central weapon for LEAs requiring electronic evidence to investigate less serious offences.

⁵¹ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), BT-Drs. 18/13013.

⁵² Refer to § 5(2), § 1(2) NetzDG. In addition, the law requires these providers to establish an authorised recipient in Germany for said requests (§ 5(1) NetzDG).

⁵³ Cf. Arts. 12-15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, OJ L 178, 17.7.2000.

⁵⁴ See Recital 35 of the EIO Directive.

In light of the *Digital Rights Ireland* and *Tele2 Sverige* judgments from the Court of Justice of the European Union, the proportionality of the envisaged proposal with the fundamental Charter rights to data protection (Art. 7) and respect for private and family life (Art. 8) will require adequate scope limitations and safeguards to be in place. In particular, a clause restricting the issuing of production orders to investigations of serious crime may prove necessary in order to ensure fundamental rights compliance – at least as regards content data. Prior authorisation by an independent judicial authority may also be required as a condition – again, at least for content data. Insofar as an issuing authority is concerned, should the option of direct issuing of a production order by the police be entertained, this may have to be limited to subscriber data, with orders to produce metadata and content data requiring the intervention of a judge.

A more legal technical question relates to the nature of the proposed instrument. One has to ask whether production orders that supersede cooperation between LEAs by directly obliging service providers to supply electronic evidence still constitute judicial cooperation based on mutual recognition. The original concept of mutual recognition in EU law was supposed to ensure market access to the European single market for products that are not subject to EU harmonisation. The Tampere European Council decided in October 1999 that the principle should also become the cornerstone of judicial cooperation in both civil and criminal matters within the EU.⁵⁵ Mutual recognition is founded on equivalence and trust between Member States. As regards a mandatory production order with extraterritorial effect, one has to ask whether this still constitutes an instrument of judicial cooperation even though no foreign authority is involved in its execution.

The competence of the EU to adopt legally binding acts in the area of judicial cooperation in criminal matters is proclaimed in Art. 82 of the Treaty on the Functioning of the European Union (TFEU). Art. 82(1) sub-para. 1 elevates mutual recognition to an overarching principle or leitmotiv, whereas Art. 82(1) sub-para. 2 contains an exhaustive list of legislative competences. Art. 82(1) clearly relates to measures on judicial cooperation, where this term stands for cooperation between judicial or equivalent authorities of the Member States. Yet as far as the term “cooperation” is concerned, Art. 82(1)(d) differentiates between “facilitating cooperation”

⁵⁵ See the Presidency Conclusions of the Tampere European Council, 15 and 16 October 1999, para. 33.

and “enforcement of decisions”. Along the logic of the mutual recognition instruments in the internal market, Art. 82(1)(d) empowers the EU legislator to adopt measures for the “enforcement of decisions” of one Member State that are then automatically valid in the entire EU. This logic would enable the EU legislator to bring the planned production order into the realm of judicial cooperation based on Art. 82 TFEU.

Finally, an EU instrument would also have to provide for effective means for its enforcement – in particular when it comes to service providers based in third countries. The aforementioned German NetzDG requires, for instance, the establishment of an authorised recipient for disclosure requests in Germany and foresees fines for non-compliance with this obligation or the omission to respond to such a request (a maximum fine of €500,000).⁵⁶ This enforcement mechanism obviates the need to rely on reciprocal responses. Reciprocal responses by third parties are a sensitive issue when it comes to fundamental rights, as third countries may not have equivalent fundamental rights standards in place. Considering that the addressees of production orders are regularly legal persons established in another country, fines and criminal penalties at the national level would obviously need to be applicable. In that regard, the issuing state would have to rely on the state where the order is executed for enforcement. If – in order to be enforceable – this procedure must be based on MLA, one may ask whether this contradicts the original intention behind the use of a cross-border production order.⁵⁷

10.3 Concluding remarks

The drive to improve the speed and efficiency of transnational investigations necessitating access to electronic evidence has led to new practices marking a paradigm shift in cross-border judicial cooperation. Classic interstate cooperation is increasingly being replaced by a practice whereby domestic law enforcement directly engages with foreign service providers. Not only do these new developments require adequate legal rules, but their coexistence with traditional judicial cooperation also demands close assessment. The legal background to such an assessment is constituted by aspects of criminal law as well as public law (data protection and privacy) and even private law (secondary obligations to protect a counterparty’s legitimate interests).

⁵⁶ See § 4(1) Nos. 7 and 8 and § 4(2) NetzDG.

⁵⁷ Commission non-paper 1 (op. cit.), para. 2.3.2.

PART III

CONCLUSIONS

11. CONSTITUTIONALISING THE SECURITY UNION

SERGIO CARRERA AND VALSAMIS MITSILEGAS

This collective volume has provided a multidisciplinary examination of the key issues, challenges and gaps associated with the EU's security policy and the implementation of the Security Union, particularly in relation to common policies aimed at countering terrorism and crime. The various chapters have aimed at contributing to the European Commission's "Comprehensive Assessment of EU Security Policy". The Comprehensive Assessment, published on 26 July 2017, sought to review the Union's action on internal security over the last 15 years.¹ This chapter identifies and explores the main findings emerging from the analysis presented in the contributions comprising this book. Special attention is given to the constitutional issues and dilemmas facing the Security Union in relation to the EU standards enshrined in the Treaties, the EU Charter of Fundamental Rights and secondary law.

Section 11.1 starts by contextualising the Security Union in light of the Lisbon Treaty and EU Better Regulation principles. Section 11.2 moves on to explore the necessity and effectiveness of two of the main EU policy priorities in addressing terrorism: information exchange and interoperability. Section 11.3 brings to the fore the effects and compatibility of EU security policies with the EU Charter of Fundamental Rights, notably the fundamental right of privacy. It sheds similar light on efforts to counter violent radicalisation. Section 11.4 considers the relationship between the Security Union and the 'justice dimension', the relevance of a criminal justice-led approach when countering terrorism and crime, and the

¹ The Comprehensive Assessment was published together with the "Ninth Progress Report towards an Effective and Genuine Security Union". See European Commission, "Comprehensive Assessment of EU Security Policy", Commission Staff Working Document, SWD(2017) 278 final, Brussels, 26.7.2017; and Commission Communication, "Ninth Progress Report towards an Effective and Genuine Security Union", COM(2017) 407 final, Brussels, 26.7.2017.

importance of upholding the rule of law for the principle of mutual recognition in criminal matters. Section 11.5 concludes by presenting a way forward towards ‘constitutionalising’ the Security Union.

11.1 ‘Lisbonisation’ and Better Regulation

During the last 15 years the EU has developed a dynamic legal and policy framework on issues related to countering terrorism and cross-border serious crime. Curtin’s chapter highlights that the EU Area of Freedom, Security and Justice (AFSJ) has witnessed significant policy developments since the 1990s, and has gradually moved to the top of the Union’s political agenda. This has been despite the fact that ‘internal security’ has traditionally been conceived as an exclusive competence of the Member States.²

The Union’s competence on security policies has experienced a widening in reach and scope, especially since the entry into force of the Lisbon Treaty in 2009. The Lisbon Treaty brought judicial cooperation in criminal matters and police under Title V, “Area of Freedom, Security and Justice” and to *shared legal competence* between the Union and the Member States. Chapter 4 of the TFEU (Arts. 82-86) lays down the legal basis for judicial cooperation in criminal matters, which shall be based on, and driven by, the principle of mutual recognition of judgments and judicial decisions. Chapter 5 TFEU offers the normative foundations of EU measures establishing police cooperation among the Member States’ competent authorities, including “police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences”.

The Lisbonisation of EU policies on criminal justice and policing meant for the first time the expansion of the ‘ordinary legislative procedure’ to these fields. The application of the Community method of cooperation injected enhanced democratic scrutiny into EU security cooperation. The European Parliament was formally granted the role of co-legislator in the adoption of

² Art. 72 of the Treaty on the Functioning of the European Union (TFEU) puts it thus: “This Title 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.” Refer also to Art. 73 of the TFEU.

secondary legislation and the power to approve international agreements on security matters.³

Protocol 36 of the EU Treaties nevertheless stipulated transitional provisions limiting the powers of the Court of Justice of the European Union (CJEU) and the Commission. For a period of five years from the entry into force of the Lisbon Treaty (December 2009), the Commission was not able to fully exercise its role as ‘guardian of the Treaties’ and start infringement proceedings against Member States in breach of their obligations to implement EU criminal justice and policing laws. The CJEU had no full jurisdiction to review and answer questions from the Member States’ national courts on the interpretation of these policies, except if they had accepted such jurisdiction optionally.

The transitional arrangements, however, came to an end in December 2014.⁴ This meant the effective shift from ‘intergovernmentalism’ – which used to characterise European cooperation in these areas⁵ – to ‘supranationalism’ in EU third-pillar law and the assumption of the full powers of European institutions in the field. The expectations behind the Lisbonisation in these sensitive policy areas related mainly to enhanced EU legal and judicial accountability and the monitoring of trust in the EU AFSJ.

The widening of the Commission’s powers to enforce EU criminal justice and police law has been a positive step forward to ensure a more consistent and uniform application of EU law in this area, and presents great potential to address current implementation gaps in EU security instruments and tools at the national level.

³ S. Carrera, N. Hernanz and J. Parkin, “The ‘Lisbonisation’ of the European Parliament – Assessing progress, shortcomings, and challenges for democratic accountability in the area of freedom, security and justice”, Working Paper No. 58, CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels, 2013, pp. 6-7.

⁴ S. Carrera, V. Mitsilegas and K. Eisele, “Who Monitors Trust in the European Justice Area? The End of the Transitional Period for the Measures under Police and Judicial Cooperation in Criminal Matters Adopted before the Lisbon Treaty”, Study for the European Parliament, DG IPOL (Internal Policies), Brussels, 2014.

⁵ See S. Carrera and E. Guild, “No Constitutional Treaty? Implications for the Area of Freedom, Security and Justice”, in T. Balzacq and S. Carrera (eds), *Security versus Freedom? A Challenge for Europe’s Future*, Aldershot: Ashgate Publishing, 2006, pp. 223-239. See also S. Carrera, E. Guild and T. Balzacq, “The Changing Dynamics of Security in an Enlarged European Union”, in S. Carrera, D. Bigo, E. Guild and R. Walker, *Europe’s 21st Century Challenge: Delivering Liberty*, Aldershot: Ashgate Publishing, 2010, pp. 31-48.

From a Lisbon Treaty perspective, 'more EU' has formally meant putting the individual, the democratic rule of law and fundamental rights at the centre of EU action in AFSJ policies. The legally binding nature of the EU Charter of Fundamental Rights, which now has the same legal value as the Treaties, has positioned and formally enshrined fundamental rights at the heart of the European justice area. Privacy and the rights of the defence are now inextricably linked to the effective and trust-based supranational cooperation on security and criminal justice. The fundamental rights of suspects in criminal proceedings⁶ are crucial ingredients necessary to facilitate mutual recognition of judgments and judicial decisions.

Still, the Lisbonisation of EU policies on criminal justice and police has not always been able to catch up with the ways in which decision-shaping and decision-making processes have taken place in security measures. It is far from clear how the pre-Lisbon Treaty ways of setting priorities and adopting decisions have actually and meaningfully changed in practice.

The set-up of a Security Union Task Force,⁷ and its goal to bring together all the relevant Commission services with direct or indirect portfolios on security, is a welcome step in ensuring a more consistent EU policy approach in the domain of security. Commissioner King's initiative of launching a "Comprehensive Assessment of EU Security Policy" represented a further advance in that direction and provided momentum to review the EU *acquis* in these domains as well as to identify gaps requiring further action. The assessment concluded with an "overall positive appreciation of EU action in this area". The Commission's assessment outlines some important findings related to the relevance and general value (as perceived by selected stakeholders) of the EU's intervention in the field of security cooperation.

⁶ Chapter VI of the EU Charter (justice) provides for the rights to an effective remedy and fair trial, the presumption of innocence and rights of the defence as well as the principles of legality and proportionality of criminal offences and penalties, and the *ne bis in idem* principle.

⁷ European Commission, "President Juncker consults the European Parliament on Sir Julian King as Commissioner for the Security Union", Press Release IP 16/2707, Brussels, 2.8.2016.

The assessment presents some limitations in providing an in-depth evaluation or ‘fitness check’⁸ – in line with the Better Regulation guidelines – of existing Union security policies, instruments and agencies.⁹ Such an evaluation exercise would require a more detailed and qualitative assessment (instrument by instrument) of their *effectiveness* (how successful EU action has been in achieving or progressing towards its objectives), *efficiency* (are the costs and benefits of EU action justified and proportionate) and *coherence* (how well or not different actions work together).

De Londras underlines in chapter 4 of this volume that EU counter-terrorism policies have grown and mushroomed usually following terrorist attacks and threats, particularly since 2001. She argues that they have not always done so based on a careful assessment – drawing from the best and independent academic/scientific knowledge from the social sciences and humanities and from civil society inputs – of their actual need and effectiveness. The EU Better Regulation guidelines¹⁰ call for “a rigorous evidence base to inform decision-making”, in order to “inform political choices with evidence – not the other way around”.¹¹ Indeed, the Inter-Institutional Agreement on better law-making of April 2016 stipulates the need for high-quality legislation and well-informed policy-making, which generally include carrying out an impact assessment,¹² public and

⁸ See “Fitness checks” (http://ec.europa.eu/smart-regulation/evaluation/docs/fitness_checks_2012_en.pdf).

⁹ Refer to European Commission, “Better Regulation Toolbox” (http://ec.europa.eu/smart-regulation/guidelines/docs/br_toolbox_en.pdf).

¹⁰ See the European Commission’s webpage on “Better Regulation: Why and How”. See also European Commission, “Better Regulation Guidelines”, Staff Working Document, SWD(2015) 111 final, Strasbourg, 19.5.2015.

¹¹ European Commission, “Better Regulation Toolbox” (op. cit.).

¹² Refer to the Inter-Institutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law Making, 13 April 2016 (OJ L 123/1, 12.5.2016), point 12:

Impact assessments should cover the existence, scale and consequences of a problem and the question whether or not Union action is needed. They should map out alternative solutions and, where possible, potential short and long-term costs and benefits, assessing the economic, environmental and social impacts in an integrated and balanced way and using both qualitative and quantitative analyses. The principles of subsidiarity and proportionality should be fully respected, as should fundamental rights ... Impact assessments should be based on accurate, objective and complete information and should be

stakeholder consultation/feedback, and an *ex post* evaluation of existing legislation.¹³

This book illustrates how in a post-Lisbon Treaty landscape ‘better policy-making’ should remain an ongoing and consistent policy objective. Several chapters bring to the fore examples where EU security measures have been adopted without a robust examination of their *effectiveness*, *efficiency* and *coherence*, as well as a full compatibility test with EU standards and fundamental rights.

Chapters 4 and 7 by de Londras and Brouwer respectively, for instance, show how some EU security legislation has been passed without a proper *ex ante* impact assessment and ‘added value’ examination. In other cases, EU security measures have been adopted in expedited ways and later on have been struck down or invalidated by the Court of Justice in Luxembourg because of their incompatibility with the EU principles and fundamental rights envisaged in the EU Charter of Fundamental Rights.

In chapter 4, de Londras highlights that the mere existence of security measures in the EU anti-terrorism and crime *acquis* seems to predetermine or presume their effectiveness and that they are ‘fit for purpose’. A *truly* comprehensive evaluation of EU security policies, in her view, would call for analysing whether the set of laws and policies under review actually ‘work’ in practice in light of their objectives. Such a critical exercise would need to go hand-in-hand with an effectiveness assessment, consisting of checking whether the policies actually achieve the purported public goals (both meta-objectives and specific objectives) for which they were designed. It should also involve the Commission more vigorously using the powers it has had since 2014 to ensure the consistency of EU policy in these fields in Member States’ implementation of the *acquis*.

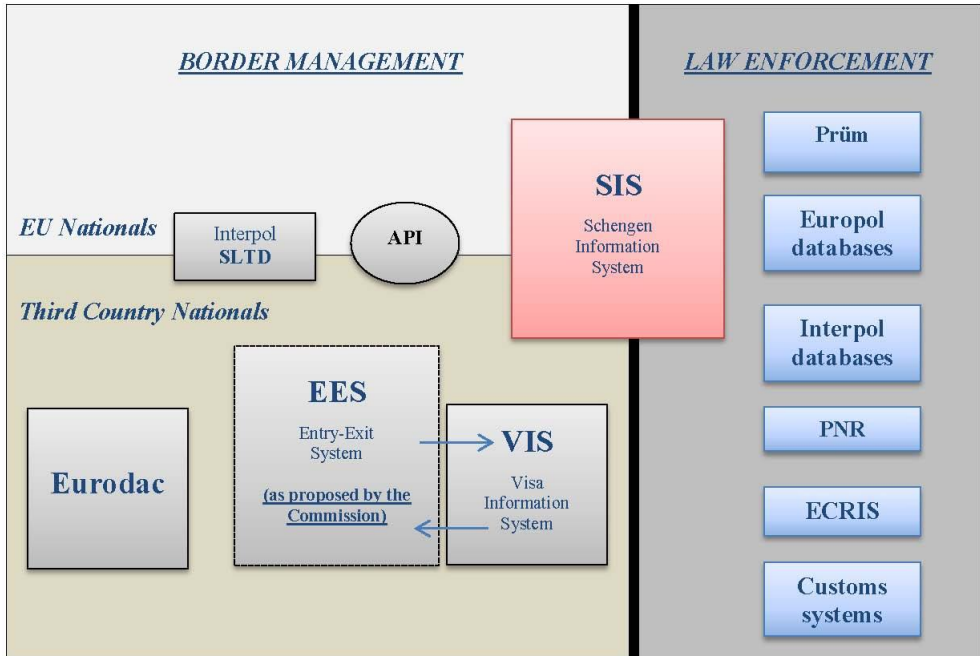
proportionate as regards their scope and focus ... The Commission’s Regulatory Scrutiny Board will carry out an objective quality check of its impact assessments.

¹³ Following point 22 of the Agreement, “[i]n the context of the legislative cycle, evaluations of existing legislation and policy, based on efficiency, effectiveness, relevance, coherence and value added, should provide the basis for impact assessments of options for further action”.

11.2 Information sharing and interoperability

The exchange of information among national law enforcement authorities has constituted a long-standing priority in EU counter-terrorism policies. Curtin points out in chapter 6 that information sharing has become a central tool in EU internal and external security policy. Over the last two decades, the EU has developed a plethora of information systems and databases, such as the Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac (the European Automated Fingerprint Identification System) and the Europol Information System.¹⁴ Figure 1 provides a schematic overview of the present EU information systems and databases covering border management and law enforcement.

Figure 1. EU information systems (border management and law enforcement)



¹⁴ S. Carrera, D. Bigo, B. Hayes, N. Hernanz and J. Jeandesboz, “Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals”, Study for the European Parliament, DG IPOL, Brussels, 2012. For an updated overview of EU information systems, refer to Council of the European Union, “Manual on Law Enforcement Information Exchange”, 6261/17, Brussels, 4.7.2017.

Note: API refers advance passenger information, ECRIS to European Criminal Records Information System, PNR to passenger name record and SLTD to Interpol's stolen and lost travel documents.

Source: European Commission, Communication, "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205, Brussels, 6.4.2016, p. 6.

The Security Union seems to be inspired by the goal of 'maximisation' and further 'centralisation' of information sharing across current EU information systems and various law enforcement authorities. According to the Commission's Communication on "Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union" of April 2016, overcoming the fragmentation of information sharing seems to be the most fundamental goal of the Security Union:

In a Security Union, a police officer in one Member State should have the same reflex to share relevant information with colleagues over the border, as he would do with fellow officers within his country. This requires a step change in two respects. At European level, we need to urgently address the remaining gaps, fragmentation and operational limitations of the information exchange tools in place, to make sure that structures for cooperation are as effective as possible, and to make sure that European legislation to tackle terrorist criminals and their activities is up to date and robust. *This is necessary to create an environment of confidence among national authorities and the legal and practical tools that allow them to work together to address common challenges.* The full added value of an effective Security Union depends crucially on the use that is made of these tools and structures to close any future operational loopholes and police intelligence gaps. That requires a *culture change*, at the level of Member States, for their law enforcement authorities to acquire the habit of systematic cooperation and information sharing, right down to the last policeman. A sense of common responsibility, and the will and capacity to turn that into action, are essential if we are to overcome the fragmentation which terrorists and criminals are so effective at exploiting. (Emphasis added)¹⁵

¹⁵ European Commission, Communication, "Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union", COM(2016) 230, Brussels, 20.4.2016.

The Commission's Comprehensive Assessment identified "shortcomings" regarding EU information systems, including "(a) sub-optimal functionalities of existing information systems, (b) gaps in the EU's architecture of data management, (c) a complex landscape of differently governed information systems, and (d) a fragmented architecture of data management for border control and security".¹⁶ The "solution" for addressing these deficits in the Commission's opinion is the interoperability of information systems "for security, border and migration management by 2020 to ensure that border guards, law enforcement officers including customs officials, immigration officials and judicial authorities have the necessary information at their disposal".¹⁷

The way in which the Security Union aims to be genuine and effective is to put special emphasis on the *full use* of existing databases or information systems, chiefly the interoperability of databases. Interoperability, however, is far from new as a concept in EU policy documents,¹⁸ as exemplified by the 2004 European Council Declaration on Combating Terrorism following the Madrid terrorist attacks:

The European Council calls on the Commission to submit proposals for enhanced interoperability between European databases and to explore the creation of synergies between existing and future information systems (SIS II, VIS and EURODAC) in order to exploit their added value within their respective legal and technical frameworks in the prevention and fight against terrorism.

In its 2016 Communication on "Stronger and Smarter Information Systems for Borders and Security",¹⁹ the Commission defined interoperability as "the ability of information systems to exchange data and to enable the sharing of

¹⁶ European Commission, Comprehensive Assessment, SWD(2017) 278 final, 2017 (op. cit.), p. 80.

¹⁷ Ibid.

¹⁸ Council of the European Union, "Additional Measures to combat terrorism - Proposals by the German delegation", 13176/01, 24.10.2001. The document stated that "the Council instructs the Article 36 Committee to submit immediate proposals on: interconnection of data by making on-line access authorisation to the databases of the SIS available to Europol, national public prosecutor's offices, immigration and asylum authorities; enabling Europe-wide computerised profile searches to be conducted".

¹⁹ European Commission, Communication, "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final, Brussels, 6.4.2016, p. 14.

information".²⁰ It identified four main dimensions under the notion of interoperability:

- a single search interface to query several information systems simultaneously and to produce combined results on one single screen;
- the interconnectivity of information systems where data registered in one system will automatically be consulted by another system;
- the establishment of a shared biometric matching service in support of various information systems;
- a common repository of data for different information systems (core module).²¹

The interoperability agenda has subsequently been reconfirmed by various EU official documents. The joint statement by EU ministers for justice and home affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016²² stated the need to

increase as a matter of urgency the systematic feeding, consistent use and interoperability of European and international databases in the fields of security, travel and migration by making full use of technological developments and including privacy safeguards from the outset. This is particularly relevant for reliable identity verification.

The priority given to interoperability was reiterated in a recent report²³ of May 2017 by the High-Level Expert Group on Information Systems and Interoperability set up by the Commission, whose actual membership has

²⁰ Refer also to European Commission, *European Interoperability Framework for Pan-European e-government services*, Luxembourg: Office for Official Publications of the European Union, 2004 (<http://ec.europa.eu/idabc/servlets/Docd552.pdf>).

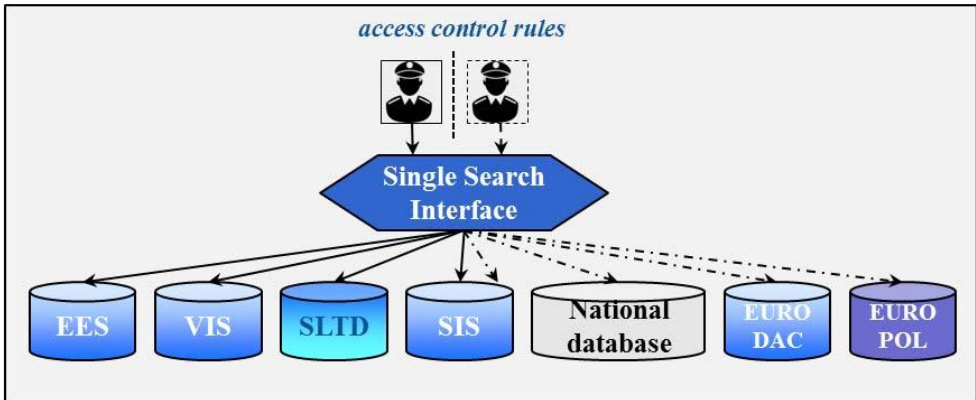
²¹ *Ibid.*

²² Council of the European Union, Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016, 7371/16, Brussels, 24.3.2016.

²³ See the High-Level Expert Group on Information Systems and Interoperability, "Final report", European Commission, DG for Migration and Home Affairs, May 2017 (<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>).

not been publicly disclosed.²⁴ The core task of the group was to “address the legal, technical and operational aspects of various options to achieve interoperability of information systems”. The report called for more interoperability of existing EU information systems and recommended that the EU mainly consider the option of a centralised “single search interface” (SSI), as represented in Figure 2.²⁵

Figure 2. Single search interface



Note: EES refers to entry–exit system, and SLTD refers to Interpol’s stolen and lost travel documents.

Source: European Commission, Communication, “Stronger and Smarter Information Systems for Borders and Security”, COM(2016) 205, Brussels, 6.4.2016, p. 16.

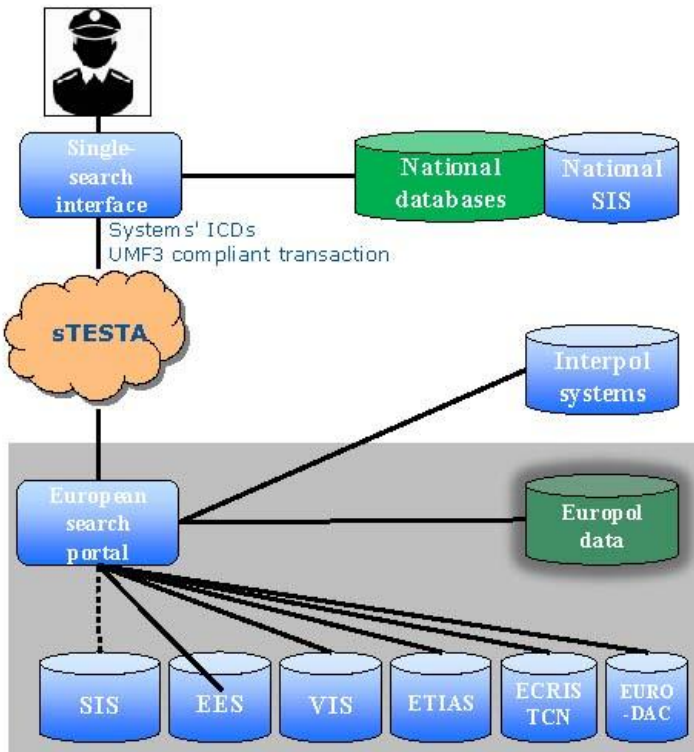
²⁴ See European Commission’s Register of Commission Expert Groups and Other Entities, High-Level Expert Group on Information Systems and Interoperability (<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435>).

²⁵ The group drew this conclusion in its report (p. 27):

An important finding was that the second option (interconnectivity of systems) should only be considered on a case-by-case basis, while evaluating if certain data from one system needs to be systematically and automatically reused to be entered into another system. Consider the example with two systems, A and B, that can be consulted via a single-search interface. The interconnectivity of system B with system A only makes sense if system A systematically and automatically needs to store and process data from system B. If no data reuse is necessary or if such reuse requires a human (legal) decision, the interconnection is without interest: the single-search interface is a better and sufficient option.

As illustrated in Figure 3, the interface or functionality would aim at facilitating the possibility to “query several information systems simultaneously, and to produce combined results on one single screen for border guards and police officers”, by setting up a platform offering the ability to consult all relevant EU information systems with one query/procedure.²⁶ Still, the report expressly states that “the potential practical and operational challenges for Member States and relevant agencies to fully exploit the benefits of such a centralised SSI would need to be further explored”.²⁷

Figure 3. Conceptual overview of the European search portal



Note: EES refers to the entry-exit system, ECRIS TCN to the European Criminal Records Information System for third-country nationals, ETIAS to the European travel information and

²⁶ Ibid., p. 15. According to the report, the SSI would not connect with national databases, and “an assessment of such a European search portal would be undertaken, but it would be expected to require relatively minor technical changes on the national side”, p. 28.

²⁷ Ibid., p. 29.

authorisation system, STESTA to the Secured Trans European Services for Telematics between Administrations, and UMF to Universal Message Format.

Source: High-Level Expert Group, on Information Systems and Interoperability, “Final Report”, May 2017, p. 29.

The High-Level Expert Group recommended the establishment of a shared, biometric matching system for all the centralised databases that would include both fingerprints and facial images, and would match biometric data from so-called ‘parent systems’ like the SIS, VIS, Eurodac, etc.²⁸ The group took no account of the data protection implications of such a proposal and the implementation challenges that it would entail. The report also recommended the setting-up of a “common identity repository” of alphanumeric identity data “that would allow for a complete view of all claimed biographic identities used by a person” and single identifications.²⁹

The report provides no evidence substantiating the usefulness or the potential negative impacts of interoperability or the legal and technical questions intimately related to its practical implementation. It has provided no evidence that the gaps resulting from the existence of compartmentalised EU information systems represent a security threat, nor on what these gaps actually are. The High-Level Expert Group report does not either explain the necessity and proportionality of the proposed SSI, shared biometric system and common identity repository.

Kreissl underlines in chapter 9 of this volume that the equation of more data equals more security ignores the conceptual and practical challenges inherent in data analysis. The Commission’s Comprehensive Assessment has rightly underlined the need to improve the quality of data going into EU databases. This indeed remains a key challenge in cross-border cooperation on law enforcement. The technical discussions that have taken place in the scope of the High-Level Expert Group should now be coupled with a

²⁸ The report (p. 31) explains it as follows:

A person who is the subject of a check can be registered in several systems simultaneously – potentially under different identities – given the specific purpose of each system. Public authorities should be able to obtain reliable and up-to-date information about the status of such persons on the basis of possible matches from all relevant EU systems.

²⁹ *Ibid.*, p. 32.

detailed examination of the legal implications and questions raised by the various ideas being recommended.³⁰

Each EU information system relies on different national ministries and domestic coordinating authorities. It is often the case that these national authorities differ substantially from one another depending on the EU database at stake, and that designated domestic actors (which are often a single point of contact or which correspond with one or more than one central, national access point) have different access rights depending on their domestic responsibilities and the kind of information on each EU information system.

This book calls for a realistic discussion about the scope and actual reach of the principle of interoperability. The questions of ‘who’ has access to what information and under whose control and oversight often reflect the organisational and administrative structures fulfilling Member States’ constitutional or legal national systems. Information systems dealing with migration and asylum matters are usually in the hands of or ‘owned’ by domestic authorities that have central responsibility for issuing visas or those in charge of asylum, and not the police.³¹ When and if national law enforcement authorities have certain access to these databases for the purpose of countering terrorism and crime, access rights are subject to detailed and well-regulated requirements and in well-defined cases. The picture becomes even more complex in those Member States that have a decentralised division of competences regarding migration and policing.

Furthermore, the High-Level Expert Group refers to the proposal for establishing a European travel information and authorisation system (ETIAS) as already putting the concept of a common identity repository into practice, and how this system would share a common repository of personal data of third-country nationals with the proposed entry-exit system, which is currently under inter-institutional negotiations. Yet previous research has demonstrated that the European Commission’s 2016 proposal on ETIAS

³⁰ S. Alegre, J. Jeandesboz and N. Vavoula, “European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection”, European Parliament Study, DG IPOL, Brussels, 2017.

³¹ See for instance the “List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS)” (2016/C 187/04), OJ L 187/4, 26.5.2016.

lacked any proper impact assessment justifying its necessity, effectiveness, fundamental rights compliance or added value.³²

In addition to the legality check of the specific ways in which interoperability will take shape, it is important to underline that not all EU institutions and Member States in fact agree on exactly what *interoperability* actually means or how widely the net should be cast. What is clear is that the concept would entail a major widening of the group of actors with rights of access to EU information systems.

Therefore, a *broad* notion of ‘interoperability’ would constitute a far-reaching transformation of the ways in which centralised EU information systems work and the ownership of the data stored in each of them. Curtin explains in chapter 6 of this volume that the notion of interoperability is a more general and less passive term than the principle of availability formerly proposed at the EU level, which implied full availability and interconnections between systems and actors.³³ It would be important to examine the impact and costs of ‘non-interoperability’ or a *narrow* notion and scope of interoperability in the AFSJ, and to explore other options for addressing the operational challenges in the current use of EU databases.

Mitsilegas points out in chapter 1 that the cross-sectoral approach called for by the European Agenda on Security is based on an axiom of maximum collection and exchange of data across EU databases, irrespective of their main purpose or rationale. Widening access to sensitive information beyond the actors with specific and clearly defined expertise and powers can be detrimental to effective cooperation and fundamental rights.

Experience has shown that trust works best among a limited number of actors with well-defined roles and who share competences and similar objectives. The increasing reliance on and calls for interoperability of existing electronic information databases might not always be the most effective way of countering terrorism and crime. Ownership of data seems to be an issue of critical importance in creating confidence in EU information systems. The wider the interoperability and the circle of actors with access to databases,

³² See Alegre, Jeandesboz and Vavoula (2017), *op. cit.*

³³ The former principle of availability implied an obligation for the Member States to give access to or provide certain types of information available to their authorities to equivalent authorities of other Member States. It would hinder the national authorities concerned from saying no to the request and from working under the agreement about ‘what information is’, how to handle it and its uses ([http://www.europarl.europa.eu/RegData/etudes/note/join/2006/378272/IPOL-LIBE_NT\(2006\)378272_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2006/378272/IPOL-LIBE_NT(2006)378272_EN.pdf)).

the more reluctant some actors may become to input sensitive information into a particular EU information system.

The priority given to ever-wider access to databases may in turn have a deleterious effect on the quality of the data that actors are willing to share with others in the EU. Counter-terrorism magistrates may be able to share information without too much difficulty across borders. But if they know that the data that they share with their counterparts in another Member State may also become available to other actors, such as border and coast guards or police, this may no longer be the case. Furthermore, sensitive information may end up in the hands of national authorities with no experience in specific areas or pose risks to vulnerable categories of individuals, such as asylum seekers.

Interoperability reinvigorates a ‘preventive justice’ approach, as it effectively means the interlinkage and blurring between migration management tools and those designed for the purposes of fighting terrorism and crime. Increasing linkages between law enforcement databases with those covering migration and asylum should not nurture the stigmatisation and discrimination of third-country nationals and asylum seekers in the EU. The use of information stored in EU data systems such as Eurodac leads to an automatic veil of suspicion over people seeking international protection in the EU, which has been said to have negative legal and societal consequences.³⁴ Kreissl reminds us in chapter 9 of this book that the migration–security nexus, which is too easily taken for granted in some policy discussions and extreme-right populist agendas, “should be disentangled to better understand and more effectively address the challenges of data-driven intelligence strategies ... and approaches aimed at governing mobility and identity”.

11.3 Fundamental rights and societal impacts

The Human Rights Commissioner of the Council of Europe has declared that “laws and policies that are human rights compliant preserve the values the

³⁴ Refer for instance to the Note prepared by the Meijers Committee on “The amended proposal for the Eurodac Regulation (COM(2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes (COM(2009) 344, 10.9.2009), CM0910, Utrecht, 30 December 2009.

terrorists are trying to destroy, weaken the pull of radicalisation, and strengthen the public's confidence in the rule of law and democratic institutions".³⁵ A majority of the contributions to this book have called upon the EU to place the fundamental principles and values enshrined in the Treaties at the heart of EU security policy, beyond the usual formalistic statements that can often be found in EU official documents concerning fundamental rights compliance. Chapter 3 by Bárd highlights that the premise of proponents of a preventive justice model for EU security cooperation is that security and human rights are competing areas that might mutually exclude one another.

EU counter-terrorism policies tend to start from an understanding of security that frames EU constitutional principles – democracy, rule of law and fundamental rights – as obstacles to effective counter-terrorism and law enforcement policies. Liberty and security then become competing values that are to be 'balanced' against one another. The European Commission's Comprehensive Assessment states:

In a European Union founded on respect for human dignity, freedom, democracy, equality, the rule of law and human rights, protecting and fostering citizens' security and complying with fundamental rights *are complementary and mutually reinforcing*.
(Emphasis added)

This is a welcome statement. The challenge remains how to systematically and effectively operationalise it in practice. In 'times of crisis' or in the wake of terrorist attacks, as de Londras well explains, the standards that were considered to be 'exceptional' when the security law or policy was first introduced later on become normalised and the new way of doing things. This way of working in security policy-making may lead to 'downward' renegotiations of existing standards and fundamental rights protection, which challenges national and EU constitutional principles.

In its above-mentioned 2016 Communication on a "Stronger and Smarter Information System for Borders and Security", the Commission identified the principle of purpose limitation as one of the main causes of the current fragmentation of the EU's architecture on data management for border control and internal security:

³⁵ See the Commissioner for Human Rights, "National human rights structures: Protecting human rights while countering terrorism", Human Rights Comment, Council of Europe, Strasbourg, 6 December 2016.

With the new comprehensive framework for the protection of personal data in the EU in place and significant developments in technology and IT security, the principle of purpose limitation can be more easily implemented at the level of access and use to data stored, in full compliance with the Charter of Fundamental Rights and with recent European Court of Justice's jurisprudence. Safeguards such as compartmentalising data within one system and specific access and use rules for each category of data and user should ensure the necessary purpose limitation in integrated solutions for data management.³⁶

It is not entirely clear how the 'unification' laying behind the principle of interoperability will be compatible with CJEU and EU privacy standards. In fact, in a previous Communication providing an "Overview of information management in the area of freedom, security and justice",³⁷ the Commission rightly stated that

[p]urpose limitation is a key consideration for most of the instruments covered in this communication. A single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing. Creating such a system would, however, constitute *a gross and illegitimate restriction of individuals' right to privacy and data protection* and pose huge challenges in terms of development and operation. In practice, policies in the area of freedom, security and justice have developed in an incremental manner, yielding a number of information systems and instruments of varying size, scope and purpose. *The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' right to privacy than any centralised alternative.* (Emphasis added)

This tension was reiterated in the European Commission's "Seventh Progress Report towards an Effective and Genuine Security Union" of 16 May 2017,³⁸ which underlined that a key task in moving forward in discussions related to the interoperability of EU information systems is to

³⁶ See European Commission, COM(2016) 205, 2016 (op. cit.), p. 4.

³⁷ European Commission, Communication, "Overview of information management in the area of freedom, security and justice", COM(2010) 385 final, Brussels, 20.7.2010.

³⁸ European Commission, "Seventh Progress Report towards an Effective and Genuine Security Union", COM(2017) 261 final, Strasbourg, 16 May 2017.

devise “the necessary strict rules on access and use without affecting the existing purpose limitation”.

In addition to statements in the Commission’s Comprehensive Assessment that interoperability will comply with fundamental rights, a crucial challenge remains on how to effectively implement it in practice. How would interoperable information systems respect their specific data protection provisions and rules on access by competent authorities, separate purpose limitation rules for each category of data and dedicated data retention norms?

The fundamental rights to privacy and data protection enshrined in Arts 7 and 8 of the EU Charter of Fundamental Rights fully apply in respect of EU security policies and information systems designed to counter crime and terrorism. The principle of purpose limitation is a main component of EU data protection law.³⁹ Brouwer highlights in chapter 7 that this principle includes “the ban on ‘aimless data collection’ and the obligation of purpose specification”. The need to transparently lay down norms according to which information will be stored and shared and for what purposes plays a fundamental role under this principle. The way in which the Security Union agenda frames ‘compartmentalisation’ as a problem for effective security policies stands in a difficult relationship with this very principle, which lays at the foundations of EU privacy law and has direct effect, and thus could be directly enforceable by potentially affected individuals.

³⁹ See Art. 5.1 of the General Data Protection Regulation (EU) 2016/679 of 27 April 2016, which states that personal data shall be

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’).

See also para. 26 of the Preamble and also Art. 4(2)(a) of Directive (EU) 2016/680 of the European Parliament 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, OJ L 119/89, 4.5.2016. On the purpose limitation principle, see E. Brouwer, “Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation”, in L.F.M. Besselink, F. Pennings and S. Prechal (eds), *The Eclipse of the Legality Principle in the European Union*, The Hague: Kluwer, 2011.

The CJEU has played a major role in upholding EU rule of law principles in security policies. In a series of landmark judgments, the Luxembourg Court confirmed the importance of the rights to privacy and data protection, and maintained the unlawfulness of pre-emptive generalised or large-scale surveillance. Chapter 8 in this book by González Fuster argues that the European Commission's Comprehensive Assessment too easily draws the conclusion that everything is globally fine when it comes to the fundamental rights compliance of EU security measures. She holds that the compliance of EU actions in this regard should be better guaranteed to prevent the CJEU from intervening and invalidating EU legal instruments and international agreements, owing to their shortcomings.

The CJEU's rejection of generalised surveillance should be taken fully into account by the other Union institutions in developing a trust-based and rights-compliant Security Union. In times of upheaval, it is the judiciary that has reminded us of the importance of fundamental rights guarantees and 'better regulation' in the process of constitutionalising the Security Union, and of setting limits to an uncritical move towards prevention and insecurity.

The CJEU for instance has clarified, in such landmark rulings as *Digital Rights Ireland*, *Schrems* or *Tele2*, that generalised, large-scale and unlimited surveillance is contrary to EU privacy and data protection rights, and constitutes a disproportionate response in any democratic society.⁴⁰ The Luxembourg Court has equally underlined the need to show, for any data access and sharing, a link with specific, reasonable and individualised suspicion. These are clear warnings against temptations inherent to preventive justice approaches in the Security Union agenda. They confirm that any interference with the right to privacy must be strictly necessary. Moreover, González Fuster reminds us that "the general and indiscriminate retention of everybody's data is incompatible with EU law".

Cases of large-scale collection and transfer of data between EU and third countries pose equally open questions in light of these same judge-

⁴⁰ See V. Mitsilegas, "Surveillance and Digital Privacy in the Transatlantic 'War on Terror': The Case for a Global Privacy Regime", Legal Studies Research Paper No. 251/2017, Queen Mary University of London, 2017; and S. Carrera and E. Guild, "Safe harbour or into the storm? EU-US data transfers after the Schrems judgment", CEPS Paper in Liberty and Security in Europe, Centre for European Policy Studies, Brussels, 2015.

made standards. Brouwer's chapter clarifies how international agreements on the transfer of personal data between the EU and third states must offer clear rules on scope and content, be transparent, comply with the purpose limitation principle, be subject to independent control and guarantee effective remedies to individuals. These conditions are essential for assessing their legality in light of EU law.

This view has been confirmed in the recent Opinion by the CJEU on the EU-Canada Agreement on Passenger Name Records (PNR),⁴¹ which struck down the validity of the Agreement because of its incompatibility with the EU Charter of Fundamental Rights and EU data protection law. In this same Opinion, the Court also laid down a set of benchmarks for assessing the legality of current and future security measures, particularly the transfer of passengers' data in the scope of international agreements. These EU legal standards include, among others, the provision of sufficient guarantees of the integrity of individuals' personal data and their ability to seek effective remedies against the risk of abuse in third countries. They also require that access to and processing of electronic data are necessary (proportionate) and non-discriminatory, and that clear and precise rules specify the conditions justifying the interference with privacy, subject to a review carried out either by a court or an independent administrative body.

The Court of Justice has also brought the Lisbonisation of EU security policy to the fore by reminding the EU legislator about the right legal basis in the Treaties, under the headings of police cooperation *along with* data protection, and not public security and the activities of the state in areas of criminal law. The Opinion stated that the choice of the legal basis "must be founded on objective criteria amenable to judicial review, and those objective criteria include the purpose and the content of the act at issue". In this regard, the CJEU held that the purpose of the agreement envisaged is to combat terrorism and serious transnational crime "while safeguarding the right to respect for privacy and the right to protection of personal data", which it interpreted as the need to reconcile the two objectives, as they constitute two essential components of the Agreement.

The Court's Opinion clarified that it was clear from the content of the Agreement that the transfer and processing of data would be authorised "only if the data in question benefits from an adequate level of protection". In light of this Opinion, countering terrorism and crime with respect for the

⁴¹ See Opinion 1/15 of the Court (Grand Chamber) on the EU-Canada PNR Agreement, 26 July 2017.

rights of privacy and data protection are in this way inseparable and must be pursued simultaneously. On these grounds, the Court concluded that the correct legal basis for a PNR agreement between the EU and Canada should be Art. 87(2)(a) TFEU (police cooperation) in conjunction with Art. 16(2) TFEU (protection of personal data).

It is important to note here the relevance of this finding from the perspective of the Lisbonisation of police cooperation since 2009. Indeed, during the proceedings of the case, the European Commission argued before the Court that on the basis of the CJEU 2006 judgment, *Parliament v Council and Commission* (C-317/04 and C-318/04), which invalidated Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America,⁴² the purpose and content of the Agreement with Canada were “public security and the activities of the Member States in areas of criminal law”. In the view of the Court, the Commission was taking “out of context” the findings in that case, “which, it must be recalled, was delivered well before the adoption of the Treaty of Lisbon”.⁴³

The Court has thus sent a clear message to EU institutions and Member States that exchange and sharing of information for the purposes of fighting terrorism and crime – including in frameworks for international cooperation – fall under shared EU-Member States competence and are subject to EU judicial scrutiny in a post-Lisbon Treaty landscape. Measures framing international cooperation on the transfer and processing of data for the purposes of countering crime and terrorism must go hand-in-hand with privacy. Moreover, they must no longer fall under the notion of ‘public security’ and the exclusive competence of EU Member States on matters of policing (as they did prior to the entry into force of the Lisbon Treaty), as they are now a *shared* competence between Member States and the EU.

The Court also clearly differentiated in this Opinion between policing measures adopted for the purposes of prevention, detection and investigation of criminal offences – which may include the collection, storage, processing, analysis and exchange of relevant information – and

⁴² See E. Guild and E. Brouwer, “The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US”, CEPS Policy Brief No. 109, Centre for European Policy Studies, Brussels, July 2006; refer also to *Parliament v Council and Commission* (C-317/04 and C-318/04), 30 May 2006, paras 54-58 of the judgment.

⁴³ See para. 84 of Opinion 1/15, *op. cit.*

those covering judicial cooperation in criminal matters as envisaged in Art. 82(1)(d) TFEU. Lastly, the Court's Opinion means not only the need to open new negotiations with Canada with the aim of concluding a new agreement,⁴⁴ but also the automatic annulment of similar PNR agreements that the EU currently has with the US and Australia.⁴⁵ It furthermore casts a shadow over the legality of the EU's PNR Directive.⁴⁶

In chapter 6, Curtin quotes Tuori's⁴⁷ critique of the normative concerns pertaining to the EU's security constitution, which mainly relates to treating individuals as "passive recipients of collective security goods rather than active citizens and bearers of rights". Curtin argues that despite the fact that EU information exchange initiatives and tools profoundly affect people's privacy, there is very little that affected individuals can actually do to challenge these processes and reclaim the ownership of their data. Furthermore, as Curtin's chapter highlights, the central issues remain regarding how to make information gathering, mining and interoperable sharing of data (which often remain "invisible") transparent, and "how we make informal, unseen and multijurisdictional arrangements accountable".

Furthermore, careful consideration should be paid to the wider societal effects of certain EU security policies. Identifying, detecting and addressing the underlying factors that lead individuals to commit extreme forms of violence are prominent themes in EU counter-terrorism policies. The concept of 'radicalisation' hides extremely complex and dynamic phenomena. An

⁴⁴ European Commission, Recommendation for a Council Decision authorising the opening of negotiations on an Agreement between the European Union and Canada for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime, COM(2017) 605 final, Brussels, 18.10.2017.

⁴⁵ See the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186, 14.7.2012, pp. 4-16; and also the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, pp. 5-14.

⁴⁶ See Directive (EU) 2016/681 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, OJ L 119, 4.5.2016.

⁴⁷ K. Tuori, *European Constitutionalism*, Cambridge, MA: Cambridge University Press, 2015, p. 317.

‘easy policy fix’ simply does not exist. As the European Parliament Resolution on the prevention of radicalisation and recruitment of European citizens by terrorist organisations of November 2015 rightly acknowledged, radicalisation calls for a careful examination of the various global, sociological and political factors, and needs to be understood on a case-by-case basis, against the background and interactions of the individuals concerned.

These are all factors deserving careful consideration in the design and implementation of public policies addressing terrorism in the EU. Counter-radicalisation policies in the EU have so far included ‘hard’ counter-terrorism responses, such as the adoption of new laws in various Member States allowing for pre-emptive judicial powers, deprivation of nationality and stop-and-search activities.⁴⁸

As examined in chapter 5 by Davila Gordillo and Ragazzi, they have also included ‘softer measures’. Among these are the setting-up of the Radicalisation Awareness Network (RAN) and the focus it has given to supporting the involvement of local service providers, in sectors such as health and education, in preventing terrorism through the involvement of “front-line practitioners” and communities. Chapter 5 explains how counter-radicalisation policies frame communities as both the objects and the subjects of security practices. They both work through suspicion but also through trust relations. The impact of these policies on societal mistrust cannot be underestimated.⁴⁹ While softer in nature, these initiatives have been shown to have important societal implications and often negative repercussions that are counterproductive in meeting their intended goals.

Counter-radicalisation policies call for a large degree of caution, particularly regarding their adequacy for diagnosing the phenomenon and their actual consequences and wider societal impacts in the communities concerned. If not carefully designed and implemented, counter-

⁴⁸ D. Bigo, L. Bonelli, E.P. Guittet and F. Ragazzi, “Preventing and Countering Youth Radicalisation in the EU”, Study for the European Parliament, DG IPOL, Brussels, 2014; V. Mitsilegas, *EU Criminal Law after Lisbon*, Hart Studies in Criminal Law, Oxford: Hart Publishing, 2016.

⁴⁹ Open Society Justice Initiative, “Eroding Trust: The UK’s PREVENT Counter-Extremism Strategy in Health and Education”, New York, NY, 2016; UK House of Commons (Home Affairs Committee), “Radicalisation: The counter-narrative and identifying the tipping point”, Eighth Report of Session 2016–17, HC 135, 25 August 2016, pp. 36-37.

radicalisation efforts involving a broad range of social actors – e.g. social workers, schoolteachers and health professionals – may in fact be detrimental to their objectives. Davila Gordillo and Ragazzi argue that these policies controversially give front-line practitioners the task of “propagating the state-sanctioned narrative of radicalisation, with the concomitant exclusion of alternative voices”. Special attention should also be paid to ensuring that counter-radicalisation policies do not result in denigrating the value of diversity and pluralism in political debates.⁵⁰

As highlighted in the Commission’s Comprehensive Assessment, the Commission should foster more coordination and synergies between law enforcement approaches to countering radicalisation and other EU policies aimed at fostering social inclusion, tackling inequalities, and preventing marginalisation and the stigmatisation of certain communities.

11.4 EU criminal justice standards: Mutual recognition and the rule of law

The challenges and risks posed by current EU counter-terrorism and crime policies to fundamental rights are not exclusively confined to privacy. Preventive justice policies, as described in chapter 1 of this book, also give rise to profound dilemmas in ‘justice-related’ fundamental rights, which are of central relevance to safeguarding the rights of suspects in criminal investigations and proceedings. These include, chiefly, the right to a legal defence and fair trial guarantees for suspects in criminal investigations and proceedings, the presumption of innocence and the principle of legality of criminal offences and sanctions enshrined in Arts 47-50 of the EU Charter of Fundamental Rights.

As Ligeti and Robinson show in chapter 10, ‘big data’ practices and electronic communications held by IT companies are increasingly in demand by pre-emptive counter-terrorism policies.⁵¹ Calls for direct access to or ‘legal

⁵⁰ F. Ragazzi, “Suspect community or suspect category? The impact of counter-terrorism as ‘policed multiculturalism’”, *Journal of Ethnic and Migration Studies*, Vol. 42, No. 5, 2016, pp. 724-741.

⁵¹ S. Carrera, G. González Fuster, E. Guild and V. Mitsilegas, “Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights”, CEPS Report, Centre for European Policy Studies, Brussels, 2015. See also D. Lyon, “Big Data Surveillance: Snowden, Everyday Practices and Digital Futures”, in T. Basaran, D. Bigo, E.P. Guittet and R.B.J. Walker (eds), *International Political*

hacking' of electronic data stored by the private sector lead to an acute legal uncertainty and exposes companies to conflicting demands, which may expose them to legal liabilities and mistrust by their clients regarding privacy.

Mitsilegas clarifies in chapter 1 that the European Commission non-papers on "Improving cross-border access to electronic evidence" of May 2017,⁵² and the three scenarios outlined concerning cross-border access to electronic evidence, challenge key principles of judicial cooperation in criminal matters, bypassing EU legal standards like those laid down in the European Investigation Order (EIO). There is also a reframing of issues from 'criminal justice' to 'cybercrime', which puts police efficiency, demands and priorities first and relegates individuals' safeguards and criminal justice guarantees to second place.

The various options presently being discussed by the European Commission to request and even oblige IT companies to give access to their customers' data in the scope of criminal investigations raise very profound legal and rule of law issues in the EU legal system and some Member States' constitutional regimes. The idea of developing an EU production order that would compel a service provider in another EU Member State to provide information about a user would stand at odds with the model elaborated in the EIO. In chapter 10, Ligeti and Robinson rightly call for the need to clarify, as a matter of priority, the relationship between the EIO and any such production order. It is in our view central that the EU should stop talking about 'electronic evidence' when what is being discussed is actually 'electronic information', which *may* be useful for criminal investigations but which has certainly not yet been validated as proper 'evidence' by an independent, rule of law court.

Moreover, the Directorate-General for Justice and Consumers of the European Commission should be cautious when discussing the idea of a production order. Its very nature takes us far beyond judicial cooperation in the domain of criminal matters towards those of policing and internal security. The goal of forcing the private sector to provide access to electronic

Sociology: Transversal Lines, London: Routledge Studies in International Political Sociology, 2017, pp. 254-285.

⁵² European Commission, Non-Paper, "Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward" (undated) (https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf).

data gives no service to facilitating mutual recognition of judgments and judicial decisions in the EU. It also directly alienates the involvement of and the critical role played by judicial authorities in criminal justice proceedings and in ensuring the rule of law in the adjudication of justice. For any future production order to find a sound legal foundation in the Treaties, its legal basis could not possibly be Art. 82(1)(d) TFEU, but rather Art. 87(2) TFEU (on police cooperation).

As Brouwer explains in chapter 7, “there is no such principle of ‘blind trust’”, and mutual trust also concerns the reliability and accuracy of the information shared and the lawfulness of the processing. Calls for ‘big data’ and more information overlook the questions of the actual nature and quality of that information, and the extent to which it will be admissible as electronic evidence in criminal proceedings before an independent tribunal. Criminal justice and police investigations require data that are considered ‘admissible’ by an independent judge.⁵³ In contrast, data qualified as ‘intelligence’ include any kind of information irrespective of its reliability, origins and quality, or compliance with admissibility and jurisdictional rules.⁵⁴

This book has also provided evidence that the EU criminal justice area remains incomplete and subject to a number of gaps. Weyembergh’s contribution in chapter 2 illustrates the need for more consistency and complementarity among EU (criminal justice) instruments on mutual recognition. This could help to address the issues of ‘overuse’ of the European Arrest Warrant for prosecutorial purposes as well as the overuse of pre-trial detention. Furthermore, mutual recognition does not yet cover the whole judicial cooperation realm, such as the transfer of proceedings or disqualification decisions.

Weyembergh also recalls in chapter 2 the need to better ensure a closer relationship with and application of EU law standards laid down in criminal justice instruments on mutual recognition, such as the EIO, and in cross-border investigations and operational activities coordinated by EU agencies, such as joint investigation teams (JITs). JITs consist of judges, prosecutors

⁵³ D. Bigo, S. Carrera, N. Hernanz and A. Scherrer, “The Use of Intelligence Information, the National Security or State Secrets Rule and Secret Evidence in National Legislation and Its Interpretation by Courts”, Study for the European Parliament, DG IPOL, Brussels, 2014.

⁵⁴ D. Bigo, S. Carrera, E. Guild and V. Mitsilegas, “The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more information sharing”, CEPS Commentary, Centre for European Policy Studies, Brussels, 2016.

and law enforcement authorities who are brought together for a fixed period for the purpose of conducting criminal investigations in one or several Member States. She additionally underlines the need to optimise recourse to and the relationships between the various instruments composing the EU criminal justice toolbox. This corresponds with calls in previous research to ensure the compatibility and consistency between the JITs and the EIO benchmarks when exchanging information for the purposes of fighting criminal activities in the EU.⁵⁵

The independence of the judiciary and full compliance with the fundamental rights of suspects in criminal proceedings represent the *sine qua non* for the EU principle of mutual recognition to operate and – more importantly – to survive. Bárd’s chapter points out that when fundamental rights and the principle of separation of powers are systematically and routinely violated, these abuses have the potential to be ‘exported’ to other Member States belonging to the EU’s AFSJ. Rule of law backsliding will also undermine the mutual trust laying at the basis of European cooperation and hamper the exercise of the rights of individuals EU-wide. When the courts are no longer independent, or when detention conditions are not human rights-compliant, criminal justice decisions and requests will be legitimately contested and mistrusted by other Member States.

11.5 Conclusions

This book has brought to light some of the most important open questions and challenges that the evolution of the European security strategy and a Security Union relying increasingly on a paradigm of ‘preventive justice’ poses for the rule of law, the protection of fundamental rights and citizenship in Europe. The management of Union security responses has taken the form of regular reports on the Security Union, combined – also in response to repeated terrorist incidents in major European cities – with separate communications by the European Council and the Commission.

The 2017 European Commission “Comprehensive Assessment of EU Security Policy” has constituted a welcomed step in the need to review the EU *acquis* in these domains as well as to identify gaps requiring further policy action. This book has called for ensuring that EU security policies are

⁵⁵ S. Carrera, E. Guild, L. Vosyliūtė, A. Scherrer and V. Mitsilegas, “The Cost of Non-Europe in the Area of Organised Crime”, Study for the European Parliament, DG EPRS, Brussels, 2016.

firmly embedded in the EU Lisbon Treaty and Better Regulation commitments. Prior to the Security Union resulting in yet more EU law in the field, detailed and serious thought should be given to three matters:

- 1) the efficiency and effectiveness of the existing – and already quite extensive – Union legal framework on security, and of newly proposed initiatives;
- 2) the compatibility of each Union security instrument with the EU Treaties and other parallel EU policies; and
- 3) key EU values, including fundamental rights and the rule of law.

The chapters making up this book have recalled and stressed the value of conducting *ex ante* evaluations or impact assessments (or both) in an attempt to ensure a high level of expertise and objectivity in such a sensitive policy domain. As Weyembergh reminds us, “if the EU intervention in the field lacks credible justification, then it will face a real problem of legitimacy”. This is critically important in light of the fact that *ex ante* impact assessment enables the gathering of civil society inputs on the repercussions of the proposed measures, as well as social sciences and humanities research on the societal and fundamental rights effects.

Bárd reminds us in chapter 3 of this volume that the actual question on which any ‘comprehensive’ assessment of EU security policy should be solidly anchored is the rationality and the development of legal means to prevent abuses called into life by risks of hysteria and illiberalism. She concludes that establishing an *ex ante* mechanism of the EU rule of law (which would involve the monitoring of fundamental rights) based on objectivity, scientific rigour and a sound methodology is therefore inevitable. Chapter 8 by González Fuster equally underlines the importance of security measures being supported by strict consideration of the need for each data processing operation, which would require an *ex ante* evaluation of their necessity and the existence of other less invasive options. In her view, EU security measures should comply with EU rule of law and fundamental rights standards “from the very start, by design and by default”. Similarly, in chapter 7 Brouwer stresses the need to base the negotiation of agreements with third countries allowing data transfers on evidence substantiating their necessity and proportionality.

Overreacting on security and disregarding fundamental rights in the process poses a direct challenge to the very values and founding principles upon which the Union is based, values that the Union is constitutionally bound to uphold and promote in its external action, especially since the entry into force of the Lisbon Treaty in 2009. With the Security Union based

increasingly upon operational cooperation, interoperability and the generalised collection and exchange of data under a model of pre-emptive surveillance, the risks entailed for fundamental rights and also for essential bonds of trust and citizenship across the Union are acute.

The underlying assumption is that more and systemic information exchange/sharing will lead to more confidence among national authorities to address common challenges. The various chapter contributions have illustrated how 'more information' (exceeding purpose limitation and actor-field specialisation or competence) does not always necessarily mean 'more Union' and 'more trust' in EU security cooperation. An 'Information Union' may lead to 'less Union' and 'more mistrust' among practitioners on EU information tools.

A Security Union based on a wide notion of interoperability will face important challenges from the perspective of the EU's rule of law system of checks and balances, and the division of responsibilities that have been designed in the national constitutional systems of Member States and which have slowly been reflected and developed in the EU Treaties since Lisbon so as to guide Union activities in these fields. A certain degree of 'fragmentation' - understood as the diversity/plurality of 'who is doing what' and with 'which data for what purpose' at the domestic and supranational levels in countering terrorism and crime - is also an inherent consequence of the division of competences at the Member State and EU levels in different policy domains.

As Bigo⁵⁶ convincingly put it, "this inherent problem in the problematization of this norm is that of delegitimation of all segmentation of information. Still, democracy lives within its own limits, frontiers of penal law, oppositions and necessary counter-powers for the power of the police in the sense of an institution or of a network of institutions." The blurring division of responsibilities and competences/expertise among different national security actors, which underlies calls for more interoperability and *purposeless information exchange*, will inevitably lead to an increasing lack of confidence. It undermines the principle of property or ownership of information, which is by nature de-compartmentalised, and tends to forget that under EU data protection law the individual is the ultimate holder or 'owner' of his or her data.

⁵⁶ D. Bigo, "The Principle of Availability of Information", European Parliament Briefing Paper, DG IPOL, Brussels, 2006.

A key lesson emerging from this book is that the EU needs to be realistic and honest about what it can actually deliver in the field of security, and what it can really expect from Member States in this policy domain. Current and future policy attempts to address gaps and dilemmas must take place under the democratic rule of law and fundamental rights standards of the Lisbon Treaty, and EU Better Regulation principles. This is what will make the Security Union *genuine* with respect to its founding constitutional values and principles and to its citizens.⁵⁷

⁵⁷ S. Carrera, E. Guild and V. Mitsilegas, “Reflections on the Terrorist Attacks in Barcelona: Constructing a principled and trust-based EU approach to countering terrorism”, CEPS Policy Insight No. 2017-32, Centre for European Policy Studies, Brussels, August 2017.

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
CCTV	Closed-circuit television camera
CISA	Convention on Implementing the Schengen Agreement
COSI	Standing Committee on Operational Cooperation on Internal Security
CJEU	Court of Justice of the European Union
EAW	European Arrest Warrant
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EPPO	European Public Prosecutor's Office
ESO	European Supervision Order
ETIAS	European travel information and authorisation system
eu-LISA	European Agency for the Operational Management of large-scale IT systems in the Area of Freedom, Security and Justice
Eurodac	European Automated Fingerprint Identification System
FATF	Financial Action Task Force
GFCC	German Federal Constitutional Court
GDPR	General Data Protection Regulation ((EU) 2016/679)
JHA	Justice and home affairs
JIT	Joint investigation team
LEA	Law enforcement authority
MLA	Mutual legal assistance
NGO	Non-governmental organisation
OLAF	European Anti-Fraud Office
PNR	Passenger name record
RAN	Radicalisation Awareness Network
SIS	Schengen Information System
SSI	Single search interface
TEU	Treaty on European Union
TESAT	EU Terrorism Situation and Trend Report
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Financing Tracking Program
VIS	Visa Information System

LIST OF CONTRIBUTORS

Petra Bárd is Associate Professor in Criminology at Eötvös Loránd University, Visiting Professor at the Central European University and Senior Researcher at the National Institute of Criminology in Budapest.

Evelien Brouwer works as a Senior Researcher in migration law at the Vrije Universiteit Amsterdam. Her current research activities concern border and visa policies, legal protection, data protection and privacy, and the meaning of mutual trust in EU migration law.

Sergio Carrera is a Senior Research Fellow and Head of the Justice and Home Affairs Programme at CEPS in Brussels and a part-time Professor at the Migration Policy Centre at the European University Institute in Florence. He is a Visiting Professor at the Paris School of International Affairs at Sciences Po, Associate Professor/Senior Research Fellow at the Faculty of Law at Maastricht University and Honorary Industry Professor at the School of Law at Queen Mary University of London.

Deirdre Curtin is Joint Chair of European Law and Politics at the European University Institute in Florence. She has been Professor at the Law Faculty of the University of Amsterdam since 2008 and held the Chair in European Law from 2008 to 2015.

Diana Davila Gordillo is a PhD candidate at Leiden University.

Fiona de Londras is the inaugural Professor of Global Legal Studies at the University of Birmingham, where she is also the Deputy Head of the Birmingham Law School. She has written widely on counter-terrorism, particularly from a comparative perspective, and led the FP7 project consortium on SECILE (Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness).

Gloria González Fuster is a Research Professor and a member of the Law, Science, Technology & Society Research Group at the Vrije Universiteit Brussels.

Reinhard Kreissl is a sociologist and is presently Director of the Vienna Centre for Societal Security. He has overseen and coordinated major European research projects on surveillance, security and privacy, and published numerous articles and books in the field.

Katalin Ligeti is Professor of European and International Criminal Law, Director of the LLM programme in European Economic and Financial Criminal Law, co-leader of the ICT/Criminal Law Research Group at the University of Luxembourg's Research Unit in Law, and the coordinator of the Doctoral Training Unit on Enforcement in Multi-Level Regulatory Systems. In 2015, she was appointed to the European Commission's Expert Group on Criminal Policy. Since April 2017 she has been a Special Adviser to the Commissioner for Consumer Protection and Fundamental Rights, Věra Jourová.

Valsamis Mitsilegas is Professor of European Criminal Law, Dean for Research (Humanities and Social Sciences) and, since 2012, Head of the Department of Law at Queen Mary University of London. He has been the Director of the Queen Mary Criminal Justice Centre since 2011.

Francesco Ragazzi is a Lecturer at the University of Leiden.

Gavin Robinson is a Postdoctoral Researcher in criminal law and IT law, at the Faculté de Droit, d'Économie et de Finance, Université du Luxembourg.

Anne Weyembergh is a full-time Professor at the Institute for European Studies (IEE) at the Université libre de Bruxelles (ULB). Together with Serge de Biolley, she has founded and coordinates the European Criminal Law Academic Network. In addition, she is the coordinator of the IEE-ULB team on European criminal law.

ANNEX. PROGRAMME OF THE POLICY WORKSHOP CO-ORGANISED BY CEPS AND DG HOME

Reappraising EU Security Policy Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime

12 May 2017

08:30–09:00 Registration

09:00–09:15 Introduction to the Policy Meeting

- **Welcome** (Sergio Carrera, CEPS)
- **EU Security Policy: A comprehensive assessment**
(Silvio Mascagna, European Commission, Member of the Cabinet of
Commissioner Julian King)

09:15–11:15 **Challenge I: Cross-Border Criminal Investigations**

Moderator: Tania Schroeter (European Commission, DG JUST)

Speakers

- Valsamis Mitsilegas (Queen Mary University of London)
- Anne Weyembergh (ULB)
- Petra Bárd (CEU)
- Fiona de Londras (University of Birmingham)

Discussants

- Andrei Stefanuc (European Commission, DG JUST)
- Michal Nesporek (EU Agency for Fundamental Rights – FRA)

Open Discussion

11:15–11:30 Coffee Break

11:30–13:30 Challenge II: Information Sharing

Moderator: Cecilia Verkleij (European Commission, DG HOME)

Speakers

- Didier Bigo (Sciences Po Paris and Kings' College London) & Julien Jeandesboz (ULB)
- Reinhard Kreissl (Vienna Centre for Societal Security)
- Deirdre Curtin (EUI)

Discussants

- Richard Rinkens (European Commission, DG HOME)
- Sandra Nunes (eu-LISA)
- Priscilla de Locht (EDPS)

Open Discussion

13:30–14:30 Lunch break

14:30–16:30 Challenge III: International Cooperation

Moderator: Olivier Onidi (European Commission, DG HOME)

Speakers


- Judith Rauhofer (Edinburgh Law School)
- Evelien Brouwer (Vrije Universiteit Amsterdam)
- Katalin Ligeti (University of Luxembourg)

Discussants

- Christiane Hoehn (EU Counter-Terrorism Coordinator's Office)
- Dietrich Neumann (Europol)
- Jorge Bento Silva (European Commission, DG HOME)

Open Discussion

16:30 **Closing Remarks** by Olivier Onidi (European Commission)



This book provides a multidisciplinary examination of the critical issues and challenges associated with the EU's initiative to build a Security Union, particularly in relation to common policies adopted at the Member State level aimed at countering terrorism and crime. It delves into EU efforts to support cross-border investigations, the exchange of information and international cooperation, taking stock of the effects on freedom and privacy.

The various contributions offer key research findings, which contributed to the European Commission's 2017 Comprehensive Assessment of EU Security Policy. They identify and explore the main constitutional dilemmas facing the Security Union concerning EU standards enshrined in the Lisbon Treaty and the commitments undertaken in the context of the EU Better Regulation agenda. Hence, this timely examination of EU security policies sheds light on their effectiveness, proportionality, fundamental rights and societal implications.



9 789461 386434

