GERMAN LAW JOURNAL

Developments in German, European and International Jurisprudence

www.germanlawjournal.com

ISSN: 2071-8322 / ISSNL: 2071-8322

Vol. 19 No. 05 **Pages 1117-1290** **1 October 2018**

EU Security Governance and Financial Crimes

Guest Editors
Els De Busser & Ester Herlin-Karnell

Table of Contents

Table of Contents, cont.

The Role of Data and Privacy

Articles

EU Security Governance and Financial Crimes

By Els De Busser[*] & Ester Herlin-Karnell[**]

A. Introduction

This special issue aims to investigate the regulatory challenges facing the EU with regard to security governance in the broad area of the fight against financial crimes and by adopting a wider outlook on how to map and understand these phenomena in their salient contexts. In recent years, security as a key word can be witnessed as increasingly penetrating policies on a national, international, and supranational level. This development is also visible in EU policies, inter alia in the EU's policy concerning the area of freedom, security, and justice (AFSJ). Coupling the word security to the concept of governance in the somewhat thought-provoking phrase "security governance" prominently cements its position in the entirety of processes and mechanisms that steer people as well as corporations or markets. Security in the EU internal context concerns to a great extent the fight against terrorism and its financing as well as the policing of EU borders. Security in this regard concerns the structure of EU law and how it can be justified at the macro-level.

Security governance at the micro-level, though, concerns the behavior of individuals. Coercing a natural person in the right direction can—but does not need to[1]—be done by the deterrence of punishment, for example in law.[2] Steering corporations or markets in the right direction, however, is a particularly testing endeavor due to the different set of mechanisms and interests that are at stake when dealing with these actors. For instance, risk regulation,[3] supply chains,[4] reporting mechanisms,[5] and commercial interests

[*] Els De Busser is Assistant Professor of Cyber Security Governance at the Institute of Security and Global Affairs, Leiden University, email: e.de.busser@fgga.leidenuniv.nl.

[**] Ester Herlin-Karnell is Professor of EU Constitutional Law and Justice and a University Research Chair at the VU University Amsterdam, email:e.herlinkarnell@vu.nl.

[1] *See* Alberto Alemanno & Alessandro Spina, *Nudging Legally: On the Checks and Balances of Behavioral Regulation*, 12 INT'L J. CONST. L., 429–56 (2014) (providing example theories on the use of nudging in administrative law).

[2] *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD., 661–91 (1998).

[3] *See* Peter Mülbert & Ryan Citlau, *The Uncertain Role of Banks' Corporate Governance in Systemic Risk Regulation* (European Corp. Governance Inst., Working Paper NO. 179, 2011), https://ssrn.com/abstract=1885866.

[4] *See* J.M. Denolf et al., *The Role of Governance Structures in Supply Chain Information Sharing*, J. ON CHAIN & NETWORK SCI., 83–99 (2015).

significantly influence the governance of security in relation to corporations and markets. With a particular focus on financial crimes as the connection between security on the one hand and the EU internal market on the other hand, this special issue zooms in on new security governance concerns in this context. An additional hurdle is posed by the double role that corporations can play in investigations into financial crimes. Companies can find themselves on both sides of such investigations: As a data supplier on the one hand and as a potential liable actor on the other hand. Also, this dichotomy and its effect on EU security governance is thoroughly examined by the authors contributing to this special issue.

B. The Questions Covered

The EU is a prominent actor regarding both security governance within the policy area of AFSJ and financial crimes regulation. The EU is particularly interested in financial crime regulation, as it has the ambition of achieving an honest market place as well as protecting the EU budget against irregularities. Security regulation in this internal context is connected to the EU's promise of establishing an area of freedom, security, and justice. Against the backdrop of the wider governance issues with the EU as a supranational organization and the sensitive question of security governance, which is to a large extent a national competence when it concerns the Member States' own security (Article 4 TEU), this special issue sets out to zoom in on a number of pertinent questions. Throughout the papers, four groups of questions can be distinguished.

First, the AFSJ is in itself a broadly defined area of law dealing with inter alia security issues, criminal law, border control, migration, and civil law cooperation. Furthermore, many of the AFSJ policies have a clear internal market dimension. Therefore, the juncture of these policy areas can be difficult to clearly define and different EU measures are often enacted in both policy areas regulating the same questions. The special issue focuses on the interrelation of the AFSJ and the EU internal market by exploring questions such as the EU fight against terrorism financing, money laundering, and trafficking, which have both a market focus and a security rationale. The Financial Action Task Force (FATF) and its '40 Recommendations on Money Laundering' is a particularly significant actor in the global war against money laundering and an important trendsetter for the EU in these matters. The main justification for extended EU powers in the area of anti-money laundering has been the need to update EU law in light of the FATF and norms set by the UN Security Council for fighting terrorism worldwide. Questions that are covered by the authors refer to the EU's legislative approach in general but also to the EU's legislative approach to specific crimes.

[5] For example, the recently adopted (fifth) anti-money laundering directive: Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, 2018 O.J. (L 156).

The question on the reach of EU legislative competence can be described as cross-cutting through our main focus of EU security governance and the internal market. Several authors touch upon this—for the EU institutions and for the member states—sensitive subject of marrying the protection of national sovereignty with the need for supranational legislation and cooperation. Due to this search for legislative competence and the complexity of financial crimes, authors have looked into other jurisdictions—especially the US—as well as into other disciplines, to rely on lessons learned for the efficient development of EU legislation and practice.

Second, the special issue looks at what happens in the digital sphere and how data protection can be upheld when the EU sets out to ensure a high level of security. The security aspect and the question of the EU's jurisdiction to rule on questions partially or wholly outside the EU territory are also highlighted by the high profile cases in the Court of Justice of the EU concerning the transfer of data to the US.[6] We emphasize the role of data and privacy in the area of transnational crimes with financial aspects and financial crimes. Gathering information to be used as evidence in criminal proceedings for these crimes means obtaining personal data within the EU and outside the EU that may be protected by the right to a private life but also by the right to data protection. Recent momentous cases include the Digital Rights case[7] and the aforementioned Schrems cases. The contributing authors therefore explore the scope of regulation on cross-border digital evidence and go as far as rethinking the concept of data collection by drawing inspiration from other scientific disciplines.

Third, EU practices when fighting financial crimes and related activities are discussed. Financial crimes are those crimes that have the illicit gain of money or property as the main goal but can still cover a range of different offenses, including money laundering, terrorism financing, fraud, and even market abuse and trafficking in human beings.[8] The crime of terrorism, and related activity, is an offense that can have many forms and therefore always lacked a uniform international definition.[9] Financing can be needed to

---

[6] *See* Case C-317/04 Parliament v. Council, 2005 E.C.R. I-02457; Case C-318/04, Parliament v. Council, 2005 E.C.R. I-02467; and Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650; *see also* Data Prot. Comm'r v. Facebook Ireland Ltd. & Schrems, [2018] NO. 4809 P. (H. Ct.) (Ir.) (discussing the most recent referral of the follow-up Schrems II case by the Irish High Court to the CJEU and the appeal against this referral); Data Prot. Comm'r v. Facebook Ireland Ltd & Schrems, 2018 NO. 2018/68 (SC) (Ir.).

[7] *See* Case C-293/12 Dig. Rights Ir. et al. v. Minister for Commc'n, Marine & Nat. Res., ECLI:EU:C:2014:238.

[8] For the definition offered by the Financial Conduct Authority, see FINANCIAL CONDUCT AUTHORITY, FINANCIAL SERVICES AUTHORITY HANDBOOK (2001), https://www.handbook.fca.org.uk/handbook/glossary /G416.html.

[9] The EU has a more concrete attempted definition, Directive 2017/541 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. *See e.g.*, MYRIAM FEINBERG, SOVEREIGNTY IN THE AGE OF GLOBAL TERRORISM (2016); Sara Poli, *The EU External Anti-Terrorism Policy in Its External AFSJ Policy, in* THE EUROPEAN UNION AS AN AREA OF FREEDOM, SECURITY AND JUST. 389, 389–416 (Maria Fletcher, Ester Herlin-Karnell & Claudio Matera eds. 2016); CIAN MURPHY, EU COUNTER-TERRORISM LAW: PRE-EMPTION AND THE

carry out attacks. Trafficking in human beings is an offense that is mostly committed for financial gain, a form of modern slavery. The laundering of these proceeds, as well as the trafficking of human beings in the global supply chain, shows financial elements that need specific attention. The EU has, of course, relevant legislation in place, inter alia, with the New Counter Terrorism Directive, the establishment of a European Public Prosecutor Office,[10] and the Fifth Money Laundering Directive[11] being recent examples of EU measures in this area. In addition, the EU also has a Directive against the trafficking of human beings in place.[12] Questions covered by the authors include the legitimacy of a prosecution service on EU level and the limits of criminal, administrative, and civil liability for corporate crime.

Fourth, the focus on EU security governance and internal market generates a twofold perspective on the role that companies play. Companies are at the receiving end of a massive amount of data—personal and non-personal—handed over to them by consumers while conducting daily activities, such as communicating, purchasing items, or surfing the internet. This data—in digital form or otherwise—can be vital for the companies in developing advertising approaches, pricing strategies, and offering personalized services to customers. As a consequence, companies are also at the supplying end of this data because specific information could reveal criminal activity by their customers and require further analysis by law enforcement authorities. That is when companies become important actors in criminal investigations, especially into financial crimes. The papers by Els De Busser and Anne de Hingh zoom in on the specific aspects of regulating companies delivering raw data or suspicious activity reports to law enforcement authorities for the purpose of criminal investigations, in particular, investigations into financial crimes. The papers also explore the dynamic area of data protection. When companies themselves are suspects of criminal offenses, their role in the investigation obviously changes. The regulatory approach to corporate liability, prosecuting, and sentencing of companies for financial crimes and even for trafficking in human beings, provoke questions in to the European-wide prosecution of fraud against the EU budget by the European Public Prosecutor's Office and the legitimacy thereof, the EU's approach to criminal liability and corporate sentencing, as well as the potential for applying reflexive law to human trafficking in global supply chains. Maria O'Neill, Carlos Gómez-Jara Díez, Ester Herlin-

---

RULE OF LAW (2012); MARIA O'NEIL, THE EVOLVING EU COUNTER-TERRORISM LEGAL FRAMEWORK (2011); and CHRISTINA ECKES, EU COUNTER-TERRORIST POLICIES AND FUNDAMENTAL RIGHTS (2009).

[10] Council Regulation 2017/1939 of 12 October 2017, Implementing Enhanced Cooperation on the Establishment of the European Public Prosecutor's Office, 2017 O.J. (L 283).

[11] Case C-293/12 Dig. Rights Ir. et al. v. Minister for Commc'n, Marine & Nat. Res., ECLI:EU:C:2014:238.

[12] Directive 2011/36, of the European Parliament and of the Council of 5 April 2011 on Preventing and Combating Trafficking in Human Beings and Protecting Its Victims, and Replacing Council Framework Decision 2002/629/JHA; Directive 2017/541, on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

Karnell, and Vanessa Franssen study these and other questions in their respective papers. Maria Bergström and Nicholas Ryder discuss the connection between the anti-money laundering framework and that of counter terrorism financing and the involvement and dangers of private actors, such as banks, in the monitoring process and the outsourcing of responsibility.

C. Outline of the Special Issue

In the first part of this special issue the focus is turned to the analysis of specific crimes that can be labeled as financial crimes. Money laundering, financing of terrorism, and trafficking in human beings in global supply chains all have strong relations to corporations and markets. At the same time, they all fall under the wider definition of financial crimes. By starting with a study of these particular crimes, the special issue aims to highlight a number of concerns that should be considered when developing new regulation in the field without losing sight of relevant human rights questions.

We will start with Teubner's ideas on a reflexive law approach to steering behavior in the right direction, as it is applied in **Maria *O'*Neill's** paper. She provides a transnational law perspective on combatting trafficking in human beings in global supply chains and specifically the laundering of proceeds of human trafficking.[13] Using these two key points of intersection between the commercial and the criminal world, she explores the use of reflexive law in the UK's Modern Slavery Act 2015 and in anti-money laundering regimes. The paper concludes that reflexive law shows promise particularly in extending the reach of the command and control state into the areas where the transnational criminal world bisects the transnational commercial/banking world. This raises a number of human rights issues.

In just over thirty years, a global Anti Money Laundering (AML) regime has developed that is constantly being updated and expanded, not only geographically, but most importantly in both width and depth. Today, it affects a large part of modern society, including both private and public actors, and is key in a steadily growing number of interconnected areas. In her Paper, **Maria Bergström** provides an overview of the variety of purposes and interests involved in the global and EU regional AML regimes, while at the same time pointing out some of the most pressing legal concerns in AML regulation. These concerns include blurred accountability in the cooperation between public and private actors, the protection of individual rights and fundamental freedoms in administrative and criminal law contexts, data retention and privacy, as well as decreasing state sovereignty. Also, in the context of anti-money laundering, but with a focus on the countering of financing of terrorism, **Nicholas Ryder** introduces a critical analysis of the appropriateness and

[13] *See e.g.*, Gunther Teubner, *Substantive and Reflexive Elements in Modern Law*, *in* THE LAW AND SOCIETY CANON 75, 75–122 (Carroll Seron, ed., 2006).

effectiveness of the so-called "profit" reporting model towards the financing of terrorism by focusing on the UK and the US in particular. By assessing the policy of the UN, FATF, and the EU in using reporting mechanisms for the prevention and investigation of money laundering, the article concludes that this approach is not successful in preventing and investigating the financing of terrorism. As he explains, balancing the low cost of terrorist attacks with the variety of financial tools significantly raises the difficulty in combatting terrorism financing. The paper draws lessons from the US's war on terror before concluding on the effectiveness of both the EU and the UK counter-terrorism strategies, including these reporting mechanisms.

Subsequently, the focus shifts to investigation and prosecution of financial crimes with one of the most contested EU criminal law measures in recent years, the idea of the creation of a European Public Prosecutor Office (EPPO). **Carlos Gómez-Jara Díez** and **Ester Herlin-Karnell** discuss the establishment of the EPPO as a federal agent and the effects of this agent for establishing a robust EU financial crimes regime. Comparisons with the US system of US Attorneys (federal prosecutors) are drawn to show that this institution has been quite effective at enhancing the protection of the US financial market. Additionally, attention is paid to the federalization taking place at the European level through the enhanced powers of, for example, the European Securities and Markets Authority (ESMA).

Financial crime is very often, though not exclusively, committed in a business setting. **Vanessa Franssen** argues that the current EU approach to corporate financial crime does not sufficiently take into account the specific features of both criminal liability and corporate entities, as opposed to individuals, nor does it fully exploit the potential strengths of a criminal law approach. Instead of assimilating criminal liability to administrative or civil liability, the EU should more carefully consider the different objectives of those different enforcement mechanisms. Moreover, when it comes to corporate sentencing, the EU lacks ambition and creativity. Ultimately, this may undermine the effectiveness of the EU's fight against corporate financial crime.

In the final part of this special issue, we explore the role of data exchange and privacy, especially with companies being the supplier of data for the purpose of criminal investigations into financial crime. Joining the particular nature of digital data—often disconnected from a state's territory and jurisdiction—with cross-border criminal investigations and the involvement of companies, **Els De Busser** argues for the necessity of exchange mechanisms that operate fast enough to be functional for the purpose of cross-border criminal investigations but also respect the sovereignty of the states involved. **Anne de Hingh** continues on the legal aspects of the commercial use of personal data as part of online business models. By viewing personal data as a commodity, she demonstrates that the phenomenon of commercial entities transforming aspects of our being and everyday lives into merchandise is more than a privacy challenge alone. She examines the feasibility of an alternative route, i.e. human dignity. An analogy with bio-medical regulations on the

prohibition of the trade of human body parts is explored to see whether the non-commercialization principle in these laws is applicable to commercial big data practices.

D. Acknowledgments

As guest editors of this special issue on EU Security Governance, Market Regulation, and Transnational Crime, we would like to express our profound gratitude to the editors-in-chief, editors, and student editors of the German Law Journal for hosting this special issue and for their warm support in the finalization of the contributions. The selected papers were originally presented at the VU Centre for European Legal Studies and ACCESS Europe Amsterdam workshop held on October 21, 2016, at the VU University Amsterdam. We are most grateful to the authors who co-created this special issue with us for assisting us in publishing the results of their thought-provoking scholarly reflections.

Articles

International Business Encounters Organized Crime: The Case of Trafficking in Human Beings

By Maria O'Neill[*]

Abstract

With increasing globalization, transnational crime in general, and human trafficking in particular, a design of new legal framework is required in order to effectively operationalize interstate law enforcement operations and prosecutions. The development of a transnational criminal legal framework—or frameworks—can build on pre-existing transnational economic frameworks. There is also the need to extend the application of domestic law beyond national borders to influence transnational corporate behavior. Regulations based on reflexive law are one possible approach. Teubner's idea of reflexive law has been informing developments in this area. This approach uses traditional national law to inform corporate governance strategies in order to achieve effects on the market. A few jurisdictions have already adopted measures modeled on this approach to tackle human trafficking and slavery-like conditions in global supply chains. Weaknesses in the approaches adopted by the UK and the State of California have already been identified. If strengthened, this approach could be adopted in more jurisdictions—including the EU—and also to combat more areas of transnational crime—such as money laundering. This paper will examine the resulting challenges using human trafficking as a case study.

[*] Senior Lecturer in Law, University of Abertay.

A. Introduction

Trafficking of Human Beings (THB) is a core business of international criminal organizations. It is seen as a relatively low-risk/high-reward crime. At a global level, human trafficking is prohibited by the *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children*, supplementing the *United Nations Convention against Transnational Organized Crime* published in 2000,[1] and more recently by *EU Directive 2011/36/EU*,[2] for the EU member states. THB does not involve "voluntary" prostitution—as understood by the law enforcement community—and can arise in circumstances similar to, but as a crime, is separate from traditional slavery, human smuggling, or poor working conditions. It builds on pre-existing and pre-defined crimes of slavery, servitude, forced labor, and compulsory labor. In the context of this paper it also involves the production of products—more so goods, rather than services—for global supply chains using harsh and degrading working conditions—including bonded labor. Transnational corporations are responsible for the procurement, manufacturing, and delivery of a very large percentage of the commodities in our domestic markets. While national laws address criminal law and labor conditions within our own jurisdictions, they have little effect in governing behavior outside their relevant jurisdiction.

With increasing globalization, the issue of "the application of domestic law to international actors" arises.[3] In the case of both transnational criminal law and transnational commercial law "the power of command-and-control regulation largely stops at the border."[4] The international business world bisects the world of cross border criminal law in a number of key areas. This paper will examine the resulting theoretical challenges using human trafficking as a case study. Two key points of intersection between the commercial and criminal world are: Human trafficking—and related slavery conditions—in global supply chains, now addressed in a number of jurisdictions, including the UK; and combating the laundering of proceeds of human trafficking, which is currently a global effort. The focus of this paper will be on the efforts of EU states to combat these two issues, and the need for EU measures to have extraterritorial effect, given the nature of global supply chains. Measures to combat money laundering through the financial and banking sector generally are more developed than the more recently recognized phenomenon of human trafficking

[1] *See* Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime, *opened for signature* Nov. 15, 2000, 2225 U.N.T.S. 209.

[2] *See* Directive 2011/36, of the European Parliament and of the Council of 5 April 2011 on Preventing and Combating Trafficking in Human Beings and Protecting its Victims, and Replacing Council Framework Decision 2002/629/JHA, 2011 O.J. (L 101) 1 (EU) [hereinafter Council Directive 2011/36].

[3] Bradley Girard, *Corporate Transparency Through the SEC as an Antidote to Substandard Working Conditions in the Global Supply Chain*, 21 GEO. J. ON POVERTY L. & POL'Y 317, 321 (2014).

[4] *Id.* at 322.

in global supply chains. While measures taken to combat money laundering could be further developed, those measures already taken to date are likely to inform how human trafficking and slavery like conditions can be tackled in global supply chains.

Reflexive law is an attempt by jurisdictions to make transnational businesses link to those jurisdictions in order to structure and manage their transnational businesses in a way that complies with the laws and norms of the legislating jurisdiction. The design of UK law in its response to its requirement to implement Directive 2011/36/EU,[5] reflecting the idea of Teubner's reflexive law, to address both human trafficking in global supply chains, allied to a similar response being adopted by anti-money laundering regimes, would together provide additional mechanisms, if adopted more widely, —working with the global business and banking communities, —to combat this form of organized crime. Reflexive law shows promise, particularly in extending the reach of the command and control state into the areas where the transnational criminal world bisects the transnational commercial and banking world. Reflexive law has been adopted in a number of measures, which will be discussed below. Concrete evidence of reflexive law's effectiveness still needs to be measured, and it is arguable that those measures already adopted will need to be made more robust in order to ensure that effectiveness. This paper will critically analyze the potential for adopting and further developing reflexive law mechanisms to combat the transnational crime of human trafficking, and its connection to anti-money laundering issues.

Human trafficking—while it can occur within one state—is more often encountered across a number of jurisdictions, these being countries of origin, transit, and destination. The same can be said about corporate global supply chains. An individual jurisdiction's laws, or those of the EU, will not address—either directly or indirectly—behaviors or crimes that occur in third states. There is a need to develop extraterritorial effect for state or EU laws. As stated by Girard, "the power of command-and-control regulation largely stops at the border."[6] Corporations, or financial systems which are based, or operate, in European or EU jurisdictions, are required to meet the laws of the jurisdictions in which they are based or operate. Reflexive law is an imperfect tool, but it is currently being adopted by both the UK and the EU in order to gain some extraterritorial effect for their internal standards and laws—particularly where transnational crime concerns bisect the realm of private commercial operators.

This paper will start with an examination of reflexive law, building on Teubner's original concept. It will then go on to examine the relevance of reflexive law to the challenges of human trafficking in global supply chains. Three pieces of legislation from three different jurisdictions, the EU, the US State of California, and the UK are examined here. The EU's

[5] *See* Modern Slavery Act 2015, c. 30, § 54 (Eng.).

[6] Girard, *supra* note 3, at 322.

Directive 2014/95/EU on the disclosure of non-financial and diversity information[7] comes close to but does not expressly cover the issue of human trafficking in global supply chains. Its approach—modeled on reflexive law—is very similar to those adopted by the UK in Section 54 of the Modern Slavery Act 2015. The UK's approach to human trafficking in global supply chains has also been heavily influenced by the State of California's Transparency in the Supply Chains Act of 2010,[8] with California having been a first mover on this issue. Much can be learned, not only from earlier adopters of provisions modeled on reflexive law in global supply chains, but also from evaluation of the adoption of laws modeled on reflexive law in other areas of practice such as social and environmental law. With some jurisdictions having adopted a reflexive law approach to tackling human trafficking and slavery in global supply chains—and the possibility of this approach being adopted in further jurisdictions—there is then the issue of making the reflexive law approach to regulation actually work. This issue is examined later on in the article and is followed by an examination of trafficking as a test case for reflexive law.

B. Reflexive Law

Teubner's concept of reflexive law is a development of earlier responsive law theories. It relies on the "fusion of public and private governance regimes."[9] The underlying premise is that law is supposed to "provide congruent generalizations of the expectations for the whole of society."[10] In addition to the traditional "'vertical' subordination of citizens to their sovereigns," there is a need for "'horizontal' relations between equally situated market actors"[11] in public-private governance regimes. These horizontal relations become relevant in the context of globalization.

Reflexive law recognizes "the limits of regulatory law"[12]—limits, which we recognize in the context of globalization. Reflexive law originates "from a social theoretical perspective

[7] *See* Directive 2014/95, of the European Parliament and of the Council of 22 October 2014 Amending Directive 2013/34/EU as Regards Disclosure of Non-financial and Diversity Information by Certain Large Undertakings and Groups, 2014 O.J. (L 330) 1 (EU) [hereinafter Council Directive 2014/95].

[8] *See* Transparency in the Supply Chains Act, CAL. CIV. CODE § 1743.43 (2012) [hereinafter Californian Act].

[9] Agnieszka Janczuk-Gorywoda, *Public-Private Hybrid Governance for Electronic Payments in the European Union*, 13 GERMAN L.J. 1438, 1439 (2012).

[10] Gunther Teubner, *Substantive and Reflexive Elements in Modern Law*, 17 L. & SOC'Y REV. 239, 273 (1983).

[11] Daniela Caruso, *Private Law and State-Making in the Age of Globalization*, 39 N.Y.U. J. INT'L L. & POL 2, 3 (2002).

[12] Olivier De Schutter & Simon Deakin, *Reflexive Governance and the Dilemmas of Social Regulation, General Introduction*, *in* SOCIAL RIGHTS AND MARKET FORCES; IS THE OPEN COORDINATION OF EMPLOYMENT AND SOCIAL POLICIES THE FUTURE OF SOCIAL EUROPE?, 7 (Olivier De Schutter & Simon Deakin eds., 2005).

rather than a strictly legal one,"[13] recognizing the "complexity of social life and the diversity of the many institutions created to achieve various ends," and aims "to guide rather than to suppress" that complexity.[14] Given the levels of complexity that are to be regulated by reflexive law, legislators need to constantly reflect on its effect and adjust accordingly: Having created a "disclosure based system" traditional enforcement is then reserved as a back-up to that system.[15]

In designing "horizontal" relations, which can extend outside the territorial boundary of the state, reflexive law "seeks to design self-regulating social systems through norms of organization and procedure."[16] In this way "semi-autonomous social systems" are not only reshaped, but so also are their "methods of coordination with other social systems."[17] This type of law therefore is "characterized by particularism, result-orientation, an instrumentalist social policy approach, and the increasing legalization of formerly autonomous social processes."[18] As Teubner has said, "reflexive rationality in law obeys a logic of procedural legitimation,"[19] thereby having "institutional legal characteristics quite different from its substantive counterpart."[20]

The drive to develop the concept of reflexive law arose from the understanding that "judicial control and state regulation of associated behavior seem to [have reached] the limits of their control capacity."[21] This is particularly true in the context of globalization—in both transnational economic law and effectively addressing transnational security—and law enforcement threats. The strategy is to have large, multi-national companies and global supply chains "substitute for outside interventionist control," something which is highly problematic in the transnational sphere, for the development of "effective internal control structure[s]."[22] This would be regulated when the large multi-national company—or key parts of the global supply chain—bisect one or more key state jurisdictions, those jurisdictions being sites of reflexive law regulation. As stated by Shaffer, "in a globalized

---

[13] Eric W. Orts, *A Reflexive Model of Environmental Regulation*, 5 BUS. ETHICS Q.779, 780 (1995).

[14] *Id.* at 780.

[15] *Id.* at 787.

[16] Teubner, *supra* note 10, at 254–55.

[17] *Id.* at 255.

[18] *Id.* at 267.

[19] *Id.* at 270.

[20] *Id.* at 256.

[21] *Id.* at 278.

[22] *Id.*

world, much of law is subject to transnational influences and pressures, but more powerful states are the primary exporters of legal norms."[23] The larger economies of the US, the EU, and the UK would be key players in influencing global commercial entities. In this way most—if not all—of the large multi-national companies or global supply chains would become subject to the provisions of reflexive law regulation, thereby either facilitating better transnational commercial effectiveness—something that is of direct interest to the commercial world—while effectively contributing to the minimization of global security and law enforcement threats. This should also be of interest to responsible business.

Therefore—as stated by Teubner—"law's role is to decide about decisions, regulate regulations, and establish structural premises for future decisions, in terms of organization, procedure and competencies."[24] Law's role in one subsystem should have specific outcomes in other related or parallel subsystems. Law therefore "attempts to balance bargaining power, but this only indirectly controls specific results,"[25] and has been shown by different researchers to have had variable success in different areas of business and law.[26] Of relevance to this point is who has or should have the necessary bargaining power. The effectiveness of reflexive law measures also need to be subjected to "strong empirical testing" before they can be claimed to be truly effective. As Teubner himself points out, "the 'fallacy of misplaced concreteness' is almost inevitable."[27]

C. The Relevance of Reflexive Law to Human Trafficking in Global Supply Chains

Globalization is not just affecting the economic sphere of activities. As is becoming obvious to more and more people in their ordinary lives, globalization is also bringing with it new security threats. There is a need to develop a transnational criminal law framework to address issues that range from worldwide cyber threats to international terrorism movements. One particular crime that needs a transnational approach is THB, which was one of the earliest crimes that the EU addressed, in 1997.[28] The vast majority of THB cases are connected with organized crime, as by the nature of movement, control, and exploitation of individuals requires a number of people to be involved. This is evidenced by the fact that the UN Protocol to Prevent, Suppress and Punish Trafficking in Persons,

[23] Gregory Shaffer, *Transnational Legal Process and State Change*, 37 L. & SOC. INQUIRY 229, 231 (2011).

[24] Teubner, *supra* note 10, at 275.

[25] *Id.* at 276.

[26] *Id*.

[27] *Id*.

[28] *See* Joint Action 97/154, of 24 February 1997 Adopted by the Council on the Basis of Article K.3 of the Treaty on European Union Concerning Action to Combat Trafficking in Human Beings and Sexual Exploitation of Children, 1997 O.J. (L 63) 2 (EU).

Especially Women and Children is attached to the UN Convention on Transnational Organized Crime 2000. The predominant motivational factor for THB is money. This poses a challenge for both law enforcement and financial services generally. The challenges arising from the crime of THB are multifaceted. An area for development—and the focus of this paper—could be on those issues which are of relevance to law enforcement, but are more closely related to the commercial world. This paper addresses the potential for development of this transnational commercial-crime nexus, using one of the tools used by transnational economic law to date, reflexive law.

The line of reasoning that reflects the idea of reflexive law has recently been adopted to address the issue of THB in global supply chains. In an effort to address the behavior of business operating global supply chains—and reflecting the limitations of the command and control approach of domestic jurisdictions—a new way of conceptualizing law needs to be developed. Both international trade and transnational crime bridge jurisdictions. There is a need to develop legal frameworks which occupy the space between national jurisdictions, and which addresses issues which arise when there are gaps or weaknesses in one of the interconnected jurisdictions relevant to both criminal and commercial global supply chains. One way would be to develop inter-jurisdictional legal frameworks under the umbrella of the UN Convention on Transnational Crime 2000. Another is to develop the extraterritorial effect of domestic jurisdictions. One of the tools being used by domestic jurisdictions is to enact provisions to require international business—with a substantial connection with that jurisdiction—to manage their businesses in ways which meet the laws and norms of that particular jurisdiction. These are therefore laws which require internal corporate processes to be implemented as part of the company's corporate governance framework.

While provisions based on reflexive law have yet to be adopted by the EU to directly address THB—or security provisions in general—the approach is not unknown to the EU. The reflexive law approach has already been adopted within the EU legal framework, and it is the argument of this paper that the EU would benefit from provisions similar to those adopted by the US State of California, or those in the UK, to combat trafficking in human beings in global supply chains. Similar provisions have already been written into the EU legal framework through Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards to disclosure of non-financial and diversity information by certain large undertakings and groups.[29] Directive 2014/95/EU applies to "[l]arge undertakings which are public-interest entities exceeding on their balance sheet dates the criterion of the average number of 500 employees during the financial

[29] *See* Directive 2013/34, of the European Parliament and of the Council of 26 June 2013 on the Annual Financial Statements, Consolidated Financial Statements and Related Reports of Certain Types of Undertakings, Amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC, 2013 O.J. (L 182) 19 (EU) [hereinafter Council Directive 2013/34].

year."[30] Directive 2013/34/EU[31] defines public-interest entities as "companies governed by the laws of a member state," and are so designated by member states as having "significant public relevance because of the nature of their business, their size or the number of their employees."[32] The obligation is to make a non-financial statement. This statement needs to cover "the extent necessary for an understanding of the undertaking's development, performance, position and impact of its activity, relating to as a minimum environmental, social and employee matters, respect for human rights, anti-corruption and bribery matters."[33]

Packaged as part of corporate social responsibility, rather than as an effort to combat—*inter alia*—human trafficking, this EU provision was enacted in order to facilitate the "disclosure of non-financial information" in order to assist in "the measuring, monitoring and managing of undertakings' performance and their impact on society,"[34] with an eye specifically on social, to include corruption, and environmental issues. The intention behind the reporting mechanism—and its audit—is to require businesses to seriously take into consideration set EU and national environmental and social objectives. In giving proper consideration to these objectives, businesses are expected to modify their decision-making processes, thereby reorienting the entirety of their operations in order that the business aims to achieve outcomes which are more in line with objectives set in other EU laws and policy documents. The resulting fusion of public law—the directive—with an anticipated refocusing of internal corporate governance strategies, should lead to a change of behavior of a large number of the dominant players on the market. This should then have a knock-on effect of changing the market as a whole, with many larger companies requiring their suppliers to operate to the same high standards, in order to maintain transnational supply chain integrity.

Directive 2014/95/EU was to be implemented in EU member states by December 06, 2016, with a view to applying to financial years either starting on January 01, 2017, or during the 2017 calendar year, depending on business practice in the EU. The effectiveness of these provisions modeled on reflexive law therefore still have to be evaluated. A weakness in this provision—in the context of this paper—is that it does not expressly address the issue of THB, something which has been addressed in other jurisdictions, initially in the US State of California, and more recently in the UK. In addition, there is no corresponding provision elsewhere in the EU Area of Freedom Security and Justice legal framework. Little amendment would be required of Directive 2014/95/EU in order to address the issue of THB.

---

[30] Council Directive 2014/95, *supra* note 7, at art. 1.

[31] Council Directive 2013/34, *supra* note 29.

[32] *Id.* at art. 2.

[33] Council Directive 2014/95, *supra* note 7, at art.1 (inserting a new art. 19(a) to Directive 2013/34).

[34] *Id.* at para. 3.

Nevertheless, any such amendment might be informed by the drafting of both the Californian and UK provisions, and post-enactment evaluation of effectiveness. In addition, a reflexive law approach to tackling money laundering within the EU legal framework would also be useful. The EU's approach to legislative drafting in Directive 2014/95/EU already has some similarity with the UK provision on human trafficking in global supply chains, as pointed out in the UK Home Office guide to Transparency in Supply Chains.[35]

The lead jurisdiction on tackling human trafficking in global supply chains is the US State of California. There, the crime of human trafficking at the US federal level is addressed by the Victims of Trafficking and Violence Protection Act of 2000, as amended, which, *inter alia*, amended the U.S. Code to cover this crime.[36] This is supplemented by the State of California through the Transparency in Supply Chains Act 2010—the Californian Act—which came into effect in 2012.[37] The Californian Act required every retail seller and manufacturer doing business in this state—as defined by Californian tax law—and with annual worldwide gross receipts exceeding US $100 million to meet certain disclosure requirements.[38] These disclosure requirements are for the purposes of informing, at a minimum, other businesses, the authorities, and consumers the extent that the "retail seller or manufacturer" verifies the integrity of its supply chain to be free from human trafficking and slavery, and conducts audits of suppliers, with the requirement to state if the "verification was not an independent, unannounced audit."[39] In addition, all materials from suppliers incorporated into their own products must be similarly certified.[40] Further, internal corporate governance structures must include "internal accountability standards and procedures for employees or contractors failing to meet company standards regarding slavery and trafficking."[41] In addition, employees, and management responsible for ensuring that supply chains do not include products of human trafficking or slavery, must be given appropriate training.[42]

The focus of the Californian Act is on disclosure and informing the consumer and other interested parties. The intention is that greater transparency will lead to peer and public pressure to adjust behavior. There is no requirement in the Californian Act to actually adjust

---

[35] *See* HOME OFFICE, TRANSPARENCY IN SUPPLY CHAINS: A PRACTICAL GUIDE, 2015, at 26 (Eng.).

[36] *See generally* 22 U.S.C. § 7101 (2018*), e.g.* inserting, *inter alia*, new arts. 1589–1591.

[37] ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE, LEVERAGING ANTI-MONEY LAUNDERING REGIMES TO COMBAT TRAFFICKING IN HUMAN BEINGS 26 (2014).

[38] Californian Act at § 3.

[39] *Id.* at §§ 3(a)(1) & 2.

[40] *See id.* at § 3(3).

[41] *Id.* at § 3(a)(4).

[42] *See id.* at § 3(a)(5).

corporate behavior to ensure that the supply chain is actually free of products produced by human trafficking or slavery victims. Nonetheless, the reflexive law element would arise for companies which do wish to comply with the higher standards and want to be seen to be delivering human trafficking and slavery free products to the market. At the time of the enactment of the Californian Act it was "expected to apply to approximately 3,200 global companies."[43] It introduced novel features, which have been built on by the UK in its Modern Slavery Act 2015.

While the Modern Slavery Act 2015 is primarily focused on the jurisdiction of England and Wales, its transparency in supply chains provisions,[44] with regard to slavery and human trafficking, applies to the whole of the UK. Whether the UK global supply chains provisions are or will be effective in achieving their stated objectives is a matter that requires further examination. Section 54 applies to commercial organizations which supply goods or services and have a total turnover[45] as specified by regulation made by the Secretary of State, currently at STG £36 million.[46]

Neither the above-mentioned UK, nor the EU initiatives in the area of human rights reporting by businesses operate in a vacuum, with both the UN[47] and the Organization for Economic Cooperation and Development (OECD)[48] having similar provisions in their relevant policy documents. Human trafficking is addressed by three different pieces of legislation in the UK, reflecting the fact that this issue is predominantly a matter for the devolved governments in both Scotland and Northern Ireland. The England and Wales legislation—the Modern Slavery Act 2015[49]—provides for two distinct crimes: Section 1 offense of "slavery, servitude and forced or compulsory labour," which arguably in itself could be viewed as four different but overlapping crimes, and the Section 2 offense of "human trafficking." The Scottish and Northern Irish legislations[50] take a similar approach. The breadth of definitions used would

[43] Jonathan Todres, *The Private Sector's Pivotal Role in Combating Human Trafficking*, 3 CAL. L. REV. CIR. 80, 81 (2012).

[44] Modern Slavery Act 2015, § 54 (which came into force on October 29, 2015, pursuant to the Modern Slavery Act 2015 (Commencement No. 3 and Transitional Provision) Regulations 2015, SI 2015/1816 (Eng.)).

[45] *See* Modern Slavery Act 2015 at § 54(3).

[46] Modern Slavery Act 2015 (Transparency in Supply Chains) Regulations 2015, SI 2015/1833, § 2 (Eng.).

[47] *See* UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights Implementing the United Nations "Protect, Respect and Remedy" Framework (2011).

[48] *See* ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES FOR MULTINATIONAL ENTERPRISES RESPONSIBLE BUSINESS CONDUCT MATTERS (2014).

[49] A number of provisions of the Modern Slavery Act 2015 apply to the whole of the UK, to include the Section 54 provision on human trafficking in global supply chains. *See* Modern Slavery Act 2015 at § 54.

[50] *See generally* Human Trafficking and Exploitation (Scotland) Act 2015, (ASP 12); *see also* The Human Trafficking and Exploitation (Criminal Justice and Support for Victims) Act (Northern Ireland) 2015 c. 2.

cover abusive situations that would not fall within the definitions of human trafficking used in UN, Council of Europe, or EU texts. This difference in approach may have an effect on addressing this type of exploitation in an otherwise legitimate businesses global supply chain.

Another point where ostensibly legitimate business bisects THB, is in the context of money laundering of criminal proceeds. At least some of the funds associated with THB are being handled by reputable financial and business entities in Western Europe.[51] Financial institutions and money transfer services have been key in all THB case studies published to date in "moving the proceeds and instrumentalities of THB." The Organization for Security Cooperation in Europe (OSCE) has advocated the full leverage of "the private sector's access to the financial transactions of criminals," in order for countries to be more effective in tackling this crime.[52] There is, therefore, scope for the further development of reflexive law mechanisms in this area.

There have been, at least to date, a very low number of Suspicious Activity Reports (SARs) identifying either human trafficking or its related crime, human smuggling.[53] As the OSCE has stated, while THB is "in many respects a unique crime," its associated money laundering processes are "identical to those used for other types of crime."[54] This has been echoed in the Financial Action Task Force (FATF) report on the topic,[55] which points out that "there is no specific guidance on money laundering associated with THB[/ smuggling of migrants]," as "the instruments and the sectors implied are the same as for other criminal activities." The OSCE has pointed out that THB related financial transactions have often been carried out through money or value transfer services—in particular money transmitters and cash couriers—which face little supervision and monitoring in most countries.[56] For example, Guzman, reporting on a US/Canadian case, pointed out the use of prepaid cards to move funds across borders.[57] The traditional banking system has also been used effectively to move traffickers' monies. Harnessing the financial—and related sectors—abilities and

[51] LEVERAGING ANTI-MONEY LAUNDERING REGIMES, *supra* note 37, at 14.

[52] *Id.* at 9.

[53] Susan Grossey, *I am not a number, I am a free man*, MONEY LAUNDERING BULLETIN 15 (Sept. 2011), http://www.airant.it/system/files/MLB%20Sept%202011.pdf.

[54] LEVERAGING ANTI-MONEY LAUNDERING REGIMES, *supra* note 37, at 9.

[55] FINANCIAL ACTION TASK FORCE, MONEY LAUNDERING RISKS ARISING FROM TRAFFICKING IN HUMAN BEINGS AND SMUGGLING OF MIGRANTS 63 (2011).

[56] LEVERAGING ANTI-MONEY LAUNDERING REGIMES, *supra* note 37, at 18.

[57] *See* Daniela Guzman, *How Financial Institutions Lead Way in Battle Against Human Trafficking*, INSIGHT CRIME, (May 6, 2014), https://www.insightcrime.org/news/analysis/how-financial-institutions-lead-way-in-battle-against-human-trafficking/.

knowledge of their own business's practices to combat transnational THB would be a step forward.

Reliance is often made on private or commercial actors for security related services, as will be required in the development of reflexive law for transnational law enforcement or security purposes. Reflexive law attempts to address the "application of domestic law to international actors."[58] The approach of reflexive regulation is to set the required objective by way of law—which is mandatory on the legal entities operating within a particular jurisdiction—but leaving to the market operators to "determine the most efficient and effective ways to achieve [the] desired results."[59]

Regulating through reflexive law, therefore, can lead to many forms of state adjustment. For example, the shift of responsibility from the state to, in the commercial world, the market, will in some cases "create . . . new public-private hybrid models of governance."[60] While the security and law enforcement world will be less interested in the state ceding power to the market, nevertheless new—or at least additional—modes of governance will be required in order to effectively tackle transnational threats. In the absence of a global regulatory framework in this area, a number of new strategies will have to be developed. While the state will increasingly be moving from rowing to steering, the combination of "territorially focused as well as deterritorialized normative structures" will be leading to "increasingly complex forms of steering mechanisms."[61] In addition, there may be a need to engage in a paradigmatic shift from the traditional state-centered top-down approach of legislative drafting, and to adopt an approach to regulation, which also allows the development of a bottom-up system. In this way it should be possible to develop "regulatory mechanisms [created using the] cooperative efforts [of] various kinds of actors below the state level,"[62] and which operate in the global economic community. In approaching this issue there is a need to recognize that transnational economic law—as it has developed to date—has been recognized to induce "legal change [and] can have broader systemic effects within states" while "reconfiguring the respective roles of the state, the market, and other forms of social ordering."[63]

D. Making the Reflexive Law Approach Work

[58] Girard, *supra* note 3, at 321.

[59] *Id.* at 338.

[60] Shaffer, *supra* note 23, at 244.

[61] CHRISTIAN TIETJE ET AL., PHILIP C. JESSUP'S *TRANSNATIONAL LAW* REVISITED 28 (Christian Tietje et al. eds., 2006).

[62] *Id.* at 29.

[63] Shaffer, *supra* note 23, at 243–44.

If the ideas underpinning reflexive law are being adopted to tackle human trafficking—and slavery-like practices—in corporate global supply chains, then this approach to lawmaking needs to actually work. As stated by Dorf, "reflexive law is a mechanism by which collective decisions of society as a whole steer other actors and institutions."[64] Reflexive law "is concerned with procedures for multi-participant law-making rather than with the resulting substantive norms."[65] Based on "social science systems theory and autopoiesis theory," reflexive law "refers to learning and exchange of demands, expectations and best practices between social sub-systems."[66] Autopoiesis theory originates from biology, covering "the basic principles of self-reproducing and self-organising systems."[67] Reflexive law theory points out the "need for law to focus on regulation of self-regulation."[68] It needs, therefore, to be "tentative, experimental, and learning"[69] in developing its steering mechanisms, and evaluating their effectiveness, as "certain institutional frameworks facilitate reflexivity, while others discourage it."[70]

Reflexive law requires constant self-critical review of social institutions and their processes.[71] The legal framework is used to establish incentives and procedures which requires institutions to think critically, creatively, and continually about their internal process and methods of operating, with a view to establish their effect on external structures, individuals, and society at large.[72] The complexity of how society—and sub-sets of society—operate precludes the legal framework from directly specifying how internal corporate procedures and processes are to be managed, merely stating that they have to be managed. While reflexive law, it is acknowledged, "cannot and should not replace command-and-control regulation in all domains,"[73] it is argued that modern society and—in

[64] Michael Dorf, *The Domain of Reflexive Law*, 103 COLUM. L. REV. 384, 398 (2003).

[65] Karin Buhmann, *Reflexive Regulation of CSR to Promote Sustainability: Understanding EU Public-Private Regulation on CSR Through the Case of Human Rights*, 8 INT'L & COMP. CORP. L.J. 38, 55 (2010).

[66] *Id.* at 16.

[67] RALF ROGOWSKI, REFLEXIVE LABOR LAW IN THE WORLD SOCIETY, 63 (2013).

[68] *Id.* at 38.

[69] Peer Zumbansen, *Law after the Welfare State: Formalism, Functionalism and the Ironic Turn of Reflexive Law*, 56 AM. J. OF COMP. L. 769, 794 (2008).

[70] De Schutter & Deakin, *supra* note 12, at 4.

[71] Orts, *supra* note 13, at 780.

[72] *See id.*

[73] Dorf, *supra* note 64, at 398.

the context of this paper—the businesses that operate in modern society are "so complex and fractured that command-and-control regulation is bound to fail."[74]

The reflexive law approach can be considered successful if it proves its capacity, in a particular context, "to engender responses of a certain kind within the relevant sub-systems."[75] In order to engender these responses, it may be necessary to use "combinations of 'hard' and 'soft' law in varying degrees."[76] As pointed out by Deakin and McLaughlin, "a reflexive approach does not imply the absence of 'hard law.'"[77] Rather, they say, "the legal framework has a number of roles to play: Inducing efficient disclosure, setting default rules and encouraging bargaining in the shadow of the law."[78] These roles are set for reflexive law through the use of "both public and private law, official and unofficial" allied with "soft and hard norms."[79] Default conditions need therefore to be set, which will "apply in the absence of agreement between social actors,"[80] "legitimating the collective actors concerned," and "mandating disclosure of information needed for meaningful negotiation."[81] The mechanisms, by which this legal framework will operate, need to be "identified, and once identified, must be affirmatively created."[82] As pointed out by Deakin and McLaughlin, there is also a need for "bridging institutions" beyond the legal and enforcement framework "in which effective deliberation and participatory decision-making can occur."[83] In the context of engagement with the corporate world, the "managerialization" of law is also key, whereby in-house corporate lawyers gain leverage over their internal governance structures, and can "use the threat of litigation, with the

[74] *Id.* at 395.

[75] Catherine Barnard et al., *Reflexive Law, Corporate Social Responsibility and the Evolution of Labour Standards: The Case of Working Time* 5 (ESRC Ctr. for Bus. Research, U. of Cambridge, Working Paper no. 294, 2004), https://www.cbr.cam.ac.uk/fileadmin/user_upload/centre-for-business-research/downloads/working-papers/wp294.pdf.

[76] *Id.* at 4.

[77] Simon Deakin & Colm McLaughlin, *Gender Inequality and Reflexive Law: The Potential for Different Regulatory Mechanisms for Making Employment Rights Effective* 25, (ESRC Ctr. for Bus. Research, U. of Cambridge, Working Paper No. 426, 2011), https://www.cbr.cam.ac.uk/fileadmin/user_upload/centre-for-business-research/downloads/working-papers/wp426.pdf.

[78] *Id.* at 21–22.

[79] Zumbansen, *supra* note 69, at 24.

[80] Deakin & McLaughlin, *supra* note 77, at 5.

[81] *Id*.

[82] *Id*.

[83] *Id.* at 6.

potential for substantial liabilities and wider reputational losses, to persuade employers" to alter their course.[84]

E. Trafficking as a Test Case of Reflexive Law

Unlike the Californian Act—which focuses only on the supply chains for goods—the UK legislation covers both the supply of goods and services,[85] and is to cover all sectors of these business operations.[86] In addition, the UK Home Office envisages that it is to cover organizations carrying out any part of their business in the UK, with no minimum level of presence required in the jurisdiction for this legislative provision to apply.[87]

As referred to above, section 54 of the Modern Slavery Act 2015,[88] takes the approach of making a business organization publish statements on its web site setting out the "steps the organisation has taken during the financial year to ensure that slavery and human trafficking is not taking place," "in any of its supply chains," and "in any part of its own business."[89] The assumption being taken is that such statements are reliable and rely on a properly conducted audit. If no such steps have been taken to ensure that slavery and human trafficking is not taking place within the business's global supply chain, then the organization must make a statement to that effect.[90] If no such statement is made under Section 54 of the Modern Slavery Act, then the Secretary of State may bring "civil proceedings in the High Court for an injunction, or in Scotland, for specific performance of a statutory duty."[91] Failure to comply with the injunction, or order of specific performance, would be contempt of court, and be "punishable by an unlimited fine."[92] As stated by the Home Office, a statement to the effect that the undertaking has taken no such measures may damage the reputation of

---

[84] *Id*.

[85] *See* Modern Slavery Act 2015, § 54(2).

[86] *See* HOME OFFICE, MODERN SLAVERY AND SUPPLY CHAINS GOVERNMENT RESPONSE SUMMARY OF CONSULTATION RESPONSES AND NEXT STEPS, 6 (2015) (Eng.).

[87] *See id.* at 6, para. 5(4).

[88] Now supplemented by the Modern Slavery act 2015 (Transparency in Supply Chains) Regulations 2015/1833, which came into force on October 29, 2015). *See* Modern Slavery Act 2015 (Transparency in Supply Chains) Regulations 2015, SI 2015/1833, § 2 (UK).

[89] Modern Slavery Act 2015, § 54(4).

[90] *See id.* at § 54(4)(b).

[91] *Id.* at § 54(11).

[92] HOME OFFICE, *supra* note 35, at 6.

the business and should lead to pressure on the business from consumers, investors, and non-governmental organizations.[93]

The statements need to be signed by those responsible for the business—such as company boards and directors or a partner of the organization—so that "those at the top level take this issue seriously and understand the implications of taking little or no action."[94] Statements need to be published on the undertaking's website, with "a link to the slavery and human trafficking statement in a prominent place on that website's homepage."[95] If the business has no website, alternative requirements have been set out in the act.[96] In addition, there is an obligation on senior managers to "ensure everyone in the organisation is alive to the risks of modern slavery."[97] The intention is to "create a race to the top by encouraging businesses to be transparent about what they are doing, thus increasing competition to drive up standards."[98]

Under the current UK legal framework, there is an assumption that consumers, investors, and non-governmental organizations have sufficient power, whether that be commercial, moral pressure, or under the legal framework, to be able to bring pressure to bear on the transnational corporations.[99] This may be the case with regard to some, but not all relevant global supply chains.

The UK legal framework has addressed the disclosure aspects of laws modeled on the reflexive law approach, and there are hard law requirements compelling disclosure for companies with sufficient turnover. What is to happen once the necessary disclosure has been made, or the conditions required to be put in place in the lead up to the necessary disclosure, is, however, left unaddressed by the legal framework. The emphasis of the concepts underpinning reflexive law is to guide complexity. Standard setting in the public domain through traditional legislation is meant to have an effect on the private domain of internal corporate governance structures. This effect is then supposed to spill over into inter-business relations on the relevant market generally, and—in the context of this paper—through global supply chains. This is meant to occur through focusing business

---

[93] See *id.* at 6.

[94] HOME OFFICE, MODERN SLAVERY AND SUPPLY CHAINS CONSULTATION ON THE TRANSPARENCY IN SUPPLY CHAINS CLAUSE IN THE MODERN SLAVERY BILL 17 (2015).

[95] Modern Slavery Act 2015, § 54(7).

[96] *See id.* at § 54(8).

[97] HOME OFFICE, *supra* note 35, at 14.

[98] *Id.* at 5.

[99] *Id.* at 6.

decision-making on meeting objectives already set by states and leaving to business to establish how best to attain those objectives in the context of their individual commercial activities. Disclosure requirements are meant to be merely one step in the process of orientating business through corporate governance structures to achieve those objectives. Default rules for disclosures, which are unsatisfactory or misleading, or even disclosures of negative information with regard to addressing modern slavery in global supply chains, in the absence of sufficient external pressure, have not been addressed by the UK legislation. There is an assumption by the UK legislators that consumers, investors, and non-governmental organizations[100] will have sufficient power and resources to develop Deakin and McLaughlin's "bargaining in the shadow of the law."[101] In order for the UK legislature to better reflect the concepts underpinning reflexive law, and in order to make its current Section 54 of the Modern Slavery Act 2015 provisions properly effective, further legal provisions are required.

Default conditions to be applied "in the absence of agreement between social actors,"[102] and the relevant transnational corporations, are missing from the current UK legal framework. Criminal sanctions for non-engagement with these external stakeholders would also make this system more robust in light of the seriousness of the underlying crime of modern slavery. Also missing are bridging institutions beyond the legal and enforcement framework "in which effective deliberation and participatory decision-making can occur."[103]

Flaws also arise in the context of the UK mandated information disclosure. As pointed out by Girard—writing in the context of substandard employment practices in global supply chains—not only is the issue that information is disclosed, but also "*how* the corporation discovers the reported information."[104] Under the Californian Act there is a requirement, in Section 3, on corporations not only to "disclose audits of their supply chains,"[105] but also to disclose whether those "audits were unannounced and performed by an independent party."[106] In addition, the Californian law requires, at Section 3(c)(3), that direct supplies need to certify that materials incorporated into the product comply with slavery and human trafficking laws. This level of detail is currently missing from the provisions in Section 53 of the UK's Modern Slavery Act 2015. This issue is important, as, as pointed out by Narine, in

---

[100] *See id*.

[101] Deakin & McLaughlin, *supra* note 77, at 21–22.

[102] *Id.* at 5.

[103] *Id.* at 6.

[104] Girard, *supra* note 3, at 332.

[105] *Id.* at 337.

[106] *Id.* at 337–38.

her paper on the U.S. Dodd-Frank Wall Street Reform and Consumer Protection Act 2010, in a survey on global supply chains, while 2,508 companies were surveyed, 28% had human rights policies, and 21% planned to implement them, only 6% claimed to actively monitor their global supply chains and only 7% had enforcement mechanisms.[107] If all multi-national companies operate in essentially the same way, then similar issues will arise with the effectiveness of Section 53 of the UK's Modern Slavery Act 2015. The training requirements in section 53.5(f) of the UK laws or "its staff" appear to be broader than section 3(c)(5) of the California Act's requirements that company employees and management, who have direct responsibility for supply chain management, get the appropriate training.

The approach being taken in the UK's transparency in supply chains provisions are building on similar developments in the area of business ethics and human rights in a number of different *forae*, none of which, other than the above referred to Californian Act, specifically refer to human trafficking. For example, within the UK, companies are required under the Companies Act 2006 (Strategic Report and Directors' Report) Regulations 2013[108] to report "to the extent necessary for an understanding of the development, performance or position of the company's business, include . . . information about . . . social, community and human rights issues . . . including information about any policies of the company in relation to those matters and effectiveness of those policies."[109] Failure to properly prepare a strategic report leads to being guilty of an offense under which an individual can be criminally fined.[110] The Home Office is of the view that for those companies obliged to provide both the Companies Act 2006 strategic report covering human rights—normally quoted companies—and to make the disclosure requirements under the Modern Slavery Act transparency in supply chains provisions, could prepare a statement that would meet with both requirements. As stated by the act, "it is envisioned most companies will opt for two separate statements."[111]

While the Californian Act has been used above to identify and analyze weaknesses in the UK law on combatting human trafficking in global supply chains, substantial weaknesses remain in the US legal framework on this issue. The Californian Act does not have a direct counterpart at the US federal level, however, other, more limited, related provisions do operate. A US wide act, the Dodd-Frank Wall Street Reform and Consumer Protection Act 2010, at Section 1502, addresses the use of "any conflict minerals from the Democratic

---

[107] *See* Marcia Narine, *From Kansas to the Congo: Why Naming and Shaming Corporations Through the Dodd-Frank Act's Corporate Governance Disclosure Won't Solve Human Rights Crisis*, 25 REGENT U. L. REV. 351, 371 (2013).

[108] *See* Companies Act 2006 (Strategic Report and Directors' Report) Regulations 2013, SI 2013/1970 (Eng.).

[109] *Id.* at § 3 (inserting a new § 414(C)(7)(b)(iii) into the Companies Act 2006, c. 46 (Eng.)).

[110] *See* Companies Act 2006, c. 46, § 414(A) (Eng.).

[111] HOME OFFICE, *supra* note 35, at 25.

Republic of Congo (DRC) in their supply chains."[112] While limited in focus, Feasley argues that it has "been a model for other US regulatory efforts to eliminate forced labor from supply chains."[113] It has also been subject to criticism. For example, Narine points out that transnational corporations "often do not have as much leverage with their suppliers as one would think."[114] In addition, she argues that the drive to keep costs down and lax laws in a host country could undermine supply chain transparency rules. In addition, suppliers can always do business with less demanding transnational corporations, with a consequent change in suppliers being also very costly and time-consuming for the transnational corporation, and can adversely affect local employees, and by extension, the local economy.[115]

There is currently a proposed act before Congress, the Business Supply Chain Transparency on Trafficking and Slavery Act 2015—currently HR 3226—which is, at the time of writing, at the committee stage. Already in force at the federal level in the US is the 2012 Executive Order - Strengthening Protections Against Trafficking In Persons In Federal Contracts, or EO 13627. This Executive Order covers contracts "exceeding USD 500,000 that are performed abroad to develop robust risk assessment and compliance plans" to combat THB in their supply chain.[116] While seen as being broad and ambitious, the order does not extend to non-US government procurement contracts.[117] In addition, the US has in place the Alien Tort Statute, which some US writers see as being relevant in this area. The Alien Tort Statute (ATS) was initially enacted as part of the Judicature Act of 1789. While a long-standing piece of US legislation, it is only recently being pleaded in the context of human rights law. A recent case, *Doe I et al. v. Nestle USA*,[118] before the Ninth Circuit did rule that slavery was "a universally prohibited customary international rights violation."[119] Nevertheless, as Feasley points out, "no contested corporate ATS case has resulted in a jury verdict in favor of the human rights abuse victims in a US federal court."[120] Concerns have been raised as to the levels of extraterritoriality being argued for in its application. Whether the US Alien Torts

---

[112] Ashley Feasley, *Eliminating Corporate Exploitation: Examining Accountability Regimes as Means to Eradicate Forced Labor from Supply Chains*, 2 J. OF HUM. TRAFFICKING 15, 24 (2016).

[113] *Id.*

[114] Narine, *supra* note 107, at 371.

[115] *See id.*

[116] Feasley, *supra* note 112, at 25.

[117] *Id.*

[118] *See Doe I v. Nestle USA, Inc.*, 738 F. 3d 1048 (9th Cir. 2013).

[119] Feasley, *supra* note 112, at 27.

[120] *Id.* at 26.

Statute will have any relevance to human trafficking in supply chain cases going forward has yet to be established.

While attempts by two jurisdictions—the UK and the early moving State of California—to address human trafficking and slavery in global supply chains have been addressed above to include the flaws and criticisms of their approach and perceived effectiveness to date, the EU has yet to make any attempts to legislate in this area. This is despite the fact that the EU was an early mover in legislating to combat human trafficking generally. The approaches modeled on reflexive law being taken by the UK and the State of California are not unknown to the EU, which has already adopted similar provisions in Directive 2014/95/EU. The EU should give some consideration to similarly legislating—perhaps using the concepts that underpin reflexive law—to combat human trafficking in global supply chains, while also benefiting from the experience and criticism of the earlier attempts to so legislate by the UK and the State of California.

Lessons can also be learned, by all jurisdictions, from other policy areas where the ideas underpinning reflexive law have informed legislative drafting. Reflexive law based regimes have been operating in a number of areas of transnational business in recent years, with an "analysis of the efficacy" of those regimes leading "to a conclusion that the most successful approach is a hybrid of all of the accountability regimes,"[121] requiring, in the context of business, "international regulation, market-based, civil-liability, and domestic regulation."[122] In addition, there would be a need for criminal liability provisions to be in place in the context of modern slavery, where appropriate, and the "bridging institutions" of Deakin and McLaughlin, where the "effective deliberation and participatory decision-making can occur,"[123] in order to ensure that the objectives of the reflexive laws actually operate.

Commenting on the National Contact Points set up under the OECD Guidelines on Multinational Enterprises, Feasley stated that "as long as procedures . . . are voluntary" then they "cannot function as the sole mechanism" to combat forced labor in supply chains.[124] Gold, Tautrims, and Trodd state that "the traditional managerial paradigm of profit maximisation" requires ensuring that a company's global supply chain is slavery free in order to "trade-off against the risks of litigation and reputation damage."[125] This logic requires not just voluntary action to combat potential reputational damage, but also potentially high risks

[121] *Id.* at 16.

[122] *Id.* at 15.

[123] Deakin & McLaughlin, *supra* note 77, at 6.

[124] Feasley, *supra* note 112, at 23.

[125] Stefan Gold et al., *Modern Slavery Challenges to Supply Chain Management*, 20 SUPPLY CHAIN MGMT.: AN INT'L J. 485, 486 (2015).

of litigation, whether that be criminal or civil. It would appear that regulation based on reflexive law by itself will not achieve its anticipated objectives. It needs to be backed up by traditional hard law. A reflexive law regulatory approach may, however, better negotiate complexity and extend the territorial reach of national and EU laws in ways that traditional hard laws cannot achieve by themselves. It is not clear that there are such high risks of litigation under the current UK legal framework. An effective "reflexive, negotiating government does keep (and does need) . . . certain teeth and claws."[126] Reliance on the market solely in order to achieve these objectives would be an error. As pointed out by Feasley, many believe that "corporate accountability for human rights" is a "disposable concept" when human rights promotion and corporate interests diverge.[127]

G. Conclusion

Globalization is clearly posing challenges for the regulation of both transnational and economic law, and for the need to address transnational criminality through transnational criminal law. Under traditional legal frameworks, the effectiveness of state command and control models stop at the border.[128] There is a need to examine how states—in particular the larger and more economically active jurisdictions—can have an effect on the behavior of transnational business. Laws based on the approach of reflexive law are emerging as a possible additional tool for addressing these concerns. As stated above, the approach of "reflexive regulation" is to set the required objective by way of law—which is mandatory on the legal entities operating within a particular jurisdiction—but leaving to the market operators to "determine the most efficient and effective ways to achieve desired results."[129] Mechanisms based on reflexive law need to be properly designed and implemented in order to be effective.

The reflexive law approach has already been deployed in a number of areas of commercial activity by a number of jurisdictions. Assessments have already been made as to the effectiveness and weaknesses of reflexive law mechanisms in the commercial world. THB is one point at which the ostensibly legitimate commercial world bisects the transnational criminal world. Global anti-money laundering provisions and processes is a second. Measures have already been taken by a small number of jurisdictions to regulate for THB in global supply chains using reflexive law methodology. Similar measures could also be taken to tackle anti-money laundering. Weaknesses are already emerging in those reflexive law mechanisms adopted to tackle THB in global supply chains. In particular, the recently

[126] Marius Aalders & Ton Wilthagen, *Moving Beyond Command-and-Control: Reflexivity in the Regulation of Occupational Safety and Health and the Environment*, 19 L. & POL'Y 415, 436 (1997).

[127] Feasley, *supra* note 112, at 18–19.

[128] Girard, *supra* note 3, at 322.

[129] *Id*. at 338.

enacted UK provisions, set out in section 54 of the Modern Slavery Act 2015, shows such weaknesses. In order to be effectively regulating by reflexive law provisions, which by its very nature is "tentative, experimental, and learning,"[130] the law needs to be subject to constant self-critical review of its institutions, and their processes, as to whether and how they are achieving the required steering mechanism.[131] It also needs to be subjected to strong empirical testing before its effectiveness in any particular context can be truly established.[132] There is already a need to revisit the UK provisions to tighten them up, in order to make them more effective, in lights of lessons learned elsewhere.

Some may argue that a weakness of all of the legal frameworks discussed above is that they are focused on larger multi-national companies. It is accepted by this writer that the burdens being imposed on companies by regulations based on reflexive law would be disproportionate if used against smaller companies, and smaller companies are "not likely to be regulated successfully by internal management systems,"[133] as smaller companies are typically more focused on survival. These smaller operations are best influenced through the larger multinational companies, and their horizontal provisions, developed by the larger companies for their particular context, and operating under transnational reflexive law regulation.

The use of transnational reflexive law—as opposed exclusive reliance on traditional, jurisdictionally based, command and control law—requires new, additional, ways of conceptualizing, designing, and assessing the effectiveness of law. For example, the "multi[i]-directional nature of transnational legal processes"[134] would need to be acknowledged, together with their effect on "states that are strong and proximate to international institutions," or the relevant regulatory authority or jurisdiction. In addition the effect of these initiatives would have to be examined on those states "that are weak, distant, and peripheral."[135] Shaffer points out that not only does the law need to change, but so too does the perception of the relationship between the state and the market, and how the state operates this type of law.[136] In addition, the role of governance structures

[130] Zumbansen, *supra* note 69, at 25.

[131] *See* Orts, *supra* note 13, at 780.

[132] *See* Teubner, *supra* note 10, at 276.

[133] Aalders & Wilthagen, *supra* note 126, at 432.

[134] Shaffer, *supra* note 23, at 260.

[135] *Id.*

[136] *See id.* at 259.

within transnational corporations in achieving the objectives of the reflexive law and new accountability mechanisms needs to be developed.[137]

Reliance on reputation sensitivities—where these exists—market forces, and consumer pressure assumes that the public at large have access to relevant information, and can engage in "democratic control of enterprises' behaviour."[138] As Aalders and Wilthagen have pointed out, this requires "(1) systems monitoring, (2) intermediary structures and networks [echoed by Deakin and McLaughlin[139]], (3) corporate social responsibility, and (4) other market-oriented regulatory tools."[140] A number of these are still missing from the UK legal framework on THB in global supply chains. An effective "reflexive, negotiating government does keep (and does need) . . . certain teeth and claws."[141]

The State of California has made a start in the US to tackling human trafficking and slavery in global supply chains. Other jurisdictions in the US need to catch up. Given the level of seriousness that the EU attributes to the issue of human trafficking, it should also consider legislating for human trafficking and slavery-like practices in global supply chains. Within Europe, both the UK and EU legal frameworks still require further development. The issues raised above will need to be considered in reviewing the effectiveness of these provisions based on reflexive law.

---

[137] *See id*.

[138] Aalders & Wilthagen, *supra* note 126, at 431.

[139] *See* Deakin & McLaughlin, *supra* note 77, at 6.

[140] Aalders & Wilthagen, *supra* note 126, at 431.

[141] *Id.* at 436.

Articles

The Many Uses of Anti-Money Laundering Regulation—Over Time and into the Future

By Maria Bergström[*]

Abstract

Given the fast development of the field of AML Regulation, this Article aims to answer the following questions: First, how is money laundering dealt with and regulated on the EU level? Second, to which legal concerns do the chosen regulatory strategy give rise? Accordingly, this Article provides an overview of the various regulatory strategies in the global and EU regional AML Regime while at the same time points out some of the most pressing legal concerns in AML Regulation. These include the blurred line between administrative and criminal law measures and the protection of individual rights and fundamental freedoms including data protection and privacy issues in administrative and criminal law contexts respectively. Although briefly mentioning the global and international context, the focus of this Article is the EU regulatory action, its outcome and critique, and possible future.

[*] Associate Professor in European Law, Faculty of Law, Uppsala University.

A. Introduction

Modern regulatory activities often span from global initiatives and regional legislative processes to national implementation and application. The regulatory field of anti-money laundering (AML) regulation is no exception. AML regulation is a fascinating field that not only embraces various types of actors and interests, actions, and processes, but also faces challenges and shortcomings on a variety of levels and contexts. More specifically, within the European Union (EU), the applicable administrative and criminal law frameworks stem mainly from EU Regulation, which in turn transpose and closely follow complementary activities carried out in international fora, in particular those of the Financial Action Task Force (FATF),[1] the United Nations, the Council of Europe, and also banking organizations.[2]

Whereas money laundering and terrorist financing are frequently carried out in an international context with regulation on different levels beyond the national level, the regulatory context is widened in other respects as well. The European Agenda on Security[3] published in 2015 called for additional measures in the areas of terrorist financing and money laundering. The 2016 Action Plan to strengthen the fight against terrorist financing[4] highlighted the need to counter money laundering by means of criminal law and the need to ensure that criminals who fund terrorism are deprived of their assets. After the entry into force of the Lisbon Treaty in 2009, money laundering is one of the so-called *Euro-crimes* with a specific criminal law legal basis in Article 83(1) of the Treaty on the Functioning of the European Union (TFEU). Additionally, the fourth AML Directive—soon to be amended by the fifth AML Directive—includes tax crime as a new predicate offence.[5]

---

[1] FATF is an inter-governmental body that was established in 1989 by the Ministers of its member jurisdictions FATF home page at http://www.fatf-gafi.org/about/ (last visited Mar. 6, 2018).

[2] *See, e.g.*, Maria Bergström, *EU Anti-Money Laundering Regulation: Multilevel Cooperation of Public and Private Actors*, *in* CRIME WITHIN THE AREA OF FREEDOM, SECURITY AND JUSTICE: A EUROPEAN PUBLIC ORDER (Christina Eckes & Theodore Konstadinides eds., 2011) [hereinafter Bergström 2011].

[3] *See* European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, the European Agenda on Security,* COM (2015) 185 final (Apr. 28, 2015).

[4] *See Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight Against Terrorist Financing*, COM (2016) 50 final (Feb. 2, 2016).

[5] Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 2015 O.J. (L 141) 73. [hereinafter Fourth AML Directive] (In the case of money laundering, a predicate offense may cover actions used to obtain the initial funds.).

Given the fast development of the field of AML Regulation, this Article aims at answering the following questions: First, how is money laundering dealt with and regulated on the EU level? Second, to which legal concerns do the chosen regulatory strategy give rise? Accordingly, this Article provides an overview of the various regulatory strategies in the global and EU regional AML Regime while at the same time points out some of the most pressing legal concerns in AML Regulation. These include the blurred line between administrative and criminal law measures and the protection of individual rights and fundamental freedoms including data protection and privacy issues in administrative and criminal law contexts respectively. Although briefly mentioning the global and international context, the focus of this Article is EU regulatory action, its outcome and critique, and possible future.[6]

B. The Broader Regulatory Framework—The EU Security Agenda and Transnational Crime Prevention

In April 2015, the European Commission presented the European Agenda on Security for the period of 2015–2020.[7] Highlighting that the primary goal of organized crime is profit and that international criminal networks use legal business structures to conceal the source of their profits, the European Agenda on Security called for a strengthening of the capacity of law enforcement to tackle the finance of organized crime. Besides the fight against organized crime and cybercrime, preventing terrorism and countering radicalization are identified as the most pressing challenges.

The European Agenda on Security will support Member States' cooperation in tackling these security threats. Key actions include effective measures to "follow the money" and cutting the financing of criminals, where cooperation between competent authorities will be strengthened, in particular the national Financial Intelligence Units (FIUs), which will be connected to Europol. In addition, Eurojust could offer more expertise and assistance to national authorities when conducting financial investigations. The idea is that cross-border cooperation between national FIUs and national Asset Recovery Offices (AROs) will help to

---

[6] This Article builds upon and develops from my previous publications. *See generally* Bergström 2011, *supra* note 2; Maria Bergström, *The Place of Sanctions in the EU System for Combating the Financing of Terrorism*, *in* EU SANCTIONS: LAW AND POLICY ISSUES CONCERNING RESTRICTIVE MEASURES (Lain Cameron ed., 2013); Maria Bergström, *Money Laundering*, *in* RESEARCH HANDBOOK ON EU CRIMINAL LAW (Valsamis Mitsilegas, Maria Bergström & Theodore Konstadinides, eds., 2016) [hereinafter Bergström 2016]; Maria Bergström, *The Global AML Regime and the EU AML Directives – Prevention and Control*, *in* THE HANDBOOK OF CRIMINAL AND TERRORISM FINANCING LAW (Colin King, Clive Walker & Jimmy Gurule eds., 2018) [hereinafter Bergström 2018a]; Maria Bergström, *Legal Perspectives on Money Laundering*, *in* RESEARCH HANDBOOK ON TRANSNATIONAL CRIME (Valsamis Mitsilegas & Saskia Hufnagel eds., Edward Elgar, forthcoming in 2018) [hereinafter Bergström 2018b].

[7] *The European Agenda on Security*, *supra* note 3.

combat money laundering and to access the illicit proceeds of crime.[8] The powers of FIUs will thereby be reinforced to better track the financial dealings of organized crime networks and to enhance the powers of competent national authorities to freeze and confiscate illicit assets. The European Agenda on Security thus aims at "tackling the nexus between terrorism and organized crime, highlighting that organized crime feeds terrorism through channels like the supply of weapons, financing through drug smuggling, and the infiltration of financial markets."[9]

The European Agenda on Security for 2015–2020 specifically called for additional measures in the area of terrorist financing and money laundering. Indeed the rules against money laundering and terrorist financing adopted in May 2015, such as the fourth AML Directive[10] and the first AML Criminal Law Directive proposed in December 2016,[11] are key actions.[12] Besides legislation against money laundering, the EU further contributes to preventing the financing of terrorism through the network of EU FIUs and the EU-US Terrorist Finance Tracking Programme.[13]

In February 2016, the Commission presented an Action Plan to further step up the fight against the financing of terrorism.[14] In brief, the plan has two main objectives. First, it aims to prevent the movement of funds and identify terrorist funding. In this respect, key actions include: Ensuring virtual currency exchange platforms are covered by the AML Directive; tackling terrorist financing through anonymous pre-paid instruments such as pre-paid cards; improving access to information and cooperation among EU FIUs; ensuring a high level of safeguards for financial flows from high risk third countries; and giving EU FIUs access to

---

[8] *Id.*

[9] *Proposal for a Directive of the European Parliament and of the Council on Countering Money Laundering by Criminal Law*, COM (2016) 826 final (Dec. 21, 2016).

[10] *See* Fourth AML Directive, *supra* note 5; Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on Information Accompanying Transfers of Funds and Repealing Regulation (EC) 1781/2006, 2015 O.J. (L 141) 1.

[11] *See Proposal for a Directive of the European Parliament and of the Council on Countering Money Laundering by Criminal Law*, COM (2016) 826 final (Dec.21, 2016) [hereinafter AML Criminal Law Directive].

[12] *The European Agenda on Security*, *supra* note 3; Press Release, European Commission, Commission Takes Steps to Strengthen EU Cooperation in the Fight Against Terrorism, Organised Crime and Cybercrime (Apr. 28, 2015), http://europa.eu/rapid/press-release_IP-15-4865_en.htm (last visited Apr. 8, 2017); *see also* European Parliament Resolution of 17 December 2014 on Renewing the EU Internal Security Strategy, 2014/2918(RSP), PARL. DOC. P8_TA(2014)0102, www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2014-0102+0+DOC+XML+V0//EN.

[13] *See* European Commission, *Fact Sheet: European Agenda on Security: Questions and Answers*, MEMO/15/4867 (28 Apr. 28, 2015), http://europa.eu/rapid/press-release_MEMO-15-4867_en.htm.

[14] *See Action Plan for Strengthening the Fight against Terrorist Financing*, *supra* note 4, at 2.

centralized bank and payment account registers and central data retrieval systems. Secondly, the plan aims to disrupt sources of revenue for terrorist organizations. Key actions include: Tackling terrorist financing sources—such as the illicit trade in goods, cultural goods, and wildlife, and working with third countries to ensure a global response to tackling terrorist financing sources.[15] Accordingly, the EU AML Regime is central also for the Action Plan for Strengthening the Fight Against Terrorist Financing.[16]

Whereas the European Agenda on Security called for additional measures in the area of terrorist financing and money laundering, the Commission's Action Plan[17] highlighted the need to counter money laundering by means of criminal law and the need to ensure that criminals who fund terrorism are deprived of their assets. The next step is therefore to investigate how these regulatory challenges have been dealt with by the EU legislator.

C. A Two-Tier European Union Power to Regulate

After the entry into force of the Lisbon Treaty in 2009, TFEU has given particular attention to a number of cross-border crimes such as money laundering. Thus, money laundering is one of the so-called Euro-crimes with a specific criminal law legal basis in Article 83(1) TFEU. Despite the new criminal law competence to adopt EU criminal law measures directly based on Article 83(1) and the proposal for a first EU AML Criminal Law Directive,[18] the current AML framework mainly consists of two legal instruments, both based on Article 114 TFEU on the internal market: The fourth AML Directive,[19] soon to be amended by the recently adopted fifth AML Directive,[20] and the Transfer of Funds Regulation.[21]

In order to avoid annulment by the Court of Justice of the European Union (CJEU), the predominant purpose of both instruments is ostensibly to improve the conditions for the establishment and functioning of the internal market, rather than to define criminal law

---

[15] *See* European Commission, *Fact Sheet: Action plan to strengthen the Fight Against Terrorist Financing. European Agenda on Security* (Dec. 2016), http://ec.europa.eu/newsroom/document.cfm?doc_id=40720.

[16] *See generally* Bergström 2018b, *supra* note 3.

[17] *See Action Plan for Strengthening the Fight Against Terrorist Financing, supra* note 4.

[18] *See* AML Criminal Law Directive, *supra* note 11.

[19] *See* Fourth AML Directive, *supra* note 5.

[20] *See* Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU, 2018 O.J. (L 156) 43.

[21] *See* Regulation (EU) 2015/847, *supra* note 10.

offenses and sanctions. Yet, their main aim is still the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.[22] This has indirectly been confirmed by the Court of Justice in *Jyske Bank Gibraltar*.[23] In this case, the Court stated that, admittedly, the now repealed third AML Directive[24] was founded on a dual legal basis,[25] and it also sought to ensure the proper functioning of the internal market. The Court then went on to state that the Directive's main aim was the prevention of the use of the financial system for the purposes of money laundering and terrorist financing. This was apparent both from its title and the preamble, and from the fact that it was adopted, like its predecessor,[26] in an international context in order to apply and make binding in the EU the recommendations of the FATF. In other words, both instruments now in force, update existing EU legal instruments on money laundering and the financing of terrorism and aim to implement and extend the newest FATF recommendations issued in February 2012, most recently updated in February 2018.[27]

Yet, despite all assumptions and suggestions that the current EU AML framework is mainly administrative in character, there is a floating and vague line between administrative law and criminal law and sanctions, not least since national laws and EU law are intertwined and interrelated.

First, because the fourth AML Directive provides for an EU-wide definition of money laundering,[28] it might be argued that the current AML framework does establish harmonized rules when it comes to the definition of money laundering. EU rules stipulate what behavior is considered to constitute a criminal act, but does not state what type and level of sanctions are applicable for such acts. More specifically, the Directive clearly states that Member States shall ensure that money laundering and terrorist financing are prohibited,[29] but it

---

[22] *See also* Bergström 2016, *supra* note 6.

[23] *See* Case C-212/11, Jyske Bank Gibraltar v. Administración del Estado, ECLI:EU:C:2013:270, para. 46, Judgement of 25 April 2013.

[24] *See* Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, 2005 O.J. (L 309) 15 [hereinafter Third AML Directive].

[25] Treaty on the Functioning of the European Union, Oct. 26, 2012, 2012 O.J. (C 326), arts. 53(1) & 114.

[26] Council Directive 91/308/EEC of 10 June 1991 on Prevention of the Use of the Financial System for the Purpose of Money Laundering, 1991 O.J. (L 166) 77 [hereinafter First AML Directive].

[27] Financial Action Task Force, The FATF Recommendations, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html#UPDATES.

[28] Fourth AML Directive, *supra* note 5, art. 1(3) (not changed by the fifth AML Directive).

[29] *Supra* note 5, art. 1(2) (not changed by the fifth AML Directive).

cannot and may not require States to have certain criminal law provisions in place with certain specific minimum and maximum sanctions for breaches.[30] In other words, the internal market measures may not establish minimum rules concerning the definition of criminal offences and sanctions within the scope of Article 83(1) TFEU. Under the present situation, the Member States should ensure that administrative sanctions and measures in accordance with the fourth AML Directive and criminal sanctions in accordance with national law are in place. If adopted, the AML criminal law directive will change this situation.[31]

In this respect, the Commission claims that "All Member States criminalize money laundering but there are significant differences in the respective definitions of what constitutes money laundering, on which are the predicate offences—i.e. the underlying criminal activity which generated the property laundered—as well as the level of sanctions."[32] The Commission further argues that the current legislative framework is neither comprehensive nor sufficiently coherent to be fully effective, and that "The differences in legal frameworks can be exploited by criminals and terrorists, who can choose to carry out their financial transactions where they perceive anti-money laundering measures to be weakest."[33]

The definitions, scope, and sanctions of money laundering offences affect cross-border police and judicial cooperation among national authorities and the exchange of information. Practitioners have reported that differences in criminal law pose obstacles to effective police co-operation and cross-border investigation.[34] According to the Commission, there are significant differences in the respective definitions of what constitutes money laundering, the predicate offences, and the level of sanctions. Such differences in the scope of predicate offences make it difficult for FIUs and law enforcement authorities in one Member State to coordinate with other EU jurisdictions to tackle cross-border money laundering.[35]

Second, to provide a specific example of the interrelationship between criminal and administrative law under the Directive, according to recital 59, Member States should ensure the imposition of administrative sanctions and measures in accordance with this

---

[30] *See* Ester Herlin-Karnell, *Is Administrative Law Still Relevant? How the Battle of Sanctions has Shaped EU Criminal Law*, *in* RESEARCH HANDBOOK ON EU CRIMINAL LAW, *supra* note 6.

[31] At the time of writing in May 2018, the proposal has not been adopted.

[32] AML Criminal Law Directive, *supra* note 9, at 1.

[33] *Id.*

[34] *Id.* at 2.

[35] *Id.* at 1. This section builds upon and develops from Bergström 2018b, *supra* note 2.

Directive, and the imposition of criminal sanctions, in accordance with their national law, does not breach the principle of *ne bis in idem*. In other words, it is the responsibility of the Member States to ensure that the parallel systems of administrative and criminal law sanctions do not breach the principle of *ne bis in idem*.[36]

Third, the fourth AML Directive further emphasizes that sanctions or measures for breaches of national provisions transposing the Directive must be effective, proportionate, and dissuasive.[37] As pointed out by Koen Lenaerts and José Gutiérrez-Fons,[38] the CJEU in *Åkerberg Fransson* recalled that, when EU legislation does not specifically provide any penalty for an infringement of EU law or refers for that purpose to national laws, regulations and administrative provisions, the Member States have the freedom to choose the applicable penalties, i.e., administrative, criminal or a combination of the two.[39] Yet, the resulting penalties must comply with the Charter of Fundamental Rights of the European Union (EU Charter) and be effective, proportionate, and dissuasive.[40] Any measure based on Article 83(1) TFEU, however, will leave no such freedom to the Member States.

I. The Criminal Law Proposal

On December 21, 2016, two days after the compromise proposal aiming at amending the fourth AML Directive was adopted by the Council,[41] the Commission submitted a proposal for a Directive on countering money laundering by criminal law—AML Criminal Law

---

[36] *See, e.g.,* ECJ, Case C-524/15, Luca Menci, ECLI:EU:C:2018:197, Judgement of 20 March 2018; Case C-537/16 Garlsson Real Estate v. Consob, ECLI:EU:C:2018:193, Judgement of 20 March 2018; Joined Cases C-596/16 and C-597/16, Enzo Di Puma v. Consob v. Antonio Zecca, ECLI:EU:C:2018:192, Judgement of 20 March 2018.

[37] Fourth AML Directive, *supra* note 5, art. 58(1) (not changed by the fifth AML Directive).

[38] *See* Koen Lenaerts & Jose Gutiérrez-Fons, *The European Court of Justice and Fundamental Rights in the Field of Criminal Law*, *in* RESEARCH HANDBOOK ON EU CRIMINAL LAW.

[39] *See* Case C-617/10 Åklagaren v. Hans Åkerberg Fransson, ECLI:EU:C:2013:105, para. 34, Judgement of 26 February 2013.

[40] *See id.*, para. 36.

[41] On December 21, 2016, the Commission submitted two legislative proposals: The proposal for the Criminal Law AML Directive, COM (2016) 826 final (AML Criminal Directive, *supra* note 9), and a proposal for a Regulation on the mutual recognition of freezing and confiscation orders.

Directive. This was the first proposal based on Article 83(1) TFEU,[42] which identifies money laundering as one of the so called "Euro-crimes" with a particular cross-border dimension.

The proposal aims to counter money laundering by means of criminal law and enables the European Parliament and the Council to establish the necessary minimum rules on the definition of money laundering by means of directives adopted in accordance with the ordinary legislative procedure. The proposal would complement different pieces of EU legislation that require Member States to criminalize some forms of money laundering. It will partially replace Council Framework Decision 2001/500/JHA as regards the Member States bound by this proposal.[43] According to the Commission proposal, the existing instruments at the EU level—and in particular the above-mentioned Framework Decision—are limited in scope and do not ensure a comprehensive criminalization of money laundering offences.[44]

The proposal further complements Directive 2014/42/EU that aims at creating a common set of minimum rules for the detection, tracing, and confiscation of proceeds of crime across the EU, and Council Framework Decision 2008/841/JHA, which criminalizes the participation in an organized criminal group and racketeering.[45] In addition, it reinforces and complements the criminal law framework with regard to offences relating to terrorist groups, in particular the Directive on Combating Terrorism,[46] which sets a "comprehensive definition of the crime of terrorist financing, covering not only terrorist offences, but also terrorist-related offences such as recruitment, training and propaganda."[47]

As stated in the Explanatory Memorandum of the criminal law proposal, the rationale behind the proposal was that terrorists often resort to criminal proceeds to fund their activities and use money laundering schemes in that process. Thus, the underlying idea is that criminalization of money laundering would contribute to tackling terrorist financing.[48]

---

[42] AML Criminal Law Directive, *supra* note 11.

[43] Council Framework Decision 2001/500/JHA of 26 June 2001 on Money Laundering, the Identification, Tracing, Freezing, Seizing and Confiscation of Instrumentalities and the Proceeds of Crime, 2001 O.J. (L 182) 1.

[44] AML Criminal Law Directive, *supra* note 9.

[45] *Id.* at 5.

[46] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA, 2017 O.J. (L 88) 6.

[47] AML Criminal Law Directive, *supra* note 9, at 5.

[48] *Id.*

Hence, one of the key measures was to consider a possible proposal for a minimum Directive on the definition of the criminal offence of money laundering,[49] applying it to terrorist offences and other serious criminal offences, and to approximate sanctions. In other words, the proposed AML Criminal Law Directive is embedded in the global fight against money laundering and terrorist financing. It implements international obligations in this area including the Warsaw Convention and Recommendation 3 of the FATF. FATF Recommendation 3 in turn calls on countries to criminalize money laundering on the basis of the Vienna Convention of 1988 and the Palermo Convention of 2000.[50]

According to the Progress Report from the Presidency to the Council, work on the proposal is progressing well in the Working Party on Substantive Criminal Law (DROIPEN).[51] Since January 2017, the Working Party has been preparing a compromise text of the proposal as a basis for reaching a general approach at the Council. On May 30, 2017, a compromise text was presented by DROIPEN, which would constitute the basis for future negotiations with the European Parliament in the context of the ordinary legislative procedure.[52]

The consolidated compromise text of the proposed Directive, as resulting from these discussions and confirmed at COREPER on May 24, 2017, seeks to reflect the compromises achieved on the basis of the positions expressed by delegations.[53] On the one hand, if the latest proposal for an AML Criminal Law Directive is adopted, it would expand the current EU focus from prevention to the control of money laundering and terrorist financing. On the other hand, as suggested by the Commission, the proposal, if adopted, will also reinforce the measures in place aimed at detecting, disrupting, and preventing the abuse of the financial system for money laundering and terrorist financing purposes, notably the fourth AML Directive. This Directive, along with the Transfer of Funds Regulation,[54] sets out rules which are designed to prevent the abuse of the financial system for money laundering and terrorist financing purposes.[55]

---

[49] *Action Plan for Strengthening the Fight Against Terrorist Financing*, *supra* note 4.

[50] United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.

[51] Interinstitutional Files: 2016/0414 (COD) 2016/0412 (COD), Progress Report from Presidency to Council, Combatting Financial Crime and Terrorism Financing (Mar. 20, 2017).

[52] Interinstitutional File: 2016/0414 (COD), Progress Report from Presidency to Council, Concerning Proposal for a Directive of the European Parliament and of the Council on Countering Money Laundering by Criminal Law [First reading] General Approach (May 30, 2017).

[53] *Id.*

[54] Regulation (EU)2015/847, *supra* note 10.

[55] *See also* Bergström 2018b, *supra* note 2; Bergström 2018a, *supra* note 2.

II. The EU Administrative Law Directives

1. Compensatory Measures and the Risk-based Approach

The EU AML Directive from 1991—the first AML Directive—was the first stage in combating money laundering at the European level.[56] The preamble of the first AML Directive stated that money laundering must be combated mainly by penal means and within the framework of international cooperation among judicial and law enforcement authorities. Yet, the directive recognized that a penal approach should not be the only way to combat money laundering "since the financial system can play a highly effective role."[57] The preamble further stated that money laundering has an evident influence on the rise of organized crime in general and drug trafficking in particular. It continued on to say that there is increasing awareness that combating money laundering is one of the most effective means of opposing this form of criminal activity, which constitutes a particular threat to the Member States' societies.

The shift towards the risk-based approach and the extension to include the financing of terrorism[58] as money laundering predicate offence were both introduced with the third AML Directive at the European level.[59] Even today these remain two of the major changes within this regulatory field. This shift brought the regional EU rules in line with the global standard, revised and expanded FATF recommendations.[60]

First, each country should criminalize the financing of terrorism, terrorist acts, and terrorist organizations, and ensure that such offences are designated as money laundering predicate offences.[61] FATF also agreed upon rules about freezing and confiscating terrorist assets,[62] rules about reporting suspicious transactions related to terrorism,[63] and rules concerning international co-operation, alternative remittance, wire transfers, and non-profit

---

[56] First AML Directive, *supra* note 26.

[57] *Id.*, n.18.

[58] Third AML Directive, *supra* note 24, recital 8.

[59] *Id.*

[60] FATF, *FATF 40 Recommendations* (Oct. 2004).

[61] *Id.*, Special Recommendation II.

[62] *Id.*, Special Recommendation III.

[63] *Id.*, Special Recommendation IV.

organizations.[64] On 22 October 2004, a ninth special recommendation on cash couriers was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments.[65]

Second, the "risk-based approach"[66] was given a prominent position in the third AML directive, as well as in the amended FATF recommendations upon which it builds.[67] The starting point is that risks differ among countries, customers, and business areas over time. The operators themselves are the best analysts of where the risk areas are, or might arise, as they know best their businesses and their customers. The idea is that resources should be used where needs arise and the framework is supposed to be more flexible and adjustable to risk. Within a risk-based approach, businesses are expected to make risk assessments of their customers and divide them into low and high-risk categories. In order to enable operators to assess whether a situation involves a risk of money laundering and terrorist financing and to act accordingly, the directive introduced more detailed provisions. For this purpose, the directive specified a number of customer due diligence (CDD) measures that are more extensive and far-reaching for situations of higher risk, such as appropriate procedures to determine whether a person is a politically exposed person (PEP). The risk-based approach further emphasizes that the evaluation of who is high or low risk is to be a continuous process. As a result, the concept of "know your customer," as used in the financial sector, in practice became applicable to all covered by the directive.[68]

---

[64] *Id.*, Special Recommendations V–VIII (Recommendation VI has been covered by Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services (PSD) in the Internal Market, 2007 O.J. (L 319) 1, and Recommendation VII was addressed by Regulation (EC) 1781/2006 of the European Parliament and of the Council of 15 November 2006 on Information on the Payer Accompanying Transfers of Funds, 2006 O.J. (L 345) 1.).

[65] *Id.*, Special Recommendation IX (being covered by Regulation (EC) 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, 2005 O.J. (L 309) 9).

[66] *See generally* MICHAEL POWER, THE RISK MANAGEMENT OF EVERYTHING (2004); MICHAEL POWER, ORGANIZED UNCERTAINTY (Oxford Univ. Press, 2007) (explaining that risk management is expanding in both range and scope across organizations in the public and the private sectors and has become something of a contemporary standard for dealing with uncertainty in an organized manner). For an integrated analysis of the concepts of risk and securitization, *see generally* Maria Bergström, Ulrika Mörth & Karin Svedberg Helgesson, *A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management*, 5 J. COMMONS MKT. STUD. 1043 (2011) (showing between the concepts of risk and securitization, both emphasizing the structural threats and uncertainties in the case of AML); *see also* VALSAMIS MITSILEGAS, MONEY LAUNDERING COUNTER-MEASURES IN THE EUROPEAN UNION 3 (2003) (discussing "reconceptualizing security in the risk society").

[67] *See generally* Ester Herlin-Karnell, *The EU's Anti Money Laundering Agenda: Built on Risks?*, *in* CRIME WITHIN THE AREA OF FREEDOM, SECURITY AND JUSTICE, *supra* note 2 (a critical analysis of the risk-based approach).

[68] *See generally* Bergström 2018a, *supra* note 2.

2. Towards a More Targeted and Focused Risk-Based Approach

The current AML framework consists of two legal instruments both based on Article 114 TFEU on the internal market: The fourth AML Directive [69] and the Transfer of Funds Regulation.[70] Both instruments update existing EU legal instruments on money laundering and the financing of terrorism and aim to implement and extend the newest recommendations issued in February 2012 by the FATF.[71]

The fourth AML Directive aims to prevent the Union's financial system from abuse for purposes of money laundering and terrorist financing.[72] The risk-based approach[73] has been further developed towards a more targeted and focused risk-based approach using evidence-based decision-making, as well as guidance by European supervisory authorities.[74] In this respect, the new framework clarifies how AML supervisory powers apply in cross-border situations. These changes have the aim of updating the EU rules to implement the newest FATF recommendations, with their increased focus on the effectiveness of regimes to counter money laundering and terrorist financing, as well as addressing the shortcomings of the third AML Directive identified by the European Commission. [75]

---

[69] Fourth AML Directive, *supra* note 5.

[70] Regulation (EU) 2015/847, *supra* note 10.

[71] *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations* (2012, most recently updated Feb. 2018), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[72] Fourth AML Directive, *supra* note 5, art. 1(1).

[73] *See, e.g.*, Herlin-Karnell, *supra* note 67; Bergström, *supra* note 2; Bergström, 2016, *supra* note 6, n. 27.

[74] Fourth AML Directive, *supra* note 5. Recital 23, for example, states that underpinning the risk-based approach is the need for member states and the Union to identify, understand, and mitigate the risks of money laundering and terrorist financing that they face. The importance of a supranational approach to risk identification has been recognized at the international level, and the European Supervisory Authority (European Banking Authority) (EBA), established by Regulation (EU) 1093/2010 of the European Parliament and of the Council, the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (EIOPA), established by Regulation (EU) 1094/2010 of the European Parliament and of the Council, and the European Supervisory Authority (European Securities and Markets Authority) (ESMA), established by Regulation (EU) 1095/2010 of the European Parliament and of the Council, should be tasked with issuing an opinion, through their Joint Committee, on the risks affecting the Union's financial sector. Recital 24 of the Fourth AML Directive then states that national and Union data protection supervisory authorities should be involved only if the assessment of the risk of money laundering and terrorist financing has an impact on the privacy and data protection of individuals.

[75] *See* European Commission, *Report on the Application of the Third Anti-Money Laundering Directive: Frequently Asked Questions*, MEMO/12/246 (Apr. 11, 2012), http://europa.eu/rapid/press-release_MEMO-12-246_en.htm?locale=en (last visited Mar. 15, 2018) (explaining the review of the third AML Directive undertaken by the Commission, with a view to addressing any identified shortcomings).

According to the Council, the Directive's strengthened rules "reflect the need for the EU to adapt its legislation to take account of the development of technology and other means at the disposal of criminals."[76]

In general, the Directive's scope is extended by reducing the cash payment threshold that triggers reporting obligations from EUR 15,000 to EUR 10,000, by including providers of gambling services within its scope, and by including tax crimes as new predicate offenses. The new framework reinforces the sanctioning powers of the competent authorities,[77] and the Directive stipulates a maximum administrative pecuniary sanction of up to twice the amount of the benefit derived from the breach where such benefit can be determined, or up to EUR 1 million.[78] In addition, the fourth AML Directive incorporates new provisions on data protection. Besides these general changes, a few specific issues are worth mentioning.

First, risk-assessments are required at several different levels. At the EU level the Commission is obliged—at least biennially—to assess the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.[79] The Member States in turn, shall assess the risks affecting them, including any data protection concerns.[80] Member States shall also ensure that obliged entities make risk assessments relating to their customers, countries or geographic areas, products, services, transactions, or delivery channels, all proportionate to the nature and size of the obliged entities.[81]

Second, there are tougher rules on customer due diligence (CDD), which require that banks and other relevant entities have in place adequate controls and procedures so that they know their customers and understand the nature of their customers' businesses. To the benefit of those involved, these rules have been clarified. As under the previous Directives, relevant entities can take simplified measures where risks are demonstrated to be lower,[82] but are required to take enhanced measures where the risks are greater,[83] including specific

---

[76] Press Release, European Council, Money Laundering: Council Approves Strengthened Rules (Apr. 20, 2015), www.consilium.europa.eu/en/press/press-releases/2015/04/20-money-laundering-strengthened-rules.

[77] Els De Busser & Cornelia Riehle, *Money Laundering: Fourth Anti Money Laundering Directive Released*, 1 EUCRIM 6 (2013).

[78] Fourth AML Directive, *supra* note 5, art. 59(2)(e) (not amended by the fifth AML Directive).

[79] *Id.,* art. 6(1) (not amended by the fifth AML Directive).

[80] *Id.*, art. 7(1) (not amended by the fifth AML Directive).

[81] *Id.*, art. 8(1) (not amended by the fifth AML Directive).

[82] *Id.*, art. 15–17 (not amended by the fifth AML Directive); *Id.*, Annex II (slightly amended by the fifth AML Directive).

[83] *Id.*, art. 18–24, (will be partly amended by the fifth AML Directive, including the insertion of the new articles 18a and 20a).

provisions on politically exposed persons (PEPs) at domestic level, and PEPs working for international organizations.[84] The new Directive, however, will prescribe minimum factors to be taken into account before applying simplified measures, and obliged entities need to prove why they have considered the risk to be low.

Third, in order to enhance transparency, specific provisions on the beneficial ownership of companies have been introduced. Information about beneficial ownership will be stored in a central register accessible to competent authorities, FIUs, entities required to take CDD measures, and other persons with a legitimate interest.[85] Such access to information needs to be in accordance with data protection rules and may be subject to online registration and the payment of a fee, not exceeding the administrative costs of obtaining the information.[86] This section will be replaced by the fifth AML Directive, and in the future, Member States may, under conditions to be determined in national law, provide for access to additional information enabling the identification of the beneficial owner. That additional information shall include at least the date of birth or contact details in accordance with data protection rules. According to recital 14, access to accurate and up-to-date information on the beneficial owner is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. In addition, new rules on traceability of fund transfers have been introduced.

Fourth, with the introduction of the fourth AML Directive, there will be more cooperation between national authorities. Of central importance, the role of national FIUs is to receive, analyze the exchange, and disseminate reports raising suspicions of money laundering or terrorist financing to competent authorities in order to facilitate their cooperation.[87] In this respect, the FIUs have been given strengthened powers to identify and follow suspicious transfers of money and facilitate exchange of information.[88] They now have the access to financial, administrative, and law enforcement information and are empowered to take early action if requested from the law enforcement authorities. According to recital 58, Member States should in particular ensure that their FIUs exchange information freely,

---

[84] *Id.* art. 20–23 (with a new article 20a inserted by the fifth AML Directive).

[85] *Id.*, art. 30 (will be amended by the fifth AML Directive).

[86] *Id.*, art. 30(5) para. 2 (will be amended by the fifth AML Directive).

[87] *Id.*, art. 32(3) (not amended by the fifth AML Directive).

[88] *See also* Council Decision 2000/642/JHA of 17 October 2000 Concerning Arrangements for Cooperation Between FIUs of the Member States in Respect of Exchanging Information, 2000 O.J. (L 271) 4 (the Commission also plans to update); European Commission, *Report on the Application of the Third Anti-Money Laundering Directive: Frequently Asked Questions*, MEMO/12/246 (Apr. 11, 2012) http://europa.eu/rapid/press-release_MEMO-12-246_en.htm?locale=en.

spontaneously or upon request, with third-country FIUs, having regard to Union law and to the principles relating to information exchange developed by the Egmont Group of Financial Intelligence Units.[89]

Despite the internal market legal basis, the wider regulatory framework can therefore be said to have changed from a predominantly single market context via criminal law concerns to the fight against organized crime, terrorist financing, and an internal security context based on the risk-based approach. The main focus of the global and regional EU measures based on the risk-based approach is, however, still set on preventive measures, whereas AML control is still a matter for national jurisdictions and the developing framework of international cooperation among judicial and law enforcement authorities. It remains to be seen if the proposal for an AML Criminal Law Directive will be adopted that would expand the current EU focus from prevention to control of money laundering and terrorist financing. Meanwhile, Member States are obliged to implement the fourth AML Directive,[90] to which changes have already been adopted by the text of the fifth AML Directive signed on May 30, 2018. It will enter into force twenty days after its publication in the Official Journal (Article 5), and the Member States need to implement its provision eighteen months thereafter (Article 4).[91]

3. Implementing the Action Plan for Strengthening the Fight Against Terrorist Financing

About two years earlier, on July 5, 2016, the European Commission adopted the proposal to amend the fourth AML Directive and Directive 2009/101. The latter established the European Central Platform interconnecting Member States' central registers holding beneficial ownership information.[92] The idea behind the amendments was to reinforce the preventive framework against money laundering,[93] in particular by addressing emerging

[89] Egmont Group of Financial Intelligence Units Charter (July 2013) https://egmontgroup.org/en/document-library/8.

[90] Fourth AML Directive, *supra* note 5, art. 66–67 (Article 6 will be amended by the fifth AML Directive.).

[91] *See also* Bergström 2018b, *supra* note 2; Bergström 2018a, *supra* note 2.

[92] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on Coordination of Safeguards Which, for the Protection of the Interests of Members and Third Parties, are Required by Member States of Companies Within the Meaning of the Second Paragraph of Article 48 of the Treaty, with a View to Making Such Safeguards Equivalent 2009 O.J. (L 258) 11.

[93] *The Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, COM (2016) 450 final (July 5, 2016) (for the procedure, see http://eur-lex.europa.eu/procedure/EN/2016_208).

risks and increasing the capacity of competent authorities to access and exchange information.[94]

These amendments aim at ensuring a high level of safeguards for financial flows from high-risk third countries, enhancing the access of FIUs to information, including centralized bank account registers, and tackling terrorist financing risks linked to virtual currencies and pre-paid cards. In this respect, this recently adopted fifth AML Directive takes a stricter approach to the problem of effectively countering money laundering and terrorist financing and focuses on new channels and modalities of transferring illegal funds to the legal economy, such as virtual currencies and money exchange platforms.

The proposal was a coordinated action with the G20 and the OECD, aiming at tackling tax evasion by both legal and natural persons in order to establish a fairer and more effective tax system. In this respect, it formed part of a wider EU effort to improve tax transparency and tackle tax abuse.[95] About five months after the Commission proposal, on December 19, 2016, the Council adopted a compromise text on the proposal aiming at amending the AML Directive, Directives 2009/138/EC (Solvency II), [96] and 2013/36/EU, but not Directive 2009/101, focusing mainly on AML and terrorist financing. [97] Although the purpose of fighting tax evasion is no longer explicitly mentioned, tools that were designed to achieve that purpose remain, although somewhat modified.[98] Set in a broader picture, this initiative was the first proposal to enforce the Action Plan for Strengthening the Fight Against Terrorist Financing,[99] which was adopted by the Commission on February 2, 2016 to better counter

---

[94] *See generally* Bergström 2018b, *supra* note 2.

[95] Press Release, European Commission, Fair Taxation: The Commission Sets Out Next Steps to Increase Tax Transparency and Tackle Tax Abuse (July 5, 2016), http://europa.eu/rapid/press-release_IP-16-2354_en.htm.

[96] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the Taking-up and Pursuit of the Business of Insurance and Reinsurance (Solvency II) (recast), 2009 O.J. (L 335) 1. Solvency II is the new, risk-based supervisory framework for the insurance sector that entered into effect on 1 January 2016.

[97] *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, COM (2016) 450 final (Dec. 19, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15605_2016_INIT&from=EN.

[98] Council of the European Union, Presidency Compromise Text (Dec. 13, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15468_2016_INIT&from=EN (last visited Apr. 8, 2017). For the procedure, see http://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52016PC0450&qid=1491076566465.

[99] *Action Plan for Strengthening the Fight Against Terrorist Financing*, *supra* note 4.

the financing of terrorism, and to ensure increased transparency of financial transactions following the so-called "Panama Papers" revelations.[100]

Nevertheless, the proposed amendments have been criticized by the Data Protection Agency for introducing other policy purposes than countering money laundering and terrorist financing that do not seem clearly identified: Processing personal data collected for one purpose for another, completely unrelated purpose. This infringes on the data protection principle of purpose limitation and threatens the implementation of the principle of proportionality. The amendments, in particular, raise questions as to why certain forms of invasive personal data processing, acceptable in relation to AML and the fight against terrorism, are necessary out of those contexts and whether these invasive data processing are proportionate.[101]

The Data Protection Agency also criticizes the proposed amendments due to the lack of proportionality, in particular concerning the broadened access to beneficial ownership information by both competent authorities and the public as a policy tool to facilitate and optimize enforcement of tax obligations. The Data Protection Agency sees, "in the way such solution is implemented, a lack of proportionality, with significant and unnecessary risks for the individual rights to privacy and data protection."[102]

Eventually, on May 14, 2018, after almost two years of negotiations and counterproposals, the European Parliament and the Council adopted the fifth AML Directive. It was signed on May 30, 2018 and will enter into force twenty days after its publication. Member States will then have up to eighteen months to transpose the new provisions into their national legislation.[103]

D. Conclusions

---

[100] *Communication from the Commission to the European Parliament and the Council: Communication on Further Measures to Enhance Transparency and the Fight against Tax Evasion and Avoidance*, COM (2016) 451 final*; see also* European Commission, *Commission Strengthens Transparency Rules to Tackle Terrorism Financing, Tax Avoidance and Money Laundering* (July 5, 2016) http://europa.eu/rapid/press-release_IP-16-2380_en.htm.

[101] European Data Protection Supervisor, Summary of the Opinion of the European Data Protection Supervisor on a Commission Proposal Amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to Beneficial Ownership Information and Data Protection Implications, 2017 O.J. (C 85) 3.

[102] *Id.*

[103] Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU (May 30, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:PE_72_2017_REV_1.

Despite all assumptions and suggestions that the current EU AML framework is mainly administrative in character, there is not a clear line between administrative and criminal law and sanctions, not least since national laws and EU law are intertwined and interrelated. This may have detrimental effects concerning procedural safeguards and fundamental rights protection—for example if sanctions are in fact criminal rather than administrative in character, or if the different solutions chosen in different Member States, lead to variations in fundamental rights protection throughout the European Union.

So far, it is mainly the responsibility of the Member States to ensure that the parallel systems of administrative and criminal law sanctions do not breach fundamental rights including the principle of *ne bis in idem*, the rules on privacy and data protection, and the principle of proportionality. EU Law measures may, however, by themselves infringe fundamental rights. Processing personal data collected for one purpose for another, completely unrelated purpose infringes on the data protection principle of purpose limitation and threatens the implementation of the principle of proportionality. The Data Protection Supervisor—in particular concerning the proposed amendments to the fourth AML Directive—raised questions as to why certain forms of invasive personal data processing, acceptable in relation to AML and the fight against terrorism, are necessary out of these contexts and whether they are proportionate. Such issues need to be evaluated against national human rights catalogues, the European Convention of Human Rights, and the EU Charter of Fundamental Rights. This is even more important when dealing with criminal, rather than purely administrative, law provisions and sanctions, which might necessitate further legal analysis.

Articles

Is It Time to Reform the Counter-terrorist Financing Reporting Obligations? On the EU and the UK System

By Nicholas Ryder *

Abstract

This Article critically considers the effectiveness of the European Union's (EU) counter-terrorist financing (CTF) strategies. In particular, it concentrates on the use of financial intelligence gathered from the submission of suspicious activity reports (SARs) by reporting entities to Member States Financial Intelligence Units (FIU). The Article identifies a series of weaknesses in the United Kingdom's (UK) reporting regime: Defensive reporting, increased compliance costs, and the definition of suspicion. It concludes by making a series of recommendations that are aimed at improving the effectiveness of the EU and UK CTF reporting obligations.

* Dr. Ryder is a Professor in Financial Crime at Bristol Law School and Faculty of Business and Law at the University of the West of England, Bristol.

A. Introduction

The European Union is suffering from the second decade of the most intense wave of international terrorism since the 1970s. Within this recent wave, nation states have been increasingly subjected to terrorist attacks. For example, since 2016 there have been terrorist attacks in France, Belgium, Germany, Sweden, Spain, Turkey, the United Kingdom, Finland, and Russia. These terrorist attacks have three common themes: Evidence of a sophisticated terrorist support network, the use of low capability weapons, and inexpensive acts of terrorism. This Article focuses on the last of these three themes.

The al-Qaeda terrorist attacks in September 2001 resulted in the introduction of a wealth of legislative and innovative enforcement provisions designed to tackle terrorism and its financing. These measures were heavily influenced by the declaration of the War on Terrorism by President George Bush and the UN's introduction of several Security Council Resolutions that sought to tackle international acts of terrorism. The terrorist attacks acted as a galvanizing factor for both the international community and the many nation states who had previously neglected to tackle the threat posed by terrorist financing. Therefore, for the purpose of this Article, the most significant part of the War on Terror is the Financial War on Terrorism.

This Article is divided into three parts. The first section concentrates on the anti-money laundering (AML) legislative measures of the United Nations (UN), the EU, and the soft law Recommendations of the Financial Action Task Force (FATF). The section highlights how the AML reporting obligations focused on the proceeds of drug trafficking offences and not terrorism. This approach has been categorized as a profit-driven reporting model directed at targeting the proceeds of financial crime. The second section moves on to highlight the influence that the terrorist attacks on September 11, 2001, (9/11) had on extending the profit-reporting model to the financing of terrorism. This second section illustrates that the profit reporting model is inappropriate when applied to the financing of terrorism. Accordingly, the section is further divided into two sub-parts. The first sub-part illustrates that terrorists may exploit an extensive array of financial mechanisms to circumvent CTF reporting mechanisms. The second sub-part notes the increasing threat posed by inexpensive acts of terrorism to further highlight the weaknesses of the CTF reporting obligations. Here, specific reference is made to several inexpensive terrorist attacks that have taken place within the EU. The third section of the Article focuses on the United Kingdom (UK) and critically assesses the effectiveness of its CTF reporting obligations.

I. The US Financial War on Terror

President George Bush initiated the Financial War on Terrorism on September 24, 2001,[1] with his solemn declaration: "We will starve terrorists of funding, turn them against each other, rout them out of their safe hiding places, and bring them to justice."[2] The Financial War on Terrorism resulted in a seismic alteration in the financial crime strategies of an international community that had previously concentrated on money laundering. This approach, as outlined below, was wholly inadequate for dealing with how the 9/11 terrorists were financed. The National Commission on the Terrorist Attacks Upon the United States noted that "the 19 operatives were funded by al-Qaeda, either through wire transfers or cash provided by [Khalid Sheikh Mohammed] . . . ."[3] The National Commission added that some of the terrorists received wire transfers ranging between $5,000 to $70,000[4] and added that Khalid Sheikh Mohammed had "delivered a large amount of cash, perhaps $120,000, to the plot facilitator Abdul Aziz Ali in Dubai . . . ."[5] Abdul Aziz Ali sent several bank-to-bank transfers—including transactions for $10,000, $20,000, and $70,000—to bank accounts at the SunTrust Bank in Florida belonging to two of the terrorists: Marwan al Shehhi and Muhamad Atta.[6] The amount of each of these transactions is important because US deposit taking institutions are legally required to complete and submit a Currency Transaction Report (CTR) to the Financial Crime Enforcement Network (FinCEN) for all financial transactions of $10,000 or more. The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act, or Bank Secrecy Act of 1970 imposes this obligation.[7] SunTrust Bank was thus required to submit the CTRs to FinCEN and file a SAR for any wire transfer that they deemed to be suspicious.[8] Nevertheless, the National Commission found that "no financial institution [had] filed a Suspicious Activity Report (SAR) in connection with any transaction of any of the 19 hijackers before 9/11" and that "[e]ven in hindsight, there [was] nothing . . . to indicate that any SAR should have been filed or [that] the hijackers

[1] *See* Press Release, President George Bush, President Freezes Terrorists' Assets (Sep. 24, 2001) (on file with author).

[2] Press Release, Office of the Press Secretary, Fact Sheet on Terrorist Financing Executive Order (Sep. 24, 2001), (on file with author). It is not the purpose of this Article to provide a detailed commentary on the Financial War on Terrorism. For a more detailed examination on the subject please see NICHOLAS RYDER, THE FINANCIAL WAR ON TERROR: A REVIEW OF COUNTER-TERRORIST FINANCING STRATEGIES SINCE 2001 30–62 (2015).

[3] NAT'L COMMISSION ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 172 (2004) [hereinafter THE NATIONAL COMMISSION].

[4] JOHN ROTH, DOUGLAS GREENBURG & SERENA WILLE, NAT'L COMMISSION ON TERRORIST ATTACKS UPON THE U.S, MONOGRAPH ON TERRORIST FINANACING 53 (2004) [hereinafter THE MONOGRAPH].

[5] *Id.* at 26.

[6] THE MONOGRAPH, *supra* note 4, at 132.

[7] 31 U.S.C. § 5311 (2012).

[8] The Annunzio-Wylie Anti-Money Laundering Act of 1992, § 1517(b), Pub. L. No. 102–550, 106 Stat. 3762 (1992) (introducing the obligation to submit a suspicious activity report).

[should have] otherwise [been] reported to law enforcement."[9] This conclusion is perhaps best explained by the inherent inadequacy of the Bank Secrecy Act of 1970 in curtailing terrorist financing. The Bank Secrecy Act of 1970 was not meant to tackle the problem terrorist financing and was instead introduced to "build a system to combat organized crime and white-collar crime and to deter and prevent the use of secret foreign bank accounts for tax fraud."[10]

Prior to the terrorist attacks, terrorist financing had attracted limited attention in a number of academic studies. For example, researchers in the US had concentrated their efforts on assessing the prevention of other types of financial crimes, including money laundering [11] and fraud.[12] The evolution of the US literature on money laundering can be traced and presented in chronological order through the enactment of legislation: the Bank Secrecy Act of 1970,[13] the Racketeer Influence and Corrupt Organization Act of 1970,[14] the Money Laundering Control Act of 1986,[15] the Annunzio-Wylie Anti-Money Laundering Act of 1992,[16] and the USA Patriot Act of 2001.[17] A similar picture can be presented of the approach adopted by researchers of financial crime policies and legislative provisions of the EU. A plethora of research has been published on the EUs AML Directives,[18] the EU's counter-fraud

[9] THE MONOGRAPH, *supra* note 4, at 141.

[10] *Hearings Before the Subcomm. on Fin. Inst. of the Comm. on Banking and Currency*, 91st Cong. 170 (1970) (statement of Eugene Rossides, Former Assistant Secretary, Treasury for Enforcement and Operations).

[11] *See generally* Mike Levi & Peter Reuter, *Money Laundering*, 34 CRIME & JUST. 289 (2006).

[12] *See generally* Ellen Podgor, *Criminal Fraud*, 48 AM. U. L. REV. 729 (1999).

[13] *See generally* Sarah Hughes, *Policing Money Laundering through Funds Transfers: A Critique of Regulation under the Bank Secrecy Act*, 67 IND. L.J. 283 (1992).

[14] *See generally* Barry Tarlow, *RICO Revisited*, 17 GA. L. REV. 291 (1983).

[15] *See generally* Joshua Schwartz, *Liability for Structured Transactions under the Currency and Foreign Transactions Reporting Act: A Prelude to the Money Laundering Control Act of 1986*, 6 ANN. REV. BANKING L. 315 (1987).

[16] *See generally* Matthew Hall, Note, *An Emerging Duty to Report Criminal Conduct: Banks, Money Laundering, and the Suspicious Activity Report*, 84 KY. L. J. 643 (1995–1996).

[17] *See generally* Andres Rueda, *International Money Laundering Law Enforcement and the USA Patriot Act of 2001*, 10 MICH. ST. U. DET. C. OF L. J. OF INT'L L. 141 (2001).

[18] *See generally* Valsamis Mitsilegas & Bill Gilmore, *The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in Light of Evolving Global Standards*, 56 INT'L & COMP. L.Q. 119 (2007).

measures under the management of the European Anti-Fraud Office,[19] market manipulation,[20] insider dealing, [21] and market abuse.[22]

The terrorist attacks in September 2001 resulted in the publication of numerous interesting studies on the threat posed by the financing of terrorism. For example, commentators began to take an interest in the funding models used by al-Qaeda,[23] the association between misapplied charitable donations and terrorists,[24] the interpretation of the Financial War on Terrorism, and the efforts by the international community to tackle terrorist financing.[25] More recently, scholars have concentrated on the funding streams of Islamic State of Iraq and the Levant.[26] While the association between the EU and the financing of terrorism has attracted some academic commentary, a large proportion of it has concentrated on other types of financial crimes and only a small number of studies have reviewed the EUs stance on terrorist financing.[27] Normark and Ranstrop noted that none of the published research on terrorist financing in the EU has presented a "high-resolution picture of the sources of funding for terrorist plots."[28] Therefore, this Article seeks to provide an enhanced understanding of the weaknesses of the EU's CTF reporting obligations, the continued threat posed by inexpensive acts of terrorism, and the extensive array of sources that fund acts of terrorism.

B. International Financial Crime Legislative Measures: The Profit Model

[19] *See generally* Xavier Groussot & Ziva Popov, *What's Wrong with Olaf—Accountability, Due Process and Criminal Justice in European Anti-Fraud Policy*, 47 COMMON MKT. L. REV. 605 (2010).

[20] *See generally* R.C.H. ALEXANDER, INSIDER DEALING AND MONEY LAUNDERING IN THE EU: LAW AND REGULATION (2007).

[21] *See generally* JANET AUSTIN, INSIDER TRADING AND MARKET MANIPULATION INVESTIGATING AND PROSECUTING ACROSS BORDERS (2017).

[22] *See generally* JERRY MARKHAM, LAW ENFORCEMENT AND THE HISTORY OF FINANCIAL MARKET MANIPULATION (2014).

[23] *See generally* ROHAN GUNARATNA, INSIDE AL QAEDA: GLOBAL NETWORK OF TERROR (2002).

[24] *See generally* JIMMY GURULE, UNFUNDING TERROR: THE LEGAL RESPONSE TO THE FINANCING OF GLOBAL TERRORISM (2008).

[25] *See generally* RYDER, *supra* note 2.

[26] *See generally* RYDER, *supra* note 2.

[27] *See* THE NATIONAL COMMISSION, *supra* note 3.

[28] MAGNUS NORMARK & MAGNUS RANSTROP, UNDERSTANDING TERRORIST FINANCE- MODUS OPERANDI AND NATIONAL CTF REGIMES 8 (2015).

I. The Profit Model

Before 9/11, international efforts against financial crime focused on tackling the laundering of the proceeds from the illegal manufacturing, distribution, and sale of narcotic substances. These measures largely originate from the US led War on Drugs, a term commonly associated with a series of controversial legislative measures introduced by President Richard Nixon in the 1970s.[29] The UN adopted these legislative measures in the form of the Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (the Vienna Convention of 1988). This was followed by the UN Convention Against Transnational Organized Crime of 2000 (the Palermo Convention of 2000) and extended by the UN Convention Against Corruption of 2003.[30] Similarly, the EU introduced the Money Laundering Directives of 1993 and 2001 to tackle the laundering of narcotic substances.[31] The FATF published its first set of money laundering Recommendations in 1990.[32] Collectively, these measures were described as a "major breakthrough in attacking the benefits derived from drug trafficking activities and . . . a forceful endorsement of the notion that attacking the profit motive is essential if the struggle against drug trafficking is to be effective."[33] Nelen stated that "by dismantling their organi[z]ations financially, criminals must be hit at their supposedly more vulnerable spot: [T]heir assets."[34] Nevertheless, the profit driven model is not appropriate when used against the financing of terrorism. The financial process adopted by terrorists to accumulate funds is different from the processes adopted by money launderers. Terrorist financing is more commonly referred to as reverse money laundering, where clean or legitimate money is transformed into dirty money that is then funneled to finance acts of terrorism. Comparatively, regular money laundering involves the conversion of dirty or illegal money into clean money via its laundering through three recognized phases: Placement, layering, and integration. Therefore, the extension of the profit model to tackle the financing of terrorism is inappropriate.

---

[29] *See generally* DAN BAUM, SMOKE AND MIRRORS: THE WAR ON DRUGS AND THE POLITICS OF FAILURE (1997).

[30] *See* NICHOLAS RYDER, MONEY LAUNDERING—AN ENDLESS CYCLE? A COMPARATIVE ANALYSIS OF THE ANTI-MONEY LAUNDERING POLICIES IN THE UNITED STATES OF AMERICA, THE UNITED KINGDOM, AUSTRALIA AND CANADA 8–39 (2012) (providing a more detailed discussion of international anti-money laundering legislative provisions).

[31] *See* Directive 91/308, of the European Council on the Prevention of the Use of the Financial System to Launder Money, 1993 O.J. (L 166); Directive 2001/97/EC, of the European Parliament and of the Council of 4 December 2001 Amending Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering, 2001 O.J. (L 344).

[32] *See* FINANCIAL ACTION TASK FORCE, THE 40 RECOMMENDATIONS (2004).

[33] D.W. Sproule & Paul St-Denis, *The UN Drug Trafficking Convention: An Ambitious Step*, 27 CANADIAN Y.B. OF INT'L L. 263, 281–82 (1990).

[34] Hans Nelen, *Hit Them Where it Hurts Most? The Proceeds-of-Crime Approach in the Netherlands*, 41 CRIME, L. & SOC. CHANGE 517 (2004).

Nonetheless, the profit driven model contains a number of preventative measures that require the reporting entities of signatory states to implement a series of pre-placement money laundering reporting obligations. For example, Article 7 of the Palermo Convention of 2000 provides that each signatory should implement a far-reaching AML regime for a wide range of reporting entities that are vulnerable to money laundering. The scheme should include requirements for customer identification, record keeping, and the reporting of suspicious transactions.[35] Furthermore, it provides that signatories shall "consider the establishment of a financial intelligence unit to serve as a national center for the collection, analysis and dissemination of information regarding potential money laundering."[36] Additionally, the FATF Recommendations outline a number of preventative measures aimed at tackling the threat posed by money laundering.[37] For example, Recommendations 10 and 11 relate to customer due diligence and record keeping obligations.[38] Recommendations 12 to 16 provide additional measures for specific customers and activities, which include politically exposed persons, correspondent banking, money or transfer value services, new technology, and wire transfers.[39] Recommendations 17 to 19 deal with reliance, control, and financial groups, while Recommendations 20 and 21 deal with the reporting of suspicious transactions and the criminal offense of "tipping off."[40]

The EU profit-reporting model began in the 1970s when the European Council's European Committee on Crime Problems created a Select Committee to investigate the illegal transfer of proceeds from crime between member states. The Select Committee made a recommendation stipulating that banks should ensure that identity checks are undertaken on all clients when an account is opened or money deposited.[41] This recommendation, however, was not fully implemented. Another set of AML measures were proposed when the European Ministers of Justice asked the European Committee on Crime Problems to create a stance regarding the proceeds of drug trafficking that paralleled the one adopted

[35] G.A. Res. 55/25, United Nations Convention Against Transnational Organized Crime art. 7(1)(a) (Jan. 8, 2001)..

[36] *Id.* art. 7(1)(b) (extending these measures through Article 14 of the United Nations Convention Against Corruption).

[37] FINANCIAL ACTION TASK FORCE, THE FATF RECOMMENDATIONS: INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 12–17 (2012).

[38] *Id.* at 14–15.

[39] *Id.* at 16–17.

[40] *Id.* at 18–19.

[41] Kern Alexander, *Multi-National Efforts to Combat Financial Crime and the Financial Action Task Force*, 2 J. OF INT'L FIN. MKTS. 182 (2000).

by the UN.[42] It was not until the introduction of the First Money Laundering Directive that there was a coordinated effort to impose the profit model on Member States.[43] The Directive contained several important features based upon 40 recommendations from the FATF which included the need to ensure client identification, the examination and reporting of suspicious transactions, indemnities for good faith reporting of suspicious transactions, storage of identification records extending for five years beyond the end of the client relationship, co-operation with the authorities, and the adoption of adequate internal procedures and training programs. Nevertheless, the First Money Laundering Directive concentrated on combating the laundering of drug proceeds though the financial sector instead of combating the financing of terrorism. At the start of the new millennia, it became clear that the scope of the First Directive was too narrow.[44] Accordingly, the EU introduced a broader Second Money Laundering Directive that expanded the list of predicate offences for which the suspicious transaction reports were compulsory. This new list ranged from drug trafficking offences to all serious criminal offences.

II. The Influence of 9/11

In 1994, the UN adopted the term "terrorist financing" through its Declaration to Eliminate International Terrorism.[45] Subsequently, a General Assembly Resolution called for Member States to "take steps to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations."[46] Nevertheless, the scope of this Resolution was limited to terrorist bombings and nuclear terrorism. The al-Qaeda bombings of the US embassies in Kenya and Tanzania resulted in a re-think causing the passing of Resolutions A/RES/52/165 and A/RES/53/108, which in turn highlighted the need to tackle the financing of terrorism.[47] Consequently, the International Convention for the Suppression of the Financing of Terrorism of 1999 criminalized the collection or distribution of funds for the purposes of supporting an act of terrorism.[48] Despite the importance of preventing terrorist financing, only 41 UN Member States signed the Convention, with only 6 ratifying

[42] *Id.*

[43] *See* Directive 91/308, of the European Council on the Prevention of the Use of the Financial System to Launder Money, 1993 O.J. (L 166).

[44] *See* Mitsilegas, *supra* note 18.

[45] G.A. Res. 49/60, Annex (Dec. 9, 1994).

[46] G.A. Res. 51/210 (Dec. 17, 1996); *see also* G.A. Res. 45/121, Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Dec. 14, 1990).

[47] G.A. Res. 52/165, para. 3 (Dec. 15, 1997); G.A. Res. 53/108, para. 11 (Jan. 26, 1999).

[48] International Convention for the Suppression of the Financing of Terrorism, arts. 2(1)(a)(b), 4, Dec. 9, 1999, 2178 U.N.T.S. 197.

it.[49] Additionally, it is also important to consider UN Security Council Resolution 1267, which created a sanctions regime that targeted individuals and entities associated with al-Qaeda, Osama bin Laden, and/or the Taliban. Another important measure was UN Security Council Resolution 1269, which asked nation states to implement the UN's anti-terrorist conventions. More specifically, the Resolution provided that countries should, *inter alia*:

> [P]revent and suppress in their territories through all lawful means the preparation and financing of any acts of terrorism; deny those who plan, finance or commit terrorist acts safe havens by ensuring their apprehension and prosecution or extradition; take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for the purpose of ensuring that the asylum-seeker has not participated in terrorist acts; [and] exchange information in accordance with international and domestic law, and cooperate on administrative and judicial matters in order to prevent the commission of terrorist acts . . . .[50]

The terrorist attacks of 9/11 led to a monumental shift in attitudes towards the detection and prevention of terrorist financing. The International Convention served as a precedent for UN Security Council Resolution 1373. This Resolution imposes four obligations on members of the UN:[51] (i) it specifically requires states to thwart and control the financing of terrorism; (ii) it criminalizes the collection of terrorist funds in states territory; (iii) it freezes funds, financial assets, and economic resources of people who commit or try to commit acts of terrorism; and (iv) it prevents any nationals within their territories from providing funds, financial assets, and economic resources to people who seek to commit acts of terrorism.[52] This UN Security Council Resolution is the most important international legislative measure that seeks to prevent terrorist financing.[53] In contrast to the 1999 Convention, all 191 Member States submitted reports to the UN Security Council Counter-Terrorism Committee on the actions they had taken to suppress international terrorism, which included how they

---

[49] *See* Angela Leong, *Chasing Dirty Money: Domestic and International Measures Against Money Laundering*, 10 J. MONEY LAUNDERING CONTROL 145 (2007).

[50] S.C. Res. 1269, para. 4 (Oct. 19, 1999).

[51] *See* CABINET OFFICE, THE UK AND THE CAMPAIGN AGAINST INTERNATIONAL TERRORISM—PROGRESS REPORT 24 (2002).

[52] S.C. Res. 1373, para. 1 (Sept. 28, 2001).

[53] *See* Anders Kruse, *Financial and Economic Sanctions—From a Perspective of International Law and Human Rights*, 12 J. FIN. CRIME 218 (2005).

have gone about blocking terrorist finances as required by Resolution 1373.[54] Nevertheless, in 2004, the European Commission concluded that it was necessary to introduce a Third Money Laundering Directive[55] to extend the scope of its reporting obligations to include the financing of terrorism.[56] The Third Directive came into force in December 2005 and Member States were required to implement it by December 2007. In June 2017, a Fourth Money Laundering Directive repealed the Third Directive following the publication of a new set of FATF Recommendations in 2012.[57] The Fourth Directive introduced several important amendments that included an alteration in the risk-based approach, new rules to deal with the threat posed by electronic money, registers for ultimate beneficial owners, and an improved sanctions regime. What becomes clear after briefly highlighting the response to the terrorist attacks in September 2001 is that the UN, FATF, and EU have continued to mistakenly use the profit-driven reporting model to tackle the financing of terrorism. The Article has thus far illustrated how the Bank Secrecy Act of 1970 was unsuitable to prevent the 9/11 terrorists from acquiring the necessary finances via several wire transfers. The next Section of the Article provides more evidence demonstrating that the profit reporting model is inappropriate for tackling the financing of terrorism.

C. Sources of Terrorist Financing and Inexpensive Terrorism

The first part of this Section provides a commentary on the extensive number of sources that terrorists may exploit to fund their activities. Each of these sources has been designed to avoid having to interact with reporting entities. The second part of this Section concentrates on the increasing number of terrorist attacks that can be classified as inexpensive acts of terrorism.

I. Sources of Terrorist Financing

Preventing terrorist financing is difficult because of the large number of mechanisms that may be used to fund acts of terrorism.[58] Traditionally, terrorists have relied on two sources

[54] THE WHITE HOUSE, PROGRESS REPORT ON THE GLOBAL WAR ON TERRORISM 6 (2003).

[55] Directive 2005/60/EC, of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, 2005 O.J. (L 309) (repealed).

[56] Richard Alexander, *Reputational Issues Arising Under the EU Third Money Laundering Directive*, 27 COMPANY LAW. 373 (2006).

[57] Directive 2015/849, of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, 2015 O.J. (L 141) (EU).

[58] *See* Matthew Levitt, *Stemming the Flow of Terrorist Financing: Practical and Conceptual Challenges*, 27 FLETCHER F. WORLD AFF. 63, 64 (2003).

of funding: State and private sponsors.[59] State sponsored terrorism refers to nation states providing logistical and financial support to terrorist organizations.[60] Since the terrorist attacks in 2001, state-sponsored acts of terrorism have declined and the trend has shifted to terrorists receiving funding from private sponsors or donors.[61] As acknowledged by the official report on the terrorist attacks on London on July 7, 2005, terrorist organizations have also become increasingly self-sufficient.[62] Terrorists generate funds through a broad spectrum of measures including kidnappings , robberies, and drug trading.[63] Other sources include counterfeiting[64] and the sale of conflict diamonds.[65] Terrorists have also acquired funding through traditional criminal activities, including benefit and credit card fraud, identity theft, the sale of counterfeit goods, and drug trafficking.[66] The wide range of sources available to terrorists is illustrated by the activities of ISIL, who have exploited four funding streams: The control of oil reserves, kidnappings, foreign and private financial benefactors, and antiquities. Another terrorist group that utilizes a vast array of sources is Al Shabaab, a Somali-based militant Islamist group that has obtained funding from the illegal smuggling of ivory.[67] Al Shabaab have "earned more than $25 million a year from illicit exports of charcoal to Gulf Arab states and from taxing the trucking of charcoal to the Somali ports of Kismayu and Barawe."[68] The UN reported that Al Shabaab receives a majority of its funding via charcoal exports and the illegal importation of contraband sugar.[69]

---

[59] Ilias Bantekas, *The International Law of Terrorist Financing*, 97 AM. J. OF INT'L L. 315 (2003).

[60] Alison Chase, *Legal Mechanisms of the International Community and the United States Concerning State Sponsorship of Terrorism*, 45 VA. J. INT'L L. 41 (2004).

[61] *See* Mark Basile, *Going to the Source: Why Al Qaeda's Financial Network is Likely to Withstand the Current War on Terrorist Financing*, 27 STUD. IN CONFLICT & TERRORISM 183 (2004).

[62] HOUSE OF COMMONS, REPORT OF THE OFFICIAL ACCOUNT OF THE BOMBINGS IN LONDON ON 7TH JULY 2005 23 (2005).

[63] PETER ALLDRIDGE, MONEY LAUNDERING LAW 215 (2003).

[64] Peter Lowe, *Counterfeiting: Links to Organised Crime and Terrorist Funding*, 13 J. FIN. CRIME 255 (2006).

[65] GLOBAL WITNESS, BROKEN VOWS: EXPOSING THE "LOUPE" HOLES IN THE DIAMOND INDUSTRY'S EFFORTS TO PREVENT THE TRADE IN CONFLICT DIAMONDS (2003).

[66] Courtney Linn, *How Terrorists Exploit Gaps in US Anti-Money Laundering Laws to Secrete Plunder*, 8 J. MONEY LAUNDERING CONTROL 200 (2005).

[67] Vldhi Doshi, *Elephant Campaign: How Africa's 'White Gold' Funds the al-Shabaab Militants*, THE INDEPENDENT NEWSPAPER (Feb. 3, 2014), http://www.independent.co.uk/voices/campaigns/elephant-campaign/elephant-campaign-how-africas-white-gold-funds-the-alshabaab-militants-9102862.html.

[68] William Maclean, *Shabaab Finances Face Squeeze After Kenya Attack*, REUTERS (Sep. 26, 2013), http://www.reuters.com/article/2013/09/26/us-kenya-attack-shabaab-funding-idUSBRE98P05Z20130926.

[69] *See* Rep. of the Monitoring Group on Somalia and Eritrea Pursuant to Security Council Resolution 2060 (2012): Somalia, U.N. Doc. S/2013/413 (2013).

Another example of a terrorist group that has been able to exploit a wide range of sources of funding are Boko Haram. Boko Haram are funded "through black market dealings, local and international benefactors, and links to al-Qa[e]da and other well-funded groups in the Middle East."[70] The Inter-governmental Action Group against Money Laundering in West Africa noted that Boko Haram has been partly financed through private donors and misapplied charitable donations.[71] The FATF provided several examples of how Boko Haram acquires its financing including the sale of goods and other lucrative activities, business profits/logistical support, extortion of civilians through intimidation, proceeds from arms smugglers and cash couriers, and financial contributions of political leaders.[72] The prevention and detection of terrorist financing is impossible. Such difficulties are partly due to the ability of terrorists to exploit an extensive array of financial resources that necessarily lie outside of the scope of reporting mechanisms. The extension of the profit-driven reporting model is unsuitable for the financing of terrorism because it is aimed at preventing legitimate entities from accepting deposits of proceeds from criminal activities. Terrorists are unlikely to deposit funds in a heavily regulated sector that is subject to reporting obligations.

II. Cheap Terrorism

In addition to the wide array of funding avenues available to terrorists, it is also important to discuss the concept of inexpensive terrorism. The threat posed by inexpensive terrorism was identified by Her Majesty's Treasury who took the view that the "UK experience bears out the relatively low costs required for an effective terrorist attack. The Bishopsgate bomb in the City of London in 1993 caused over £1bn worth of damage to property yet cost only £3,000 to mount."[73] Another example of inexpensive terrorism was the first attack on the World Trade Center in 1993, where six people were murdered and over 1,000 were injured at an estimated cost of only $400. This terrorist attack was "less devastating . . . because of the group's limited financial resources."[74] Two years after the World Trade Center attack, Timothy McVeigh detonated a truck bomb outside of the Alfred P. Murrah Federal Building in Oklahoma City. In an interview with MSNBC, Timothy McVeigh estimated that the total costs of the attack, including the truck rental, fertilizer, nitro methane, and other costs

[70] Terrence McCoy, *Paying for Terrorism: Where Does Boko Haram Gets its Money From?* THE INDEPENDENT NEWSPAPER (June 6, 2014), http://www.independent.co.uk/news/world/africa/paying-for-terrorism-where-does-boko-haram-gets-its-money-from-9503948.html.

[71] INTER GOVERNMENTAL ACTION GROUP AGAINST MONEY LAUNDERING IN WEST AFRICA, THREAT ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING IN WEST AFRICA 94 (2010).

[72] FINANCIAL ACTION TASK FORCE, *supra* note 37.

[73] ED MOLONEY, A SECRET HISTORY OF THE IRA (2002) 291.

[74] Thomas Biersteker & Sue Eckert, *Introduction in* COUNTERING THE FINANCING OF TERRORISM 1 (Thomas Biersteker and Sue Eckert eds., 2008).

amounted to $5,000.[75] The terrorist attacks by Al Shabaab on the Westgate Mall in Kenya "cost less than $5,000 to execute, and the materials used in the Boston Marathon bombings [in 2013] reportedly cost about $500."[76] The two explosive devices used by the bombers**,** Tamerlan and Dzhokhar Tsarnaev, cost as little as $100 each.[77] In none of these terrorist attacks was there any evidence of a SAR submitted to a FIU by a reporting entity. Furthermore, the terrorist attacks in London on July 7, 2005, cost were estimated to have cost between £100 and £200.[78] Waszak estimated that "the cost of making a suicide bomb can be as low as $5, while the deployment of a suicide bomber including transportation and reconnaissance, can cost as little as $200."[79] Therefore, if the terrorist or terrorist cell is significantly self-sufficient, there is no need for them to be involved in funding activities that would lead to the submission of an SAR by a reporting entity.

More recently, there has been an increase in the number of inexpensive acts of terrorism within Members States of the EU. For example, in August 2017, a terrorist driving a van killed 13 people in Barcelona. In June 2017, one person was killed outside Finsbury Park Mosque in a terrorist attack, while terrorists killed eight others on London Bridge and Borough Market. A month before the terrorist attacks in London, 23 people were killed and 59 others were injured following a terrorist attack by a suicide bomber in Manchester. Additional terrorist attacks within the EU occurred in Paris, Stockholm, Berlin, Normandy, Nice, and Brussels. Several of these attacks have involved terrorists using a rental vehicle to target pedestrians. Of course, the relative ease of self-funding the renting of a vehicle provides further evidence that demonstrates how inexpensive forms of terrorism exploit loopholes in the profit reporting model. There are two common themes in these type of terrorist attacks: The use of low capability weapons and the relative inexpensiveness associated with such acts of terrorism. These two factors illustrate that extending the profit reporting model to tackle the financing of terrorism is unsuitable for achieving the intended goal.

C. The United Kingdom

[75] "*The McVeigh Tapes: Confessions of An American Terrorist*," NBC NEWS (Apr. 15, 2010), http://www.nbcnews.com/id/36135258/ns/msnbc_tv/#.VDJpOU10zIU.

[76] *Remarks of Under Secretary for Terrorism and Financial Intelligence David Cohen Before the Center for a New American Security on "Confronting New Threats in Terrorist Financing*," U.S. DEP'T OF TREASURY (March 4, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx.

77 Todd Wallack & Beth Healy, *Tsarnaev Brothers Appeared to Have Scant Finances*, BOSTON GLOBE (Apr. 24, 2013), http://www.bostonglobe.com/metro/2013/04/23/tsarnaev-brothers-appeared-have-scant-finances/ZbNBuN2Gcz8IOFddKDIU0N/story.html.

[78] See Jeffrey Robinson, *Brown's War Just Doesn't Add Up: You Can't Kill Terrorist With a Calculator*, THE TIMES NEWSPAPER (Feb. 14, 2006), http://www.thetimes.co.uk/tto/law/columnists/article2049933.ece.

[79] John Waszak, *The Obstacles to Suppressing Radical Islamic Terrorist Financing*, 36 CASE WESTERN RES. J. INT'L L. 673 (2004).

The UK has a long history of tackling terrorism and has accordingly introduced extensive legislation dealing with the subject of preventing the financing of terrorism. The development of the UK's terrorist related legislation is associated with the end of the eighteenth century and the start of the nineteenth century. Such legislative measures included the Explosive Substances Act of 1883, Criminal Law and Procedure (Ireland) Act of 1887, and the Civil Authorities (Special Powers) Act (Northern Ireland) of 1922.[80] One of the first terrorist financing related legislation was the Prevention of Terrorism (Temporary Provisions) Act of 1989 which criminalized terrorist financing,[81] attempted controls of terrorist financing,[82] and imposed forfeiture provisions on items used to support acts of terrorism.[83] The next legislative amendment was the Criminal Justice Act of 1993, which brought terrorist financing provisions that were in line with the anti-money laundering measures in the Drug Trafficking Offences Act of 1986. Additionally, the Criminal Justice (Terrorism and Conspiracy) Act of 1998 permitted the courts to order into forfeiture any property connected with proscribed terrorist organizations.[84] The Terrorism Act of 2000 also created a number of criminal offences relating to the financing of terrorism.[85] These were further extended by the Anti-terrorism, Crime, and Security Act of 2001; the Terrorism Act of 2006; the Counter-Terrorism Act of 2008; the Terrorist Asset-Freezing etc. Act of 2010; the Crime and Courts Act of 2013; the Serious Crime Act of 2015; the Money Laundering, Terrorist Financing, and Transfer of Funds Regulations of 2017; and the Criminal Finances Act of 2017.

I. CTF Reporting Obligations

A key part of the UK's CTF measures has been the reporting requirements on financial institutions where there is a risk of money laundering or terrorist financing. The first money laundering reporting requirements were contained in the Drug Trafficking Offences Act of 1986. The Criminal Justice Act of 1993 amended these reporting obligations after the introduction of the First Money Laundering Directive. The Proceeds of Crime Act of 2002 and the Money Laundering Regulations of 2017 have since consolidated these reporting

[80] Ben Brandon, *Terrorism, Human Rights and the Rule of Law: 120 years of the UK's Legal Response to Terrorism*, CRIM. L. REV. 981, 982 (2004).

[81] Prevention of Terrorism (Temporary Provisions) Act 1989 c. 4, § 9 (Eng.) (repealed).

[82] *Id.* §§ 9, 11.

[83] *Id.* § 13.

[84] Criminal Justice (Terrorism and Conspiracy) Act 1998 c. 40, § 4(3) (Eng.) (repealed).

[85] Terrorism Act 2000 c. 11, §§ 15–9 (Eng.).

obligations.[86] The Terrorism Act makes it a criminal offense to fail to disclose knowledge or suspicion of another person that has committed an offense under the terrorist financing criminal offences.[87] Such a failure to disclose information is identical to the offense of failing to disclose information under the Proceeds of Crime Act 2002.[88] An individual or organization who suspects that an offense has been committed under the Terrorism Act 2000 is legally required to complete a SAR. In addition to the traditional means of gathering financial intelligence via the use of SARs the Terrorism Act 2000 also contained a number of statutory measures related to financial information orders. For example, Schedule 6 of the Terrorism Act 2000 "deals with orders empowering the police to require financial institutions to supply customer information relevant to terrorist investigation."[89] An application for an order can be made by a police officer that could "require a financial institution [to which the order applies] to provide customer information for the purposes of the investigation."[90] The order could apply to "(a) all financial institutions, (b) a particular description, or particular descriptions, of financial institutions, or (c) a particular financial institution or particular financial institutions."[91] If a financial institution fails to comply with the financial information order it is guilty of a criminal offence.[92] The financial institution, however, does have a defense to breaching the financial information order when they can illustrate that "(a) that the information required was not in the institution's possession, or (b) that it was not reasonably practicable for the institution to comply with the requirement."[93] Additionally, the Terrorism Act 2000 permits the use of account monitoring orders.[94] Leong stated that an account monitoring order

> [I]s an order that the financial institution specified in the application for the order must, for the period stated in the order, provide account information of the description specified in the order to an appropriate

[86] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692 (Eng.).

[87] Terrorism Act 2000, s.19 .

[88] Proceeds of Crime Act 2002, c. 4, §§ 330–32 (Eng).

[89] Omer Elagab, *Control of Terrorist Funds and the Banking System*, 21 J. OF INT'L BANKING L. & REG. 40 (2006).

[90] Terrorism Act 2000 c. 11, sch. 6 (Eng.).

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

> officer in the manner, and at or by the time or times, stated in the order.[95]

Judges can grant an account monitoring order if they are satisfied that "(a) the order is sought for the purposes of a terrorist investigation, (b) the tracing of terrorist property is desirable for the purposes of the investigation, and (c) the order will enhance the effectiveness of the investigation."[96] When an application is made for account monitoring, the order must contain information relating to accounts of the person who is subject to the order.[97]

One of the most controversial pieces of CTF legislation is the Counter-Terrorism Act 2008. The Act "has added to those financial provisions in significant ways. The Act implements a new regime of financial directions in Schedule 7 . . . the scheme is very wide-ranging in application and effect."[98] Goldby stated that the Counter-Terrorism Act "provides new anti-money laundering and counter-terrorism financing provisions applicable to the private sector."[99] Schedule 7 of the 2008 Act provides Her Majesty's Treasury with the ability to give a direction where the FATF has requested actions to be pursued against a country in which risks of terrorist financing or money laundering are present. Furthermore, Her Majesty's Treasury is permitted to impose an action where it reasonably believes that a country poses a significant risk of terrorist financing or money laundering to the UK. Finally, Her Majesty's Treasury may impose a direction where it believes there is substantial risk to the UK posed by the development, manufacturing, or facilitation of the development of nuclear, radiological, biological, or chemical weapons. The second part of Schedule 7 outlines the class of people that may become subject to the direction, which includes people working in the financial sector. Schedule 7 of the Counter-Terrorism Act 2008 further provides the sort of obligations that can be imposed. For example, obligations can be imposed on transactions or business relationships where a person carries on business activities in the country or with the government of the country, or where the person is a resident of or incorporated in the country in which the business activities occur. Once a direction has been imposed pursuant to Schedule 7 of the Counter-Terrorism Act 2008, the recipient will be required to improve their due diligence measures. Part 5 of Schedule 7 permits the relevant enforcement agency to obtain information and part 6 permits the use of financial sanctions on those who fail to

---

[95] Angela Leong, *Financial Investigation: A Key Element in the Fight Against Organised Crime*, 27 COMPANY LAW. 219 (2006).

[96] Terrorism Act 2000 c.11, sch. 6(5) (Eng.).

[97] *Id.*

[98] Gareth Rees & Tim Moloney, *The Latest Efforts to Interrupt Terrorist Supply Lines: Schedule 7 to the Counter-Terrorism Act 2008*, CRIM. L. REV. 127 (2010).

[99] Myriam Goldby, *The Impact of Schedule 7 of the Counter-Terrorism Act 2008 on Banks and Their Customers*, 13 J. OF MONEY LAUNDERING CONTROL 352 (2010).

observe the directions. The powers of Her Majesty's Treasury under Schedule 7 of the Counter-Terrorism Act 2008 were challenged in *Bank Mellat v. HM Treasury* (No.2).[100] Here, the Supreme Court determined that the directions authorized by Her Majesty's Treasury under Schedule 7 breached Article 6 of the European Convention of Human Rights as well as the rules of natural justice.

There are a number of other weaknesses that are associated with the reporting of suspicious transactions and the financing of terrorism. For example, one of the most common criticisms lies in the seemingly unsatisfactory approach that courts have taken with regard to the definition of the term "suspicion."[101] Courts have offered sparse guidance on the term as it relates to the money laundering reporting obligations imposed by the Proceeds of Crime Act 2002. For example, in the case of *R v. Da Silva*, the court stated that "the essential element of the word suspect and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice."[102] Further guidance on the interpretation of suspicious activity is offered by the Joint Money Laundering Steering Group who stated that:

> Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example: "[a] degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not . . . [and] [a]lthough the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."[103]

The reporting obligations have contributed to a sense of fear among the regulated sector that has caused a dramatic increase in the number of SARs submitted to FIUs. For example, between 1995 and 2002, the number of SARs submitted to the UK's FIU increased from 5,000 to 60,000. More recently, it has been reported that the UK FIU received 210,524 SARs in

[100] Bank Mellat v. HM Treasury [2013] UKSC 39 (Eng.).

[101] Terrorism Act 2000 c.11, § 19 (Eng.).

[102] R v. Da Silva [2006] EWCA (Crim) 1654 (Eng.); *see also* K v. Nat'l Westminster Bank [2006] EWCA (Civ) 1039 (Eng.); Shah v. HSBC [2010] 3 All ER (EC) 477 (Eng.).

[103] JOINT MONEY LAUNDERING STEERING GROUP, PREVENTION OF MONEY LAUNDERING/COMBATING TERRORIST FINANCING 2011 REVIEW VERSION 133 (2011).

2008,[104] 240,582 in 2010,[105] 247,601 in 2011,[106] 278,665 in 2012,[107] 316,527 in 2013,[108] 354,186 in 2014, 381,882 in 2015, and 643,000 in 2017.[109] There are a number of possible reasons for these increases. First, the increase may be directly attributable to the threat of sanctions by organizations like the Financial Conduct Authority, which has imposed a tactic upon the regulated sector that has been referred to as defensive or preventative' reporting. Second, reporting entities have complained about the significant increase in compliance costs, which has resulted in suggestions that the CTF reporting requirements could be abandoned and that resources should be redirected elsewhere

II. BREXIT

On June 24, 2016, the electorate determined that it no longer wanted the UK to be a member of EU. Will this decision have any impact on how the UK complies with the EU AML and CTF obligations? The UK is at the forefront of the international and regional efforts to tackle financial crime. The UK has implemented a number of international money laundering legislative instruments. For example, it signed the Vienna Convention in December 1988 that was then ratified in June 1991.[110] The impact of the Vienna Convention is illustrated by the Criminal Justice (International Co-operation) Act (1990), part two of which is also entitled the Vienna Convention. Furthermore, the judiciary has taken the Vienna Convention into account on several occasions in relevant money laundering cases. Such cases include *R v. Montila*,[111] *R v. Rezvi*,[112] *Crown Prosecution Service v. Richards*,[113] *Lodhi v. Governor of Brixton Prison (No.2)*,[114] and *R v. Hussain*.[115] The UK signed the UN Convention against Transnational Organized Crime, or Palermo Convention in December 2000, and ratified it in

[104] SERIOUS ORGANISED CRIME AGENCY, THE SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2008 15 (2008).

[105] SERIOUS ORGANISED CRIME AGENCY, THE SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2010 4 (2011).

[106] SERIOUS ORGANISED CRIME AGENCY, THE SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2011 (2012).

[107] SERIOUS ORGANISED CRIME AGENCY, THE SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2012 (2013).

[108] NAT'L CRIME AGENCY, THE SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2013 5 (2014).

[109] *See* NATIONAL CRIME AGENCY, THE SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2017 (2018)

[110] FINANCIAL ACTION TASK FORCE, THIRD MUTUAL EVALUATION REPORT ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM: THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND 250 (2007).

[111] R v. Montila [2005] 1 All ER 113 (Eng.).

[112] R v. Rezvi [2002] 1 All ER 801 (Eng.).

[113] Crown Prosecution Service v. Richards [2006] EWCA (Civ) 849 (Eng.).

[114] Lodhi v Governor of Brixton Prison [2002] EWHC (Admin) 2029 (Eng.).

[115] R v. Hussain [2002] EWCA (Crim) 6 (Eng.).

February 2006. Evidence of its influence is illustrated by its being referenced in the Serious Organized Crime and Police Act (2005).[116] Furthermore, the UK has fully implemented the UN Convention against Corruption 2003 via the enactment of the Bribery Act 2010.

The UK is also obliged to implement several money AML legislative provisions from the EU. For example, the EU introduced the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990).[117] The UK signed the Convention in November 1990 and it was ratified in September 1992. The scope of this Convention was broadened by the Council of Europe through the Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (2005), which was adopted in Warsaw in 2005 and entered into force in 2008. In addition, the EU has introduced four Money Laundering Directives, which have all been implemented by the UK in 1993,[118] 2003,[119] 2007,[120] and by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.[121] The UK has also fully implemented UN Security Council Resolutions 1267 and 1373.[122] The latter of these Security Council Resolutions was introduced by the Terrorism (United Nations Measures) Order 2001,[123] Terrorism (United Nations Measures) Order 2006,[124] and the Terrorism (United Nations Measures) Order 2009.[125] Her Majesty's Treasury manages the financial sanctions regime by virtue of the Terrorist Asset-Freezing etc. Act 2010, which is also assisted by the directions given under Schedule 7 to the Counter Terrorism Act 2008 as well as Council Regulation (EU) No.833/2014. The UK proactively implemented legislative measures to keep consistency between the practices of the UN and EU, and it seems highly unlikely that the UK will fail to guarantee its commitment to implementing the financial crime provisions.

---

[116] Serious Organised Crime and Police Act 2005 c.4, § 95 (Eng.).

[117] Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Aug. 11, 1990, ETS No 141.

[118] The Money Laundering Regulations 1993, SI 1993/1933 (Eng.).

[119] The Money Laundering Regulations 2003, SI 2003/3075 (Eng.).

[120] The Money Laundering Regulations 2007, SI 2007/2157 (Eng.).

[121] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692 (Eng.).

[122] *See* The Terrorism (United Nations Measures) Order 2001, SI 2001/3365; The Terrorism (United Nations Measures) Order 2006, SI 2006/2657; The Terrorism (United Nations Measures) Order 2009, SI 2009/1747; and The Terrorist Asset-Freezing (Temporary Provisions) Act 2010 (Eng.).

[123] The Terrorism (United Nations Measures) Order 2001, SI 2001/3365.

[124] The Terrorism (United Nations Measures) Order 2006, SI 2006/2657.

[125] The Terrorism (United Nations Measures) Order 2009, SI 2009/1747.

D. Conclusions and Recommendations

This Article was written during an unprecedented era of inexpensively financed acts of terrorism in the EU and its Member States. France has experienced a large number of inexpensive terrorist incidents that include the attacks on Charlie Hebdo and the Hyper Cacher which resulted in the death of 17 people. In November 2015, eight terrorists instigated several concurrent acts of terrorism murdering 130 people and injuring 350 at a concert, an international football match, and at surrounding restaurants. Additionally, there were several terrorist attacks in Turkey associated with ISIL and the PKK.[126] UK citizens have been subjected to terrorist attacks in Sousse in 2015, the attempted murder of two train commuters in December 2015, and the terrorist attacks outlined in the second Section of this Article. Therefore, it is essential that the CTF reporting obligations become an effective mechanism for preventing terrorists from being able to move and access their funds. EUROPOL, however, concluded that "2016 has seen lower amounts of funds moved regularly through the financial sector. These small denomination values sent by [terrorist] supporters and family members are transferred to support [terrorists] and their organi[z]ational expenses."[127]

The Article thus provided a critical examination of the appropriateness and effectiveness of the use of the profit reporting model in the fight to suppress the financing of terrorism. The Article illustrated how the UN, FATF, and the EU have all introduced reporting mechanisms that aim to prevent money laundering in a wide range of institutions that receive deposits. The differences between money laundering and terrorist financing are clear and the profit model is inappropriate for tackling the financing of terrorism. Therefore, a new approach needs to be considered by the international community and the UK. The second part of the Article provides extensive evidence that illustrates that the CTF reporting obligations have done very little to prevent acts of terrorism from being financed. The wide variety of sources that terrorists use suggests that they obtain or transfer financing from resources that inherently lie outside the remit of the CTF reporting obligations. Detecting and preventing terrorist finances under the CTF reporting regime is thus extremely difficult if not impossible—especially considering the extensive financial tools available and the low costs of terrorist operations. The final part of the Article provides a commentary on the UKs efforts to implement the CTF reporting obligations. The UK has fully implemented the international AML and CTF reporting obligations that are outlined in the first part of the Article. Further, it is likely that Brexit will have a minimal effect on these obligations. Nevertheless, the UK has mistakenly adopted the profit or reporting model to fight the financing of terrorism. The Article accordingly highlights several weaknesses in this latter approach, including the inappropriate definition of suspicious, the increased costs of compliance, and a fear within

[126] UNITED STATES DEPARTMENT OF STATE, COUNTRY REPORTS ON TERRORISM 88–89 (2016).

[127] EUROPOL, EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2017 12 (2017).

reporting entities that has resulted in defensive reporting. To tackle the threat posed by terrorist financing, this Article suggests that reporting entities, FIUs, policy makers, and the international community adopt a different and innovative approach. Such an approach would involve revisiting the interpretation of suspicious and departing from a definition aimed at money launderers that attempt to disguise large sums of illegally obtained funds. Importantly, deposit taking institutions should focus their CTF obligations not on suspicious deposits that they receive, but on suspicious withdrawals. Such examples could include bank accounts that are closed with little or no notice, irregular cash withdrawals that are inconsistent with the financial character or behavior of the account holder, or an unexpected use of an overdraft. The scope of CTF reporting obligations must reach beyond institutions that receive deposits and should include providers of credit, especially considering the use of student loans to finance acts of terrorism in Manchester and Brussels. Extending reporting obligations to providers of credit could limit one funding avenue that has been previously exploited by terrorists. The success of such an approach would doubtlessly require a closer working relationship between the reporting entities themselves and the FIU.

Articles

Prosecuting EU Financial Crimes: The European Public Prosecutor's Office in Comparison to the US Federal Regime

By Carlos Gómez-Jara Díez [*] *& Ester Herlin-Karnell* [**]

Abstract

Why is the fight against financial crimes such a central task for the EU? The EU has a strong interest to counter financial crimes and fraud against the EU budget as those crimes—so the EU legislator's claim is—hamper the trust in the market and undermine consumer confidence to engage in internal market transactions. In this Article, we aim to discuss the establishment of the European Public Prosecutor Office as a federal agent and the effects of this agent for establishing a robust EU financial crimes regime. Comparisons with the US system of US Attorneys—federal prosecutors—will be drawn to show that this institution has been quite effective at enhancing the protection of US financial market. The Article will then discuss to what extent the EU can, and should, learn from the American experience. We are particularly interested in the strong security focus in the EU and its consequences when it ventures into the area of financial crimes.

[*] Professor of Criminal Law at the Universidad Autónoma de Madrid and practicing lawyer at Corporate Defense, Madrid. Email: cgj@corporatedefense.es

[**]Professor of EU Constitutional Law and Justice and University Research Chair, VU University of Amsterdam. Email: e.herlinkarnell@vu.nl. Both authors wish to thank Els de Busser and the GLJ editors Matthias Goldmann and Christoff Safferling for their helpful comments on this paper. Thanks also to the GLJ student editorial team for their excellent support. The usual disclaimer applies.

A. Introduction

In this Article, we explore some of the current regulatory challenges in EU financial crimes practices and EU market regulation by focusing on the recent establishment of a European Public Prosecutor Office—EPPO.[1] The idea behind the creation of an EPPO is perhaps one of the most contested EU criminal law measures in recent years and one which originates from the longstanding idea of creating a comprehensive EU anti-fraud regime. This EU mission of constructing its own prosecutor has lasted for over two decades, with the EPPO as representing something of a *pièce de résistance*, with legal consequences spanning both the EU criminal law domain and the internal market. As such the EPPO is a follow-up to the previous *Corpus Juris* project.[2] The EPPO regulation was recently adopted, but prior to its enactment, it had triggered two yellow cards in the legislative process with regards to the earlier proposals for this legislation.[3] Eventually the EU Commission resorted to enhanced cooperation, a flexible mode of integration where not all Member States participate in the legislative measure—but at least nine Member States do—and this has attracted a lot of attention and debate in EU law scholarship.[4]

Specifically, in this Article we will discuss some of the legal implications of the establishment of the EPPO and in particular, the potential of this agent for establishing a robust financial crimes regime across the EU. In addition, we will look at the security dimension of the EU's legislative powers in this area. We argue that the EU's approach to fighting financial crimes is closely connected to the general security theme of the EU—"Area of Freedom, Security and Justice" (AFSJ)—as well as to the EU legislators' goal of improving market integrity and consumer confidence in the internal market. Therefore, as we try to show in this Article, it would be consistent with other EU policies to expand the current jurisdiction of the EPPO to cover a wider area than simply the EU budget. This Article argues to extend the EPPO jurisdiction to comparable areas included within the jurisdiction of the US system of US Attorneys.

---

[1] Commission Regulation 2017/1939 of Oct. 12, 2017, Implementing Enhanced Cooperation on the Establishment of the European Public Prosecutor's Office, 2017 O.J. (L 106) 1, 1-71 [hereinafter EPPO].

[2] *E.g.*, MIREILLE DELMAS-MARTY, THE IMPLEMENTATION OF THE CORPUS JURIS IN THE MEMBER STATES (John Vervaele ed. 2000).

[3] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community art. 12(b), Dec. 13, 2007, 2007 O.J. (C 306) (providing for a competence of national Parliaments to see that the principle of subsidiarity is respected in accordance with Protocol No. 2) [hereinafter Treaty of Lisbon].

[4] *See e.g.*, JACOB ÖBERG, LIMITS TO EU POWERS: A CASE STUDY OF EU REGULATORY CRIMINAL LAW ch. 7 (2017) (On the adoption of the EPPO Regulation). It should be recalled that before the Lisbon Treaty entered into force, the enhanced cooperation mechanism was almost impossible to use. This was a result of the very high procedural thresholds that were in place, which took the form of restrictions regulating such cooperation.

Additionally, given the current prosecution discretion granted to the EPPO, we will highlight the heavy criticism that has been levied against the raw discretionary power of the American federal prosecutors.

Against the backdrop of the broader issues of the establishment of the EPPO, it is the contention of this Article that the EU is in need of a more detailed empirical account of what occurs in practice. This is especially true when looking at the regulatory challenges the EU is facing when legislating on financial crimes as part of the AFSJ venture. As noted, the EU has a very strong interest in countering financial crimes, as it could potentially undermine the confidence in the market and its realization as an "honest" market place. Financial crimes are generally any kind of criminal conduct relating to money or to financial services or markets.[5] As will be shown, there is also a strong security dimension to the EU's fight against financial crime. For example, terrorism is often financed through laundered money. In addition, the claim of the EU legislator is that the occurrence of financial crimes within the EU territory could—and does—harm the EU budget.

Within this complex mixture of security concerns and the EU mission to establish a "clean" market, the establishment of the institute of EPPO represents a pertinent example of possible challenges in this area as it, *inter alia*, keeps the criminal law of defense on a national level and moreover grants the EPPO very limited enforcement powers.[6] There is then a curious relationship between the establishment of the EPPO and that of the EU security mission. The question is how to reconcile the EPPO with the constitutional questions in the EU. Crucial constitutional principles in the EU framework are of course, *inter alia*, competence allocation, subsidiarity, proportionality, and fundamental right protection.[7] Those axioms are important for the general understanding of the relationship between the EU mission to fight financial crimes and that of the security project of the AFSJ and should be kept in mind. This is especially true considering that Member State security is to a large extent a national competence under Article 4.2 Treaty of the European Union (TEU).

This Article is structured as follows. First, we will discuss the broader questions of the establishment of the EPPO and how it fits into the EU world of security governance and anti-financial crimes policies. Second, we will look more closely at what the EPPO Regulation properly entails. Subsequently, we will discuss the possibilities of extending the jurisdiction of the EPPO to EU financial crimes in general, as well as the question of data protection and

---

[5] *See e.g.*, Financial Services and Markets Act 2000, c. 8 (Eng.), https://www.legislation.gov.uk/ukpga/2000/8/contents.

[6] EPPO, *supra* note 1, at 1-71.

[7] *See e.g.*, STEPHEN WEATHERILL, LAW AND VALUES IN THE EUROPEAN UNION (2016); GRAINNE DE BURCA AND PAUL CRAIG, THE EVOLUTION OF EU LAW (2011); TAKIS TRIDIMAS, GENERAL PRINCIPLES OF EU LAW (2011).

profiling. Finally, we will discuss the EPPO in a comparative context by looking at its similarities and differences with the American federal prosecutor.

B. Prosecuting EU Financial Crimes as Part of the Wide Grid of EU Security Governance

The establishment of the EPPO represents one of the latest layers in the EU's measures to fight financial crime, but before looking in further detail at this prosecutor, we need to ask why the fight against financial crimes is such a central task for the EU. As mentioned above, the EU has a strong interest in countering financial crimes and fraud against the EU's budget as these crimes hamper the trust in the market and often—so the EU legislators claim is—undermine consumer confidence to engage in internal market transactions.[8] Specifically, the underlying objective of the EU's involvement in the fight against financial crime and market abuse more generally is to boost investor confidence and thereby contribute to the functioning of the internal market—for example through harmonization under Article 114 Treaty of the Functioning of the European Union (TFEU).[9] The idea is moreover that investors and consumers would be discouraged if the EU budget is corrupted.[10] There are then, multiple reasons for the EU to be actively engaged in the countering of financial crimes: From the functioning of the market and increasing consumer confidence in the market, to protecting the EU's budget against fraud. These are distinct, albeit interrelated goals, for the EU legislator. In particular, the occurrence of financial crimes has—since the early days of the EU—been considered as constituting one of the main threats to the establishment of the internal market.[11] For example, the legislative carousel on the market abuse regime—the anti-money laundering scheme—and the question as to why the suppression of financial crimes is relevant in EU law, offer good examples of a longstanding case of cross-over competences between the AFSJ and the internal market sphere.[12]

With the global financial crisis in 2008, the fight against white collar crime and fraud against the EU budget was intensified and as such has been considered a priority for the EU as a crisis management tool.[13] A decade later, in 2018, the priority of fighting financial crimes is still high on the agenda, but with an added considerably increased security dimension by also tackling the threat of financing of terrorism and related activity to a greater extent—as

[8] NIAMH MOLONEY, EU SECURITIES AND FINANCIAL MARKETS REGULATION (2014).

[9] *See e.g.*, Commission Regulation 596/2014 of April 16, 2014, Market Abuse Regulation and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives, 2014 O.J (L 173).

[10] EPPO, *supra* note 1, at 59.

[11] *See* DELMAS-MARTY, *supra* note 2.

[12] *See e.g.*, Ester Herlin-Karnell, *White-Collar Crime and European Financial Crises: Getting Tough on EU Market Abuse,* 37 EUR. L. REV. 487 (2012).

[13] *See* contributions by Maria Bergström and Nicholas Ryder in this special issue of the German Law Journal.

compared to the legislation adopted in the aftermath of 9/11.[14] In addition, there is an overlap—or hybridity—in legal sources not only between the EU's internal market policies and the growing importance of the AFSJ, but also in relation to the external dimension of the EU. This is because a majority of the measures currently adopted to fight the financing of terrorism and financial crimes in the EU partially fall within the remit of international norms that are being adopted by the EU—for example, the Financial Action Task Force.[15]

Moreover, the EU's strategy to fight irregularities in the market should be seen in light of the history of the debate on the competences of the EU to enact criminal law. Before the EU asserted a competence with the Lisbon Treaty in place—Article 83 TFEU—it was necessary for the EU to tie its claimed authority to the internal market and thereby adopt administrative sanctions—that were very close to criminal law penalties—to increase the effectiveness of the system.[16] As one of us previously charted in the German Law Journal, the EU sanctions regime is built around the notion of regulatory powers involving different actors and processes—often through administrative sanctions rather than criminal law.[17] While much has been said about the purpose of fighting financial crimes within the internal market,[18] much less has been said with regard to the impact of these findings and enforcement questions within the AFSJ. Recent examples of directives that illustrate the EU's activity in the area, are the aforementioned MAD Directive,[19] the related MAR regulation,[20] and the Fourth Money Laundering Directive.[21] These were based on Article 83 TFEU and Article 114 TFEU respectively. The Fourth Money Laundering Directive is about to be superseded soon, however. The EU recently adopted a proposal for a Fifth Money Laundering Directive.[22] The Fifth Money Laundering Directive sets out a series of measures

---

[14] *Id.*

[15] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

[16] *See* CARLOS GÓMEZ–JARE DÍEZ, FEDERAL EUROPEAN CRIMINAL LAW (2015).

[17] *See* Ester Herlin-Karnell, *Constructing Europe's Area of Freedom, Security, and Justice through the Framework of "Regulation": A Cascade of Market-Based Challenges in the EU's Fight Against Financial Crime*, 16 GERMAN L.J. 49, 71 (2015).

[18] *See e.g.*, CHRISTOPH STEFANOU & HELEN XHANTHAKI, FINANCIAL CRIME IN THE EU (2005).

[19] *See* DELMAS-MARTY, *supra* note 2.

[20] *See* HERLIN-KARNELL, *supra* note 12.

[21] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation No 648/2012 of the European Parliament and of the Council, 2015 O.J. (L 141) 73.

[22] *Commission Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the Prevention of the use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, COM (2016) 185 final (July 5, 2016). Directive (EU) 2018/843 of

to better counter the financing of terrorism and to ensure increased transparency of financial transactions and of corporate entities under the preventive legal framework in place in the Union.

Likewise, the EU Security Agenda 2015 is crucial here.[23] In short, the EU's Security Agenda identifies, *inter alia*, three priorities for the EU: Fighting terrorism and its financing, organized crime, and the suppression of cybercrime. To address these threats, the Security Agenda claims to strengthen and increase both the effectiveness of information exchange and operational co-operation between Member States, EU Agencies, and the IT sector. Significantly, however, terrorism also encompasses online activity, not necessarily just physical movement across the EU—which is stressed in the new counter Terrorism Directive 2017.[24] While this remains an important task, there should be a critical debate on how the EU could construct an AFSJ that integrates its mission of establishing an effective response to the growing global security threat posed by the unstable situation in the world with the EU values of human rights and promotion of justice. In other words, the phenomenon of globalization also affects the EU and the constitutional structure for addressing these problems and needs to uphold the rule of law and values—Article 2 Treaty of the EU. The Security Agenda tries to address this complex issue by stressing the need for more joined-up inter-agency cooperation and a cross-sectorial approach.[25]

Given the increased nexus between different types of security threats and policy, action on the ground must—according to the previously mentioned Security Agenda—be fully coordinated among all relevant EU agencies and institutions. Particular law enforcement agencies—such as Europol and Eurojust—provide a specialized layer of support and expertise for Member States and the EU. According to the Security Agenda, they function as information hubs, help implement EU law, and play a crucial role in supporting operational cooperation, such as joint cross-border actions.[26] There is, at present, a wide-ranging debate as to what extent these agencies can be held accountable and their legitimacy as key players

the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, 2018 O.J. (L 156) 43-74.

[23] *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions on The European Agenda on Security*, COM (2015) 185 final (Apr. 28, 2015).

[24] *See* Directive 2017/541 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA, 2017 O.J. (L 88) 6-21.

[25] *See id. (*as pointed out in the EU Security Agenda).

[26] *See id.,* at 4 & 9.

in the AFSJ regime.[27] The establishment of the EPPO is now added to the controversy of the trend of "agencification" in the EU treadmill.

Consequently, the EPPO represents a milestone in EU activity against financial crimes, the EU's budget, and is responsible for investigating, prosecuting, and bringing to judgment—where appropriate in liaison with Europol—the perpetrators of and accomplices in offenses against the Union's financial interests, as determined by the regulation provided for in Article 86 TFEU. Moreover, in the general context of the need for an EPPO in the EU, it is interesting to note that while financial market regulation relies on a range of tools, anti-fraud rules remain imperative.[28] Thus, in the EU context, the fight against fraud and related activities always sparks a complex debate as to the competences of the EU.

In the policy area of the AFSJ, Article 83 TFEU provides far-reaching powers in criminal law concerning cross-border criminality. But "mainstream" internal market powers—such as Article 114 TFEU—are still crucially important in the context of the EU's fight against financial crimes. These powers are particularly significant with respect to the effect on the national arena, as Article 114 TFEU also allows for the adoption of regulations, thereby directly affecting citizens and Member State legislation. Consequently, the EPPO is also interesting as regards to the relationship between the internal market and the AFSJ, as financial crimes are relevant to both of these policy areas. In short, most arguments against the establishment of an EPPO concern the inaccuracy of the figures presented by the Commission, as well as the lack of added value from EPPO investigations.[29] It was also argued that its establishment possibly had a detrimental impact on the existing actors in the area and their future cooperation with non-EPPO Member States. It is difficult to separate rules relating to investigations and prosecutions, at the EU level, and trials at Member State level.

As noted above, the EU has, for a long time, had preferences for relying on the slogan "confidence in the market" as an all-embracing justification for approximation under Article 114 TFEU and where criminal law has been used as a tool for boosting such confidence.[30] The often over-reliance on confidence as a justification for harmonization has long been observed—and criticized—in the context of private law and more lately spilled over into the

---

[27] *E.g.,* Madalina Busuioc, Deirdre Curtin, & Martijn Groenleer, *Agency Growth Between Autonomy and Accountability: the European Police Office as a "living institution,"* 18 J. EUR. PUB. POL'Y 848 (2011); *See also,* P Schammo, *The European Union Securities and Market Authority: Lifting the veil on the Allocation of Powers*, 49 COMMON MKT. L. REV. 1879, 1887 (2011).

[28] *See e.g.*, NIAMH MOLONEY, EU SECURITIES AND FINANCIAL MARKETS REGULATION (2014).

[29] *See e.g.*, Aandras Csúri, *The Proposed European Public Prosecutor's Office—from a Trojan Horse to a White Elephant?*, 18 CAMBRIDGE Y.B. OF EUR. LEGAL STUD., 122 (2016); Irene Wieczorek, *The EPPO Draft Regulation Passes the First Subsidiarity Test: An Analysis and Interpretation of the European Commission's Hasty Approach to National Parliaments' Subsidiarity Arguments*, 16 GERMAN L.J. 1247, 1248 (2016).

[30] *See e.g.,* Directive 2015/849, *supra* note 21.

field of EU criminal law.[31] Hence, in short, there is a reason why the question of the fight against financial crimes—and financing of terrorism—has become a key issue for the EU legislator. Thus, a majority of the current instruments adopted by the EU in the area of the suppression against financial crimes have been enacted on the basis and justification that there is still a need for increased regulatory response to financial crises that started in 2008 and to the current security threat of terrorism confirming the overlap between market oriented approaches and that of security.[32] Indeed the recently adopted Directive[33] to counter terrorism in the EU highlights the strong market elements to the fight against the financing of terrorism. In its preamble—recital 13—it is stated that:

> Illicit trade in firearms, oil, drugs, cigarettes, counterfeit goods and cultural objects, as well as trafficking in human beings, racketeering and extortion have become lucrative ways for terrorist groups to obtain funding . . . increasing links between organized crime and terrorist groups constitute a growing security threat to the Union and should therefore be taken into account by the authorities of the Member States involved in criminal proceedings.

After having outlined the wider picture of the current EU approach to countering financial crimes and its strong security dimension, this Article will now turn to the EPPO in further detail.

C. The European Public Prosecutor Office

I. Background

The establishment of an EPPO has been met with serious opposition. Eleven national parliaments voted against the proposal in the yellow card procedure. Based on this vote, one would have thought that the enhanced cooperation mechanism would have been triggered earlier. Instead, the Commission maintained its proposal essentially intact, notwithstanding the fact that the yellow card procedure has been used for the only second

---

[31] *E.g.,* Stephen Weatherill, *The Limits of Legislative Harmonization Ten Years after Tobacco Advertising*, 12 GERMAN L.J. 827 (2011).

[32] *See e.g.*, LUCIA QUAGLIA, THE EU AND GLOBAL SECURITIES MARKETS REGULATION (2014); *See also*, Ryder and Bergstrom in this special issue.

[33] Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, 2017 O.J. (L 88) 6-21.

time since its inclusion in the Treaties.[34] Specifically, the EPPO has, with regards to the original draft, triggered reasoned opinions—or so called yellow cards—issued by fourteen chambers of eleven different national parliaments.[35] This attracted a lot of attention and debate in academia and legal practice.[36] The only possibility for the EPPO project to survive was eventually through the invocation of the enhanced cooperation mechanism, according to which some Member States—nine or more—could pursue flexible integration. This could, of course, be considered as a subsidiarity-friendly alternative as it allows for differentiation within the EU and thereby for national divergence between the Member States. So, the classic notion of enhanced cooperation means that some Member States go further than other States. The concept accepts that there is room for action outside the EU model and that not all Member States have to be in the same boat, while still respecting each other through the fundamental loyalty principle of Article 4.3 TEU. From the perspective of the establishment of an EPPO—through the notion of flexible integration—it also raises concerns about a system that seems to offer a half-baked solution. After all, it may be asked what the function of an EPPO is if the whole EU does not join.

When discussing the use of enhanced cooperation in the EPPO context, it is essential to understand the general climate in which this type of alternative integration takes place. Indeed, Member States—like the UK and Denmark—already enjoy a major opt-out arrangement from the AFSJ. Accordingly, with the UK leaving through its Brexit negotiations, only Denmark has an "out" of the mayor AFSJ scheme.[37] Moreover, other Member States—like Sweden and the Netherlands—announced early that they would not participate due to what they consider the far-reaching competences of the EPPO, including the possibility of extending the competences of the EPPO to criminality not related to the EU budget. Indeed, Article 86(4) provides for the possibility of a future European Council to adopt a decision amending the competences of such a prosecutor to include serious crime with a cross-border dimension in a broader sense, we will return to this below. More recently, the

[34] *Id.*

[35] Treaty of Lisbon, *supra* note 3.

[36] *E.g.*, Gerard Conway, *The Future of a European Public Prosecutor in the Area of Freedom, Security and Justice, in* THE EUROPEAN UNION AS AN AREA OF FREEDOM, SECURITY AND JUSTICE (Maria Fletcher et al. eds., 2016); Jacob Öberg*, Limits to EU Powers: A Case Study of EU Regulatory Criminal Law* ch. 7 (2017); *The Establishment of a European Public Prosecutor's Office: Between "Better Regulation" and Subsidiarity Concerns, in* THE ESTABLISHMENT OF THE EUROPEAN PUBLIC PROCEUTOR'S OFFICE (EPPO): "STATE OF PLAY AND PERSPECTIVE" (Willem Geelhoed et al. eds., 2018); TOWARD A PROSECUTOR FOR THE EUROPEAN UNION (Katlin Ligeti ed., 2012); Dianne Fromage, *The Second Yellow Card on the EPPO Proposal: An Encouraging Development for Member State Parliaments*?, 35 Y.B. OF EUR. L. 5 (2016).

[37] *See* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) protocol 22.

Netherlands changed its mind and has decided to participate in the establishment of the EPPO.[38]

As mentioned, the idea of an EPPO is, however, not new. It had first publicly been developed by the so-called *Corpus Juris* group of academics and practitioners in the 1990s in response to a request by the Commission, with a model proposal in 1997 and which was revised in 2000.[39] This *Corpus Juris* formed the basis for a *Commission Green Paper*,[40] which eventually led to Article 86 TFEU. Yet the question of enforcement of EU anti-fraud policies seems to have been largely left to the EU Court of Justice through its case law. According to the well-established case law starting with the *Greek Maize* case,[41] Member States have to protect EU interest the same way as it protects national interests. Specifically, this case concerned fraud against the EU where the Court held that: ". . . the Member States must ensure that infringements of EU law are penalised under conditions, both procedural and substantive, which are analogous to those applicable to infringements of national law of a similar nature and importance and which, in any event, make the penalty effective, proportionate and dissuasive."[42]

The main argument in favor of establishing the EPPO—as presented by the Commission—is that Eurojust and Europol have a general mandate to facilitate the exchange of information and coordinate national criminal investigations and prosecutions but lack the power to carry out acts of investigation or prosecution themselves. According to the Commission, action by national judicial authorities often remains slow, prosecution rates on the average are low, and results obtained in the different Member States over the Union as a whole are unequal. Based on this track record, the judicial action undertaken by Member States against fraud may currently not be considered as effective, equivalent, and deterrent as required under the Treaty. Yet, there is a fundamental flaw in the creation of a European Public Prosecutor: It is difficult to separate rules relating to investigations and prosecutions, at the EU level, and trials at Member State level.

---

[38] As to Sweden's position on not joining the EPPO *see* Council 2017, EPPO General Approach, point no. 11. On the Dutch position *see,* Etienne Verschuren, *Nederland doet toch niet mee aan Europees OM*, NRC (Nov. 24, 2016), https://www.nrc.nl/nieuws/2016/11/23/nederlanddoet-toch-niet-mee-aan-europees-openbaar-ministerie-a1533218; *see also*, Sofie Wolf, *The Netherlands will join the European Public Prosecutor's Office*, MAASTRICHT UNIVERSITY (May 17, 2018), https://www.maastrichtuniversity.nl/blog/2018/05/netherlands-will-join-european-public-prosecutors-office-eppo.

[39] *See* Delmas-Marty, *supra* note 2.

[40] *See Green Paper on Criminal Law Protection of the Financial Interests of the Community and the Establishment of a European Prosecutor*, COM (2001) 715 final (Dec. 11, 2001).

[41] *See* Case C-68/88, Comm'n v. Greece, 1989 E.C.R. I-2965, §24.

[42] *See* Ester Herlin Karnell & Nic Ryder, *The Robustness of EU Financial Crimes Legislation: A Critical Review of the EU and UK Anti-Fraud and Money Laundering Scheme*, 27 EUR. BUS. L. REV. 427, 427 (2017).

II. Main Features

The EPPO is a centralized decision-making EU institution with a de-centralized enforcement structure that investigates, prosecutes, and brings to judgment offenses against the EU financial interests. Specifically foreseen in Article 86 of the TFEU, its final establishment created a heated discussion among EU institutions and Member States and triggered the enhanced cooperation clause.[43] In plain language: The EPPO is a controversial EU institution that raises sovereignty concerns among Member States. For the purposes of this Article it pays to separate the previous statement in three basic concepts: (i) The centralized decision-making institution; (ii) the de-centralized enforcement structure; and (iii) its jurisdiction over crimes against EU financial interests.

The need for an EU enforcement institution with centralized decision-making authority in this area has been acknowledged from its inception. The sheer fact proclaimed repeatedly by the OLAF in terms of "under-enforcement" in this area has justified the need to establish an EU Institution that would ensure adequate enforcement of EU legislation to protect the financial interests of the EU.[44] Given that pursuant to the authority conferred to Eurojust in Article 85 TFEU would not solve "the current disparities and fragmentation of national prosecution efforts,"[45] the only feasible proposal was the creation of the EPPO from Eurojust.

The centralized decision-making authority in the EPPO regulation consists of—as is stated in article 8—the "European Chief Prosecutor, who is the head of the EPPO as a whole and the

[43] The Member States that communicated its desire to establish this institution were: Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Germany, Finland, France, Greece, Lithuania, Luxembourg, Portugal, Romania, Slovakia, Slovenia, and Spain. In May 2018, the Netherlands notified the Commission of its intention to join. *See*, European Public Prosecutor's Office, EUROPEAN COMMISSION EUROPEAN ANTI-FRAUD OFFICE, https://ec.europa.eu/anti-fraud/policy/european_public_prosecutor_en.

[44] *Commission Staff Working Document Executive Summary of the Impact Assessment Accompanying the document Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office,* at 11, SWD (2013) 274 final (July 17, 2013) [hereinafter Impact Assessment]:

> Every year at least several hundred million euros are fraudulently diverted from their intended purpose. Only a small fraction of these losses are ever recovered from the criminals. These figures show that the financial interests of the European Union are insufficiently protected from fraud. In fact, the Commission's annual statistics (including those of OLAF) demonstrate that while fraud against the Union's financial interests is pervasive and causes substantial damage every year to the tax payer, national criminal enforcement efforts lag behind. In particular, OLAF's cases which are transferred to national investigation and judicial authorities are not always equally effectively followed-up.

[45] *Id.* at 14.

head of the College of European Prosecutors, Permanent Chambers and European Prosecutors." A savvy reader will quickly notice that the existence of such a variety of individuals and bodies raises some concerns as to the real centralization of the decision-making authority. This is not by chance. It is the result of a complicated negotiation process that took place once the EU Commission laid out its first proposal for the EPPO Regulation.[46]

In the EU Commission's previous Proposal for the EPPO there was no "College of European Prosecutors," nor "Permanent Chambers."[47] Nevertheless, there was a clear objection by Member States to such degree of centralization and supranational authority.[48] The resulting centralized structure functions the following way:

1. The College makes decisions on strategic matters.[49]
2. The Permanent Chambers monitors and direct investigations and ensures the coherence of the activities of the EPPO.[50]

[46] *See Proposal for a Council Regulation on the Establishment of the European Public Prosecutor's Office Brussels*, COM (2013) 534 final (July 17, 2013) [hereinafter EPPO Regulation].

[47] *See* THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE: AN EXTENDED ARM OR A TWO-HEADED DRAGON? (Marta Pawlik et al. eds., 2015).

[48] *See* Anne Weyembergh & Chloé Briere, *Towards a European Public Prosecutor, Policy paper for the European Parliament* (2016) (available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571399/IPOL_STU(2016)571399_EN.pdf):

> The idea of an entirely supranational prosecution service organised at central level and composed of a chief prosecutor and several specialized deputy prosecutors acting throughout MSs' territories was quickly abandoned. Decentralisation was the preferred option, and discussions focused on defining the most appropriate level. Negotiations have evolved towards ever less centralisation and more decentralisation, from a small hierarchical central office towards a collegial body with various layers. This development raises the question as to whether a sufficient degree of Europeanisation / verticalisation remains, or whether MSs have expanded their control over the EPPO to the extent that it has been deprived of any added value.

[49] Including determining the priorities and the investigation and prosecution policy of the EPPO, as well as on general issues arising from individual cases—for example regarding the application of this Regulation—the correct implementation of the investigation and prosecution policy of the EPPO or questions of principle or of significant importance for the development of a coherent investigation and prosecution policy of the EPPO. The decisions of the College on general issues should not affect the duty to investigate and prosecute in accordance with this Regulation and national law. The College should use its best efforts to take decisions by consensus. If such a consensus cannot be reached, decisions should be taken by voting. *See* EPPO Regulation, *supra* note 46, at 24.

[50] The composition of Permanent Chambers should be determined in accordance with the internal rules of procedure of the EPPO, which should allow—among other things—for a European Prosecutor to be a member of more than one Permanent Chamber where this is appropriate to ensure, to the extent possible, an even workload between individual European Prosecutors. *See id.* at 25.

3. The European Prosecutors supervise, on behalf of the competent Permanent Chamber, the investigations and prosecutions handled by the European Delegated Prosecutors in their Member State of origin.[51]

The de-centralized enforcement structure is carried out by the European Delegated Prosecutors in each Member State. Under the instructions of the Permanent Chamber and under the supervision of a European Prosecutor appointed to that Chamber, the European Delegated Prosecutors are entrusted with the task of doing the "ground work."[52] It is here that the famous concept of the "double-hat" prosecutors plays a major role. Although members of the national prosecutorial authorities—and therefore bound by their loyalty to the respective national authorities—these "double-hat" prosecutors are also a part of the EPPO[53] that must comply with the instructions of the Permanent Chamber when handling cases related to the protection of the EU financial interests.[54]

The benefits of these centralized and decentralized structures are manifold. First, from a sovereignty perspective, the actual authorities conducting law enforcement activities and appearing before national courts are national law enforcement authorities—not supranational authorities. The fact that they are being instructed by somewhat supranational authorities and supervised by a European Prosecutor of their own country of origin[55], does not alter the fact that the European Delegated Prosecutors are members of the prosecutorial and judicial national authorities.[56] Second, from a policy perspective, the

[51] A European Prosecutor from each Member State should be appointed to the College. They should act as liaison between the central office and the decentralized level in their Member States, facilitating the functioning of the EPPO as a single office. The supervising European Prosecutor should also check any instruction's compliance with national law and inform the Permanent Chamber if the instructions do not do so. *See id.*

[52] The investigations of the EPPO should—as a rule—be carried out by European Delegated Prosecutors in the Member States. They should do so in accordance with this Regulation and, as regards matters not covered by this Regulation, in accordance with national law. European Delegated Prosecutors should carry out their tasks under the supervision of the supervising European Prosecutor and under the direction and instruction of the competent Permanent Chamber

[53] The European Delegated Prosecutors should be an integral part of the EPPO and as such, when investigating and prosecuting offenses within the competence of the EPPO, they should act exclusively on behalf and in the name of the EPPO on the territory of their respective Member State.

[54] The European Delegated Prosecutors should be bound to follow instructions coming from the Permanent Chambers and the European Prosecutors

[55] It must bear in mind that a European Prosecutor from each Member State is appointed to the College. Also, nothing precludes a European Prosecutor of the country of origin where the enforcement action is conducted to be a member of the Permanent Chamber instructing the European Delegated Prosecutors in charge of the investigation in that Member State.

[56] This is a well-established requirement of the EPPO Regulation: European Delegated Prosecutors should, during their term of office, also be members of the prosecution service of their Member State, namely a prosecutor or member of the judiciary, and should be granted by their Member State at least the same powers as national

Member States are able to channel their concerns regarding the enforcement actions of the EPPO at various stages of the centralized level: In the College—through their designated European Prosecutor—and in the supervising European Prosecutor of the actual case. There are certain safeguards to prevent national authorities from directly influencing the outcome of the enforcement action, but these are more theoretical than practical. Third, from a procedural perspective, the European Delegated Prosecutors are knowledgeable of the national procedural requirements for a case to proceed and given that the EPPO does not provide a comprehensive body of rules of procedure, it is necessary to resort to national procedural law in many instances. Fourth, from an economic perspective, the use of already existing national prosecutors with a "double-hat" function certainly diminishes the economic impact that would cause creating a whole new body of EU prosecutors acting in each Member States.[57]

From a practical national perspective, there are no major changes caused by the installations by the EPPO. The same national body of prosecutors that has been investigating and prosecuting these cases in the past will be exercising the same powers in the future. The only significant difference is that they will be receiving instructions from an EU body, but supervised by a European prosecutor of their own country. To be sure, the fact that these European Delegated Prosecutors are now also a part of an EU body certainly makes a difference from an institutional perspective. But this does not alter the fact that—from a national perspective—the same prosecutors will be prosecuting the same offenses. [58]

III. Jurisdiction and Competence

---

prosecutors.

[57] Impact Assessment, *supra* note 44:

> The costs of the different options for establishing the EPPO vary quite considerably. The most expensive option is the centralised one, which assumes that all investigations and prosecutions will be handled at the European level, leading to a higher number of required EU staff. The decentralised option does not entail as much costs, also because use is made to a large extent of resources existing in the Member States, at Eurojust and at OLAF. The costs for the centralised option over twenty years are expected to be over €800 million, whereas the costs for the decentralised option are expected to be about €375 million. These costs include all costs expected to arise from establishing a new European body.

[58] Fabio Guiffrida produced a useful chart depicting the basic structure of the EPPO. It clearly shows the horizontal rather than vertical approach of the EPPO and the importance of the national prosecutors in the overall functioning. *See* Fabio Giuffrida, *The European Public Prosecutor's Office: King Without Kingdom?*, CEPS Research Report No. 2017/03, (Feb. 2017), http://aei.pitt.edu/84218/1/RR2017%2D03_EPPO.pdf.

Currently, the EPPO only has competence regarding the protection of the EU financial interests. As noted previously, the EU institutions and European academics have been dealing with the possibility of establishing an EPPO for decades. A constant factor in the myriad of contributions related to the EPPO has been its intrinsic connection to the overall discussion of how to protect the EU financial interests. In this sense, since the first version of the *Corpus Juris* for the Protection the EU financial interests in 1997, the convenience of establishing a European Public Prosecutors Office to secure the protection of the EU financial interest has been a silent consensus. Therefore, when the Lisbon Treaty introduced specific provisions related to the EPPO, it came to no surprise that, out of the immense catalog of crimes that have been harmonized at a European level, only the protection of the EU financial interests was specifically referred. As is clear from article 86 TFEU:

> 1. In order to combat crimes affecting the **financial interests of the Union**, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust.
> 2. The European Public Prosecutor's Office shall be responsible for investigating, prosecuting and bringing to judgment, where appropriate in liaison with Europol, the perpetrators of, and accomplices in, **offenses against the Union's financial interests**, as determined by the regulation provided for in paragraph 1. It shall exercise the functions of prosecutor in the competent courts of the Member States in relation to such offenses.

The term “offenses against the Union's financial interests” stated in the TFEU seems to indicate a quite limited jurisdiction of the EPPO. Nevertheless, the final scope is more far reaching as the tasks of the EPPO are to investigate, prosecute, and bring to judgment the perpetrators of offenses against the Union’s financial interests under Directive (EU) 2017/1371 of the European Parliament and of the Council and offenses which are

inextricably linked to them.[59] Among these offenses are passive and active corruption,[60] misappropriation of public funds,[61] and damaging the Union's financial interests.

It should be noted from the outset, that the fact that the EPPO will be prosecuting active and passive corruption—for example, prosecuting local and national public officials—will surely create certain controversy with local and national authorities from time to time. This, however, is a common thread in supranational prosecuting authorities.

Also, it should be observed that traditional VAT fraud cases are also included in the Directive.[62] The consequences of such inclusion are not to be taken lightly. It means that as soon as the EPPO starts to function, the caseload of the delegated European Prosecutors will be quite significant. In this sense, it is true that the number of cases addressing procurement and non-procurement expenditure has been quite low in a number of Member States. Yet, the number of VAT fraud cases currently enforced in certain jurisdiction is quite staggering.

IV. Extending the Jurisdiction of the EPPO to EU Financial Crimes?

The EPPO currently has the competence to prosecute offenses against the EU financial interests. Yet, it is fair to say that the drafters of the TFEU probably had in mind a broader expansion of EPPO's jurisdiction to include other offenses. Article 86.4 TFEU specifically enables the European Council—by way of a unanimous decision—to extend the powers of

---

[59] *See* Directive 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the Fight Against Fraud to the Union's Financial Interests by Means of Criminal Law, 2017 O.J. (L 198) 29.

[60] "Passive corruption" means the action of a public official who—directly or through an intermediary—requests or receives advantages of any kind, for himself or for a third party, or accepts a promise of such an advantage, to act or to refrain from acting in accordance with his duty or in the exercise of his functions in a way which damages or is likely to damage the Union's financial interests. "Active corruption" means the action of a person who promises, offers or gives, directly or through an intermediary, an advantage of any kind to a public official for himself or for a third party for him to act or to refrain from acting in accordance with his duty or in the exercise of his functions in a way which damages or is likely to damage the Union's financial interests. *See id.* at art. 4.

[61] "Misappropriation" means the action of a public official who is directly—or indirectly—entrusted with the management of funds or assets to commit or disburse funds or appropriate or use assets contrary to the purpose for which they were intended in any way which damages the Union's financial interests.

[62] *See* Directive 2017/1371, *supra* note 59, at art. 3. In respect of revenue arising from VAT own resources, any act or omission committed in cross-border fraudulent schemes in relation to:

(i) The use or presentation of false, incorrect or incomplete VAT-related statements or documents, which has as an effect the diminution of the resources of the Union budget;

(ii) non-disclosure of VAT-related information in violation of a specific obligation, with the same effect; or

(iii) the presentation of correct VAT-related statements for the purposes of fraudulently disguising the non-payment or wrongful creation of rights to VAT refunds.

EPPO to include serious cross-border criminality.[63] The question is: Which EU financial crimes should be subject to EPPO enforcement?

A reasonable approach to this issue is to determine which type of financial crimes—in a broad sense—has already been subject to EU harmonization pursuant to the clause included in Article 83.1 TFEU. Out of the wording of this legal provision, the following areas stand out: Money laundering, corruption, and counterfeiting of means of payment. As we shall see, these areas are traditionally enforced by federal institutions in other countries—most notably by American Federal Prosecutors.

Approaching this expansion solely from an Article 83.1 TFEU perspective could prove to be short sided. In this sense, a reasonable interpretation could also include those cases which are included in the criminal harmonization movement pursuant to Article 83.2 TFEU. For example, ensuring an effective implementation of a Union policy, that—being serious enough—affects more than one Member State.

The specific instance that comes to mind is the above mentioned EU Market Abuse. Since July 3rd, 2016, the Directive 57/2014 establishing criminal sanctions for Market Abuse entered into force. The Directive establishes the elements of the crimes of market manipulation and insider trading. When such misconduct affects more than one Member State it would seem reasonable that the EPPO could have jurisdiction. This holds especially true when EU Supervisory Agencies are already exerting EU power over this area. To this extend, the European Securities and Markets Authority—ESMA—has initiated various enforcement actions since its inception[64] and, actually, the hotly contested enforcement powers was a key issue over which the Court of Justice of the European Union—CJEU—had to rule on in Case C-270/12, *UK v. Council of the European Union and European Parliament.*[65]

In this area it should also be noted that the recent—and to some extent, revolutionary—case law of the CJEU regarding the *ne bis in idem* principle, supports the importance of

[63] The European Council may—at the same time or subsequently—adopt a decision a mending paragraph one in order to extend the powers of the European Public Prosecutor's Office to include serious crime having a cross-border dimension and amending accordingly paragraph two as regards the perpetrators of, and accomplices in, serious crimes affecting more than one Member State. The European Council shall act unanimously after obtaining the consent of the European Parliament and after consulting the Commission.

[64] *See Enforcement Actions,* EUROPEAN SECURITIES AND MARKETS AUTHORITY, https://www.esma.europa.eu/supervision/enforcement/enforcement-actions

[65] *See* Case C-270/12, United Kingdom of Great Britain and Norther Ireland v. European Parliament and Council of the European Union, 2014 I.C.J. 562 (Sept. 12).

market abuse in the context of the EU. In this sense, both in *Garlsson*[66] and *Di Puma*,[67] the CJEU stresses the importance of protecting both the integrity of the financial markets of the EU and public confidence in financial instruments. To achieve these objectives, combating infringements of the prohibition on market manipulation and duplicating criminal and administrative proceedings, penalties may be justified. Therefore, an extension of the EPPO's jurisdiction in this area would be consistent with the importance that the CJEU weighs in on combating market manipulation.

Moreover, it cannot be ruled out that there be a potential extension of the EPPO's powers to areas related to banking supervision and the resolution of credit institutions. For example, contexts in which the existence of EU Agencies has to be kept in mind. This, again, holds especially true when in some instances EU legislation is already imposing the obligation on EU Institutions to ensure that individuals and companies are hold criminally accountable, and Member States are obliged to impose "effective, proportionate and dissuasive" sanctions for not complying with the obligations of EU legislation.[68] In this sense—in the context of the resolution of credit institutions by the Single Resolution Mechanism—Regulation 806/2014[69] establishes as a general principle a governing resolution—Article 15—that the Board, the Council, and the Commission ensure that natural and legal persons are made liable, subject to national law, under civil or criminal law**,** for their responsibility for the failure of the institution under resolution.

---

[66] *See* Case C-537/16, Garlsson Real Estate and Others v. Commissione Nazionale per le Societ à e la Borsa (CONSOB), 2018 I.C.J 193 (Mar. 20).

[67] *See* Joined Cases 596 & 597/16, Enzo Di Puma v. Commissione Nazionale per le Societ à e la Borsa (CONSOB) and Commissione Nazionale per le Societ à e la Borsa (CONSOB), v. Antonio Zecca, 2018 I.C.J. 192 (Mar. 20).

[68] Directive 2014/59, of the European Parliament and of the Council of 15 May 2014, Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms, art. 110, 2014 O.J. (L 173) 190-348**.**

> Without prejudice to the right of Member States to provide for and impose criminal penalties, Member States shall lay down rules on administrative penalties and other administrative measures applicable where the national provisions transposing this Directive have not been complied with, and shall take all measures necessary to ensure that they are implemented. Where Member States decide not to lay down rules for administrative penalties for infringements which are subject to national criminal law they shall communicate to the Commission the relevant criminal law provisions. The administrative penalties and other administrative measures shall be effective, proportionate and dissuasive.

[69] *See* Regulation 806/2014 of the European Parliament and of the Council of 15 July 2014, establishing Uniform Rules and a Uniform Procedure for the Resolution of Credit Institutions and Certain Investment Firms in the Framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation 1093/2010, 2014 O.J. (L 225) 1-90; Directive 2014/59, of the European Parliament and of the Council of 15 May 2014, Establishing a Framework for the Recovery and Resolution of Credit Institutions and Investment Firms, art. 34, 2014 O.J. (L 173) 190-348.

As the current wording shows, for now it seems enough for those EU Institutions to make a referral to the national authorities in order to ensure that the individuals and companies face criminal charges—if necessary—for the failure of the credit institution. Yet, it cannot be ruled out that—as a future development of the EPPO powers—in the near future those powers are extended to cases in which the failure of the credit institution affects more than one Member State, when the credit institution is subject to the Single Resolution Mechanism.

As a summary, there are three potential avenues for expanding EPPO powers: (a) Those areas already subject to EU criminal harmonization on the basis of serious cross-border criminality—contained in Article 83.1 TFEU; (b) those cases subject to EU criminal harmonization on the basis of a need to implement a EU policy, that additionally affect more than one Member State; and (c) those cases not subject to EU criminal harmonization, but that are governed by EU law and affect more than one Member State. Yet how does a possible extended jurisdiction of the EPPO correspond with the EU idea of subsidiarity and better regulation?[70] And what does it tell us about the EU's legislation against fraud against the EU's budget in general?

V. The Fraud Directive and the Better Regulation Agenda and Links to the EPPO Project

The discussion above should also be seen in the general context of the EU combat against financial crimes beyond the EU's budget. For example, an additional development in the EU's anti-fraud strategy and related to the establishment of an EPPO more generally, is the recent Directive on the fight against fraud to the Union's financial interests by means of criminal law.[71] The Directive is based on Article 325 TFEU and the fight against fraud against the EU's budget—at first instance this appears to be a significant development in the evolution of the EU's counter fraud strategy. Yet similarly to the EPPO, the scope of the proposed Directive is limited to fraud committed against the financial interests of the EU. The Directive claims that the anti-fraud framework of Article 325 TFEU is complemented by general Union criminal law measures for the fight against certain illegal activities particularly harmful to the licit economy, such as money laundering and corruption—although not specific to the protection of the Union's financial interests they also contribute to their protection.[72]

---

[70] For studies of subsidiarity and EU criminal law, *see e.g.*, JACOB ÖBERG, LIMITS TO EU POWERS: A CASE STUDY OF EU REGULATORY CRIMINAL LAW ch. 7 (2017); SAMALI METTINEN, EU CRIMINAL LAW (2013); Ester Herlin-Karnell, *Subsidiarity in the Area of EU Justice and Home Affairs—A Lost Cause*, 15 EUR. L. J. 351 (2009).

[71] *See* Directive (EU) 2017/1371, *supra* note 59, at 29-41.

[72] *See Proposal for a Directive of the European Parliament and of the Council on the fight against fraud to the Union's financial interests by means of criminal law*, COM (2012) 363 final (July 11, 2012); *See* Council Regulation 2988/95, of 18 December 1995 on the protection of the European Communities financial, 1995 O.J. (L 312) (setting out administrative rules for dealing with illegal activities at the expense of the Union's financial interests).

A key question is whether the EU antifraud system needs to be complemented by the additional establishment of the EPPO. Moreover, one could for instance ask if the EPPO represents "better regulation." In the 2016 Better Regulation Agenda entitled "Better Regulation: Delivering better results for a stronger Union," the Commission pointed out that alternative approaches will be explored where regulatory costs are found to be disproportionate to help achieve the intended goals.[73] In the Better Regulation Agenda of 2017, the EU promises that it will remain big on big things, and respect subsidiarity and proportionality when not.[74] The EU claims that by safeguarding the principles of better regulation, this will ensure that measures are evidence-based, well designed, and deliver tangible and sustainable benefits for citizens, businesses, and society as a whole. Hence, it could be asked if the EPPO really complies with the idea of "better regulation."[75] Article 5 of the EPPO Regulation says that when a matter is governed by a Regulation and national law than the latter shall prevail. The Regulation also states that only procedural matters can be challenged. Of course, the Regulation also assures us again that it complies with fundamental rights—for example the EU Directive on Access to Lawyer.[76] Limiting it to procedural questions might be difficult in practice, and yet, it might be in line with subsidiarity, at least on paper. Still, the EPPO has clearly far-reaching implications for the legal systems of the Member States, in what is generally acknowledged to be the sovereignty-sensitive area of criminal law and procedure. Thus, an EPPO would use standard national methods of investigation and prosecution procedures. Yet a uniform treatment of crime is one of the main reasons given for the adoption of the EPPO in the first place.

VI. Profiling and Data Protection: A Glimpse

[73] *See Communication from the Commission to the European Parliament, the European Council and the Council*: *Better Regulation: Delivering better results for a stronger Union*, COM (2016) 615 final (Sept. 14, 2016).

[74] *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,* COM (2017) 651 final (Oct. 24, 2017).

[75] *See also,* the discussion in Ester Herlin-Karnell, *The Establishment of a European Public Prosecutor's Office: Between 'Better Regulation' and Subsidiarity Concerns, in* THE ESTABLISHMENT OF THE EUROPEAN PUBLIC PROCEUTOR'S OFFICE (EPPO): "STATE OF PLAY AND PERSPECTIVE" (Willem Geelhoed et al. eds., 2018).

[76] *See* Directive 2013/48, of the European Parliament and of the Council of 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 2013/48/EU, 2013 O.J. (L 294) 1, 1-12.

It is obvious that the EPPO Regulation touches upon delicate questions on data protection.[77] Data protection is a fundamental EU right as it is stated in Article 7-8 Charter of Fundamental Rights, Article 16 TFEU, and Article 8 European Convention on Human Rights.[78]

For this reason, Article 52 in the EPPO Regulation is interesting here. The provision makes it clear that if it emerges that incorrect operational personal data has been transmitted, or operational personal data has been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the operational personal data shall be rectified, erased, or processing shall be restricted in accordance with Article 61 stating that, *inter alia*, the data subject shall have the right to obtain from the EPPO without undue delay the rectification of inaccurate operational personal data relating to him or her.

Also, Article 56 of the EPPO Regulation is interesting in this respect concerning "automated individual decision-making, including profiling." It stated that:

> The data subject shall have the right not to be subject to a decision of the EPPO based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her. As a general rule, the controller shall provide the information in the same form as the request.[79]

Of central importance to the processing of data is also who is to be counted as a processor. Article 65 of the Regulation sets out to regulate the notion of processing. Specifically, it stipulates that:

> Where processing is to be carried out on behalf of the EPPO, the EPPO shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner

[77] *See* Directive 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 Offenses or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision, 2008/977/JHA, 2016 O.J. (L 119) 89-131.

[78] *See also,* discussion in Els de Busser and Anne De Hing's article in this special issue; *see, e.g.*, Case C-293/12, Dig. Rights Ir. v. Minister for Commc'ns, Marine and Nat. Res. & Others, 2014 I.C.J. 238 (April 8); Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 I.C.J 650 (Oct. 6, 2015).

[79] EPPO Regulation, *supra* note 46, at art. 56-65.

> that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.[80]

Yet the definition of what processing means remains unclear as well as who is a reliable "processor" in this context.

Needless to say, this is uncharted territory and the cooperation with Europol, and other EU key agents, regarding the processing of data and what is considered "proportionate" will have a very interesting future ahead of it. Moreover, in the Preamble—recital nr 98 of the EPPO Regulation—it is stated that that European Data Protection Supervisor should have the tasks laid down in the EPPO Regulation and should have effective powers, including investigative, corrective, and advisory powers to the EPPO which constitute the necessary means to perform those tasks. This seems welcome. In addition, the EPPO is already bound by the provision in Article 5 of the Regulation, and by EU principles in general on fundamental rights, that it must confirm with proportionality and the rule of law.

Let us now turn to the other side of the Atlantic and discuss the American model of federal prosecutors and see how different that system really is from the EU.

D. A Comparative Perspective: The American Federal Prosecutors

I. Background

Although American federal criminal law is based on vertical federalism, and EU criminal law shows signs of horizontal federalism, it pays to summarily note certain key features of the American system in order to assess the different structure used by both Unions to secure the same goal.[81]

Federal prosecution in the US is assigned to the US Attorney's Office. Yet, their competence goes beyond criminal law enforcement, as they are also involved in civil litigation when the US is a party. As a general statement, the 93 US Attorneys work to enforce federal laws throughout the US ensuring "that the laws be faithfully executed."[82] The Judiciary Act of 1789 directs the President of the USA to appoint, in each federal district, "a meet person

[80] Article 65. 1 of the EPPO Regulation.

[81] *See* CARLOS GÓMEZ-JARA DÍEZ, FEDERAL EUROPEAN CRIMINAL LAW (2015); Auke Willems, Mutual Trust as a Core Principle of EU Criminal Law: Conceptualizing the Principle with a view to Facilitate Mutual Recognition in Criminal Justice Matters (2017) (unpublished PhD thesis) (on file with Vrije Universiteit Brussel and Université Libre de Bruxelles).

[82] U.S. CONST. art II.

learned in the law to act as an attorney for the United States."[83] According to the pertaining legislation, the function of the United States Attorney was "to prosecute in [each] district all delinquents for crimes and offenses cognizable under the authority of the United States, and all civil actions in which the United States shall be concerned."[84]

Important to note is that before the US Civil War, US Attorneys prosecuted only the cases mentioned specifically in the Constitution; namely, piracy, counterfeiting, treason, felonies committed on the high seas, or cases resulting from interference with federal justice—perjury, bribery—extortion by federal officers, thefts by employees from the United States Bank, and arson of federal vessels.[85] Over the years, however, their powers have expanded, as we will relate below.

Similar to the EU process, in the US the federal prosecutors were provided with the powers to prosecute cases specified in the founding text—similar to the protection of the EU financial interests as noted in Article 86 TFEU. But in the US, those powers were subsequently extended over the years; a situation that probably will also take place in the EU.

There are 93 US Attorneys with over 350 Assistant US Attorneys. In addition to their main offices, many US Attorney's maintain smaller satellite offices throughout their districts.[86] US Attorneys are appointed by the President, confirmed by the Senate, and they serve terms of four years, or at the President's discretion. While the US Attorney is a political appointee, the Assistants, by law, hold non-partisan jobs, so political affiliations or beliefs should play no role in how they are hired, fired, or promoted—but this has not always been the case.

In general, the USAO consists of two major divisions: Criminal and civil. The criminal division, which is significantly larger than the civil division in most offices, prosecutes violations of the federal criminal laws. Many criminal divisions have specialized units or sections within them. Many criminal divisions now have a national security section or unit and work with state and local governments to combat terrorist activities.

The structure of the criminal division of the US Attorney's Office—for example, the American Federal Prosecutor's Office— shows the vertical approach of the US system and the highly specialized sections that are integrated into a coherent body. The local prosecutors of the

[83] Judiciary Act of 1789, § 35, 1 Stat. 73.

[84] *Id*.

[85] *See* JAMES EISENSTEIN, COUNSEL FOR THE UNITED STATES: U. S. ATTORNEYS IN THE POLITICAL AND LEGAL SYSTEMS 9 (1978).

[86] *Find Your United States Attorney,* DEPARTMENT OF JUSTICE, http://www.justice.gov/usao/districts.

various States that conform the US do not play any role.[87] The structure of the American Federal Prosecutor's Office and the EPPO is substantially different, especially with the introduction of the "College of European Prosecutors" and the "Permanent Chambers." Put simply, the American Federal Prosecutor's Office does not have to manage the various interests of enforcement authorities of Member States that—although guided by the same goal of protecting the Union's financial interests—might have conflicting agendas. Also, it seems reasonable that as the case load increases, there will be a need to establish various sections in the EPPO that specialize in different areas. If the expansion of the EPPO powers takes place, this will be even more necessary.

In any event, the United States Attorney retains a large degree of independence and prosecutorial discretion.[88] Obviously, United States Attorneys receive direction and policy advice from the Attorney General and other Department officials, but the United States Attorney has wide latitude in determining what cases are taken under consideration in his or her district. "The discretionary power to decide whether to prosecute is awesome," admitted one US Attorney.[89] This power is so formidable that, "if the United States Attorney abuses this power, the only available remedy is removal."[90]

From this perspective, the EPPO regulation seems to also provide a great deal of discretion to the European Prosecutors, and no specific regime of liability for abuse of its power—absent from the data protection provisions contained in Art. 47—seems to be foreseen.

Granting such prosecutorial discretion to the EPPO should give us pause. The experience of the US federal system in which, as noted, the AFPO's prosecutorial discretion goes largely un-reviewed,[91] has generated considerable criticism. The alleged gatekeeper function of prosecutors has no real enforcement mechanisms, and instead is dependent upon the

[87] *Organizational Chart,* DEPARTMENT OF JUSTICE, https://www.justice.gov/criminal/sectionsoffices/chart.

[88] For some classic explanations, *see* John Kaplan, *The Prosecutorial Discretion—a Comment*, 60 NW. U. L. REV. 174 (1965); Wayne LaFave, *The Prosecutor's Discretion in the United States*, 18 AM. J. COMP. L. 532 (1970).

[89] *Id.* at 47.

[90] *Id.*

[91] For an introductory view from the Government side, *see* James Gorelick & Harry Litman, *Prosecutorial Discretion and the Federalization Debat*e, 46 HASTINGS L.J. 967 (1995) (explaining why the principle that the federal courts should never, or even rarely, be able to exercise criminal jurisdiction over areas of criminal law that also fall under the concurrent jurisdiction of the state system is flawed); for a general overview, *see* Gerard E. Lynch, *Our Administrative System of Criminal Justice*, 66 FORDHAM L. REV. 2117, 2138-2142 (1998); some interesting statistics were provided by Richard S. Frase, *The Decision to File Federal Criminal Charges: A Quantitative Study of Prosecutorial Discretion*, 47 U. CHI. L. REV. (1980) at 246, 257, 278 .

ethical personal integrity of the member of the US Attorney's Office.[92] In theory, defendants may make a claim of discrimination under the selective prosecution doctrine, arguing that a prosecutor chose to pursue their case for illegitimate reasons.[93] Nevertheless, this standard is purposefully high, with a presumption that even the preliminary showing to obtain discovery should "be a significant barrier."[94] There are mechanisms within the DOJ, which in turn have congressional supervision, that provide the necessary doses of control that make the system at least bearable for the citizenry.[95] This prosecutorial leeway raises important issues in a criminal justice system where many crimes fall under concurrent state and federal jurisdiction.[96] Combined with the already discussed proliferation of federal criminal laws in the US, individual prosecutors in the US perhaps have the most say in whether or not a crime is treated as federal or left to state mechanisms.

There has also been some debate over the political dependence of US Attorneys,[97] who are appointed by the federal government, but serve in decentralized offices throughout the American landscape. It is no easy task to coordinate opposing interests, as the perception of

---

[92] Though the piece is more than 30 years old, the work of James Vorenberg, *Decent Restraints in Prosecutorial Power*, 94 HARV. L. REV. 1521, 1559 (1981) is worth revisiting. As he noted at 1554:

> Prosecutors are not held to anything remotely like what due process would require if they were engaged in an acknowledged rather than a hidden system of adjudication. No uniform, pre-announced rules inform the defendant and control the decision-maker; a single official can invoke society's harshest sanctions on the basis of ad hoc personal judgments. Prosecutors can and do accord different treatment--prison for some and probation or diversion to others--on grounds that are not written down anywhere and may not have been either rational, consistent, or discoverable in advance.

[93] *See U.S. v. Armstrong,* 517 U.S. 456 (1996) (explaining the procedural requirements of a selective prosecution claim).

[94] Not surprisingly, many consider this threshold to be virtually insurmountable in many cases, leaving prosecutorial discretion effectively unreviewable. *Id*. at 463-64. *See* Anne Bowen Poulin, *Prosecutorial Discretion and Selective Prosecution: Enforcing Protection after United States v. Armstrong,* 34 AM. CRIM. L. REV. 1081 (1997) (referring to this defense right as "The Disfavored Right"); Yaov Sapir, *Neither Intent nor Impact: A Critique of the Racially Based Selective Prosecution Jurisprudence and a Reform Proposal*, 19 HARV. BLACKLETTER L. J. 127 (2003); Richard H. McAdams, *Race and Selective Prosecution: Discovering the Pitfalls of Armstrong*, 73 CHI.-KENT L. REV. 605 (1998).

[95] *See* Daniel C. Richman, *Federal Criminal Law, Congressional Delegation, and Enforcement Discretion*, 46 UCLA L. REV. 757 (1999) (noting, however, that Congress cannot use many of the tools for monitoring and managing delegated criminal enforcement authority that it can draw on to constrain bureaucratic discretion in other areas).

[96] *See* Robert Heller, Commentary, *Selective Prosecution and the Federalization of Criminal Law: The Need for Meaningful Judicial Review of Prosecutorial Discretion*, 145 U. PA. L. REV. 1309, 1309-15 (1997) (noting that "[c]oncurrent jurisdiction due to the federalization of criminal law introduces into the criminal justice system a potential for prosecutorial abuse that was not an area of concern when crime was primarily a locally regulated phenomenon").

[97] *See* Sara Sun Beale, *Rethinking the Identity and Role of US Attorneys*, 6 OHIO ST. J. CRIM. L. 369 (2009).

certain issues from D.C. might greatly differ from the more local needs that the regional offices face. Add opposing political interests to the mix and the potential for dispute grows.

This issue is very relevant to the EPPO, especially because Brussels is perceived as even more of an outsider in the EU than Washington D.C. is in the US. The US controversy between local and federal prosecutors could be reduced or avoided in the EU if criminal law were limited to "direct" or "genuine" European offenses, so that the risk of overlapping with Member States' regulations is hence diminished. Such limitations would also reduce the power—and the problem—of federal prosecutors to invoke a different law and punishment for similar defendants at their discretion. There could still be some local hesitance to prosecute valued members of the local community, and this hesitation will be exacerbated by the fact that they will be tried in state courts applying European standards. Overall, though, the system will have a greater chance to maintain its integrity if offenses that are perceived to be only of state interest are left to the corresponding authorities of the Member States.

I. Jurisdiction of the American Federal Prosecutors

As noted before the initial powers of the American Federal Prosecutor's Office were limited to those specific areas of criminal law foreseen in the US Constitution. Given that the EPPO foresees a potential expansion of its jurisdiction, it pays to review in which areas the jurisdiction of the American Federal Prosecutor's Office has been expanded. The comparison will highlight the areas in which the expansion of the EPPO would be consistent with the approach undertaken by the US federal system. The current areas of AFPO enforcement are the following:

First, on public integrity, consider the following categories: (i) Identifying, investigating, and prosecuting corrupt government officials; (ii) providing expertise, guidance, and instruction to law enforcement agents and prosecutors on matters involving corruption; and (iii) ensuring that sensitive public corruption and election crime matters are handled in a uniform, consistent, and appropriate manner across of the US. As noted before, Directive 2017/1371 confers powers to the EPPO in order to prosecute active and passive corruption—when related to EU financial interests.[98] The American experience shows that this is as sensitive as productive area of enforcement by federal prosecutors.[99]

[98] *See* Directive 2017/1371, *supra* note 59, at 72.

[99] *See* Peter J. Henning, *Federalism and the Federal Prosecution of State and Local Corruption*, 92 KENT. L.J. 1 (2003) ("[s]ince the 1970s, federal prosecutors have been particularly active in prosecuting state and local officials for corruption"). The interesting issue is that, with time, federal prosecutors have prosecuted state and local officials even if no federal funds were involved; *see* Peter J. Henning, *Federalism and the Federal Prosecution of State and Local Corruption*, 92 KENT. L.J. 1, 2 (2003) ("[d]o federal prosecutors invade an area traditionally reserved to the states by applying federal statutes to local corruption that does not implicate the exercise of any direct federal power or the misuse of federal funds?"). A similar trend could take place in the EU given the widespread consensus against corruption and the perceived inaction by national prosecutors in some instances.

Second, when it comes to human rights and special prosecutions concerns the following**:** (i) Investigating and prosecuting cases related to human rights violations; (ii) international violent crime, and complex immigration crimes; (iii) and pursuing the US Government's commitment to holding accountable human rights violators and war criminals, both as a domestic law enforcement imperative and as a contribution to the global effort to end impunity.

Third, the crime of fraud concerns the following: Investigating and prosecuting sophisticated and multi-district white-collar crimes including corporate, securities, and investment fraud, government program and procurement fraud, health care fraud, and international criminal violations including the bribery of foreign government officials in violation of the Foreign Corrupt Practices Act. As discussed above, Directive 2017/1371 gives powers to the EPPO in order to prosecute only fraud against the financial interests of the EU in terms of procurement fraud and VAT fraud. The American legislation encompasses not only such specific fraud offenses—for example fraud against the Union—but all types of fraud when they affect interstate commerce.

Fourth, the crime of child exploitation involves: (i) Prosecuting high-impact cases involving online child pornography, the online grooming and inducement of children by sexual predators, sex trafficking of children, travel abroad by US citizens and residents to sexually abuse foreign children—sex tourism—and enforcement of sex offender registration laws; (ii) providing forensic assistance to federal prosecutors and law enforcement agents in investigating and prosecuting violations of federal criminal statutes criminalizing child exploitation; (iii) coordinating nationwide operations targeting child predators; (iv) and developing policy and legislative proposals related to these issues. By contrast, the current EPPO powers do not allow this EU agency to prosecute this type of offenses. Yet, as noted previously, Article 86.4 TFEU foresees the possibility of expanding EPPO powers to serious cross-border criminality. Given that the EU has already harmonized the area of sexual exploitation of women and children on the basis of Article 83.1 TFEU, it would be reasonable to include child exploitation among the prosecutable offenses by the EPPO in cases involving a cross-border dimension. This would not only have a specific legislative basis on Article 86.4 in connection with Article 83.1 TFEU, but it would also match the current situation in the US System.

Fifth**,** computer crime and intellectual property crime involve: (i) Working to prevent and respond to criminal cyber-attacks; (ii) improving the domestic and international laws to most effectively prosecute computer and IP criminals; (iii) and directing multi-district and transnational cyber investigations and prosecutions. Again, harmonization of criminal law among EU Member States has taken place regarding computer crime on the basis of Article

83.1 TFEU. Therefore–although not yet among the EPPO powers–computer crime with a cross-border dimension could reasonably become a prosecutable offense by the EPPO when it involves a cross-border dimension. The fact that the US system also confers such powers to the US Federal Prosecutors provides support for this option.

Sixth, regarding narcotics and dangerous drugs concern the following**:** (i) Combating domestic and international drug trafficking and narco-terrorism; (ii) drawing on available intelligence to prosecute individuals and criminal organizations posing the most significant drug trafficking threat to the US; (iii) enforcing laws that criminalize the extraterritorial manufacture or distribution of controlled substances intended for the US; (iv) and facilitating the provision of targeted intelligence support to DEA and other law enforcement agencies worldwide. The same basis and logic referred previously for child exploitation and computer crime as future prosecutable offenses by the EPPO, applies to drug trafficking. Included specifically in Art. 83.1 TFEU, this is one of the well-known pillars of enforcement by the US Federal Prosecutors.

Seventh, concerning organized crime involve the following: (i) Overseeing the Department's program to combat organized crime by investigating and prosecuting nationally and internationally significant organized crime organizations and gangs; (ii) exercising approval authority over all proposed federal prosecutions under the Racketeer Influenced and Corrupt Organizations (RICO) and Violent Crimes in Aid of Racketeering (VICAR) statutes; (iii) supporting criminal prosecutions of federal crimes involving labor-management disputes, the internal affairs of labor unions in the private sector, and the operation of employee pension and welfare benefit plans; (iv) working with US intelligence agencies and US and foreign law enforcement agencies to identify, target, and investigate transnational organized crime groups; (v) and contributing to the development of policy and legislation relating to numerous organized crime-related issues, including gambling and human trafficking.

Yet another example of currently non-prosecutable offenses by the EPPO, combating organized crime has been subject to EU harmonization through Article 83.1 TFEU and would be reasonable to include among EPPO's powers. This holds especially true if it is taken into account that organized crime many times has a cross-border dimension, even if the specific misconduct only surfaces in one Member State. It is also worth noting that offenses such as child exploitation and drug trafficking are most of times conducted by criminal organizations. Therefore, potential EPPO enforcement in such areas should also include organized crime, as is the case in the US system.

Eight, regarding money laundering and asset recovery involve the following: (i) Pursuing criminal prosecutions against financial institutions and individuals engaged in money laundering, Bank Secrecy Act, and sanctions violations; (ii) pursuing the proceeds of high level foreign corruption through the Kleptocracy Asset Recovery Initiative; (iii) developing legislative, regulatory, and policy initiatives to combat global illicit finance; (iv) returning

forfeited criminal proceeds to benefit those harmed by crime through remission and restoration processes; (v) and providing legal and policy assistance and training to federal, state, and local prosecutors, and law enforcement personnel, as well as to foreign governments.

Laundering the proceeds from the above-mentioned criminal activities is a regular activity conducted by the perpetrator of such offenses. Again, Article 83.1 TFEU has secured EU harmonization in this area, and it would be reasonable to conclude that it should also be part of the EPPO enforcement powers.

In sum, a comparison between the EPPO's and the US Federal Prosecutors' jurisdiction shows that the "expansion clause" established in Article 86.4 TFEU for the EPPO relates to the same areas of criminality currently being prosecuted by US Federal Prosecutors. The logic behind such expansion in both Unions is the need to effectively address serious cross-border criminality. Regarding the EU approach, such expansion would be consistent with the EU Security Agenda discussed previously.

E. Conclusion: Prosecuting EU Financial Crimes, Dream or Reality?

As seen above, on the one hand, the EU financial crimes system is not as developed as the American system when it comes to questions of enforcement and competences. Yet both systems are concerned with securing security across states. On the other hand, the EPPO regime and EU law in general is more matured, if you will, concerning the right to data protection and privacy as fundamental rights. A key difference between the EU and the US is the structure of both the EPPO and the USAO. While the US structure reflects the strong vertical federalism approach of the US system, the EPPO is based on the horizontal federalism that characterizes the EU approach to criminal law. The functioning of the complex structure of the EPPO is yet to be tested, but from the outset it is easy to see that it will have to surmount serious obstacles in order to provide effective responses to cross-border criminality, especially when national and supranational authorities might have conflicting interests.

The expansion of EPPO's jurisdiction would require an expansion of its budget. As noted, the current EPPO structure expects to cost about €375 million over the next 20 years. Yet, the yearly budget of the already expanded USAO Criminal Division is roughly 1.5 million USD.[100] The difference is outstanding. Yet, the amount collected by the USAO in criminal and civil debt is equally relevant: For FY 2015, it collected 21 million USD. Once the EPPO starts functioning it will be important to review the amount collected.

[100] *See* U.S. ATTORNEYS (USA), https://www.justice.gov/jmd/file/822056/download.

In conclusion, prosecuting financial crimes could be more than mere wishful thinking. The more realistic question is perhaps to what extent we need the EPPO, and why prosecuting financial crimes is so important for the EU in a time with so many challenges to the EU project beyond the sphere of financial crimes. As is stated in preamble 19 of the EPPO regulation, the EPPO should issue a public Annual Report on its general activities, which at a minimum should contain statistical data on the work of the EPPO. It remains to be seen if the number of prosecutions is a good yardstick of the successfulness of the EPPO project.

Finally, it may seem a bit odd that the EU is only legislating on the prosecution of financial crimes, but leaves the question of criminal law defense largely untouched. The EU Charter of Fundamental Rights and European Convention on Human Rights are of course instrumental here as well as measures such as, *inter alia*, the Directive on Right to Access to Lawyer.[101] While the US has federal defense lawyers in place, the specialization of EU criminal law—as seen above—the question of fraud against the EU budget and related activities are often interconnected with EU—criminal—law and security governance in general—is still in its early days.

[101] *See* Directive 2013/48/EU, on the Right of Access to a Lawyer in Criminal Proceedings and on the Right to Communicate Upon Arrest, 2013 O.J. (L 294) 1-12.

Articles

The EU's Fight Against Corporate Financial Crime: State of Affairs and Future Potential

By Vanessa Franssen[*]

Abstract

Considering the European Union's efforts to tackle various forms of financial crime more effectively, especially since the financial crisis of 2008, one would expect that the Union has also been strengthening its grip on national law with respect to corporate financial crime. Instead, this Article finds that the EU approach to corporate financial crime has actually not evolved that much over the past two decades. Moreover, this Article demonstrates that EU law still fails to sufficiently take into account the specific features of corporate entities (as opposed to individuals), as well as to fully exploit the potential strengths of a criminal law approach, as opposed to an administrative or civil law approach. In the author's view, the EU should more carefully consider the objectives and strengths of different kinds of enforcement mechanisms and adopt a more coherent approach, particularly with respect to corporations. Furthermore, when it comes to corporate punishment, the EU seemingly lacks ambition and creativity. EU legal instruments focus strongly on fines while insufficiently exploring other, potentially more adequate sanctions to achieve certain punishment goals. Ultimately, this may undermine the effectiveness of the EU's fight against corporate financial crime.

[*] Associate Professor, University of Liège, Faculty of Law, Political Science and Criminology, Liège, Belgium, Affiliated Senior Researcher, KU Leuven, Faculty of Law, Leuven, Belgium. Email: vanessa.franssen@uliege.be. The author is grateful to Els De Busser and Ester Herlin-Karnell for their comments, and to Julie Debroux for her editorial assistance.

A. Introduction

Financial crime is frequently committed in business settings. Considering the efforts of the EU to tackle various forms of financial crime[1]—efforts which have definitely intensified since the 2008 financial crisis—it would not come as a surprise that the EU had also sought to strengthen its grip on national law in order to combat corporate (financial) crime.

In addition to important regulatory efforts[2] primarily aimed at prevention and compliance, the deterrence and punishment of corporations—or "legal persons," which is the term preferred by the EU legislator—are prominent concerns for the EU legislator. Recent examples can be found in the EU legal framework on market abuse, counterfeiting of the euro, and the protection of the Union's financial interests.

Nevertheless, despite the EU's emphasis on combatting financial crime committed by or in the context of corporations, the EU does not explicitly require Member States to provide for corporate *criminal* liability. EU legal instruments encompassing a requirement to provide corporate liability leave it up to the Member States to opt for a criminal, administrative, or civil corporate liability regime. This margin of discretion can be explained by the fact that, after all these years, Member States still do not agree on the theoretical acceptability and/or practical feasibility of corporate criminal liability, despite the clearly growing trend otherwise.[3]

Yet, as demonstrated later in this Article, Member States' discretion in applying the label of their choice is not unlimited. Certain EU legal instruments set forth detailed rules on corporate liability as well as certain punishment objectives and/or specific types of sanctions. Hence, even if a Member State decides to label the corporate liability regime as

[1] Defining economic and financial criminal law is a challenge in itself. Indeed, as a branch of criminal law, it is quite ill-defined. *See* Katalin Ligeti & Vanessa Franssen, *Current Challenges in Economic and Financial Criminal Law in Europe and the US*, *in* CHALLENGES IN THE FIELD OF ECONOMIC AND FINANCIAL CRIME IN EUROPE AND THE US 2–5 (Katalin Ligeti & Vanessa Franssen eds., 2017).

[2] For a critical analysis of the EU's regulatory approach in the field of financial crime see generally Ester Herlin-Karnell, *Constructing Europe's Area of Freedom, Security, and Justice Through the Framework of "Regulation": A Cascade of Market-Based Challenges in the EU's Fight Against Financial Crime*, 16 GERMAN L.J. 49, 52 (2015).

[3] For instance, it is interesting to observe the evolution between 2000 and 2012. Whereas the authors of *Corpus Juris* still concluded that "divergence is strong" with respect to the acceptability of corporate criminal liability, the authors of a 2012 study ordered by the European Commission established that "[d]espite a tendency towards the introduction of criminal liability of legal persons for offen[s]es, significant differences still exist in the approach developed in the member states." MIREILLE DELMAS-MARTY & JOHN A. E. VERVAELE, THE IMPLEMENTATION OF THE CORPUS JURIS IN THE MEMBER STATES 74–75 (2000); GERT VERMEULEN, WENDY DE BONDT & CHARLOTTE RYCKMAN, LIABILITY OF LEGAL PERSONS FOR OFFENCES IN THE EU 10 (2012).

administrative or civil, the basic characteristics of this liability may still be essentially "criminal" in nature—i.e., according to the *Engel* criteria applied by the European Court of Human Rights, which are mirrored by the Court of Justice of the European Union in its *Bonda* case law.[4]

This Article demonstrates that, despite efforts to combat financial crime more effectively, the EU approach to corporate financial crime has not evolved significantly over the past two decades. Moreover, it will argue that EU law still does not sufficiently take into account the specific features of corporate entities (as opposed to individuals), nor does it fully exploit the potential strengths of a criminal law approach—as opposed to an administrative or civil law approach. It is this author's view that the EU should more carefully consider the objectives and strengths of different kinds of enforcement mechanisms and adopt a more coherent approach,[5] particularly with respect to corporations.

Furthermore, when it comes to corporate punishment, the EU lacks ambition and creativity. EU legal instruments focus strongly on fines while insufficiently exploring other, potentially more adequate sanctions to achieve certain punishment goals. Ultimately, this likely undermines the effectiveness of the EU's fight against corporate financial crime.

This Article will be structured as follows. To begin, Section B contains a general overview of the legal framework on corporate crime at the EU level—finding that since the Amsterdam Treaty entered into force, the EU's approach has changed very little, notwithstanding the extension of the EU's powers in the field of criminal law by the Lisbon Treaty. Next, Section C examines more closely the existing EU provisions on the liability of and sanctions for legal persons. This is accomplished by first analyzing the nature of the liability regime imposed by the EU and investigating whether the EU's approach is consistent with its own objectives. This is followed by a presentation of the different criteria for corporate liability comprised in the EU standard clause. Throughout the entire analysis, special attention is paid to the EU's method of taking into account the particular characteristics of corporate offenders. This analysis questions whether the EU's approach is sufficiently tailor-made. Subsequently, the present requirements of the EU with respect to sanctions are scrutinized, as are some astonishing gaps in the current legal framework and striking differences with EU punitive administrative law. Section D concludes that, although the EU legal framework on corporate financial crime seems firmly established, there is considerable room for improvement—not

[4] For a more extensive analysis of the *Engel* criteria and comparison with the case law of the Court of Justice see Vanessa Franssen, *La notion "pénale": mot magique ou critère trompeur? Réflexions sur les distinctions entre le droit penal et le droit quasi pénal*, *in* EXISTE-T-IL ENCORE UN SEUL *NON BIS IN IDEM* AUJOURD'HUI? 56–91 (Delphine Brach-Thiel ed., 2017).

[5] *See also, e.g.*, Michael Faure & Franziska Weber, *The Diversity of the EU Approach to Law Enforcement: Towards a Coherent Model Inspired By a Law and Economics Approach*, 18 GERMAN L.J. 823 (2017).

only with respect to the nature of and criteria for corporate liability, but also when it comes to the punishment of corporate crime.

B. General Overview of the Current EU Legal Framework on Corporate (Financial) Crime

As indicated in the introduction, the EU's fight against financial crime strongly focuses on corporate crime.

Before outlining a few prime examples of EU law in this area, it is important to note that financial crime is not exclusively committed in a corporate setting, nor by corporations alone. Yet, the fact that it is frequently committed in the context of a business or other type of organization creates particular problems and challenges. What happens inside an organization is likely to be a "black box" for the outside world. As argued elsewhere,[6] this complicates the investigation of corporate crime and pushes legislators and investigating authorities toward new investigative methods, including an increasing reliance on whistle-blowers and leniency programs[7] and the adoption of other negotiated justice strategies.[8] This "black box" phenomenon also partly explains the growing importance of compliance[9] and monitoring programs[10] as both preventive and reactive tools against corporate crime, even if the collateral consequences of corporate prosecutions often play a considerable role too.[11] Moreover, the black box of an organization also renders the attribution of criminal liability difficult, and calls into doubt the adequacy and effectiveness of certain sanctions.[12]

[6] Ligeti & Franssen, *supra* note 1.

[7] For a critical analysis see generally Christopher Harding, *The Role of Whistleblowing and Leniency in Detecting and Preventing Economic and Financial Crime: A Game of Give and Take?*, *in* CHALLENGES IN THE FIELD OF ECONOMIC AND FINANCIAL CRIME IN EUROPE AND THE US 95 (Katalin Ligeti & Vanessa Franssen eds., 2017).

[8] *See, e.g.*, ANTHONY S. BARKOW & RACHEL E. BARKOW, PROSECUTORS IN THE BOARDROOM: USING CRIMINAL LAW TO REGULATE CORPORATE CONDUCT (2011); David M. Uhlmann, *Deferred Prosecution and Non-Prosecution Agreements and the Erosion of Corporate Criminal Liability*, 72 MD. L. REV. 1295 (2013).

[9] *See, e.g.*, Alexander Cappel, *The Necessity of Compliance Programmes Under German Law: "Burden" or "Blessing"?*, *in* CHALLENGES IN THE FIELD OF ECONOMIC AND FINANCIAL CRIME IN EUROPE AND THE US 57 (Katalin Ligeti & Vanessa Franssen eds., 2017).

[10] *See, e.g.*, Vikramaditya Khanna, *Reforming the Corporate Monitor?*, *in* ANTHONY S. BARKOW & RACHEL E. BARKOW, PROSECUTORS IN THE BOARDROOM: USING CRIMINAL LAW TO REGULATE CORPORATE CONDUCT 226. (2011); Bruce Zagaris, *Prosecutors and Judges as Corporate Monitors? The US Experience*, *in* CHALLENGES IN THE FIELD OF ECONOMIC AND FINANCIAL CRIME IN EUROPE AND THE US 19 (Katalin Ligeti & Vanessa Franssen eds., 2017).

[11] Khanna, *supra* note 10, at 227–88.

[12] Vanessa Franssen, European Sentencing Principles for Corporations 260–70 (Jun. 15, 2013) (Ph.D. dissertation, KU Leuven).

The financial crisis triggered questions about the effectiveness of existing regulations and liability regimes as well as their enforcement. In an attempt to address existing weaknesses, the EU legislator adopted and amended various legal instruments in the area of financial criminal law. Such instruments include those related to insider dealing and market manipulation—in short, market abuse[13]—money laundering,[14] the counterfeiting of the euro,[15] and most recently, the protection of the Union's financial interests.[16] Each of these new instruments stresses the importance of corporate (criminal) liability and contains definitions on criminal offenses, aggravating circumstances, accomplice liability and attempt, and certain procedural provisions—e.g. on jurisdiction[17], investigative measures,[18] or even on prescription[19]—that specifically address the liability of and sanctions for legal persons.

Such provisions on corporate liability and sanctions first appeared after the entry into force of the Amsterdam Treaty, which explicitly put forward the ambition to "develop the Union as an area of freedom, security and justice."[20] At first glance, those provisions seem to have

[13] Regulation 596/2014, of the European Parliament and of the Council of 16 Apr. 2014 on Market Abuse and Repealing Directive 2003/6/EC of the European Parliament and the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, 2014 O.J. (L 173) 1 [hereinafter Market Abuse Regulation]; Directive 2014/57/EU, of the European Parliament and of the Council of 16 Apr. 2014 on Criminal Sanctions for Market Abuse, 2014 O.J. (L 173) 179 [hereinafter Market Abuse Directive].

[14] Directive 2015/849, of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) 648/2012, and repealing Directive 2005/60/EC and Commission Directive 2006/70/EC, 2015 O.J. (L 141) 73 [hereinafter The 4th Anti-Money Laundering Directive]. It should be noted, though, that this Directive only obliges Member States to adopt administrative sanctions. For an in-depth analysis of the changes introduced by the Fourth Anti-Money Laundering Directive see the paper of Maria Bergström in this issue.

[15] Directive 2014/62/EU, of the European Parliament and of the Council of 15 May 2014 on the Protection of the Euro and Other Currencies Against Counterfeiting by Criminal Law, and Replacing Council Framework Decision 2000/383/JHA, 2014 O.J. (L 151) 1 [hereinafter Euro Counterfeiting Directive].

[16] Directive 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the Fight Against Fraud to the Union's Financial Interests by Means of Criminal Law, 2017 O.J. (L 198) 29 (EU) [hereinafter: PIF Directive].

[17] *See id.* art. 11; Market Abuse Directive, *supra* note 13, art. 10; Euro Counterfeiting Directive, *supra* note 15, art. 8.

[18] *See, e.g.*, Euro Counterfeiting Directive, *supra* note 15, art. 9; PIF Directive, *supra* note 16, art. 10.

[19] *See, e.g.*, PIF Directive, *supra* note 16, art. 16.

[20] *See* Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts art. 2, Oct. 2, 1997, 1997 O.J. (C 340) 1. Further telling is that

> Without prejudice to the powers of the European Community, the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial

hardly evolved over the past two decades, which in itself is somewhat surprising. This would suggest that the questions raised in the aftermath of the financial crisis did not require an adjustment to those provisions. Such an inference would seem especially true for the provision on corporate liability, which, apart from some very minor differences, has remained unchanged and is copy-pasted from one legal instrument into another one.

Comparatively, the provisions on the sanctions for legal persons have undergone incremental changes over time. For instance, the Environmental Crime Directive of 2008[21] merely states: "Member States shall take the necessary measures to ensure that legal persons held liable pursuant to Article 6 are punishable by effective, proportionate and dissuasive penalties".[22] A similar provision can be found in the Ship-Source Pollution Directive, as amended in 2009.[23] The Directives adopted in the aftermath of the financial crisis, however, demonstrate increasing precision with respect to the minimum requirements for sanctions for legal persons:

> Member States shall take the necessary measures to ensure that a legal person held liable pursuant to [the liability of legal persons as set forth in] Article 6 is subject to effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and may include other sanctions such as
>
> (a) exclusion from entitlement to public benefits or aid;
> (b) temporary or permanent disqualification from the practice of commercial activities;
> (c) placing under judicial supervision;
> (d) judicial winding-up;
> (e) temporary or permanent closure of establishments which have been used for committing the offence.[24]

---

cooperation in criminal matters and by preventing and combating racism and xenophobia.

Id. art. 29.

[21] Directive 2008/99/EC, of the European Parliament and of the Council of 19 Nov. 2008 on the Protection of the Environment Through Criminal Law, 2008 O.J. (L 328) 28 [hereinafter Environmental Crime Directive].

[22] *See id.* at art. 7.

[23] Directive 2009/123/EC, of the European Parliament and of the Council of 21 Oct. 2009, Amending Directive 2005/123/EC on Ship-Source Pollution and on the Introduction of Penalties for Infringements, 2009 O.J. (L 280) 52 [hereinafter Ship-Source Pollution Directive]. It is worth noting that the 2005 Directive did not contain any particular provisions on legal persons, neither with respect to their liability nor regarding the applicable penalties.

[24] *See, e.g.*, Euro Counterfeiting Directive, *supra* note 15, art. 7.

One might be tempted to conclude that the additional requirements imposed by the EU—although neither stringent nor specific, as explained below—are the result of a growing awareness that corporate sanctions should be better tailored to the nature of the corporate offender and the need for a more harmonized approach throughout the Union. But, concluding as much would be far too expeditious and would not take into account the constitutional framework of the Union.

In fact, going back in time, one will find various legal instruments in the field of EU criminal law that already contain more precise requirements. Such instruments include those related to former Framework Decisions on fraud and counterfeiting of non-cash means of payment,[25] corruption in the private sector,[26] terrorism,[27] and organized crime[28]—which already included, notwithstanding some small differences, what has by now become the standard clause on sanctions for legal persons. These instruments were adopted under the former, pre-Lisbon Third Pillar, whereas the Directives in the field of environmental crime and ship-source pollution[29] were adopted under the former First Pillar in the wake of a

[25] *See* Council Framework Decision 2001/413/JHA of 28 May 2001, Combating Fraud and Counterfeiting of Non-Cash Means of Payment, art. 8, 2001 O.J. (L 149) 1 [hereinafter Framework Decision Fraud Non-Cash Means of Payment].

[26] *See* Council Framework Decision 2003/568/JHA of 22 July 2003 on Combating Corruption in the Private Sector art. 6, 2003 O.J. (L 192) 54 [hereinafter Framework Decision Corruption].

[27] *See* Council Framework Decision 2002/475/JHA of 13 June 2002 on Combating Terrorism art. 8, 2002 O.J. (L 164) 3. This Framework Decision has been replaced by Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA, 2017 O.J. (L 88) 6. Nonetheless, as far as the liability of and sanctions for legal persons is concerned, Articles 17 and 18 of the Directive simply reiterate the contents of Articles 7 and 8 of the 2002 Framework Decision.

[28] *See* Council Framework Decision 2008/841/JHA of 24 Oct. 2008 on the Fight Against Organized Crime art. 6, 2008 O.J. (L 300) 42. Organized crime is now largely viewed as economic or business crime committed by "entrepreneurs who operate under conditions of illegality." *See* Federico Varese, *What is Organised Crime?*, *in* REDEFINING ORGANISED CRIME. A CHALLENGE FOR THE EUROPEAN UNION? 33–34 (Stefania Carnevale, Serena Forlati & Orsetta Giolo eds., 2017).

[29] Case C-176/03, *Commission v. Council*, 2005 E.C.R. I-7879 (annulling Framework Decision 2003/80/JHA of 27 Jan. 2003 on the Protection of the Environment Through Criminal Law); Case C-440/05, *Commission v. Council*, 2007 E.C.R. I-9097 (annulling Council Framework Decision 2005/667/JHA of 12 July 2005 to Strengthen the Criminal Law Framework for the Enforcement of the Law Against Ship-Source Pollution). In this landmark case law, the Court of Justice of the European Union (CJEU) ruled that, prior to the Lisbon Treaty, the EC legislator could require Members States, under the former First Pillar, to adopt and apply effective, proportionate, and dissuasive *criminal* penalties if the EC considered such measures "necessary in order to ensure that the rules which it lays down on environmental protection are fully effective." *See* Case C-176/03, *Commission v. Council*, 2005 E.C.R. I-7879, para. 48. By contrast, "the determination of the type and level of the criminal penalties to be applied does not fall within the Community's sphere of competence." *See* Case C-440/05, *Commission v. Council*, 2007 E.C.R. I-9097, para. 70. This case law subsequently led to the adoption of paragraph two of article 83 of the TFEU. For an analysis of this provision see Vanessa Franssen, *EU Criminal Law and* Effet Utile*: A Critical Examination of the Union's Use of Criminal Law to Achieve Effective Enforcement*, *in* EU CRIMINAL LAW AND POLICY. VALUES, PRINCIPLES AND METHODS 87–88 (Joanna Beata Banach-Gutierrez & Christopher Harding eds., 2017).

significant institutional battle concerning the division of competences between the former European Community and the European Union.[30] This explains why the latter instruments are more cautious and less far-reaching in their requirements, sticking to the general obligation of "effective, proportionate and dissuasive penalties" imposed by the Court of Justice of the European Union (CJEU) ever since the so-called "Greek Maize" case.[31]

In sum, the provisions on sanctions for legal persons laid down in post-Lisbon, post-financial crisis Directives merely mirror the provisions of older Framework Decisions. One may thus conclude that in twenty years' time and notwithstanding the global shock caused by the 2008 financial crisis, the EU made limited progress in the way in which it deals with the punishment of corporate crime in general, and corporate financial crime more particularly.

C. A Closer Analysis of the EU's Approach to Corporate Financial Crime

Considering that the provisions on both the liability of and the sanctions for legal persons have changed so little over the past two decades, one may rightly conclude that those requirements are now firmly established. This warrants a closer and critical analysis of such requirements as well as the underlying objectives pursued by the EU legislator. Such analysis will lead to a better understanding of the EU's grip on national law with respect to corporate financial crime.

I. Corporate Criminal Liability?

The standard EU provision on the liability of legal persons is as follows:

> 1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in [these] Articles . . . committed for their

[30] *See, e.g.*, Grazia Maria Vagliasindi, *The EU Environmental Crime Directive*, *in* ENVIRONMENTAL CRIME IN EUROPE 36 (Andrew Farmer, Michael Faure & Grazia Maria Vagliasindi eds., 2017); Michael G. Faure, *Effective, Proportional and Dissuasive Penalties in the Implementation of the Environmental Crime and Ship-Source Pollution Directives: Questions and Challenges*, EUR. ENERGY AND ENVTL. L. REV. 256, 257–58 (2010).

[31] Case C-68/88, *Commission v. Hellenic Republic*, 1989 E.C.R. 339, paras. 23–4 (emphasis added). The Court of Justice ruled that (former) Article 5 TEC (current Article 4 (3) TEU) "requires the Member States to take all measures necessary to guarantee the application and effectiveness of Community law," and

> *[W]hilst the choice of penalties remains within their discretion*, they must ensure in particular that infringements of Community law are penalized under conditions, both procedural and substantive, which are *analogous to those applicable to infringements of national law of a similar nature and importance* and which, in any event, make the *penalty effective, proportionate and dissuasive*.

Id. para. 24 (emphasis added).

> benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on:
>
> (a) a power of representation of the legal person;
> (b) an authority to take decisions on behalf of the legal person; or
> (c) an authority to exercise control within the legal person.
>
> 2. Member States shall also take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control, by a person referred to in paragraph 1, has made possible the commission of an offence referred to in [these] Articles . . . for the benefit of the legal person.
>
> 3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, inciters or accessories in the offences referred to in [these] Articles . . . .[32]

As stated above, this standard clause has hardly been modified over time. Admittedly, the legislator occasionally added at the end of paragraph 1 "as well as for the involvement as accessories or instigators in the commission of such an offence,"[33] and in several legal instruments, the ending of paragraph 2 varies between "by a person under its authority"[34] or "by a natural person under its authority."[35] While the precise reasons for these minor distinctions between different iterations of the standard clause are not entirely clear, in

---

[32] *See, e.g.,* PIF Directive, *supra* note 16, art. 6; Council Directive 2013/40/EU of 12 Aug. 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA, art. 10, 2013 O.J. (L 218) 8; Council Framework Decision 2008/841/JHA of Oct. 24 2008 on the Fight Against Organized Crime art. 5, 2008 O.J. (L 300) 42.

[33] Framework Decision Fraud Non-Cash Means of Payment, *supra* note 25, art. 7.

[34] *See, e.g., id.*; Environmental Crime Directive, *supra* note 21, art. 6; Euro Counterfeiting Directive, *supra* note 15, art. 6; Market Abuse Directive, *supra* note 13, art. 8. In the pending proposal for a Directive replacing the latter Framework Decision, the excerpt will be deleted. *See Proposal for a Directive of the European Parliament and of the Council on Combating Fraud and Counterfeiting of Non-Cash Means of Payment and Replacing Council Framework Decision 2001/413/JHA,* art. 9, COM (2017) 489 final (Sept. 13, 2009).

[35] *See, e.g.,* Ship-Source Pollution Directive, *supra* note 23, art. 8b; The 4th Money Laundering Directive, *supra* note 14, art. 60 paras. 5–6.

essence, the language of corporate liability remains the same across all instruments that compel Member States to adopt criminal offenses and sanctions for certain types of misconduct.

1. Criminal or Non-Criminal?

One of the first features that stands out when taking a closer look at the corporate liability regime imposed by the EU is that the EU does not require Member States to create a *criminal* liability regime for legal persons. This is confirmed by the standard clause on sanctions for legal persons, which can be criminal or non-criminal. The EU indeed only provides that "legal persons can be held liable" for the criminal offenses defined or targeted by the legal instrument at hand. In other words, while the underlying conduct is criminal in nature, the legal person for whose benefit the offense was committed could potentially also be held civilly or administratively liable.

In this respect, and notwithstanding the fact that many Member States have accepted the principle of corporate criminal liability, the EU's position remains unchanged from the one set forth in the early 1990s when the CJEU ruled in the *Vandevenne* case that, "neither Article 5 of the EEC Treaty nor Article 17(1) of Regulation No 3820/85 requires a Member State to introduce into its national law the principle of criminal liability of legal persons."[36]

Member States that are reluctant to adopt corporate criminal liability are thus not forced to do so by the EU. In this sense, EU law only imposes minimum rules, and grants Member States a wider margin of discretion for legal persons as compared to natural persons. This difference has everything to do with the persisting lack of consensus over corporate criminal liability among Member States, especially in light of the remaining theoretical objections of some Member States.[37] For instance, under German law, corporations can only be held liable under administrative law, despite the argument that such administrative liability is basically criminal liability according to Articles 6 and 7 of the European Convention of Human Rights (ECHR).[38] Italy, whose legal tradition in criminal law is closely linked to Germany's for historical reasons, has created a *sui generis* regime of administrative liability with some

[36] Case C-7/90, *Criminal proceedings against Paul Vandevenne, Marc Willems, Jozef Mesotten and Wilms Transport NV*, 1991 E.C.R. I-4383, para. 13.

[37] For a more detailed analysis of the theoretical and practical objections to corporate criminal liability see Vanessa Franssen, *Corporate Criminal Liability and Groups of Corporations: Need for a More Economic Approach*, *in* WHITE COLLAR CRIME: A COMPARATIVE PERSPECTIVE 275–77 (Katalin Ligeti & Stanislaw Tosza eds., 2018).

[38] *See generally* Dieter Dölling & Christian Laue, *Corporate Criminal Liability in Germany. A Never Ending Story?*, *in* LA RESPONSABILITÉ PÉNALE DES PERSONNES MORALES EN EUROPE—CORPORATE CRIMINAL LIABILITY IN EUROPE 25 (Stanislas Adam, Nathalie Colette-Basecqz & Marc Nihoul eds., 2008); Marc Engelhart, *Corporate Criminal Liability and Compliance in Germany*, *in* CORPORATE CRIMINAL LIABILITY AND COMPLIANCE PROGRAM 168–69 (Antonio Fiorella & Alfonso Maria Stile eds., 2011).

characteristics of criminal liability.[39] Finally, in Sweden, corporate criminal liability has also not been introduced, but the Criminal Code provides for corporate fines ranging up to approximately one million euro, which are, formally speaking, not considered criminal sanctions but, like forfeiture and seizure of property, "special consequences of crime defined by law."[40]

Nevertheless, even if EU law does not formally oblige Member States to adopt rules on corporate criminal liability, Member States are not entirely free to choose their own liability regime. For one, Member States must still ensure that domestic law meets the standard of "effective, proportionate and dissuasive sanctions." For another, national law also has to observe the principle of assimilation or equivalence. According to the CJEU, whenever the choice of the nature of liability and corresponding penalties remains within the discretion of the Member States, they must indeed ensure that infringements of EU law "are penalized under conditions, both procedural and substantive, which are analogous to those applicable to infringements of national law of a similar nature and importance."[41]

Therefore, if a Member State provides for corporate criminal liability for similar offenses under national law, it is obliged to apply an equivalent liability regime to the offenses for which the EU has laid down minimum rules. Member States are regularly reminded of this obligation, as some legal instruments, implicitly or explicitly, reiterate this principle. For instance, Recital (18) of the Market Abuse Directive states that "Member States should, where appropriate and where national law provides for criminal liability of legal persons, extend such criminal liability, in accordance with national law, to the offences provided for in this Directive."[42]

Meanwhile, Recital (15) of the PIF Directive sets that "[i]n order to ensure equivalent protection of the Union's financial interests throughout the Union by means of measures

---

[39] For a summary of the Italian system see, e.g., Astolfo Di Amato, *Italy*, in INTERNATIONAL ENCYCLOPAEDIA OF LAWS: CRIMINAL LAW paras 145–150 (Frank Verbruggen et al. eds., 2015). For a more extensive analysis see, e.g., Fabrizio Cugia di Sant'Orsola & Silvia Giampaolo, *Liability of Entities in Italy: Was it Not Societas Non Delinquere Potest?*, 2 NJECL 59, 59–74 (2011).

[40] *See, e.g.*, Siv Jönsson, *Criminal Legal Doctrine as a Spanner in the Works? The Swedish Experience*, *in* LA RESPONSABILITÉ PÉNALE DES PERSONNES MORALES EN EUROPE—CORPORATE CRIMINAL LIABILITY IN EUROPE 298–302 (Stanislas Adam, Nathalie Colette-Basecqz & Marc Nihoul eds., 2008); Anna Salvina Valenzano, *Main Aspects of Corporate Liability "Ex Crimine" in Northern European Countries: Denmark, Sweden and Finland*, *in* CORPORATE CRIMINAL LIABILITY AND COMPLIANCE PROGRAMS. VOL. 1: LIABILITY 'EX CRIMINE' OF LEGAL ENTITIES IN MEMBER STATES 469–74 (Antonio Fiorella ed., 2012).

[41] Case C-68/88, *Commission v. Hellenic Republic*, 1989 E.C.R. 339, para. 24.

[42] Market Abuse Directive, *supra* note 13, recital (18).

which should act as a deterrent, Member States should provide for certain types and levels of sanctions when the criminal offences defined in this Directive are committed."[43]

One may thus conclude that even if Member States maintain a margin of discretion, the EU nonetheless sets important limits to this discretion.

II. A Label Corresponding to the EU's Enforcement Objectives with Respect to Financial Crime?

While the Union's minimum approach to corporate crime is perfectly understandable in light of the principle of conferral of powers,[44] one may nonetheless wonder whether a non-criminal approach for legal persons can actually fulfill the ambitions and objectives set by the EU legislature. Generally speaking, the European Commission defined the goals of criminal law enforcement in a policy statement published relatively soon after the entry into force of the Lisbon Treaty.[45] This policy statement leaves no doubt about one of the most important goals of EU criminal law: To ensure the effective implementation of EU policies.[46] According to that policy statement, EU criminal law seeks "to prevent and sanction serious offences against EU law in important policy areas."[47] Moreover, when choosing between criminal sanctions and other kinds of sanctions, "[t]he seriousness and character of the breach of law must be taken into account. For certain unlawful acts considered particularly grave, an administrative sanction may not be a sufficiently strong response."[48] Criminal sanctions "may [thus] be chosen when it is considered important to stress strong disapproval in order to ensure deterrence. The entering of conviction in criminal records can have a particular deterrent character."[49]

In other words, criminal sanctions are considered particularly deterrent and therefore more effective than other sanctions because they express strong societal disapproval and because criminal convictions are entered into criminal records. For these reasons, criminal sanctions

[43] PIF Directive, *supra* note 16, recital (15).

[44] TEU Art. 4(1).

[45] *Towards an EU Criminal Policy: Ensuring the Effective Implementation of EU Policies Through Criminal Law*, COM (2011) 573 final (Sept. 20, 2011).

[46] For a critical assessment of the EU's effectiveness approach in the field of criminal law see Franssen, *supra* note 29.

[47] *Towards an EU Criminal Policy: Ensuring the Effective Implementation of EU Policies Through Criminal Law*, COM (2011) 573 final (20 September 2011), at 5.

[48] *Id.* at 11.

[49] *Id.*

are required for more serious infringements of the law.[50] This shows that EU criminal law pursues prevention through deterrence and retributive denunciation, thereby appealing to the expressive function of criminal law and emphasizing the importance of the underlying social or moral norms.[51]

Furthermore, considering the principles of subsidiarity and proportionality as laid down in Article 5 of the Treaty on European Union (TEU), the European Commission notes that "criminal law measures . . . unavoidably interfere with individual rights" and that "[c]riminal investigations and sanctions may . . . include a stigmatizing effect," so they should be used as a *last resort* and in accordance with the principle of proportionality.[52] Therefore, the EU legislator should only oblige the Member States to enforce EU law through criminal law when the effective implementation and enforcement of EU law cannot be achieved through other less far-reaching and less stigmatizing, but equally effective sanctions.

Even if the 2011 policy statement was the first time after the adoption of the Lisbon Treaty that the Commission was so explicit about its overall objectives in the field of criminal law, the objectives as such were not at all new. One can locate similar arguments in policy papers and legal instruments adopted before the Lisbon Treaty entered into force.

---

[50] *Id.*

[51] The term "retributive denunciation" refers to a specific account of retributivism, according to which punishment is "the emphatic denunciation by the community of a crime." John Cottingham, *Varieties of Retribution*, 29 PHIL.Q. 238, 245 (1979). By giving the offender what he deserves, punishment expresses social and moral disapproval of his culpable behavior. *See, e.g.*, RALPH HENHAM, PUNISHMENT AND PROCESS IN INTERNATIONAL CRIMINAL TRIALS 139 (2005). This theory highlights the symbolic function of criminal punishment, which distinguishes it from other types of sanctions. Unlike other retributivist theories, this interpretation of retributivism can, in this Article's view, be easily applied to corporations too—their punishment being society's way to express strong public disapproval of the corporation's behavior, whether this behavior is really immoral or simply wrong as infringing essential social norms. For a further analysis, *see* Franssen, *supra* note 12, at 32–3, 254–60.

[52] *Towards an EU Criminal Policy: Ensuring the Effective Implementation of EU Policies Through Criminal Law*, COM (2011) 573 final (20 September 2011), at 7. *See also, e.g.*, Petter Asp, *The Importance of the Principles of Subsidiarity and Coherence in the Development of EU Criminal Law*, 1 EUR. CRIM. L. REV. 44 (2011); Ester Herlin-Karnell, *What Principles Drive (or Should Drive) European Criminal Law*, 11 GERMAN L.J. 1115 (2011); Maria Kaiafa-Gbandi, *The Importance of Core Principles of Substantive Criminal Law for a European Criminal Policy Respecting Fundamental Rights and the Rule of Law*, 1 EUR. CRIM. L. REV. 7 (2011); Marc S. Groenhuijsen & Jannemieke W. Ouwerkerk, *Ultima ratio en criteria voor strafbaarstelling in Europees perspectief*, *in* ROOSACHTIG STRAFRECHT: LIBER amicorum THEO DE ROOS 249 (Marc S. Groenhuijsen, Tijs Kooijmans & Jannemieke Ouwerkerk eds., 2013) ; Annika Suominen, *The Sensitive Relationship Between the Different Means of Legal Interpretation: Mutual Recognition and Approximation*, *in* THE NEEDED BALANCES IN EU CRIMINAL LAW. PAST, PRESENT AND FUTURE 176–81 (Chloé Brière & Anne Weyembergh eds., 2018).

By 2004, the European Commission had already published a Green Paper on the approximation and mutual recognition of criminal sanctions,[53] which was itself conceived as a first step in identifying the need of further EU action to harmonize national criminal sanctions in combination with the mutual recognition of judicial decisions. At that time, the Union's competences in the field of criminal law were, of course, more limited than today. Nevertheless, the criminal law policy objectives put forward in that Green Paper still correspond closely to the aforementioned post-Lisbon objectives and, to some extent, were even more all-encompassing than the latter. First, the existence of common offenses and criminal penalties at the EU level would send out a "symbolic message" and "a clear signal that certain forms of conduct are unacceptable and punished on an equivalent basis" in the EU legal order.[54] The approximation of penalties would also give the people in the EU "a shared sense of justice,"[55] an objective which clearly relates to the expressive and denunciatory function of criminal law and punishment. Second, common minimum criminal law standards would also benefit crime prevention throughout the EU because offenders would no longer be able to take advantage of the differences in national criminal law and thus profit from so-called safe havens.[56] Interestingly, the risk of offenders relocating to jurisdictions where they expect lower sentences *or* a lower probability of detection and punishment seems particularly relevant to corporate behavior.[57] Third, the approximation would serve the further elaboration of an EU area of freedom, security, and justice by enhancing mutual trust and thereby facilitating mutual recognition of judicial decisions.[58] Fourth, more compatible rules governing the execution of penalties would also benefit the rehabilitation of offenders—an idea that has been given less consideration over the past few years.[59] And last but not least, the approximation of penalties would ensure a more effective implementation of substantive EU law, particularly in harmonized areas,[60] so as to ensure "a high level of security."[61]

---

[53] *Commission Green Paper on the Approximation, Mutual Recognition and Enforcement of Criminal Sanctions in the European Union*, COM (2004) 334 final (Apr. 30, 2004) [hereinafter Green Paper].

[54] *Id.* at 9.

[55] *Id.*

[56] *Id.* at 9–10, 47.

[57] *Cf. id.* 47 ("It would be interesting to consider whether this is a purely academic hypothesis or corresponds to reality in the event, for example, of financial, business or computer crime."). That being said, for some corporations it may be easier to relocate and organize their activities in another country than for others, depending on the type of activities and the accessibility of the market.

[58] *Id.* at 10.

[59] *Id.*

[60] *Id*.

[61] *Id.* at 47.

Furthermore, some specific legal instruments in the broader field of economic crime,[62] such as the Environmental Crime Directive, highlight that:

> [T]he existing systems of penalties have not been sufficient to achieve complete compliance with the laws for the protection of the environment. Such compliance can and should be strengthened by the availability of *criminal penalties, which demonstrate a social disapproval of a qualitatively different nature compared to administrative penalties or a compensation mechanism under civil law*.[63]

The Ship-Source Pollution Directive phrases the same objective slightly differently, but confirms the qualitative difference between criminal and administrative liability:

> Criminal penalties, which demonstrate *social disapproval of a different nature than administrative sanctions, strengthen compliance* with the legislation on ship-source pollution in force and should be *sufficiently severe to dissuade* all potential polluters from any violation thereof.[64]

In more recent, post-Lisbon legal instruments relating to financial crime, such as the Euro Counterfeiting Directive, the seriousness of the criminal conduct is emphasized, as is its wide-spread harm for individuals and businesses that need to be able to rely on the authenticity of euro notes and coins.[65] For this reason, common definitions of criminal offenses are necessary "to act as a deterrent"[66] and, for individuals, imprisonment will serve as a strong deterrent for potential criminals.[67]

---

[62] Although the definition of the term "economic crime" varies, there is growing consensus on the inclusion of environmental crime. *See* Ligeti & Franssen, *supra* note 1, at 3–4. Moving beyond the terminological discussion, environmental crime undeniably has an important impact on the economy's sustainability. *See, e.g.*, Andrew Farmer, Michael Faure & Grazia Maria Vagliasindi, *Environmental Crime in Europe: State of Affairs and Future Perspectives*, *in* ENVIRONMENTAL CRIME IN EUROPE 320, 330 (Andrew Farmer, Michael Faure & Grazia Maria Vagliasindi eds., 2017).

[63] Environmental Crime Directive, *supra* note 15, recital (3) (emphasis added).

[64] Ship-Source Pollution Directive, *supra* note 23, recital (3) (emphasis added).

[65] Euro Counterfeiting Directive, *supra* note 15, recitals (2), (15).

[66] *See, e.g., id.* at recital (10).

[67] *See, e.g., id.* at recital (17).

Similarly, the Market Abuse Directive[68] insists on the importance of market integrity and investor confidence, which are both undermined by market abuse.[69] In addition, the legislator acknowledges the qualitative difference between administrative and criminal sanctions, as well as the stronger deterrent effect of the latter, by stating that "[t]he adoption of administrative sanctions by Member States has, to date, proven to be insufficient to ensure compliance with the rules on preventing and fighting market abuse."[70]

To ensure such compliance, it is essential to provide for:

> [C]riminal sanctions which demonstrate a *stronger form of social disapproval* compared to administrative penalties. Establishing criminal offences for at least serious forms of market abuse *sets clear boundaries for types of behaviour* that are considered to be *particularly unacceptable* and *sends a message to the public and to potential offenders* that competent authorities take such behaviour very seriously.[71]

Finally, in the proposal for the PIF Directive, the European Commission argued that: "[C]riminal law is needed in order to have a *preventive effect* in this area, where the *threat of criminal law sanctions*, and their *effect on the reputation* of potential perpetrators, can be presumed to act as a *strong disincentive* to commit the illegal act in the first place."[72]

The text of the Directive that was eventually adopted continues to stress the idea of deterrence and strong dissuasion[73] but, interestingly, the emphasis on the reputational effect of criminal sanctions has disappeared.

Briefly summarized, the above legislative considerations suggest that criminal sanctions are considered necessary for two primary reasons. First, they express stronger social disapproval and have a stronger stigmatizing effect than other types of sanctions. Second, and related

---

[68] For a further analysis of the justification for criminalizing market abuse see Franssen, *supra* note 46, at 95–8.

[69] Market Abuse Directive, *supra* note 13, recital (1).

[70] *Id.* at recital (5).

[71] *Id.* at recital (6) (emphasis added).

[72] *Commission Proposal for a Directive of the European Parliament and of the Council on the Fight Against Fraud to the Union's Financial Interests by Means of Criminal Law*, at 7, COM (2012) 363 final (July 11, 2012) (emphasis added).

[73] PIF Directive, *supra* note 16, recitals (15), (18), and (28).

to the first, criminal sanctions have a more deterrent effect than other sanctions, which in turn ensures a more effective enforcement of EU law.

Yet, if criminal sanctions are really of a qualitatively different nature, thereby justifying the need for the EU legislature's intervention in a particular field of crime, how can one then explain that these qualitative features are ultimately so unimportant as to be non-determinative with respect to corporations? Because if they were, surely, the EU would also require criminal sanctions for legal persons, or would it not?[74] Are the policy objectives different with respect to legal persons, or are criminal sanctions for legal persons not supposed to have the same characterizing features—strong deterrence and strong societal denunciation?

III. Criteria for Corporate Liability

In pursuing the analysis beyond the criminal/non-criminal divide, it is worthwhile to note that the EU standard clause on corporate liability, in fact, entails two layers of liability.

First, it targets criminal offenses committed by a natural person who has a leading position within the legal person, regardless of whether he or she acts individually or as part of an organ of the legal person. Moreover, liability is only imposed where criminal offenses are committed for the legal person's benefit. Second, and in addition to that, liability is also extended to the legal person for criminal offenses that result from a lack of supervision or control by the above-described person with a leading position.

The aforementioned first layer of liability presents all characteristics of a system of vicarious liability. Vicarious liability—also referred to as indirect, derivative, or agency liability[75]—is based on the civil law theory of *respondeat superior*, which a number of legal systems have transposed to the area of criminal liability. US corporate criminal liability is a prominent and

[74] *Cf.* Christopher Harding, *Tasks for Criminology in the Field of EU Criminal Law and Crime Policy*, *in* EU CRIMINAL LAW AND POLICY VALUES, PRINCIPLES AND METHODS 122 (Joanna Beata Banach-Gutierrez & Christopher Harding eds., 2017) (identifying "the imposition of criminal responsibility on corporate persons" as one of the "key questions of the present moment" at the level of EU criminal law).

[75] Celia Wells, *Corporate Criminal Liability in the United Kingdom. Much Ado About Nothing?*, *in* LA RESPONSABILITÉ PÉNALE DES PERSONNES MORALES EN EUROPE—CORPORATE CRIMINAL LIABILITY IN EUROPE 286 (Stanislas Adam, Nathalie Colette-Basecqz & Marc Nihoul eds., 2008).

well-established example thereof.[76] In the EU, countries like Spain[77] and France[78] have adopted corporate criminal liability on this basis. Under this theory, to hold a legal person liable, it suffices to establish that an individual within the legal person has committed an offense on behalf of the legal person. The material and mental element of the offense are thus established through the individual's involvement and subsequently attributed to the legal person on the basis of certain objective criteria, such as the fact that the offense has benefited the legal person.

At the same time, this first layer of corporate liability also recalls the identification theory, which can be found in jurisdictions like England and Wales,[79] because the natural person who commits the offense must be a person holding a leading position within the corporate organization.[80] Having a leading position is defined as having a power of representation of the legal person, or the authority to make decisions on behalf of the legal person, or to exercise control within that legal person. As argued elsewhere,[81] considering that the identification theory seeks to establish the directive mind of the corporate entity, it tends, in some respects, towards autonomous criminal liability—requiring guilt to be established *directly* at the level of the corporate entity. Yet, in practice, the difference between this and indirect criminal liability seems fairly limited.[82]

---

[76] *See, e.g.*, John K. Villa, *Corporate Criminal Liability: When a Corporation is Liable for Criminal Conduct By an Employee*, 2 CORPORATE COUNSEL GUIDELINES § 5:5 (2011); Han Hyewon & Nelson Wagner, *Corporate Criminal Liability*, 44 AM. CRIM. L. REV. 337, 339–47 (2007); HARRY FIRST, BUSINESS CRIME: CASES AND MATERIALS 167 (1990).

[77] For a very long time, the Spanish legislator refused to create *criminal* liability for corporations. Yet this fundamentally changed with the Organic law 5/210 of 22 June 2010. For a concise analysis of the new legal regime see, e.g., Lorena Bachmaier Winter & Antonio del Moral García, Spain, *in* INTERNATIONAL ENCYCLOPAEDIA OF LAWS: CRIMINAL LAW paras 256–61 (Frank Verbruggen, Roger Blanpain & Michele Colucci eds., 2012).

[78] Nevertheless, the vicarious nature of the French system of corporate criminal liability seems less certain than it may appear at first sight. Some argue the French system is in practice much closer to an autonomous or organizational model. In this respect, see Juliette Tricot, *Corporate Criminal Liability in France*, *in* CORPORATE CRIMINAL LIABILITY AND COMPLIANCE PROGRAM 135 (Antonio Fiorella & Alfonso Maria Stile eds., 2011).

[79] In England and Wales, the identification test is the "default position of the courts . . . when no [other] test of corporate liability is provided for in a statute." Other tests of corporate criminal liability can, however, be found in specific statutes such as the Corporate Manslaughter and Corporate Homicide Act and the Bribery Act. For a clear and critical analysis see James Gobert, *Corporate Criminal Liability—What Is It? How Does It Work in the UK?, in* CORPORATE CRIMINAL LIABILITY AND COMPLIANCE PROGRAMS 222–29, and in particular 224 for the above quote (Antonio Fiorella & Alfonso Maria Stile eds., 2012).

[80] *Cf.* VERMEULEN, *supra* note 3, at 11.

[81] *See* Vanessa Franssen, *Daderschap en toerekening bij rechtspersonen*, NULLUM CRIMEN 227, 232, 241 (2009); Raf Verstraeten & Vanessa Franssen, *Collective Entities as Subjects of Criminal Law. The Case of Belgium and the Netherlands*, *in* CORPORATE CRIMINAL LIABILITY AND COMPLIANCE PROGRAMS 254 (Antonio Fiorella & Alfonso Maria Stile eds., 2012).

[82] For a critical analysis of the identification theory under English law and the problems it causes in practice see JAMES GOBERT & MAURICE PUNCH, RETHINKING CORPORATE CRIME 62–69 (2003). See also Gobert, *supra* note 79, at 224-

The second layer of liability of the EU clause on corporate liability is of a somewhat different nature. Essentially, it corresponds to situations where someone within the legal person is able to commit an offense due to a lack of supervision or control of the persons having leadership positions. The latter can be considered as "functional perpetrators," a notion that is well-established under, for example, Dutch criminal law.[83] A functional perpetrator is someone who, due to his or her position, is liable for criminal behavior committed by other persons acting under his or her supervision or control. As such, he or she is not necessarily guilty of the same offense as the person(s) acting under their supervision or control. To elaborate, in the event of an intentional offense, the functional perpetrator does not necessarily—perhaps, only rarely—intentionally turn a blind eye to the criminal activity, but is simply negligent in performing his or her supervision tasks. A functional perpetrator can, to some extent, be compared to an accomplice, with the sole difference being that there is, in principle, no intent to participate in the commission of the offense.[84] Therefore, holding the functional perpetrator criminally liable on either the same legal basis as the "material" or "direct" offender, *i.e.*, the person who physically committed the offense targeted by the EU legal instrument, or on the basis of an accomplice liability theory, is usually impossible. A self-standing legal basis for the functional perpetrator's criminal liability thus seems indispensable.[85] As the liability of the legal person is based on the criminal liability of the functional perpetrator, one may argue that the legal person is also a kind of functional perpetrator.

The above analysis suggests that the rules on corporate liability imposed by the EU are strongly dependent on the individual's liability. This holds true for both layers of liability. This emphasis on individual liability is also expressed by paragraph three of the EU standard provision on corporate liability, which states that the legal person's liability "shall not exclude criminal proceedings against natural persons who are involved as perpetrators, inciters or accessories." Arguably, the EU criteria for corporate liability do not account for the particular features of corporations particularly well.

---

229. For the strong similarities between the identification theory and the French system of indirect liability see PHILIPPE CONTE & PATRICK MAISTRE DU CHAMBON, DROIT PÉNAL GÉNÉRAL 214–15 (2004).

[83] *See, e.g.*, JAAP DE HULLU, MATERIEEL STRAFRECHT 164–70, 209 (2003); Eelke Sikkema, *De strafrechtelijke verantwoordelijkheid van leidinggevenden in Nederland*, *in* DE STRAFRECHTELIJKE VERANTWOORDELIJKHEID VAN LEIDINGGEVENDEN—IN DE ECONOMISCHE CONTEXT 36–58 (Nederlands-Vlaamse Vereniging voor Strafrecht ed., 2010).

[84] For an in-depth analysis of accomplice liability and functional perpetratorship see, e.g., JAN VANHEULE, STRAFBARE DEELNEMING 905 (2010).

[85] It should be noted, though, that some legal systems, like the Belgian one, tend to apply a very broad notion of perpetratorship, including that of functional perpetrators, without a clear legal basis. For a further analysis, see Franssen, *supra* note 81, at 228–29. *See also* CHRISTIANE HENNAU & JACQUES VERHAEGEN, DROIT PÉNAL GÉNÉRAL 268–74 (2003).

For instance, an important disadvantage of a vicarious liability regime is that it usually leaves the corporation with few possibilities to defend itself against situations where criminal offenses are committed by individuals acting on their own initiative and for their own benefit in a corporate setting that creates a direct or indirect benefit for the corporations, without the corporation "intending" to obtain such benefit. For instance, if an individual with a leadership position abuses his or her position for private enrichment by committing VAT fraud or an act of corruption, the slightest, even purely theoretical, benefit for the legal person could be enough to expose the latter to liability claims, even if the individual's decision cannot be regarded as a decision emanating from the corporation or taken on behalf of the corporation's interest.[86] This threat of abuse is by no means illusory or hypothetical, as the practice of US corporate criminal liability shows. Under US federal law, a corporation "may be held criminally liable for the acts of any of its agents [who] . . . commits a crime . . . within the scope of employment . . . with the intent to benefit the corporation."[87] Yet, in practice, "the last two requirements are almost meaningless."[88] To elaborate, US courts have accepted corporate criminal liability even for conduct that "was specifically forbidden by corporate policy" and when the corporation "made good faith efforts to prevent the crime."[89] Some American scholars have therefore concluded that "respondeat superior is grossly overbroad,"[90] arguing that:

> A rule deeming virtually all crimes committed by institutional agents in institutional settings to be institutional crimes is easy to apply but plainly does not fit with any persuasive account of the relationship between institutional effects and individual conduct.[91]

[86] *See, e.g.*, Pamela Bucy, *Corporate Criminal Liability: When Does It Make Sense?*, 46 AM. CRIM. L. REV. 1437 (2009) (arguing that the current standard for corporate criminal liability is overly broad, rendering the corporation criminally liable "whenever one of its agents . . . commits a crime related in almost any way to the agent's employment . . . even when the corporation received no actual benefit from the offense and no one within the corporation knew of the conduct at the time it occurred").

[87] *Id.* at 1440 and accompanying references.

[88] *Id.*

[89] *Id.* at 1441 (giving the example of *United States v. Hilton Hotels Corp.*, in which the corporation was convicted of antitrust violations committed by a purchasing agent contrary to explicit corporate policy). *See also* Andrew Weissmann, *A New Approach to Corporate Criminal Liability*, 44 AM. CRIM. L. REV. 1319 (2007).

[90] Samuel W. Buell, *The Blaming Function of Entity Criminal Liability*, 81 IND. L.J. 473, 576 (2006). *See also*, *e.g.*, Jennifer Arlen, *The Potential Perverse Effects of Corporate Criminal Liability*, 23 J. LEGAL STUD. 833, 838 (1994).

[91] *Id.* at 526.

In order to counterbalance the breadth of the corporate criminal liability, US prosecutors enjoy great prosecutorial discretion—considered excessive by some authors.[92] Furthermore, the existence of an effective compliance program can be taken into account as a mitigating circumstance at the sentencing level.[93] In sum, the US example clearly shows that vicarious liability does not adequately deal with agency problems—*i.e.*, the misalignment of the interests of the corporation and its owners with those of the agents of the corporation—and such may lead to undesirable outcomes.

Moreover, liability based on the *respondeat superior* theory or the identification theory, in principle, requires identification of the individual who committed the offense, because it is this person's criminal liability that triggers the liability of the legal person. Considering that the corporate decision-making process is often a black box for outsiders, especially in larger business organizations—if only for the simple fact that some decisions are taken by a collegial body—it can be quite difficult in practice to identify the responsible individuals.[94]

In conclusion, rather than opting for a system of autonomous or direct corporate liability that would fully recognize legal persons as subjects of criminal law and which would be better adjusted to more complex organizational situations,[95] the EU adheres to a mixed system of corporate liability based on the *respondeat superior* theory, the identification theory, and functional perpetratorship. When comparing this approach to the EU's rules on corporate *administrative* liability, there are some striking differences. For instance, under the Market Abuse Regulation, legal persons have an express defense against potential abuse situations. According to Recital (30), "[w]here legal persons have taken all reasonable measures to prevent market abuse from occurring but nevertheless natural persons within their employment commit market abuse on behalf of the legal person, [such] should not be deemed to constitute market abuse by the legal person."[96]

---

[92] *See, e.g.*, Weissmann *supra* note 89, at 1320. For a more mitigated analysis see Sara Sun Beale, *A Response to the Critics of Corporate Criminal Liability*, 46 AM. CRIM. L. REV. 1481, 1491–1493 (2009).

[93] *See, e.g.*, Kendel Drew & Kyle A. Clark, *Corporate Criminal Liability*, 42 AM. CRIM. L. REV. 277, 287 (2005). For an analysis and case-law based assessment of the US Sentencing Guidelines' emphasis on compliance programs see, e.g., Diana E. Murphy, *The Federal Sentencing Guidelines for Organizations: A Decade of Promoting Compliance and Ethics*, 87 IOWA L. REV. 697 (2002).

[94] For an in-depth analysis of the difficulties encountered by courts in England and Wales when applying the identification theory, see, e.g., JAMES GOBERT & MAURICE PUNCH, RETHINKING CORPORATE CRIME 49–77 (2003). For a further analysis of the difficulties in identifying and punishing the responsible person in large corporate structures, see Franssen, *supra* note 37, at 277.

[95] *Id.* at 78. *See also* William S. Laufer, *The Missing Account of Progressive Corporate Criminal Law*, 14 N.Y.U. J.L. & BUS. 71, 83, 136–37 (2017) (proposing the term "constructive corporate liability").

[96] Market Abuse Regulation, *supra* note 13, recital (30).

This leads to the paradoxical situation that legal persons are more likely to incur "criminal" liability as opposed to administrative liability if an individual commits an offense within the scope of his or her employment. Instead of imposing stricter criteria for "criminal" liability for more serious violations of law—like the requirement to prove the corporation's criminal state of mind—the reality is that the EU opts for less strict standards of corporate "criminal" liability.[97] Once again, this raises the question about the true nature of corporate liability for criminal offenses under EU law.

IV. Criminal or Non-Criminal Sanctions

Turning to the sanctions provided for legal persons, one will immediately note a strong focus on fines. According to the aforementioned standard provision on the sanctions for legal persons, the EU indeed only requires that Member States subject legal persons "to effective, proportionate and dissuasive sanctions, which *shall include criminal or non-criminal fines*."[98] While fines are applied widely to legal persons, they are far from being a one-size-fits-all solution. Indeed, one should not overestimate the deterrent effect of fines, nor underestimate their spill-over effects to other innocent persons—such as employees, consumers, suppliers, etc. To the extent that fines may be calculated in advance, they may simply be treated as a business cost. Moreover, a fine does not necessarily send the right message to those in charge of the corporate decision-making process that have the capacity to change the corporation's behavior in the future—for instance, corporate officials or shareholders in closely-held operations to the extent that the latter are closely involved in the decision-making process.[99]

In addition to criminal or non-criminal fines, EU instruments encourage Member States to adopt other sanctions—such as excluding infringing entities from entitlements to public benefits or aid, temporarily or permanently disqualifying them from the practice of commercial activities, placing them under judicial supervision, or causing their judicial winding-up and the temporary or permanent closure of establishments which have been used for committing the offense. The PIF Directive adds a new sanction to that list: The "temporary or permanent exclusion form public tender procedures."[100] Nonetheless, these sanctions, which recall some of the recommendations made by the Council of Europe back

[97] To complete the picture, it is noteworthy that Article 9(1) of the Market Abuse Regulation defines under what circumstances the possession of inside information by a legal person should not be regarded as insider dealing or unlawful disclosure of inside information on the part of the legal person and thus constitutes legitimate behavior.

[98] *See, e.g.*, PIF Directive, *supra* note 16, art. 9 (emphasis added).

[99] For a more in-depth analysis see Franssen *supra* note 12, at 260–70 and the accompanying references.

[100] *See* PIF Directive, *supra* note 16, art. 9(b).

in 1988,[101] are mere suggestions and not hard obligations. Therefore, it is perfectly conceivable that Member States meet the general standard of effectiveness, proportionality, and dissuasiveness without applying such sanctions.

In short, Member States clearly enjoy a wide margin of discretion under the current EU standard provision on sanctions for legal persons—they can choose between criminal fines and fines of a different nature, at least from a national perspective. In addition, they may apply other sanctions, whether these correspond to the EU's suggestions or not. History has taught us the CJEU rarely rules that the level of fines under national law is not effective, proportionate, and dissuasive; only in flagrant cases will it come to that conclusion.[102] Moreover, in evaluating whether national law meets that punishment standard set by the EU legislator, the CJEU will not only consider the level of fines, but also other penalties "imposed in respect of the same infringement."[103]

The minimum approach taken by the EU with respect to sanctions for legal persons greatly contrasts with the Union's efforts to approximate national rules on maximum terms of imprisonment applicable to individuals for the same offenses.[104] The EU does not set minimum levels for the maximum fines applicable to legal persons, nor does it determine how those fines should be calculated.

The general approach with respect to corporate offenders in the field of financial crime also differs significantly, for instance, from the much more detailed rules and guidelines in the field of EU competition law[105] and the administrative prong of EU market abuse law.[106] The difference in applicable instruments matters—a Regulation is usually more precise than a Directive. But, the explanation for the diverging approach cannot be confined to this technical difference. One may also note that the harsh "administrative" fines of the

---

[101] Recommendation No. R (88) 18 of 20 Oct. 20, 1988 Concerning Liability of Enterprises Having Legal Personality for Offenses Committed in the Exercise of their Activities, art. 7.

[102] *See*, e.g., Case C-68/88, *Commission v. Hellenic Republic*, 1989 E.C.R. 339, paras 24–7. In fact, in this case, the problem was more deeply rooted than the mere levels of fines provided for by law and due to complete lack of enforcement. Greece had failed to fulfill its obligations under EU law "by omitting to initiate all the criminal or disciplinary proceedings provided for by national law against the perpetrators of the fraud and all those who collaborated in the commission and concealment of it." *Id.* para. 22.

[103] Case C-262/99*, Louloudakis v. Greece*, 2001 E.C.R. I-5547, para. 69.

[104] *See, e.g.*, PIF Directive, *supra* note 16, art. 7; Market Abuse Directive, *supra* note 13, art. 7; Euro Counterfeiting Directive, *supra* note 15, art. 5.

[105] *See* Council Regulation 1/2003 of 16 Dec. 2002 on the Implementation of the Rules on Competition Laid Down in Articles 81 and 82 of the Treaty art. 23(2), (3), 2003 O.J. (L 1) 1 (EC); Guidelines on the Method of Setting Fines Imposed Pursuant to Article 23(2) (a) of Regulation 1/2003, 2006 O.J. (C 210), 2.

[106] *See* Market Abuse Regulation, *supra* note 13, art. 30(2)(j).

European Commission and some administrative sanctions provided by the Market Abuse Regulation are quite punitive and would qualify as "criminal" sanctions under Articles 6 and 7 of the ECHR.[107] The general approach is, above all, a symptom of the unwillingness of Member States to further approximate their national rules in this respect. In the not so distant past, the European Commission attempted to go beyond the aforementioned general requirement in the field of ship-source pollution, proposing additional fines based on the legal person's turnover or the assets it owns, thereby following the example of the fines applicable under EU competition law. Nevertheless, this proposal utterly failed to convince the Member States.[108]

Furthermore, apart from the general character of requirements set by the standard provision on sanctions for legal persons in the field of financial crime, there are a couple of remarkable gaps in the list of sanctions required and suggested by the EU.

First, the list of sanctions does not include the confiscation of illegal proceeds, even if this sanction appears particularly fit for legal persons—especially considering that their liability is based on the "benefit" of the underlying criminal offense committed by an individual occupying a leadership position in the corporate organization. This gap is all the more pronounced when one considers that corporate financial crimes are typically pursued for profits.

One possible explanation for this gap is that the freezing and confiscation of instrumentalities and proceeds of crime is regulated by a separate Directive.[109] The Freezing and Confiscation Directive, however, only obliges Member States to enable confiscation of instrumentalities and proceeds "subject to a final conviction for a criminal offense" and in limited circumstances even where criminal proceedings ultimately do not lead to a criminal conviction.[110] Considering the fact that the EU does not impose criminal liability for legal persons, the application of this Directive to legal persons thus essentially rests with the respective Member State. Nevertheless, there exists one exception: The rules on third-party confiscation—*i.e.*, the situation where the illegal proceeds have been transferred to or

[107] For a further analysis of whether cartel fines qualify as criminal sanctions, *see* Franssen *supra* note 12, at 307–14.

[108] For a more detailed analysis of the *Commission's Proposal for a Council Framework Decision to Strengthen the Criminal-Law Framework for the Enforcement of the Law Against Ship-Source Pollution*, COM (2003) 227 final (May 2, 2003), *see* Franssen *supra* note 12, at 220–22.

[109] Directive 2014/42/EU, of the European Parliament and of the Council of 3 Apr. 2014 on the Freezing and Confiscation of Instrumentalities and Proceeds of Crime in the European Union, 2014 O.J. (L 127) 39 [hereinafter Freezing and Confiscation Directive].

[110] *Id.* art. 4(1), (2). For a further analysis, see, e.g., Katalin Ligeti & Michele Simonato, *Asset Recovery in the EU: Towards a Comprehensive Enforcement Model Beyond Confiscation? An Introduction*, *in* CHASING CRIMINAL MONEY. CHALLENGES AND PERSPECTIVES ON ASSET RECOVERY IN THE EU 7 (Katalin Ligeti & Michele Simonato eds., 2017).

acquired by a third party, potentially a legal person[111]—should, in any event, extend to both individuals and legal persons.[112] Furthermore, in some legal instruments, confiscation and freezing of the instrumentalities and illegal proceeds of crime is targeted by a separate provision, which appears applicable to individuals and legal persons, without distinction.[113]

Another explanation for this gap might be the lack of consensus among Member States on non-conviction based confiscation of the proceeds of crime, which could be applied regardless of the possibility of prosecuting and convicting a legal person. Indeed, the Freezing and Confiscation Directive does not contain a real obligation in this respect and far from proposes a kind of civil or non-criminal forfeiture typical of some common law systems.[114]

Whatever the explanation may be, the absence of a general obligation to ensure the confiscation of the instrumentalities and illegal proceeds for legal persons in the field of financial crime remains puzzling. This differs strikingly from other EU financial regulations. For instance, the Market Abuse Regulation entails an obligation to provide for the "disgorgement of profits" as an administrative sanction.[115] Admittedly, the idea of disgorgement is not entirely absent from the Market Abuse Directive, which states that:

> Without prejudice to the general rules of national criminal law on the application and execution of sentences in accordance with the concrete circumstances in each individual case, the imposition of sanctions should be proportionate, *taking into account the profits made or losses avoided by the persons held liable* as well as the damage resulting from the offence

[111] Freezing and Confiscation Directive, *supra* note 109, art. 6(1).

[112] *Id.* at recital (24).

[113] *See, e.g.*, PIF Directive, *supra* note 16, art. 10. This provision does not require a criminal conviction, but simply refers to "instrumentalities and proceeds from the criminal offences" on which are covered by the Directive. Therefore, in this author's view, this could include the hypothesis of a legal person being held administratively liable for one of those offenses.

[114] Ligeti & Simonato, *supra* note 110, at 8–10. For a more in-depth analysis of the concept of non-conviction based confiscation and civil forfeiture, see, e.g., Michele Panzavolta, *Confiscation and the Concept of Punishment: Can There be a Confiscation Without a Conviction?*, *in* CHASING CRIMINAL MONEY. CHALLENGES AND PERSPECTIVES ON ASSET RECOVERY IN THE EU 25. (Katalin Ligeti & Michele Simonato eds., 2017); Colin King, *Civil Forfeiture in Ireland: Two Decades of the Proceeds of Crime Act and the Criminal Assets Bureau*, *in* CHASING CRIMINAL MONEY. CHALLENGES AND PERSPECTIVES ON ASSET RECOVERY IN THE EU 77. (Katalin Ligeti & Michele Simonato eds., 2017).

[115] Market Abuse Regulation, *supra* note 13, art. 30(2)(b).

> to other persons and, where applicable, to the functioning of markets or the wider economy.[116]

Still, it is one thing to say that that the profit made by the liable persons should be taken into account to make sure that the sanctions applied are proportionate; it is yet another to require the adoption of a specific sanction aimed at disgorging the liable person from the illegal proceeds of crime.[117] The PIF Directive is the only legal instrument in the field of financial crime setting this requirement for legal persons. It remains to be seen whether the Directive marks a new trend or remains a one-time shot.

Second, another important missing sanction is the compensation of victims and restoration of the former state. This is all the more surprising considering that corporate crime tends to cause wide-spread, diffuse, and long-term harm to private and public goods that affect private and institutional victims (*e.g.,* other corporations or government entities).[118] Therefore, when harm does occur, restoration and compensation should be key sentencing goals with respect to corporations. According to some, "to remedy harm . . . should be the first goal of criminal prosecution of an organization."[119] In addition, the *deep pockets assumption* presents a very pragmatic argument for adding this sanction to the sanctioning arsenal for legal persons. One of the downsides of individual criminal liability is indeed that individuals are often unable to restore the situation to its former state and/or to pay for the

---

[116] Market Abuse Directive, *supra* note 13, recital (24) (emphasis added). In fact, this idea was already present in the former Market Abuse Directive of 2003, which did not include an obligation to criminalize certain forms of market abuse. Instead, it required that "sanctions should be sufficiently dissuasive and proportionate to the gravity of the infringement *and to the gains realised* . . . ." Recital (38) of the Preamble of Directive 2003/6/EC of 28 Jan. 2003 on Insider Dealing and Market Manipulation, 2003 O.J. (L 96) 16. Based on this recital, the CJEU ruled that the "gains realised from insider dealing may constitute a relevant element for the purposes of determining a sanction which is effective, proportionate and dissuasive." *See* Case C-45/08, *Spector v. CBFA*, 2009 E.C.R. I-12073, para. 73.

[117] Admittedly, other legal instruments requiring administrative sanctions do not always require disgorgement of profits as a separate sanction either. For instance, under the Fourth Money Laundering Directive, Member States should take into account, when determining the type and level of administrative sanctions and measures, "the benefit derived from the breach by the natural or legal person held responsible, insofar as it can be determined." The 4th Money Laundering Directive, *supra* note 14, art. 60(4)(d). This approach largely mirrors the European Commission's Guidelines on fines applicable to cartel offenses. According to Point 31 of the 2006 Guidelines on fines, the gains obtained by undertaking the commission of a cartel offense should be taken into account when the Commission determines the fine, provided that "it is possible to estimate that amount," and may lead to an increase of the fine in order to ensure deterrence.

[118] *See* Vanessa Franssen & Silvia Van Dyck, *Holsters op maat voor de bestraffing van ondernemingen? Eerst goed mikken, dan pas schieten*, *in* DE WET VOORBIJ. LIBER AMICORUM LUC HUYBRECHTS 525 (Filiep Deruyck et al. eds., 2010).

[119] Peter J. Henning, *Corporate Criminal Liability and the Potential for Rehabilitation*, 46 AM. CRIM. L. REV. 1417, 1429 (2009).

damage caused by the corporate offense. The corporation assumedly has deeper pockets, making it an attractive defendant.[120]

A third type of sanction that appears to be lacking is the publication of the very decision that holds a legal person liable. Despite the vast literature on reputational sanctions[121] and the aforementioned 1988 Recommendations of the Council of Europe, the EU standard provision on sanctions for legal persons does not suggest any requirement to publicly publish the decision. In contrast, the publication of a sanctioning decision is one of the recurring administrative sanctions under EU financial regulations. For instance, Article 34 of the Market Abuse Regulation provides for the publication of decisions, unless doing so would be disproportionate to the nature of the infringement, cause disproportionate damage to the persons involved, or jeopardize the stability of financial markets or an ongoing investigation. Such publication is considered to have "a dissuasive effect on the public at large . . . [and be] an important tool for competent authorities to inform market participants of what behaviour is considered to be an infringement of [the] Regulation and to promote good behaviour amongst market participants."[122]

Put differently, the publication of the decision sends an important message that such behavior is not tolerated and ideally prevents future infringements by potential offenders. Formally speaking, such publication is not a self-standing administrative sanction, but a kind of collateral consequence. Yet, considering its potential to significantly influence the conduct of would-be offenders, it could nonetheless be considered as a punitive sanction.

Furthermore, it is worthwhile to note that some EU institutions and authorities endowed with administrative sanctioning powers—such as the European Commission, the European Central Bank, and the European Securities and Markets Authority—publish their sanctioning decisions on a regular basis.

Still, when it comes to corporate financial crime, this idea has yet to grow. Admittedly, the Preamble of the Market Abuse Directive refers to the option of publishing the final decision

---

[120] Of course, there will also be situations in which the corporation's financial resources are not sufficient to cover restoration and compensation, for instance, because the corporation is relatively small or because its capital is intentionally kept low by its shareholders, or due to the enormous size of the harm caused by the offense.

[121] *See, e.g.*, BRENT FISSE & JOHN BRAITHWAITE, THE IMPACT OF PUBLICITY ON CORPORATE OFFENDERS (1983); Jonathan M. Karpoff & John R. Lott, Jr., *The Reputational Penalty Firms Bear from Committing Criminal Fraud*, 36 J.L. & ECON. 757 (1993); Note, *Shame, Stigma, and Crime: Evaluating the Efficacy of Shaming Sanctions in Criminal Law*, 116 HARV. L. REV. 2186 (2002-2003); Jonathan M. Karpoff, John R. Lott, Jr. & Eric W. WEHRLY, *The Reputational Penalties for Environmental Violations: Empirical Evidence*, 68 J.L. & ECON. 653 (2005); Dan M. Kahan, *What Do Alternative Sanctions Mean?*, 63 U. CHI. L. REV. 591 (1996).

[122] Market Abuse Regulation, *supra* note 13, recital (73).

of liability or sanctions, with cross-reference to the Market Abuse Regulation,[123] but does not include this sanction in the ultimate provision containing sanctions for legal persons. Considering the importance that at least some legal persons attach to their reputation[124] as well as the market effect that a publicized sanctioning decision may have, such seems like an interesting option for Member States to explore in the future.

D. Conclusion: Missed Opportunities and Potential for the Future

A first preliminary key conclusion resulting from the foregoing analysis is that the EU has made little progress in the fight against corporate financial crime since the 2008 financial crisis. Surely, several new legal instruments have been adopted and the regulatory framework has been solidified. Nonetheless, when it comes to the EU's approach for corporate liability for the most serious financial offenses that have been harmonized at the EU level, it seems the policy assessments made in the wake of the financial crisis have hardly had any effect. Indeed, the legal provision on corporate liability is still the same standard provision that was previously used, and the provision on sanctions for legal persons basically corresponds to the old mantra of the CJEU: Sanctions must be effective, proportionate, and dissuasive, with the sole difference being the addition of required fines and the encouragement of other sanctions. The lack of minimum rules with respect to those sanctions in conjunction with the nearly voluntary character of the approximation of national rules most clearly reveals the lack of consensus and unwillingness among Member States to step up against corporate crime and create a level playing field for legal persons throughout the EU.

Second, in addition to the nearly *status quo*, this Article has also shown a mismatch between the objectives pursued by the EU and the added value of criminal law enforcement, and the choice left to the Member States on whether to hold corporations criminally or otherwise liable. Admittedly, this mismatch is due, once more, to the persisting lack of consensus between the Member States, particularly with respect to the theoretical acceptability of corporate criminal liability. Yet, the result is quite unsatisfactory and sends a mixed message to legal persons across the EU. Moreover, the obstinacy of some Member States to qualify corporate liability as criminal is, to some extent, illusory because such liability may very well be defined as "criminal" by the European Court of Human Rights—which activates a considerable body of fundamental substantive and procedural rights.

Third, the analysis has demonstrated that the EU approach to corporate crime is not well adjusted to the corporate reality. On the one hand, because it adheres to a liability regime consisting of a mix of the *respondeat superior* theory and the identification theory. Notably,

[123] Market Abuse Directive, *supra* note 13, recital (18).

[124] As some rightfully point out, it takes a good reputation to lose one. *See, e.g.*, *Shame, Stigma, and Crime: Evaluating the Efficacy of Shaming Sanctions in Criminal Law*, *supra* note 121, at 2190.

both theories have proven their weaknesses at the national level. As far as the functional perpetratorship of legal persons is concerned, a further analysis of its implementation under national law is desirable to see exactly how corporate liability is regulated and applied to real-world cases. On the other hand, the EU essentially only requires Member States to provide for criminal or noncriminal fines, even though the effectiveness and deterrent effect of fines is quite uncertain and depends on many variables. Other punishment objectives such as disgorgement, compensation, and restoration—which are equally important with regard to legal persons[125]—are largely disregarded by the EU, or at the very least are not included in the current set of sanctions for legal persons. In this respect, the harmonization of punitive administrative sanctions is more advanced and satisfactory.

To conclude, the current EU approach to corporate financial crime is marked by several missed opportunities, incoherence, and inadequacy. A further reflection on proper organizational liability criteria and an appropriate arsenal of sanctions is desperately needed, notwithstanding the studies that the European Commission has ordered or funded in the recent past. On top of that, more willingness of Member States is critically required in order to move beyond the current legal framework. If the financial crisis has taught us one thing, it is definitely that corporate financial crime cannot be adequately fought by individual States. Such requires comprehensive, supranational, or even internationally coordinated action.

[125] For an extensive analysis, see Franssen, *supra* note 12, at 276-280 and 393-394.

Articles

EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow

By Els De Busser[*]

Abstract

Criminal offenses with the most different modi operandi and levels of complexity can generate digital evidence, whether or not the actual crime is committed by using information and communication technology (ICT). The digital data that could be used as evidence in a later criminal prosecution is mostly in the hands of private companies who provide services on the Internet. These companies often store their customers' data on cloud servers that are not necessarily located in the same jurisdiction as the company. Law enforcement and prosecution authorities then need to take two steps that are not exclusive for evidence of a digital nature. First, they need to discover where the data is located—with which company and in which jurisdiction. Second, they need to obtain the data. In considering digital evidence, the last step, however, is complicated by new issues that form the focus of this paper. The first concern is the practice by companies to dynamically distribute data over globally spread data centers in the blink of an eye. This is a practical concern as well as a legal concern. The second issue is the slowness of the currently applicable international legal framework that has not yet been updated to a fast-paced society where increasingly more evidence is of a digital nature. The slowness of traditional mutual legal assistance may be no news. The lack of a suitable legal framework for competent authorities that need to obtain digital evidence in a cross-border manner, nonetheless, creates a landscape of diverse initiatives by individual states that try to remedy this situation. A third issue is the position that companies are put in by the new EU proposal to build a legal framework governing production orders for digital evidence. With companies in the driver's seat of a cross-border evidence gathering operation, guarantees of the traditional mutual legal assistance framework seem to be dropped. A fourth issue is the position of data protection safeguards. US based companies make for significant data suppliers for criminal investigations conducted by EU based authorities. Conflicting legal regimes affect the efficiency of data transfers as well as the protection of personal data to citizens.

[*] Assistant Professor Cyber Security Governance, Institute of Security and Global Affairs, Leiden University.

A. Existing Phenomena and New Questions

There is a new normal in the domain of criminal investigations and that is the growing digital nature of evidence. Whether or not the crime in question is qualified as a computer related crime, a significant part of the material that could be used as evidence can be digital, such as email—messages and their attachments—communication, Facebook profiles, or Whatsapp messages. The fact that citizens are increasingly leaving digital traces while doing everyday acts potentially gives law enforcement authorities an enormous amount of digital data when one or more of these citizens becomes the suspect of a criminal offense. The content of an online shopping cart, the destination of flight tickets booked online, the addressees of email communication, or the GPS coordinates of a recently driven route—as trivial as each of these data points may seem, they can become crucial information for law enforcement officers investigating a specific crime.

In the context of financial crime, an important set of data can be added to this list of examples: Monetary transactions made by the person or persons concerned. The "follow the money" strategy has been labeled as the approach to combat the financing of terrorism and forms of organized crime,[1] but has also been the subject of criticism.[2] Regardless of its effectiveness as a strategy, the gathering of financial data for the purpose of a criminal investigation presents considerable issues concerning data protection and privacy. An individual's monetary transactions show a rather detailed picture of that person's life. Moreover, an individual's bank account and credit card number fall within the scope of the definition of personal data—information that identifies or enables an individual to be identified. The latter means that data protection legislation is applicable to safeguard the data from unlawful or incorrect processing. In the context of a criminal investigation, exceptions to a number of data protection rules are allowed. Data collected for a commercial purpose can be used for a criminal investigation, provided that the data is necessary and proportionate for the investigation and provided that this is laid down in law. The collection of the data for a commercial purpose can be located in a different state than the subsequent use as evidence in a criminal investigation. This cross-border gathering of digital data as evidence is the core topic of this Article. Because the difficulties that are sketched here are related to the digital nature of the data, rather than the type of crime, this Article does not focus on financial transactions, but on personal data as such. More precisely, this paper narrows in on the question of how digital personal data can be accessed and gathered in a cross-border setting in order to produce evidence of (financial) crimes while safeguarding

[1] *See The Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, THE FATF RECOMMENDATIONS (2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

[2] *See* E.W. Kruisbergen, *Combating Organized Crime: A study on undercover policing and the follow-the-money strategy*, 143–45 (2017), https://www.wodc.nl/binaries/Kruisbergen_dissertation_full%20text_tcm28-237785.pdf; *see also* P.E. Neumann, *Don't Follow the Money: The Problem with the War on Terrorist Financing*, FOREIGN AFFAIRS, July/Aug. 2017, at 93–102.

data protection principles. Since this is done from an EU perspective, therefore, this Article's red thread is the cross-border evidence gathering by EU states' law enforcement authorities from US based companies[3] and not vice versa.

There are thus three key phenomena to be joined for the purpose of answering the central question: "Digital personal data," "cross-border criminal investigations," and the "involvement of US based companies as the data supplier." For this analysis it is essential to highlight recent relevant EU legal instruments and proposals: The general data protection regulation[4] ("GDPR"); the directive on data protection for law enforcement purposes[5] ("DDPLE"); the proposed regulation on European production and preservation orders for electronic evidence in criminal matters ("e-evidence regulation"[6]). All three will be the subject of further analysis in this Article.

I. Three Key Phenomena

The three phenomena studied in this Subtitle are not new. All have found their place in the global society for some time. Bringing the three together, however, makes new issues emerge for which a binding legal framework does not yet exist. It is necessary to first reflect on the meaning of these three phenomena separately before examining what such legal framework should look like.

1. Digital Personal Data

The so-called mother convention of data protection—the 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data—described personal data as "any information relating to an identified or identifiable

[3] *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*, THE EUROPEAN COMMISSION (2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (citing the US as the recipient of the highest volume of requests for digital evidence from EU authorities. Non-paper from the Commission Services).

[4] Commission Regulation 2016/670 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter GDPR].

[5] Directive 2016/680 of the European Parliament and of the Council of April 27, 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 Offenses or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 110) [hereinafter DDPLE].

[6] *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM (2018) 225 final (Apr. 17, 2018) [hereinafter E-Evidence Regulation].

individual."[7] Later, this definition was written into the EU's first legal instrument on data protection: EC Directive 95/46/EC.[8] Thus, it is not necessary to know a person's name or address to identify or single out an individual.[9] Whether the data controller's capability of identifying a person is used or not has little impact on the personal character of the data.[10]

The concept of personal data has been slightly redefined in the aforementioned GDPR and the DDPLE by the addition of a separate definition of "identifiable natural person." The new definition means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name; an identification number; a location; an online identifier; or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[11] An IP address can, for example, qualify as personal data.[12] Even though under the former definition digital personal data were also included,[13] the new definition now explicitly includes digital identifiers.

To illustrate the potential relevance of digital personal data for criminal investigations, it is useful to briefly narrow in on the different types of data—subscriber data, access data, transactional data, and content data—as defined by the proposed regulation on European Production and Preservation Orders for electronic evidence in criminal matters.[14] Subscriber data pertains to the identity of the user of a service and the type of service, its duration and data related to the validation of the use of service, but not to passwords or authentication means. Access data include the date and time of use of a service—moment of logging in and logging out—and the IP address that is used at that time. Transactional data relate to the transaction of information from a source to its destination and include the sender and recipient of a message, data on the location of the device used, time, duration, size, route,

---

[7] This convention, and the 1980 OECD Guidelines governing the protection of privacy and trans-border flows of personal data, were inspired by two resolutions of the Council of Europe Committee of Ministers—Res 73(22) and Res 74(29)—and a recommendation by the Parliamentary Assembly of 1968.

[8] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

[9] *See* LEE A. BYGRRAVE, DATA PROTECTION LAW, APPROACHING ITS RATIONALE, LOGIC AND LIMITS 43 (2002).

[10] *See id.* at 44.

[11] 2016 O.J. (L 119) 4(1).

[12] Opinion 4/2007 on the Concept of Personal Data, THE WORKING PARTY (2007), https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.

[13] Opinion 2/2010 on Online Behavioural Advertising, THE WORKING PARTY (2010), https://iapp.org/media/pdf/resource_center/wp171_OBA_06-2010.pdf (noting an individual's internet surfing behavior can be so specific that it can qualify as personal data).

[14] *See E-Evidence Regulation*, *supra* note 6 at Art. 2 (7)–(10).

and format. Content data is a residual category made up of all digital data—text, image, video, or audio—that is not subscriber, access, or transactional data. All of the described types of data can encompass personal data and are protected by the EU's data protection provisions, which will be discussed later. The relevance of the distinction described here lies in the amount of protection required. Content data require a stronger protection as they can contain information that is considered to be the private life of one or more individuals. Nevertheless, transactional data are also capable of drawing a detailed picture of an individual's communications: Whom does one communicate with? How often? When? Where does the communication take place? How long does each communication take?[15] Thus, the higher degree of invasiveness of requests for obtaining such data, as compared to subscriber and access data, warrant the distinction made in the European Commission's proposed regulation on digital evidence.[16]

2. Cross-border Criminal Investigations

Criminal investigations that have links to more than one state—due to the location of the perpetrator(s), victim(s), witness(es), or evidence—require mutual legal assistance requests. These requests find their legal basis in a well-established, almost worldwide, framework of multilateral and bilateral agreements. Traditionally,[17] mutual legal assistance requests had to pass through the central authority of the requesting state—usually the ministry of justice—before it could be sent to the central authority of the requested state. The central authority would subsequently forward it to the competent local prosecution or police authority. The 2000 EU Mutual Assistance Agreement[18] introduced direct contact between competent prosecution or police authorities for the first time, but on a wider geographical scale and legal basis—Council of Europe and UN—the traditional sending of requests via the central authority is still the norm. The latter is also the case for the 2003 EU-US Mutual Legal Assistance Agreement[19] and for the 2001 Cybercrime Convention,[20] which contains a significant portion of mutual assistance provisions.

The backbone of the mutual legal assistance mechanism is territorial sovereignty of the states involved. It is thus built on the premise of physical borders defining the territories of

[15] *See* Daniel Solove, *Why Metadata Matters: The NSA and the Future of Privacy*, TEACH PRIVACY (Feb. 12, 2013), https://teachprivacy.com/metadata-matters-nsa-future-privacy/; *see also* Jennifer Daskal, *Law Enforcement Access to Data Across Borders*, 8 J. OF NAT'L SECURITY L. & POL'Y 3, 485 (2016).

[16] *See E-Evidence Regulation*, *supra* note 6; *see infra* Section B.1.

[17] *See* The 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters, E.T.S. No. 30.

[18] 2000 O.J. (C 197).

[19] 2003 O.J. (L 181).

[20] *See* The 2001 Council of Europe Convention on CyberCrime, E.T.S. No. 185.

states and restricting the geographical competence of the authorities involved. When the requested evidence is a tangible object or information of a non-digital nature, such as a paper criminal record or a witness statement, the evidence's location is clear in most circumstances, hence the addressee of a request is also clear. When the requested evidence is digital, such as email communications, however, determining territorial jurisdiction and cross-border evidence gathering becomes a more convoluted process.

3. Involvement of US based Companies[21]as the Data Supplier

Using the traditional mutual legal assistance mechanism for digital data generates a number of requests from competent authorities in all twenty-eight EU member states, most of which are addressed to US authorities.[22] The reason is obvious: Most of the companies we pass our digital personal data to on a daily basis are US based companies.[23] This does not necessarily mean that EU citizens' data will be processed and stored on US territory. Even if they are, that does not mean that they are not protected under the EU data protection legal framework.

With the newly applicable data protection legal framework, companies based outside of the EU that direct their services to EU citizens are required to comply with the provisions of the GDPR. Companies that are data controllers—deciding on the purpose and the means of data processing—as well as companies that are data processors—processing data on behalf of data controllers—are both responsible for compliance with the terms of the GDPR for the specific data processing activities that they conduct. Infringements of GDPR provisions can lead to consequences such as reprimands or suspension of the data processing activities by the supervisory authority or, at worst, it can lead to administrative fines up to twenty million euros or four percent of the total worldwide annual turnover of the preceding fiscal year. Data protection standards such as purpose limitation and data retention are applicable to a US company processing data from EU citizens in the same way they are applicable to an EU company. That should improve the level of protection EU citizens receive, but it is unrelated to the accessibility of the data for EU based law enforcement authorities. The accessibility of the data held by US companies for criminal investigations initiated in the EU is affected by how these companies store their data, however.

---

[21] In order to avoid confusion with the term "service providers," I choose to use the wider term "companies." Companies that offer search engines such as Google are not a service provider in the strict sense of the word because they do not offer Internet access. Search engines, however, collect vast amounts of data that can be requested by law enforcement authorities and should thus be included in this analysis.

[22] *See* IMPROVING CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE, *supra* note 3.

[23] Shobhit Seth, *World's Top 10 Internet Companies*, INVESTOPEDIA (Feb. 16, 2018) https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp (noting that of the top ten of the largest—based on annual revenue—Internet companies in the world, six are American and four are Chinese).

In the following Section, the above three key phenomena will be joined to demonstrate which new questions need to be dealt with in this new normal of borderless digital personal data in a world that is defined by borders.

II. On a Collision Course

When personal data gathered, processed, and stored by US based companies is needed for the purpose of a criminal investigation in the EU, how does the digital nature of those data change the mechanism? In this subtitle we look at the borderless digital storage practices of companies and how states have created different ways to obtain data needed for criminal investigations.

1. Digital Storage

Companies often use cloud storage for securely storing their data. Essentially, cloud storage means storage of data on one or more servers possibly owned by someone else rather than storage on one's own computer hard drive or portable device. Companies either have their own cloud or rent cloud storage space from another company: A cloud provider. The use of cloud storage affects the search for data by law enforcement authorities in two ways. First, the server does not need to be physically located at the premises of the cloud provider. It can even be located in a different country. Creating physical distance between administrative offices and data locations can be beneficial from a security point of view or it can be done for legal reasons—for example, a more lenient data protection regime. Second, many companies buy or rent cloud storage from cloud providers, not necessarily knowing where exactly these companies have built their servers—or data centers—or in which data center their data are located at any given moment. To secure the data stored in these centers, companies can distribute the data across servers in different locations. The data is then cut up in parts and replicated over multiple systems while the company tracks the location and status of each hard drive of their data centers.[24] Furthermore, the distribution of data over servers can change automatically depending on how the company has organized its data centers. Such a practice is used by Google "as frequently as needed to optimize for performance, reliability and other efficiencies," and led the ubiquitous company to declare in a recent court case that, at the time of an authority's request for data, the location of the data can be different from the location at the time the request is executed.[25]

Following the logic of the GDPR, a data center in itself would not qualify as the main establishment of a company. To qualify the data center would need an effective and real exercise of management activities—through stable arrangements—which determine the

[24] *See Data and Security,* GOOGLE https://www.google.com/about/datacenters/inside/locations/index.html.

[25] *In re* Search Warrant No. 16-960-M-01 to Google (E.D. Pa. 2017).

main decisions as to the purposes and means of the data processing.[26] Both situations described above can still lead to issues when the digital data in question are being moved to be stored in a data center of the company located in a third state whereas that company has a main establishment in the EU. For example, if Google has its main EU establishment in Ireland but the data wanted for a criminal investigation conducted by Spain are stored on a server in Brazil, in case of the automatic "data hopping," the data could be stored within yet a different jurisdiction at the time the Brazilian authorities would execute the request.

2. Law Enforcement Requests for Digital Data

To use the term accurately developed by Jennifer Daskal, data is infamously un-territorial,[27] especially when the above-described dynamic distribution of data or data hopping is taking place. What does this mean for criminal investigations and prosecutions? The question is particularly significant considering that criminal procedure laws are typically national laws. Thus, the legal framework governing data gathering for the purpose of investigating and prosecuting criminal offenses is territorial whereas the data themselves are not. This collision between territorial laws and un-territorial data presents two legal questions.

The first question is whether mutual legal assistance in criminal matters is a mechanism that functions when cross-border digital evidence is concerned? Traditionally, law enforcement authorities request cross-border evidence in the EU-US relations by using mutual legal assistance requests. Yet these requests are addressed to the authorities of the requested state, not the companies holding the data. Multilateral mutual legal assistance treaties do not provide indirect contact between law enforcement authorities of one country and a private company of another country. Inherently request-based, the system of mutual legal assistance is also notoriously slow. With time being an essential element in criminal investigations, especially when easily moved digital evidence is concerned, corrupted or destroyed, a number of EU member states have turned to sending direct requests for digital data to companies in third states.[28] When companies are located in a third state, a conflict of laws may arise if their national law does not allow for handing over the data.

Practice among EU member states demonstrates the relevance of questioning traditional mutual assistance. When the European Commission services distributed a questionnaire[29] among the EU member states in 2016 aiming to gain insight in how member states handled

[26] *See* GDPR, *supra* note 4 at recital 36 of the preamble.

[27] Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L. J. 326, 326–98, (2015).

[28] *See* IMPROVING CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE, *supra* note 3; *see also Questionnaire on Improving Criminal Justice in Cyberspace*, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

[29] *See Questionnaire*, *supra* note 28.

cross-border access to digital evidence, the result revealed a surprisingly diverse patchwork of terminology used as well as approaches to obtaining the evidence.[30]

At the time of the questionnaire, the European Investigation Order had not been implemented, so member states' authorities should have relied on either the unpopular European Evidence Warrant or the aforementioned EU mutual legal assistance agreement. Nonetheless, in those cases where a company was located outside the domestic jurisdiction—but still in the EU—twenty-four out of the twenty-seven member-states that replied to the questionnaire relied on sending direct requests by national authorities to companies in another member state. Of those twenty-four, seventeen member-states consider these direct requests voluntary, and seven consider them mandatory. Only three member-states indicated having specific legislation for this type of cooperation. No less than twenty-four member-states do not allow companies established on their territory to respond to direct requests from authorities in other member states or do not provide for this in their national laws.

The picture is slightly different when the wanted data should be obtained from a company based in a third state. In this context, and given that the location of the data is known, the instrument to use is clear. Mutual legal assistance requests are the only option. Mandatory orders for data outside the framework of a bilateral or multilateral agreement would most likely be considered a serious breach of the sovereignty of the third state in question. Nevertheless, the mechanism of mutual legal assistance in criminal matters is not unproblematic. A concern that is not new in this context is the time-consuming nature of mutual legal assistance requests. It is a complaint that has been haunting mutual legal assistance procedures for decades. Other concerns are related to the digital nature of the evidence such as the use of mutual legal assistance procedures for access to information where under US law no mutual legal assistance request is required—such as subscriber data, or the difficulty to establish probable cause and the lack of dual criminality. When the location of the data is unknown, member states responded to the questionnaire with a variety of approaches. Aiming to find out the location of wanted data, multiple mutual legal assistance requests could be used, but are a rather inefficient and time-consuming method. Five member-states indicated that their competent authorities could directly access digital evidence when the location is unclear or when it is impossible to establish its location. Fourteen member-states indicated that this depends on specific circumstances. Such method of working could entail significant sovereignty issues on the part of the third state.

The second question relates to the data storage practices described above. When companies store data or data parts on servers in different locations, what is the determining factor for

[30] *Measures to improve cross-border access to electronic evidence for criminal investigations following the conclusions of the Council of the European Union on improving criminal justice in cyberspace* (2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf.

deciding where to send the request for data: The main establishment of the company, or the physical location of the data? A similar question—although in the opposite direction, from a US authority requesting EU based data—was raised in the Microsoft Ireland case when Microsoft refused to comply with a warrant from US authorities to hand over data on an email account that were stored on a server in their Irish data center.[31] The question was not whether the national law applied outside the territory of the US—the parties agreed that it does not—rather, the question was whether data stored on a server in Ireland, controlled by a US based company, were located in Ireland or in the US? The answer would determine whether a mutual legal assistance request was needed, or whether it was a purely domestic request for data. The difference between both options in terms of jurisdiction, grounds for refusal of the request, and time spent are considerable. In the meantime, the case before the Supreme Court was declared moot due to the adoption of a new law by the US Congress in March 2018.[32] The so-called CLOUD Act as well as its EU counterpart will form the heart of the following subtitle.

A. Defensive Cooperation Avoiding Collisions

Both the EU and the US have recently initiated legislative solutions to improve access to digital data for the purpose of criminal investigations. The US Clarifying Lawful Overseas Use of Data or CLOUD Act was not the subject of elaborate discussion in Congress, but buried in more than 2,000 pages of a spending bill adopted on March 23, 2018. Even though the European Commission already started preparations on its own proposed legislation to regulate cross-border electronic evidence in 2016, European Justice Commissioner Jourova expressed her disappointment that the CLOUD Act's swift adoption did not allow for a compatible solution between the EU and the US.[33]

I. Proposed European Preservation and Production Order

On April 17, 2018, the European Commission presented its proposals for electronic evidence in criminal matters, the so-called e-evidence proposals. Inspired by the results of the aforementioned questionnaire, the European Commission developed several non-legislative and legislative options to rectify the situation and offer member states legal certainty on what to do when digital data is needed from a company based in a third country. The

[31] U.S. v. Microsoft, 584 U.S. 1 (2018) (per curium).

[32] CLOUD Act, H.R. 4943, 115th Cong. (2018).

[33] Nikolaj Nielsen, *Rushed US Cloud Act Triggers EU Backlash*, EUOBSERVER (Mar. 26, 2018), https://euobserver.com/justice/141446.

proposed approach is a regulation introducing a preservation and production order,[34] and a directive on how companies should select their legal representation in the EU.[35]

The European preservation and production orders are developed from the same line of reasoning as the existing mutual recognition measures. The strongest similarities exist with the freezing order and the confiscation order—now replaced by the European Investigation Order.[36] The freezing and confiscation orders could equally be used in a successive order. Whereas the freezing order ensured the immobilizing of evidence awaiting a subsequent confiscation order, the preservation order secures the wanted data in view of a subsequent order to produce the data. If no concern that the data would be deleted, moved, or otherwise modified is presented, the production order could also be used as a stand-alone measure. A European Investigation Order or a mutual legal assistance request could also follow up preservation orders.

An important characteristic of the proposed regulation that sets it apart from previous mutual recognition instruments is its significant effect on third states. The scope of the proposed regulation reaches beyond the borders of the EU, as it includes companies that provide services in the EU. Resembling the scope of the GDPR to some extent, the Commission is hereby responding to a highly digitalized world governed by companies based outside the EU. Offering its law enforcement and judicial apparatus the proper tools to work with, the Commission accompanied this wide scope of the proposed regulation with a directive that obliges all service providers operating within the EU to appoint a legal representative within the EU. This will allow the competent authority of an EU member-state wanting to obtain digital data from a US based company such as Facebook, to contact their legal representation in the EU—most likely the Dublin office—through a preservation or production order rather than by sending a mutual legal assistance request to the US central authorities.

The scope of the proposed regulation is limited to data stored at the time of receipt of the order. Real-time interception of telecommunication is thus excluded and will remain to fall within the scope of the European Investigation Order or the EU mutual legal assistance agreement. Based on the level of intrusiveness, the proposed regulation distinguishes two classes of digital data. As explained under Subtitle I.1., subscriber and access data are considered to be less sensitive in comparison to transactional and content data, bringing the latter two under a more protective regime. For obtaining transactional or content data, the

[34] *See E-Evidence Regulation*, *supra* note 6.

[35] *Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, COM (2018) 226 final (Apr. 17, 2018).

[36] Denmark and Ireland are not taking part in the European Investigation Order so for cooperation with these member states, the freezing and confiscation orders can still be used.

production order should be issued by a judge, a court, or an investigative judge. Prosecutors can only issue production orders for subscriber or access data. Moreover, production orders for transactional or content data may only be issued for the more serious of offenses.[37] The distinction in types of data only applies to production orders, not to preservation orders.

The real innovation in the proposed regulation—and the similarity with the US CLOUD Act—is the recognition of potential conflicts of laws affecting the companies involved. When a company based outside the EU offering services to EU citizens receives a production order from an EU member-state's authority, it is likely that the company is prohibited by its own national law to transfer the data—for example, the US Electronic Communications Privacy Act.[38] Such situations created legal uncertainty for the company but also created a waste of time and resources since the issuing authority had to subsequently rely on other channels to obtain the evidence needed for a running criminal investigation. To solve this unsatisfying situation, the proposed regulation introduces a right for the companies in question to raise a reasoned objection to the production order and have the case reviewed by a court—of the member state involved—if the issuing authority insists on upholding the order. When the court determines that there is a conflict of laws, an opinion should be requested of the third state. Only if the third state's laws aim to protect fundamental rights of citizens or fundamental interests related to national security or defense, the production order must be withdrawn. In the opposite case, the court should balance the interests at stake.

This is different reasoning from the traditional mutual legal assistance mechanism. The latter is based on issuing a request to a state's central authority—usually the ministry of justice—and having this authority assess whether fundamental interests of the requested state or of individuals involved should be protected before confirming or denying the execution of the request. Whether or not such assessment takes place in the context of the production order now lays in the hands of a company rather than a ministry of justice. This raises the issue of whether a company is in the right position to make such assessment. Companies' main interest is doing business and making money. Delivering data to states' competent authorities is not part of that. This does not mean companies do not want to be compliant; they are simply not equipped to handle mutual legal assistance related questions. Imagine if a company that receives a request for data does not see a conflict of law and transfers the requested data to the requesting state. After the transfer, the national authorities of the company's main seat see the transfer as a violation of their national laws. Does that make the evidence delivered to the requesting state inadmissible? Could a company be held liable for such conduct and the consequences thereof for a running criminal procedure? These are once again new questions that are, so far, unanswered.

---

[37] *See E-Evidence Regulation*, *supra* note 6 at Art. 4 (defining criminal offenses punishable in the issuing state by a custodial sentence of a maximum of at least 3 years or fraudulent money transfers, offenses related to sexual abuse and exploitation of children and terrorism offenses wholly or partly committed by means of an information system).

[38] *See infra* Section B.2.

A substantial improvement in the mechanism of cross-border evidence gathering introduced by the proposed regulation is the speed with which preservation and production orders should be executed. Preservation orders should be carried out without undue delay. Production orders should result in a transfer of the wanted data within ten days upon receipt of the order unless valid reasons are given for non-compliance. In cases of an imminent threat to life or physical integrity of a person or to a critical infrastructure, the deadline is shortened to six hours. In comparison to the 120 days for obtaining data via a European Investigation Order or the average ten months for receiving data resulting from a mutual legal assistance request,[39] the shorter deadlines are appropriate for the fast-paced character of digital evidence. Still, if the proposed regulation is adopted in an unchanged format, companies will be forced to invest considerable resources in preparing for a number of production orders that have to first be studied for potential conflict of laws and then be either objected to or complied with.

II. US CLOUD Act and Privacy Shield

The proposed EU regulation on preservation and production orders was partially inspired by the conflict of laws created by the US Electronic Communications Privacy Act ("ECPA".) The ECPA blocked disclosure of content data in most circumstances of requested cross-border transfer. In March 2018, against the background of a data sharing agreement between the US and the UK,[40] the ECPA was amended by a new act. This new act, appropriately named the CLOUD Act,[41] allows US based companies to hand over data regardless of the physical location of the data, under the condition that it does not concern data about US persons or residents. EU member states' competent authorities could thus benefit from the CLOUD Act so long as they do not need data on American citizens or residents. The requesting state, however, needs to meet a high standard of substantive and procedural protections for privacy and civil liberties.[42]

[39] *New EU Rules to Obtain Electronic* Evidence, EUROPEAN COMMISSION (Apr. 17, 2018), http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

[40] Madhumita Murgia, *UK-US pact will force big tech companies to hand over data*, FINANCIAL TIMES (Oct. 23, 2017), https://www.ft.com/content/880bc2ae-b980-11e7-9bfb-4a9c83ffa852.

[41] CLOUD Act, H.R. 4943, 115th Cong. (2018).

[42] Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018), https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

An additional agreement with the US is still necessary in accordance with article 48 of the GDPR[43] that only allows personal data transfers with a legal basis in mutual legal assistance agreements or other international agreements.[44] The EU-US mutual legal assistance agreement of 2003—applied in relation to the prior existing bilateral mutual legal assistance agreements between EU member states and the US—would not qualify as the agreement that brings the CLOUD Act in line with the GDPR because it is applicable to states exchanging data and not a state's authorities requesting a company directly for data. Moreover, the provisions of article 9 of the 2003 EU-US agreement on limitations on use of personal and other data are formulated to favor less restriction on the use of data by requesting EU or US authorities over more restriction;[45] something that is not the tone of the CLOUD Act, considering the list of factors to be fulfilled before a foreign government could receive data from a US based company. These factors include adequate substantive and procedural laws on cybercrime and electronic evidence, demonstrated respect for the rule of law and principles of non-discrimination and adherence to international human rights obligations. Formally recognizing EU member-states as fulfilling these factors would significantly improve EU-US cooperation in criminal matters.

The list of factors to be fulfilled by a non-US government prior to receiving data from a US based company reminds us of the adequacy requirement introduced in the aforementioned EC Directive 95/46/EC in the other direction, namely imposed by the EU onto third states such as the US. The EU was the first to demand a certain level of data protection in a third state as a prerequisite to that state processing any EU-originated personal data. US academics did not welcome this requirement,[46] not in the least due to the substantial differences between the EU and the US data protection legal frameworks. The disagreements made approval of the US' data protection regime as adequate doubtful. These differences were largely ironed out by the Safe Harbor agreement, replaced with the EU-US Privacy Shield.[47]

---

[43] *See* Amicus Curiae Brief of the European Commission on Behalf of the EU in the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation, U.S. v. Microsoft, 584 U.S. 1 (2018) (per curium).

[44] *See* Christin McMeley & John Seiver, *The CLOUD Act — A needed fix for US and foreign law enforcement or threat to civil liberties?* IAPP (Feb. 28, 2018), https://iapp.org/news/a/the-cloud-act-a-needed-fix-for-u-s-and-foreign-law-enforcement-or-threat-to-civil-liberties/.

[45] *See* ELS DE BUSSER, DATA PROTECTION IN EU AND US CRIMINAL COOPERATION: A SUBSTANTIVE LAW APPROACH TO THE EU INTERNAL AND TRANSATLANTIC COOPERATION IN CRIMINAL MATTERS BETWEEN JUDICIAL AND LAW ENFORCEMENT AUTHORITIES, 353–54 (2009).

[46] *See* George B. Trubow, *European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flows* 13 NE. J. OF INT'L L. & BUS., 176 (1992–1993); *see also* William J. Long & Marc Pang Quek, *Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise*, 9 J. OF EUR. PUB. POL'Y 325, 326 (2002).

[47] Commission Implementing Decision (EU) 2016/1250 of July 12, 2016 pursuant to the Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-US Privacy Shield,

In spite of the earlier critiques from US scholars on the EU adequacy requirement, the US CLOUD Act equally includes a set of prerequisites the recipient state should fulfill before a data transfer can take place. This is not the first time that a US law provides a copy of the adequacy requirement. In the Judicial Redress Act[48] we see a clear set of conditions imposed on states wishing to benefit from the expanded redress rights. The Judicial Redress Act is a law adopted after pressure from the European Commission on the US government to grant EU citizens judicial redress for unlawful processing of personal data under the 1974 US Privacy Act.[49] Pressure to adopt the law increased after both parties agreed to sign the so-called EU-US Umbrella Agreement, a pact that can be best described as a "superstructure" added to earlier concluded EU-US agreements consisting of safeguards protecting data exchanged under the terms of the agreements.[50]

III. The Effect on Data Protection

Both the EU and the US impose an a priori requirement on the recipient state's level of respect for certain rights, which adds a new dimension to cross-border data exchanges. When personal data leaves the EU to be processed in the US, the US' level of data protection should be adequate, which includes inter alia adherence to human rights. In cases where data transfers in both directions are made for law enforcement purposes, the EU-US umbrella agreement and the EU-US mutual legal assistance agreement ensure additional safeguards. When EU authorities want to receive digital data directly from a US based company, they need to show respect for the rule of law, adequate laws on electronic evidence and cybercrime, and compliance with human rights. As argued above, an additional agreement is still needed because the data transferring party is a company and not an authority.

In spite of this list of existing agreements and one future agreement, we effectively see here the imposing of rules on other states by introducing national laws rather than international

2016 O.J. (L 207) (Both the Safe Harbor agreement and the Privacy Shield are based on the same mechanism: a set of data protection principles signed by a long list of US based companies committing themselves to compliance with these principles. Since the Safe Harbor agreement was annulled due to insufficient necessity and proportionality safeguards and lacking redress for EU citizens (Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650), the Privacy Shield enhances data protection.

[48] The Judicial Redress Act of 2015, H.R. 1428, 144th Cong. (2016).

[49] *See Big Data: A Twenty-First Century Arms Race*, ATLANTIC COUNCIL (2017), http://www.atlanticcouncil.org/images/publications/Big_Data_A_Twenty-First_Century_Arms_Race_web_0627.pdf.

[50] *Id.*

agreements.[51] The adequacy requirement of Directive 95/46/EC was an example, its successor, the GDPR, follows suit. Now the US Cloud Act has a similar effect. It is not unthinkable that the GDPR's wide scope could lead to an export of EU data protection standards as US-based companies may have a hard time distinguishing between their data processing of EU customers data and non-EU customers data and will thus apply the EU standards to all their data processing activities. Ultimately, we may see data localization and market segmentation as potential consequences.[52] This norm creation without international agreements fits in the departing from traditional mutual legal assistance in criminal matters.

B. The Fast Track

Not that long ago, the European Investigation Order was considered the fastest tool in the hands of competent EU authorities to obtain information and material in the context of a cross-border criminal investigation. Aiming to speed up the notoriously slow mutual legal assistance process, limit grounds for refusal, shorten deadlines, and standardize forms created a mechanism for conducting most cross-border investigative measures between EU member states. The European Investigation Order has only been applicable for a little more than a year now; still, it is already considered too slow for digital evidence.

Even though mutual legal assistance and the European Investigation Order will remain in place, the new proposed regulation introducing preservation and production orders for digital data resembles the fast-track line at the security control section of an airport. This race to develop speedier cross-border cooperation tools is triggered by the fast-paced digital society we live in today. Mutual legal assistance procedures that make requests move between central authorities of the requesting and requested state before reaching the locally competent (judicial) authority have no place in today's digital society. Yet, that does not necessarily mean that a new mechanism should be introduced which makes a company the requested party rather than a state's central authority or competent authority.

Besides the significant investment that is expected from companies to assess every incoming production order to potential conflicting laws, the proposed regulation puts companies in a position they should not be in: The position of protecting the sovereignty of the state where they have their main seat. In fact, the ties between that particular state—whose laws allowed the company to be founded in the first place—and the physical location of digital data stored by the company are cut. When Google stores data in a data center in Brazil, a German judge can have them produced by addressing the EU legal representation of Google. The only way the Brazilian law could put a stop to it is if it would create a conflict of law that should be flagged by Google.

---

[51] Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9 (2018) (referencing to Anu Bradford, *The Brussels Effect*).

[52] *Id.*

Mutual legal assistance was developed in a slow-pace manner due to the assessment it allowed the requested state to make. That state had the chance to perform a thorough check of the compatibility of the requested investigative measure with its own sovereignty, security, or essential interests. It enabled a state to, for example, refuse cooperation to possible political prosecution in the requesting state. Even in the EU's area of freedom, security, and justice where mutual trust should theoretically exist, based on which mutual recognition should limit the grounds for refusal to cooperate more, a real risk for violation of the individual's fundamental rights was recognized as a valid reason to refuse cooperation.[53] Moving away from mutual legal assistance to make room for faster cooperation should be a beneficial development. One that is necessary considering the amount of digital evidence. It is not a beneficial development when guarantees protecting states' sovereignty and individuals' rights are left as well.

[53] *See Joined Cases C-404/15 & C-659/15 PPU Pál Aranyosi & Robert Căldăraru* (Apr. 5, 2016) http://curia.europa.eu/juris/liste.jsf?num=C-404/15.

Articles

Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation

By Anne de Hingh[*]

Abstract

As the use of the Internet and online platforms grows, the scale of collecting and processing personal data and turnovers have increased correspondingly.[1] At the same time, public awareness about the Internet turning into a genuine profiling and advertisement machine, as well as a powerful surveillance instrument, grows. More people today are concerned about the ways in which public and private actors store and use private information. Many individuals note that they lose sight of the consequences once they give consent to the collection of their sometimes most intimate personal data. The Snowden revelations and the recent Facebook and Cambridge Analytica scandal have only reinforced this public awareness.

Objections against these data processing practices cannot be explained as breaches of data protection or privacy regulation alone. In this Article, it is argued that recently passed regulations fail to solve the unease of data subjects as other, more fundamental values are at stake here. A different or complementary ethical and legal framework is needed to interpret this generally felt unease vis-à-vis current data practices and secondly to confront future developments on the data market. The concept of human dignity may be a helpful perspective in this respect. In the context of data processing, human dignity is generally interpreted in a quite specific manner, such as contributing to the empowerment and self-determination of autonomous individuals. It can be argued, however, that human dignity—in the context of the commodification and commoditization of online personal data—should be seen in a different, quite opposite, light. In sum, future regulation of privacy and data protection attention should shift towards more constraining dimensions of human dignity.

---

[*] Assistant Professor of Internet Law, Department of Transnational Legal Studies, Faculty of Law, VU University Amsterdam. E-mail: a.e.de.hingh@vu.nl. The author would like to thank Els De Busser, Ester Herlin Karnell, Galina Cornelisse, Tina van der Linden, and Arno Lodder for their valuable comments.

[1] The growth of the Dutch internet use is reflected in the results of a recent survey: of the 17 million Dutch citizens, 11.5 million use Whatsapp, 10.8 million are on Facebook, 8 million use YouTube, 4.4 million are members of LinkedIn, and 4.1 million people in the Netherlands use Instagram. *See* NEWCOM, NATIONALE SOCIAL MEDIA ONDERZOEK (Jan. 29, 2018), https://www.newcom.nl/socialmedia2018.

A. Introduction

Personal data[2] developed from the by-products of computing to the main resources and commodities of online activities.[3] Digital technologies have made it possible to expose, produce, isolate, aggregate, process, analyze, buy and sell, exploit, transfer, and circulate large amounts of data on individual human beings. Data have grown out to be an inexhaustible source of income and power for both private parties—technology companies, online platforms and social media, the advertisement industry and data brokers—and public parties—public administrations, law enforcement agencies and intelligence services. These actors constantly harvest personal data from individual human beings for their own specific purposes: Be it financial gain, political goals or purely governmental purposes like fighting crime and preventing terrorism. This had led up to what is welcomed by some as the new economy of today.[4] Others have criticized this development as a major threat to online privacy, data hunger, a new religion ("dataïsm")[5], big data surveillance,[6] data capitalism,[7] or surveillance capitalism.[8]

The collection, analysis, and trade of online personal data, and the roles of information technology companies and government in this market are highly debated issues. Serious public concerns on these matters grow only with each new revelation, like the 2018 uproar over Cambridge Analytica's massive abuse of Facebook data for political micro targeting. These concerns relate to the disturbing idea that there is a genuine market wholly

[2] "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *See* Art. 4(1) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the General Data Protection Regulation, Directive 95/46/EC, 2016 O.J. (L119) [hereinafter GDPR].

[3] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015).

[4] *See* VIKTOR MAYER-SCHÖNBERGER & THOMAS RAMGE, REINVENTING CAPITALISM IN THE AGE OF BIG DATA (2018).

[5] YUVAL NOAH HARARI, HOMO DEUS: A BRIEF HISTORY OF TOMORROW (2015); STEVE LOHR, DATA-ISM: THE REVOLUTION TRANSFORMING DECISION MAKING, CONSUMER BEHAVIOR, AND ALMOST EVERYTHING ELSE (2015).

[6] *See* Surveillance Studies Centre at Queen's University, *The Big Data Surveillance Project*, SURVEILLANCE STUD. CENTRE, http://www.sscqueens.org/projects/big-data-surveillance.

[7] Evgeny Morozov, *Digital Technologies and the Future of Datacapitalism*, SOC. EUR., (Jun. 23, 2015), https://www.socialeurope.eu/digital-technologies-and-the-future-of-data-capitalism.

[8] *See* Shoshana Zuboff, *The Secrets of Surveillance Capitalism*, FRANKFURTER ALLGEMEINE ZEITUNG (Mar. 5, 2016), www.shoshanazuboff.com.

dependent upon the trade in personal data, that this market is expanding on a great scale and that it is developing into highly undesirable directions. Personal data that are collected primarily for economic gain are subsequently transferred into other contexts and exploited for other purposes such as for political targeting or surveillance. Thus, data is constantly circulating between contexts or "silos." In this way, personal data is not only commercialized and commodified for their monetary value, but also commoditized as generic mass products.

There are, in my view, good grounds to consider specific developments of data practices as contrary to human dignity. In this Article, I will tentatively explore how the concept of human dignity can be incorporated in the debate on data, specifically big data. Elaborating further on Opinion 4/2015 of the European Data Protection Supervisor, some provisional reflections are presented on how dignity could play a constraining role—not only in the debate on, but also in the regulation of commercialization, commodification and commoditization of personal data.

Two parallel cases illustrate in what ways and to what extent this data ecosystem has developed. First, the recent revelations on the transfer of data from Facebook to Cambridge Analytica prior to the US presidential elections demonstrated the unexpected shape the resale of personal data can take. In this case, the accounts of up to eighty-seven million Facebook users were harvested, analyzed and used to shape voter targeting and messaging for the Republican presidential campaign.[9] Another Dutch example illustrates how the practices of collecting data can take up quite questionable forms. At the end of 2017, it was reported that the Joint Sigint Cyber Unit of the Dutch Intelligence and Security Services—AIVD and MIVD—had in previous years purchased large bulk sets of personal information from illegal origin. These data were stolen, hacked, or leaked and later sold by third parties on the online black market. Each of these datasets comprised names, email addresses, and passwords of more than a hundred million individuals who were not and will not be a direct target of the services.[10]

The cases presented here are just two of many examples revealing the scale by which personal data are treated as tradable goods. In addition, these examples demonstrate the ease with which data circulate and are transferred back and forth between separate parties for different purposes. Often, this takes place without the knowledge—let alone the

[9] Cambridge Analytica approached Facebook users through the Amazon Mechanical Turk platform (mturk.com) and paid them one to two dollars to download and use a personality quiz app (thisismydigitallife). The quiz "scraped" the information from the profiles of 320,000 Facebook users as well as detailed information from the profiles of their friends. *See* Zeynep Tufekci, *Facebook's Surveillance Machine*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.

[10] The Dutch oversight committee (CTIVD) concluded that one of the data sets was obtained unlawfully, such as without permission of the Minister of Interior Affairs. *See* CTIVD, *Toezichtsrapport nr 55, Over Het Verwerven Van Door Derden Op Internet Aangeboden Bulkdatasets Door de AIVD en de MIVD* (2017), https://www.ctivd.nl/documenten/rapporten/2018/02/13/index.

consent—of the data subjects concerned. Evidently, the boundaries between public and private and between legitimate and illegally obtained data sets are blurring and breaking down.[11]

This paper distinguishes two objections. The first one relates to the process of resourcification, the commodification of personal data, and to the observation that non-saleable things at one point in time became saleable. This Article argues that individuals should not be treated simply as resources of data that can be bought and sold on markets.[12] Selling data for money, I argue, is incompatible with the principle of non-commercialization of parts of the person, even if this person is voluntarily handing over her or his data. It can be defended that, for this reason, personal information should be more fundamentally protected than by data protection regulation alone.

A second objection emerges from the fact that personal data is moved back and forth, thus circulating between different realms or silos that were previously delimited. The blurring of the boundaries between the private and the public and between the legal and the criminal realms—or de-siloization—concurs with an endless recycling of information. In this process, personal data are not merely resourcified or commodified but also "commoditized." Commoditization in this context involves personal information turning into a generic bulk product. As a consequence, its original proper features lose their significance.[13] This development is reflected in the recent May 2017 Europol Regulation which does not focus on separate databases anymore, but on data processing operations.[14]

These and similar big data practices add fuel to the fire of public awareness and uneasiness because they only give a glimpse of the complexity and scale of big data exploitation in current business and surveillance models. Data exploitation "by its very nature has an underestimated impact on the ability of data subjects to understand its consequences and possible harms, and to make informed decisions."[15] Concerns accrue with every year the Internet grows older. On March 12, 2018, the twenty-ninth birthday of the Internet, Sir Tim

---

[11] *See, e.g.*, Fanny Coudert, *The Europol Regulation and Purpose Limitation: from the 'silo-based approach' to . . . what exactly?*, 3 EDPL 313–24 (2017); N. Purtova, *Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships*, 8 IDPL 1, 1–3 (2018).

[12] Beate Roessler, *Should Personal Data be a Tradable Good? On the Moral Limits of Markets in Privacy, in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 141–61 (Beate Roessler & Dorota Mokrosinska eds., 2015); MICHAEL J. SANDEL, WHAT MONEY CAN'T BUY: THE MORAL LIMITS OF MARKETS (2012).

[13] MARTIN GUNNARSON & FREDRIK SVENAEUS, THE BODY AS GIFT, RESOURCE, AND COMMODITY: EXCHANGING ORGANS, TISSUES, AND CELLS IN THE 21ST CENTURY, 9–30 (Martin Gunnarson & Fredrik Svenaeus eds., 2012).

[14] Coudert, *supra* note 11, at 313.

[15] *See* Andrej Zwitter, *Big Data Ethics*, BIG DATA & SOC., 1, 1–2 (2014) ("[T]he very nature of Big Data has an underestimated impact on the individual's ability to understand its potential and make informed decisions.").

Berners-Lee, the inventor of the world wide web as we know it, expressed his worries on the concentration of power of a few dominant platforms. In the year before, he had described the loss of control over our personal data as a major threat to the Internet of today.[16]

In short, the exploitation of data seems to put current privacy and data protection regulation under so much stress as to raise serious questions about the effectiveness of these regulations. It can be argued that this is not exclusively about market power and information asymmetry caused by the fact that individual users do not exactly know what it is that they give consent to. After all, even if users were aware of the consequences of their consent, they would likely continue to feel uncomfortable knowing someone has access to their personal information.[17]

Various surveys empirically support the notion that people are discomforted by large social platforms. A recent American poll found that the trust in all three of the major social media companies—Facebook, Twitter, and Google—is rapidly decreasing as mistrust is focused on the companies themselves, not on their technology.[18] Comparable outcomes of a recent Dutch social media survey illustrated that concerns regarding personal data are growing because only one fifth of the users feel they still trust social media—66% of the respondents are especially worried about the subsequent sale of their personal data.[19] A KPMG survey among 7,000 online consumers in twenty-four countries revealed that less than ten percent of the respondents find they have adequate control over the collection and exploitation of their personal data.[20] Respondents are especially worried about their personal data being sold to third parties, and indicate that they prefer a larger control over their personal information at the cost of other possible benefits of online shopping, like speed and convenience.

What legal or ethical interpretation should be given to this nagging unease on the large-scale collection and processing of personal data by companies and governments? It can be argued that the problem of personal data of individuals being exploited both as sources of profit and as continually circulating recycled mass products, protrudes the frame of data

---

[16] Tim Berners-Lee, *The Web Can Be Weaponised – and We Can't Count on Big Tech to Stop it*, GUARDIAN (Mar. 12, 2018), https://www.theguardian.com/commentisfree/2018/mar/12/tim-berners-lee-web-weapon-regulation-open-letter.

[17] FREDERIK J. ZUIDERVEEN BORGESIUS, IMPROVING PRIVACY PROTECTION IN THE AREA OF BEHAVIOURAL TARGETING 187 (2015).

[18] *See* Kim Hart & Ina Fried, *Exclusive Poll: Facebook Favourability Plunges*, AXIOS (Mar. 26, 2018), https://www.axios.com/exclusive-poll-facebook-favorability-plunges-1522057235-b1fa31db-e646-4413-a273-95d3387da4f2.html.

[19] *See* NEWCOM, *supra* note 1.

[20] *See* KPMG, CROSSING THE LINE: STAYING ON THE RIGHT SIDE OF CONSUMER PRIVACY (2017), https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf.

protection and privacy issues and touches upon the more fundamental question of what it means to be human. At the same time, it is hard to articulate what exactly the objections against these practices entail. Moreover, it is difficult to translate these ethical arguments into practical, legal ones, as our "data-protection centered vocabulary" might be inadequate for this.

A common explanation would be that massive data collection and processing by both public and private parties could entail an infringement of privacy or might stretch the limits of data protection principles. My position argues that principles of data protection regulation, like consent and purpose limitation, have lost much of their original usefulness. The General Data Protection Regulation (GDPR) that became effective on May 25, 2018, would be the designated legal tool in this respect. The GDPR, however, fails to offer adequate answers to the growing unease among European citizens because it does not appear to be tailored to the digital reality of today.[21] Many assume that autonomy, empowerment and self-determination are central to data protection; however, these principles seem insufficient to understand and address the ethical challenges brought about by recent digital technological developments.

This Article explores in what ways the concept of human dignity—especially through its constraining dimension—could contribute to an alternative legal framework that would set limits to certain data practices. It is structured as follows. Section B discusses Opinion 4/2015 of the European Data Protection Supervisor, the EU's independent data protection authority (EDPS), which is one of the early publications on data and dignity. In this opinion human dignity was interpreted in a very specific and narrow manner that is focused on the empowerment and self-determination of autonomous individuals; therefore, it still heavily relies on data protection principles. Section C elaborates on the thesis that the GDPR, as a regulatory instrument, and the principles of data protection alone do not suffice to cater for these generally felt sentiments of concern and unease with regard to the radical commodification and commoditization of personal data. The two cases mentioned above illustrate this point. In Section D, the possibility to approach these developments from an alternative angle is explored and the recently published report of the Ethics Advisory Group (EAG) of the EDPS is discussed. This report is the next step in the project to introduce ethics and especially the concept of human dignity into the debate on the regulation of big data. In the EAG-report, it is implicitly suggested that the interpretation of human dignity "as constraint" should have a central role in any alternative regulation of data, which is the central theme in this section.

B. The EDPS on Data and Dignity

[21] Regulation 2016/679, of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Repealing Council Directive 95/46/EC, 2016 O.J. (L119).

The concerns with regard to data processing that are highlighted above, evidently are not new but have been a common theme in academic legal literature and semi-scientific publications for quite some time now.[22] One of the contributions to the debate was published by the EDPS. His Opinion 4/2015, titled "Towards a new digital ethics. Data, dignity and technology" appeared in September 2015 when the legislative procedure of the adoption of the GDPR was still under way.[23] The EDPS suggested in the Opinion that taking a radically new approach was indispensable for the development of a more future-oriented regulation of the European data market in light of technological trends like the Internet of Things and the rise of artificial intelligence. According to the EDPS-publication, data market trends raise important ethical and practical questions for the application of data protection principles. The Opinion argues data protection principles, therefore, are aimed at exploring different routes to customize existing data protection principles to fit the global digital arena. The major trends identified, were the large scale of data collection, its ubiquity and power, the often intimate nature of the data in question, and the fact that processing takes place in increasingly opaque and complex ways.[24]

Clearly, a sense of urgency arose from Opinion 4/2015—as if it aimed at raising awareness of the fact that certain data protection principles had lost their impact altogether. In addition, new ethical and legal perspectives were now indispensable to solve current issues of privacy and data protection. It therefore proposed to explore an innovative approach by formulating a new ethical framework in which "better respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power" in the data market.[25] Human dignity "should be at the heart of a new digital ethics," according to the EDPS.[26]

The choice for dignity as a starting point could be seen against the background of human rights protection in Union law in which the inviolability of human dignity plays a pivotal role.[27] The EU Charter emphasizes dignity of a human not only is a fundamental right in itself but constitutes the foundation of fundamental rights, including the rights to privacy and to

---

[22] *See* NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US (2014); SCHNEIER, *supra* note 3; HANS SCHNITZLER, HET DIGITALE PROLETARIAAT (2015); HARARI *supra* note 5; FRANKLIN FOER, WORLD WITHOUT MIND (2017).

[23] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2015 Towards A New Digital Ethics: Data, Dignity and Technology* (2015), https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf.

[24] *Id.* at 6.

[25] *Id.* at 12.

[26] *Id.*

[27] Charter of Fundamental Rights of the European Union, art. 1 (recognizing human dignity as an inviolable right that must be respected and protected).

the protection of personal data.[28] Human dignity and data protection law are, evidently, not by definition mutually exclusive and the concept of dignity is, in the words of Floridi, almost "invisibly" present in the GDPR.[29] More specifically, Article 88 of the GDPR prescribes Member States to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of personal data in the employment context. Article 88 further states that these rules shall include suitable and specific measures "to safeguard the data subject's human dignity, legitimate interests and fundamental rights . . . ."[30] As pointed out by Floridi, it can be deduced from the phrasing of this Article that human dignity is different from "legitimate interests and fundamental rights." According to him, this is indicative of the fact that human dignity is the fundamental concept that provides the framework within which one needs to interpret what the GDPR understands by informational privacy.[31] One might consider designating human dignity as an extra layer that results in a right to privacy 2.0.

As part of the Digital Ethics project, an Ethics Advisory Group (EAG) was invited to consider wider ethical implications of the current personal data use—see also Section D of this Article.[32] Anticipating the outcomes of the deliberations by this EAG, however, the opinion offered a specific interpretation of the concept of human dignity. The opinion interpreted human dignity in the context of personal data processing which appeared to be rather strict, focusing—among others—on values like empowerment, autonomy and informational self-determination of the data subject. The opinion identified the empowered individual as the key factor in the future data protection ecosystem—joined by "accountable controllers and innovative privacy engineering."[33]

It can be argued that the perspective on dignity in the opinion was not that innovative at all. A reason for this is that the contours of the concept of dignity itself are ill-defined and could

---

[28] *See* Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02). In its judgement in Case C-377/98, Netherlands v. Parliament, 2001 E.C.R. I-7079 para. 70–77, the Court of Justice confirmed that a fundamental right to human dignity is part of Union law. It follows that none of the rights laid down in this Charter may be used to harm the dignity of another person, and that the dignity of the human person is part of the substance of the rights laid down in this Charter. It must therefore be respected, even where a right is restricted.

[29] Luciano Floridi, *On Human Dignity as a Foundation for the Right of Privacy*, 29 PHILOS. TECH. 308 (2016).

[30] GDPR, *supra* note 2, art. 88.

[31] Luciano Floridi, *On Human Dignity as a Foundation for the Right of Privacy*, 29 PHILOS. TECH. (2016).

[32] In the Opinion, it was proposed to set up an advisory group to investigate the relationships between human rights, data technology, markets and business models in the 21st century and "to assess the ethical dimension beyond data protection rules." The EDPS Ethics Advisory Group is composed of six experts: J. Peter Burgess, Luciano Floridi, Jaron Zepel Lanier, Aurélie Pols, Antoinette Rouvroy, and Jeroen van den Hoven. *See* EDPS ETHICS ADVISORY GROUP, TOWARDS A DIGITAL ETHICS (2018).

[33] EUROPEAN DATA PROTECTION SUPERVISOR, *supra* note 23.

therefore be defined in a number of ways. Unfortunately, the opinion seems to ignore that human dignity is an idea that appears in very different roles and thus did not explore any of them.[34] With its incomplete interpretation of the concept of dignity, it barely deviated from the guiding principles of the GDPR, which completely revolves around the combination of accountability and compliance on the one hand, and autonomy and empowerment on the other. Instead of choosing the safe and well-known principles of data protection, the EDPS-publication should have explored other dimensions of human dignity as a contribution to the debate. Because the notion of dignity embraces other constraining elements, the EDPS could have made reference to the dimensions of more paternalist forms of protection and dignity as human integrity and respect—for example, to the principle of non-commercialization that follows from human dignity.

On the eve of the GDPR entering into force, the EDPS called into question the effectiveness of the legal instrument itself and favored the approach of exploring the scope of human dignity. Unfortunately, his restrictive interpretation of the dignity-approach towards data processing only confirmed existing principles instead of calling them into question. On the contrary, Opinion 4/2015 was stuck in the well-worn fundaments of common data protection principles and if one had had any prior high expectations of the new dignity-approach, these were eventually not met. A more extensive interpretation would have called these principles into question and offered more room for debate. In the remaining sections, I will try to compensate for this omission. It will hopefully be demonstrated that remedies from a perspective of dignity interpreted as a constraint to the data industry, instead of an empowering tool to data subjects, would have been more fruitful.

C. Data Trade, Blurring Boundaries, and Solutions from Data Protection

In this section, the objections to current practices of data processing are analyzed and reconsidered in order to explore the different dimensions of human dignity. These objections concern, in particular, the trade and therefore commodification of personal data. In particular, these objections highlight further reaching commoditization of personal data by the abandoning of the silo-based approach. This abandonment has resulted in the formation of a global web of personal data exceeding the boundaries between formerly separated silos of data.

For adherents of dignity as empowerment, solutions to allay concerns about these developments could be found within the scope—and the limits—of the GDPR. But, drawing upon the constraining dimension of dignity, I will argue that the principles of data protection and the GDPR as a regulatory instrument are inadequate to address the general unease

[34] *See*, *e.g.,* Roger Brownsword, *Human Dignity, Ethical Pluralism, and the Regulation of Modern Biotechnologies*, *in* NEW TECHNOLOGIES AND HUMAN RIGHTS (T. Murphy ed., 2009).

surrounding data processing. It will be concluded that human dignity as a constraint offers a more hopeful perspective for this.

I. Data Trade

Personal data and information undeniably represent commercial value. The early metaphor of personal data as the new oil of the Internet demonstrates how much personal data are valued and justifies fragmentation of persons and their identity into tradable commodities.[35] Meanwhile, all aspects of being and everyday lives are transformed into tradable goods. This could be described as a process of datafication, commodification, and commercialization of individuals where human individuals consecutively become data-subjects, objects of trade and sources of profit.[36]

Virtually all types of companies, be it e-commerce firms, technology platforms, data brokers, or other types of businesses, greatly depend upon the collection, analysis and the exploitation of data for revenue. The analysis and exploitation of data enables these companies to profile their customers, micro-target users with advertisements, and sell profiles and sets of personal data. Data are a lucrative, tradable product from a source that never runs out.[37] It is said that, in the near future, data will become the pivotal asset of any business model and virtually all companies will be technology companies.[38] Most consumers who consent to exchanging personal data for services or goods, for example to get some product or online service for free or merely as an accepted part of any online transaction, consider this as part of the deal and an inevitable consequence of taking part in the digital world of today. As a consequence, their data will circulate online, and will be traded and resold by various parties infinitely—in theory.

For the human dignity as empowerment theorists, these practices can be legitimized by the consent given by the individual data subjects. From the GDPR it follows that "consent" of the data subject means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action,

[35] European Commission Press Release 09/156, The Roundtable on Online Data Collection, Targeting and Profiling (March 31, 2009) ("Personal data is the new oil of the Internet and the new currency of the digital world.").

[36] Arno R. Lodder & Anne E. de Hingh, *An Analogy Between Data Processing and The Organ Trade Prohibition* (forthcoming).

[37] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, 220 OECD DIGITAL ECONOMY PAPERS (2013), https://www.oecd-ilibrary.org/docserver/5k486qtxldmq-en.pdf?expires=1522591418&id=id&accname=guest&checksum=154F0735253121EAC53377F7E3269D23.

[38] *See* Marco van der Hoeven, *Data Will Be Central to Any Earnings*, EXECUTIVE-PEOPLE (Apr. 5, 2018), https://executive-people.nl/597065/lsquo-data-komt-centraal-te-staan-in-elk-verdienmodel-rsquo.html.

signifies agreement to the processing of personal data relating to him or her."[39] The data ecosystem completely depends on the willingness of Internet users. Were it not for their autonomous consent, their personal data could not lawfully be harvested in the first place. This doctrine is based on the assumption that consumers are well-informed, digitally skillful, and autonomous beings who have a choice. Clearly, autonomy and informational self-determination are still the crucial factors in the regulatory approach of data protection and privacy today. Likewise, the right to object to profiling related to direct marketing under the GDPR is based on this conception.[40]

The effectiveness of the principle of consent has been subject to discussion for many years because of several structural problems with the consent-based model of privacy and data protection. One of them is that individuals who consent to the collection, use, and disclosure of their data cannot foresee what it is exactly they give their consent to and are unaware of all the third parties their data are shared with afterwards. Another problem is the fact that individuals in general have no other option than to give their consent because there are no real alternatives. And although the industry will argue that users always have the freedom and choice not to use their services, in reality not using them is for the most part not an option. The issue of coercive bargaining conditions that inexorably lead to a dead end was labelled by Sandel as the objection of "coercion". This forced consent or tainted consent occurs in any context: from the trade of body parts, to schools paying sums of money to children in order to stimulate them to read books. According to Sandel, "we have drifted from *having* a market economy, to *being* a market society, in which the solution to all manner of social and civic challenges is not a moral debate but the law of the market, on the assumption that cash incentives are always the appropriate mechanism by which good choices are made."[41]

[39] GDPR, *supra* note 2, art. 4, § 11.

[40] GDPR, *supra* note 2, recital 70. "Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information." *See also* GDPR, *supra* note 2, art. 4 § 4, where profiling means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability or behaviour, location or movements."

[41] Sandel distinguishes two objections to the extending of the reach of market valuation and exchange: corruption—i.e. the degrading effect of market valuation and exchange on certain goods—and coercion—i.e. the creation of coercive bargaining conditions, or tainted consent. *See* Sandel, *supra* note 12; *see* also SANDEL, *supra* note 12.

Solutions for these problems arising from the consent-based model of data protection—or the perspective of human dignity as empowerment—are numerous. These solutions have in common that they all aim at securing, reinforcing or restoring the autonomy of the individual data subject. Empowering the data subject by strengthening the consent mechanism and giving more responsibility to the individual, is one of them.[42] It has been argued, however, that the introduction of the unambiguous consent—the former explicit consent—in the GDPR will not strengthen the legal protection by empowering the data subject. It will instead further weaken the effectiveness of the consent mechanism, as the responsibility of the user will grow, but not her or his actual negotiation position or power.[43]

Some have suggested a more differentiated system of consent based on the idea that decisions need only freely given, specific, informed, and unambiguous consent when it really matters—for example, when decisions may involve serious risks or consequences for the person who gives consent.[44] It can be argued, however, that in the current opaque data eco-system, these options are no longer feasible, as the uncertainty whether consent really matters lies at the heart of the problem.

Also, designs are proposed in which the user could negotiate the permission to access their personal data. This would solve the problem caused by the fact that the consent mechanism limits the user to a binary decision—either take it, or leave it—and having no fully-fledged alternatives. This solution would present the possibility—for example, to those who prefer not to view ads—to opt to pay an additional fee to view content.[45] A comparable suggestion, made by Berners-Lee, is to explore alternative revenue models like subscriptions and micropayments as this would "put a fair level of data control back in the hands of people."[46] This solution, however, still assumes that data represent economic value and therefore form a legitimate modality to pay for services. The fact that an autonomous choice is offered to the individual data subject between payment with his or her own data or payment with money, does not change the undesirable dimensions of the exploitation of personal information.

---

[42] FREDERIK J. ZUIDERVEEN BORGESIUS, IMPROVING PRIVACY PROTECTION IN THE AREA OF BEHAVIOURAL TARGETING 223 (2015).

[43] GDPR, *supra* note 2, art. 4.

[44] Bart W. Schermer, Bart Custers & Simone van der Hof, *The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection*, 16 ETHICS & INFO. TECH. 171, 171–82 (2014).

[45] In practical terms, this would imply that these companies would be forced to offer an opt-out possibility which would enable customers to declare that they do not want to be profiled and receive targeted information. T. BAARSLAG ET AL., NEGOTIATING MOBILE APP PERMISSIONS (2015), https://eprints.soton.ac.uk/377378/1/NegotiatingMobileAppPermissions.pdf.

[46] Tim Berners-Lee, *I Invented the Web: Here Are Three Things We Need To Change To Save It*, GUARDIAN (Mar. 12, 2017), https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet.

Adherents of the consent theory are convinced that the commodification and commercialization of personal information is purely a problem of tainted consent and asymmetric markets. The solutions listed above are all based on the conviction that autonomy, empowerment and voluntary decision-making by the data subject are the key to effective data protection. In addition, the solutions listed above rest on the assumption that the problem can be addressed by simply adjusting the background conditions that markets operate in.

Indeed, in the Cambridge Analytica case hundreds of thousands of data subjects accepted a two dollar offer to participate to a psychology-quiz offered on MechanicalTurk. By accepting the payment, participants consented to Cambridge Analytica harvesting their own data and the data of 87 million of their Facebook friends for practices of political marketing relying on micro targeting. In my view, more precise consumer information about the context and the consequences of the consent transaction would not have had significantly different outcomes. This is directly related to the fact that the Facebook users were not aware of these transactions in the first place. Furthermore, even if they had been aware of it, they could not have opted-out from having their data harvested by a company that offered a small reward to their friends. And, in the theoretical case that they could have given their consent to the collection and reuse of these data by Cambridge Analytica and transparent and fair data processing conditions would have been established, would their concerns about these extreme forms of commodification of data have been laid to rest? Probably not, as in this case, the amount of the data, the intimate character of the data, and the complex and opaque ways the data were collected for specific political marketing purposes must lead to the conclusion that something more fundamental was at stake here.[47]

However upholstered the consent may be, after all, it still does not neutralize the concerns or the fundamental objections one could have with the commodification of personal data. This has to do with the fact that consent-based solutions fail to see that tainted consent is not the real problem here. They fail to understand that commodifying personal data "is a moral dilemma that market liberalization cannot solve."[48] This has to do with what Sandel would define as corruption. He claims that certain moral and civic goods are diminished or corrupted if bought and sold for money.[49] His argument from corruption appeals to the moral importance of the goods at stake, the "ones said to be degraded by market valuation and exchange."[50]

II. Blurring Boundaries

[47] Sandel, *supra* note 12.

[48] *See id.*

[49] *See id.*

[50] *See id.*

Like the data industry, governments make ample use of the possibilities of data collection, processing, and analytics. This is especially noticeable as the practice of large-scale data collection and analytics seems to have settled permanently in the practices of law enforcement agencies and intelligence and security services to fight and prevent crime and terrorism.[51] Just like private parties collect data to be able to anticipate preferences and influence future behavior, criminal or terroristic acts of individuals can also be anticipated through data. With increasing Internet use, endless surveillance opportunities are created, and online data and personal information have become a growing source of intelligence.[52]

For this reason, intelligence and security services and law enforcement agencies depend heavily on the personal information and data collected by commercial parties.[53] To improve their information position, the services intercept bulk communication—cable and non-cable-bound—and hack computers. They also actively collect and analyze data from open sources—OSINT or open source intelligence—through cooperation with other bodies, via informants, or by scraping the web. Lastly, they acquire datasets of commercial origin offered by third parties, and sometimes they purchase bulk datasets online that were illegitimately obtained through data breaches—theft—or hacking.

In the years 2016 and 2017[54] the Dutch secret service, AIVD, was an active party on the online stolen data market to acquire bulk sets of stolen and hacked data. It purchased two data sets of criminal origin each containing personal information of around 100 million individuals.[55] This operation demonstrated that the Dutch government does business with criminal parties, and, in doing so, contributes to the maintenance of an online demand and supply system of stolen data and supports the criminal supply of data on the dark web. In addition, other moral objections of a different nature can be formulated.[56]

This case perfectly illustrates on what scale commercial, criminal, and governmental actors exchange personal data and how the present data eco-subsystems are intertwined. It is

---

[51] *See* Els De Busser, *EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow*, 19 GERMAN L.J. (2018).

[52] Arno R. Lodder & Ronald Loui, *Data Algorithms and Privacy in Surveillance: On Stages, Number and the Human Factor*, *in* RESEARCH HANDBOOK OF LAW AND ARTIFICIAL INTELLIGENCE (W. Barfield & U. Pagallo eds., forthcoming).

[53] QUIRINE EIJKMAN, NICO VAN EIJK & ROBERT VAN SCHAIK, *Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act,* INSTITUTE FOR INFORMATION LAW (2018).

[54] More specific information on the period concerned is not available due to the secret nature of the operation.

[55] CTIVD, *Toezichtsrapport nr 55, Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD* (2017).

[56] Bruce Schneier, *Data Is a Toxic Asset, So Why Not Throw It Out?*, CNN (Mar. 1, 2016), https://edition.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html.

highly relevant, therefore, to establish that the majority of personal data used by governments have their first origin in the data industry. "Governments get themselves a copy of what the corporate world was already collecting," as it was put by Schneier.[57] Some authors suggest that the current under-regulation of online personal data extractions is beneficial for governmental agencies and that "hedged with some caveats, the current willful political neglect to limit personal data hoarding may be linked to a governmental reliance on the same increased efforts to extract and store personal data."[58] Another related question is to what extent an individual could be aware of these blurring boundaries when exchanging his/her data in an online transaction and subsequently becoming the victim of a data breach. Should this individual take into account the possibility of his/her data eventually ending up in the databases of the Dutch security services?

Objections to blurring of boundaries are thus related to the question of improper use, i.e. the fact that data are used for other purposes than expected by the data subject. This was acknowledged by the Dutch oversight committee (CTIVD) that reported that by acquiring and processing, or re-using, these data sets, although considered "open sources,"[59] the secret service had seriously infringed the right to privacy. In addition, the committee concluded the legal guarantees regarding the acquiring and processing of data were clearly insufficient.

The GDPR and general data protection principles do not apply to the processing of data by Dutch security services, as these are excluded from their scope.[60] It should be noted, however, that the general data protection principles from the 1981 Council of Europe Convention apply for all types of data processing in the private and public sector.[61] This is especially relevant with regard to the principle of purpose limitation of Article 5 of the GDPR,

---

[57] SCHNEIER, *supra* note 3; Bruce Schneier, *'Stalker Economy' Here to Stay*, CNN (Nov. 26, 2013), https://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html.

[58] *See* Sylvia E. Peacock, *How web tracking changes user agency in the age of Big Data: The Used User*, BIG DATA & SOC., 1, 8 (2014); *see also* Schneier, *supra* note 57, at 94: ("The NSA didn't build a massive eavesdropping system from scratch. It noticed that the corporate world was already building one, and tapped into it . . . . This leads to a situation in which governments do not really want to limit their own access to data by crippling the corporate hand that feeds them."); Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (Or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO 3 (2014).

[59] CTIVD, *Toezichtsrapport nr 55, Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD* (2017).

[60] GDPR, *supra* note 2, art. 2. This Regulation does not apply to the processing of personal data: (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. *See also* Dutch Data protection Act art. 2(2)(b).

[61] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe art. 3, Jan. 28, 1981, E.T.S. 108.

the requirement that data must be collected and processed for a specified, explicit and legitimate purpose only—purpose specification; and the requirement that any further processing must be compatible with the original purpose for which the personal data were collected—compatible use. In other words, secret services must comply with purpose limitation and the exceptions made to purpose limitation, but under the condition that such exceptions are legal, necessary, and proportionate.[62]

Just like objections against data trade were not a matter of tainted consent alone, objections against blurring boundaries and commoditization of data are not, however, purely a matter of purpose limitation. As said, the flow of data from one sphere to the other and the blurring of boundaries between the realms of the private and the public, between the legal and the illegal, the commercial and the political, give rise to concerns that go beyond privacy and personal data protection. Purpose limitation-based solutions fail to see that the absence of a specified, explicit and legitimate purpose is not the real problem here. When data flow from one silo to the other, questions on whether it is Facebook, a criminal organization, or the secret service that is processing the data, whether the data collected are WhatsApp messages or behavioral data, and whether the purpose of processing is advertising or preventing terrorist attacks, are of secondary significance.[63]

The fact that technology companies, social media platforms, the advertising industry, criminal organizations, hackers, governments, and security services, all use and re-use, exchange, and recycle the same data bases, in theory over and over again, results not in centralized forms of surveillance—big brother—, but in different institutions that are all interconnected in exploiting and surveilling personal information of individuals—little sisters.[64] The more fundamental dilemma here is that through this endless re-use or circulation of personal data in bulk, data recycling mechanisms turn personal data into generic mass products. So, not only is personal information commodified by the fact that specific data represent an economic value and are therefore used for profiling, but a process of commoditization takes place during which these personal data risk to lose their particular character and become undifferentiated goods. This is the process of commoditization.[65]

---

[62] *See* EIJKMAN, *supra* note 53.

[63] LOKKE MOEREL, BIG DATA PROTECTION. HOW TO MAKE THE DRAFT EU REGULATION ON DATA PROTECTION FUTURE PROOF 58 (2014) (delivered lecture during the public acceptance of the appointment of professor of Global ICT Law, Tilburg University). *See also* Lokke Moerel & Corien Prins, *On the Death of Purpose Limitation* IAAP (Jun. 2, 2015), https://iapp.org/news/a/on-the-death-of-purpose-limitation/.

[64] For this metaphor and other works of Marc Schuilenburg (VU Amsterdam), see http://marcschuilenburg.nl/.

[65] Arno R. Lodder & Anne E. de Hingh, *An Analogy Between Data Processing and the Organ Trade Prohibition* (forthcoming).

It could be concluded that problems that are felt with regard to the blurring of boundaries—and giving up of silo-based approach—cannot be solved by applying general data protection principles alone. Autonomy, informational self-determination, consent, and purpose limitation: These principles all originate from the concept of dignity as a legal tool for empowerment. In the next paragraph it is argued that dignity as empowerment cannot hold as key concept in the discussion on how to curb the excesses of the digital economy.

D. Argument from Human Dignity as Constraint

The cases of Cambridge Analytica and the Dutch security and intelligence services serve as illustrative examples of the current practices within the present data-ecosystem. They, moreover, affirm once again what was demonstrated before by among others the Snowden revelations: That the essence and the origin of the problem are for the most part to be found in the under-regulated collection of personal data by corporate actors. Thus, a different approach in which individual autonomy and the role of the market play a limited role is needed.[66]

Two main concerns related to present day data-driven economy—the data ecosystem—have been presented so far. The first concern was the abundant trade and resulting commodification of personal data by commercial parties—buying, selling, and brokering of profiles and large sets of personal data. Second, the deconstruction of boundaries between industry, crime, and government with regard to personal information—resulting in a firm corporate-criminal-government nexus—leading to the increasing commoditization of personal data.

The objections to these phenomena could be formulated in terms of data protection law, for they stress the limits of data protection principles like autonomous consent, transparency, data minimization, and purpose limitation. The adherents of human dignity as empowerment believe these problems are resolvable by exactly enforcing these data protection mechanisms.

One of the problems that are highlighted in this contribution is the fact that the traditional understanding of informational privacy and data protection does not suffice because it covers only part of the current online reality and ignores large parts of the moral problems presented.[67] Measures from that perspective would therefore fail to remove the objections because they mistake them as a problem of lack of autonomy and individual control, and of coercion of individuals. Instead, they should be considered not as limiting self-determination of Internet users, but as a much more fundamental problem. A process of commoditization

[66] Sylvia E. Peacock, *How Web Tracking Changes User Agency in The Age Of Big Data: The Used User*, BIG DATA & SOC., 1, 1–2 (2014).

[67] *See* Austin, *supra* note 53, at 3.

confronts us as individuals are fragmented into bits of information that are multiplied, transferred, sold and brokered, from the timelines of Facebook to the advertising industry, voter-profiling companies, and criminal hackers—and vice versa—and eventually end up in databases of law enforcement agencies or intelligence and security services worldwide. As a result, we are confronted with an ethical and legal challenge that the GDPR will not be able to fix. In that case, other legal answers are needed.

The beginning of an answer could be found in the 2015 seminal opinion of the EDPS which admittedly started a discussion; however, it did not add many valuable new insights on data and dignity because it did not manage to get away from the dignity as empowerment-framework. As a thought experiment, it would have been useful for the opinion to argue by analogy.[68] Admittedly, it is stated in the Opinion that violations of dignity may include objectification, where a person is treated as a tool serving someone else's purposes. But, it could have gone further by exploring examples of the application of the concept of human dignity in other fields of law like in the context of bio-ethical issues, where the emancipatory dimension of dignity is commonly contrasted to its constraining dimension.

To approach moral and ethical issues in the field of biotechnology, traditionally two dimensions of human dignity are discerned: The subjective and the objective dimension or also known as the human rights approach versus the communitarian approach. Beyleveld and Brownsword were the first to discern the distinct and contradictory ways in which the concept is used in bioethics.[69] The subjective dimension considers human dignity as self-determination, emancipation, choice, and autonomy, whereas the objective dimension comprises values as respect, constraint, and collective responsibility.

In biolaw and the regulation of biotechnology, the constraining dimension of human dignity is a predominant factor supporting the legal prohibition of elements of the human body being made into objects and exploited as instruments, resources, and commodities. In general, legislators are reluctant to allow people to turn parts of their body into sources of financial gain. A commodification of the body, viz assigning monetary value to parts of the human body, occurs through illegal trade as well as in legal business but still ethically problematic businesses. Some examples of these problematic legal business include the procurement of tissues and cells from dead bodies, patients, and healthy persons, who, for various reasons, chose to give or sell parts of their body such as blood, hair, sperm, or ova.[70]

---

[68] Sandel, *supra* note 12 (suggesting we could "begin with moral intuitions we have about certain practices and to see whether or not the practices in question are relevantly similar.").

[69] BERYCK BEYLEVELD & ROGER BROWNSWORD, HUMAN DIGNITY IN BIOETHICS AND BIOLAW (1993).

[70] BRITTA VAN BEERS, *Persoon en Lichaam in het Recht. Menselijke waardigheid en zelfbeschikking in het tijdperk van de medische biotechnologie* (dissertation Vrije Universiteit Amsterdam) (2009); MARTIN GUNNARSON & FREDRIK SVENAEUS, THE BODY AS GIFT, RESOURCE, AND COMMODITY: EXCHANGING ORGANS, TISSUES, AND CELLS IN THE 21ST CENTURY

This dignity approach has its origin in the person-thing bifurcation—the Kantian idea that human beings should always be understood at the same time as an end in themselves and never merely as a means. In other words, human beings have their dignity and only things should have a price. The principle that the human body should not be a source of revenue is asserted in numerous national and international legal sources.[71] The prohibition of the commercial selling of one's own organs is an illustrative example of the illegality of commodifying one's body parts because it is incompatible with the objective dimension of human dignity: The human body is *res extra commercium* or beyond price.

Although also in the context of bioethics and biolaw, the conceptual status of dignity is complex and not without controversies. It could still be helpful to take it into account to deepen the discussion on dignity with regard to personal data processing and to explore the loopholes in contemporary data protection and privacy laws.[72] The two-dimensional interpretation of human dignity could contribute to the debate on the commodification and commoditization of personal data, which the EDPS sought to give an ethical dimension. The trade of personal information could indeed be represented as an extension of the trade of body parts. As was so beautifully articulated by Floridi: "My" in my data is not the same as "my" in my car, but it is the same as "my" in my hand.[73] The protection of data could, or should, be interpreted as the protection of personal identity or personal integrity, as personal information plays a constitutive role in who an individual is and can become.[74]

More than two years after Opinion 4/2015 was published, the Ethics Advisory Group published its report *Towards a Digital Ethics*.[75] This publication could be considered as another step forward in the debate on digital ethics, "focusing on how we can make technology work in the interests of human dignity."[76] According to the EAG report, "a re-

(Martin Gunnarson & Fredrik Svenaeus eds., 2012); *see also* Manuel Wackenheim v. France, Communication No. 854/1999, U.N. Doc. CCPR/C/75/D/854/1999 (2002).

[71] *See* Convention on Human Rights and Biomedicine of the Council of Europe art. 1, Apr. 4, 1997, E.T.S. 164; Universal Declaration on the Human Genome and Human Rights, art. 1, 2(a); International Declaration on Human Genetic Data, art. 1; Universal Declaration on Bioethics and Human Rights, art. 2(c), 3(1). *See also* Arno R. Lodder & Anne E. de Hingh, *An analogy between data processing and the organ trade prohibition* (forthcoming) for an elaboration of the analogy between (parts of) the human body and data related to the human individual.

[72] *See*, *e.g.*, NORA JACOBSON, DIGNITY AND HEALTH 186–88 (2012) (noting the objections against the use the concept of dignity in the field of bioethics).

[73] Luciano Floridi, *On Human Dignity as a Foundation for the Right of Privacy*, 29 PHILOS. TECH. (2016).

[74] *Id.*

[75] EDPS ETHICS ADVISORY GROUP, *supra* note 32.

[76] *See* Ethics Advisory Group, *Ethics*, EUROPEAN DATA PROT. SUPERVISOR (2015), https://edps.europa.eu/data-protection/our-work/ethics_en.

assertion of fundamental values at the heart of European data protection and other fundamental rights and liberties is needed."[77] In the report, it is again repeated that the right to data protection appears insufficient to understand and address all the ethical challenges brought about by recent digital technological developments and that "personal data protection regimes, like the GDPR, . . . appear inadequate to address the unprecedented challenges raised by the digital turn."[78] The EAG even goes further by suggesting that "In particular, the tensions and frequent incompatibilities of core concepts and principles of data protection with the epistemic paradigm of big data, suggest limits to the GDPR even prior to its application."[79]

In the EAG-report, it is stated that new concepts of data protection will be called for because unprecedented commodification of data gathered from persons, behaviors, and environments can be expected from the new big data ecosystem. Apart from values like freedom, autonomy, solidarity, equality, democracy, justice, and trust, the EAG refers first and foremost to dignity as a core value that will be directly challenged by this new data ecosystem.[80]

Some tentative references to the constraining dimension of human dignity are made by the EAG.[81] This is especially reflected in the "Kant-ian" way the advisors address the commodification of personal data: "When individuals are treated not as persons but as mere temporary aggregates of data processed at an industrial scale to optimize . . . interactions with them, they are arguably not fully respected, neither in their dignity nor in their humanity."[82]

In my opinion, the EAG-report should have concluded that the restriction or ban of at least some of the most excessive business models that are based on the commodification and commoditization of personal data, should be taken into account. As was stated by Berners-Lee,

> Two myths currently limit our collective imagination: The myth that advertising [based on data collection] is the only possible business model for online companies, and the myth that it's too late to change the way

[77] EDPS ETHICS ADVISORY GROUP, *supra* note 32, at 16.

[78] *See id.*, at 7.

[79] *See id.*

[80] *See id.*, at 16.

[81] *See id.*, at 9.

[82] *See id.*, at 17.

> platforms operate. On both points, we need to be a little more creative.[83]

Unfortunately, this creative, and normative, leap towards a more constraining data protection regime was not made by the EAG.

E. Conclusion

The scandal with Facebook and Cambridge Analytica and the Dutch security services case demonstrate that misuse of data collection is constantly lurking and principles of data protection law—like the informed and unambiguous consent and the principle of purpose limitation—have mostly lost their meaning.[84] Online data processing practices turning personal information into a commodity interfere with the notion that a person should be *extra commercium*. Moreover, the de-silo-ization of the data market resulting in the ongoing transfer of data between commercial, criminal, and governmental parties has detrimental effects because it commoditizes individuals and their data. Not only does this influence the protection of data and the privacy of individuals, but it has much greater implications for the lives of those individuals. The risks of the data market for individuals are related to their freedom, their feelings of control and power, but also of trust and security, legal certainty, and personal integrity. As noted by Roessler "concern can also focus on the transformation of social relationships, the idea of identity, on issues of justice and equality and on democratic political procedures."[85]

In this Article, it was argued that to address these general concerns a more substantive level of protection from the law would be appropriate, and "a broader legal canvass than simply the idea of privacy or data protection," to paraphrase Austin, is needed.[86] Leaving the solution solely to the autonomous consumer and to principles of data protection will not bring us any further towards an effective solution. Other forms of legislative intervention will be indispensable. If it is agreed upon that what is at stake here, could—at least, provisionally—be legally framed as the right to human dignity as constraint, it could be argued that at least in certain cases a more restrictive regulatory approach would be appropriate. Individuals should, in certain circumstances, be prevented from giving up parts

---

[83] Berners-Lee, *supra* note 16.

[84] LOKKE MOEREL, BIG DATA PROTECTION: HOW TO MAKE THE DRAFT EU REGULATION ON DATA PROTECTION FUTURE PROOF 58 (2014).

[85] Beate Roessler, *Should Personal Data Be a Tradable Good? On the Moral Limits of Markets In Privacy*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES (Beate Roessler & Dorota Mokrosinska eds., 2015).

[86] *See* Austin, *supra* note 53; s*ee also* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 411 (2014) (claiming "if we were designing things from scratch we would almost certainly want to use a word other than 'privacy'").

of their personal information. For not only do they lack any real idea what it is they give their consent for, but by giving this consent, I argue, they jeopardize something much more valuable—in short: Their human dignity. As Schneier proposed in this context: "Why not abolish the data-driven business model of (online) companies and social media by making certain forms of data collection and processing illegal? We can make the business models that involve massively surveilling people the less compelling ones, simply by making certain business practices illegal."[87] A prohibition of the limitless collection and circulation, the transfer of data back and forth between silos, and recycling of bulk sets of personal data could be such a protective measure.

[87] Schneier, *supra* note 56; *see also* SARAH CONLY, AGAINST AUTONOMY: JUSTIFYING COERCIVE PATERNALISM (2013).