'A Tale of Two Cities' in three themes – A critique of the European Union's approach to cybercrime from a 'power' versus 'rights' perspective

Yannis Naziris*

Given the recent adoption of a new directive on cybercrime by the EU, comparison with the US approach in this field becomes a useful tool for ascertaining whether Europe is on the right path. This paper attempts to answer that question by developing three pertinent themes: first, the structure of authority through which cybercrime regulation is channeled; second, substantive law choices made in defining offenses committed in cyberspace; and, third, the role of fundamental rights – and notably freedom of expression as enshrined in the European Convention on Human Rights and the First Amendment to the US Constitution- as limiting factors to governmental power. Accordingly, three respective lessons are drawn, converging on a single point: from a comparative perspective, measures that have proved effective in a given system cannot be 'transplanted' to another absent functional equivalence.

I. Introduction: The three 'themes'

In 'A Tale of Two Cities', Charles Dickens touches upon the themes of duality and insurgency by developing two parallel stories, one in London and one in Paris, unfolding in the period before, during, and after the French Revolution.[1] It is a tale of social transformation and its impact on the lives of individuals, which ultimately poses a fundamental question: how do you bring order into chaos, regulating what seems to be unbridled social movement? The answer to this question is anything but obvious, since it appears as though the same solutions can have significantly differing effects depending on the environment in which they are infused. One society may be receptive to a given form of exercising power, whereas another may revolt in response thereto. What preserves peace in London may cause upheaval in Paris.

Regulating cyberspace seems to present us with those very questions. One might argue that the prospect of differing effects is now diminished in the absence of borders in cyberspace.[2] Yet this would be very far from describing the actual picture.

* This paper was researched during the debate revolving around the European Commission's proposal for a new directive on cybercrime, and was later adapted to include a critical apraisal of the newly–adopted Directive 2013/40/EU 'on attacks against information systems'. I would like to thank Phil Malone, my professor at Harvard Law School (current director of the Juelsgaard Intellectual Property and Innovation Clinc at Stanford Law School), for his intriguing perspectives on US cybercrime law.

[1] C. Dickens, *A Tale of Two Cities*, New York, Dodd, Mead & Co., 1942 (first published in 1859 by Chapman Hall).

[2] On the challenges posed for law enforcement authorities worldwide due to the cross-border character of cybercrime see, *inter alia*, B.-J. Knoops and S. Brenner, *Cybercrime and Jurisdiction: A Global Survey* (Information Technology and Law Series), TMC Asser Press, 2006, *passim*; J. Westby (ed.), *International Guide to Combating Cybercrime*, American Bar Association, 2003, *passim*; E. Podgor: "Cybercrime: National, Transnational or Interna-

Although the regulated field seems to defy international borders, criminally proscribing human conduct ultimately depends on and affects people within a specific context.[3] That context is circumscribed by the rules and principles governing human behavior in all its aspects, including fundamental rights and freedoms guaranteed by national Constitutions and international instruments.

One might then pose the question: how do you go about regulating a field that seems chaotic any way you look at it? Attempts at an answer typically appear to rely on three interconnected axes: i) centralize power; ii) broaden the ambit of criminally proscribed conduct; iii) emasculate civil liberties by introducing exceptions. This pattern is evident both in the US and in Europe.[4] However, certain measures are more easily applicable in systems that are receptive to their application. Such measures cannot necessarily be easily transposed to another system in the absence of 'fertile soil'.

This paper addresses these three pillars and attempts to draw a lesson from each one. Accordingly, part II will deal with the issue of federalism as seen in the US legal system[5] in comparison with 'quasi-federalization' as currently attempted in Europe within the context of European Union integration.[6] Part III then touches upon the specific manner in which substantive criminal law addresses cybercrime on the two sides of the Atlantic, with a view to assessing the extent to which each system subscribes to such notions as the 'harm principle'.[7] Finally, part IV attempts to place the whole debate in a broader perspective, by evaluating the conformity of cyber-

---

tional?", 50 Wayne L. Rev. 97 (2004); M. Goodman and S. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace", 3 UCLA J. L. & Tech. (2002); J. Goldsmith, "The Internet and the Legitimacy of Remote Cross-Border Searches", U. Chi. Legal F. 103 (2001); N. Katyal, "Criminal Law in Cyberspace", 149 U. Penn. L. Rev. 1003 (2001); D. Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces", 4 Mich. Telecomm. & Tech. L. Rev. 69 (1998); D. Johnson and D. Post, "Law and Borders: The Rise of Law in Cyberspace", 48 Stan. L. Rev. 1367 (1996). On the challenges posed by cross-border crime in general see, *inter alia*, B. de Ruyver, T. van der Beken and G. Vermeulen (eds.), *Strategies of the EU and the US in Combating Transnational Organized Crime*, Maklu Uitgevers N. V., 2002, *passim*; P. van Duyne, V. Ruggiero, M. Scheinost and W. Valkenburg, *Cross-Border Crime in a Changing Europe*, Nova Science Publishers, 2001, *passim*.

[3] Quite interestingly, the tendency to 'internationalize' legal responses to cybercrime goes hand in hand with a demand to consolidate legislation domestically. This is evident in many aspects of cyberspace regulation: see, e. g., H. Judy and D. Satola, 'Business Interests under Attack in Cyberspace: Is International Regulation the Right Response?', Bus. L. Today 1 (2011), referring to the 2011 ONCIX Report, which was released shortly after the submission of a draft resolution concerning an 'International Code of Conduct for Information Security' to the United Nations General Assembly.

[4] On the cooperation of the EU and the US in combating cybercrime and its impact on the privacy of European and American citizens see E. 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*, MakluUitgevers N. V., 2009.

[5] See *infra*, under II/1.

[6] *Infra*, under II/2. On the 'federalization project' in the European continent as launched through the European Union see, *inter alia*, F. Laursen, *The EU and Federalism: Polities and Policies Compared*, Ashgate Publishing, 2011, *passim*; A. Menon and M. Schain, *Comparative Federalism: The European Union and the United States in Comparative Perspective*, Oxford University Press, 2006, *passim*; S. Fabbrini (ed.), *Democracy and Federalism in the European Union and the United States: Exploring post-national governance*, Routledge, 2005, *passim*; R. Kelemen, *The Rules of Federalism: Institutions and Regulatory Politics in the EU and Beyond*, Harvard University Press, 2004, *passim*; A. Moravcsik, Federalism in the European Union: Rhetoric and Reality, in K. Nicolaïdis and R. Howse (eds.), *The Federal Vision: Legitimacy and Levels of Governance in the US and the EU*, Oxford University Press, 2001, pp. 161 *et seq*.; M. Burgess, *Federalism and European Union: The Building of Europe, 1950-2000*, Routledge, 2000, *passim*.

[7] See *infra*, under III/1-2.

crime regulation with fundamental rights, both on domestic law terms (including rights enshrined in the Constitution) and based on international human rights norms.[8] These three 'themes' are *prima facie* independent of each other, and yet there is no way of discussing one without necessarily saying something about the other two. If a criminal justice system were a personal computer, the system of government would be, roughly speaking, its Central Processing Unit (CPU); substantive criminal law would be its Operating System (OS); and, finally, constitutional guarantees would comprise the motherboard, i. e. the system's 'backbone'. It will be submitted that only a harmonious coordination of these three integral parts of the system can ensure the effective operation of criminal justice in a modern State.

II. Consolidating power: Two models of 'federalism'

1. Dealing with cybercrime in a typical federal system

There are admittedly several ways to approach federalism, all the more so when the object of analysis is to assess its impact on human rights. Under a traditional approach, federalism is a system of 'checks and balances' employed in such a manner as to constrain governmental power.[9] Yet a mechanism to constrain power is not *per se* enough *in lieu* of a defining attribute of the whole system; rather, it is a built-in feature that only becomes functional once the main structure of authority has been set up.[10] The primary question, then, is how you arrange the said structure to begin with, and what possible implications arise out of it in terms of regulating specific types of crime, such as cybercrime.

Thus, one might more pertinently say that federalism is a system consisting of two complete sets of government, one central and one emanating from peripheral units, which operate independently of (and often in competition with) one another.[11] Both these systems operate under their own 'constitutional' constraints (with or without quotation marks) and are able to display elements of a complete bureaucratic arrangement featuring legislative, executive, and judiciary organs, not depending on the respective counterparts of each other.[12] How criminal law

[8] See *infra*, under IV/1-4.

[9] See esp. W. Riker, *Federalism: Origin, Operation, Significance*, Boston: Little, Brown & Co., 1964, pp. 11 *et seq*. [analogizing with the notion of 'empire': "federalism is the main alternative to empire as a technique of aggregating large areas under one government", *id*., at 5]; also see, more recently, J. Donohue and D. Pollack, Centralization and its Discontents: the Rhythms of Federalism in the United States and the European Union, in K. Nicolaïdis and R. Howse (eds.), *The Federal Vision: Legitimacy and Levels of Governance in the US and the EU*, Oxford University Press, 2001, pp. 73 *et seq*.; on the relationship between federalism and liberalism see M. Tushnet, 'Federalism and Liberalism', 4 Cardozo Journal of International and Comparative Law 329 (1996).

[10] See M. Filippov, M. Ordeshook and O. Shvetsova, *Designing Federalism: A Theory of Self-Sustainable Federal Institutions*, Cambridge University Press, 2004.

[11] In fact, competition will occur both on a 'vertical' and on a 'horizontal' level (between peripheral units themselves) or even on a local level: see D. Kenyon and J. Kincaid, *Competition among States and Local Governments: Efficiency and Equity in American Federalism*, University Press of America, 1991, *passim*.

[12] A. Føllesdal, Federalism, in E. Zalta (ed.), *The Stanford Encyclopedia of Philosophy*, 2003 (revised 2010), available online at: http://plato.stanford.edu/entries/federalism/ [last visited on 20 August, 2013].

authority (meaning the ability to prescribe and enforce criminal legislation) is distributed among the two spheres depends on the domestic particularities of each federal system.[13]

In the United States, which is a paradigmatic case of a federal system, criminal law authority is traditionally entrusted by default to the various States.[14] As a result, one comes across significant divergences in the approach adopted *vis-à-vis* crime, even when it comes to common problems faced by all States. During the last decades, this has gradually changed as federal legislation becomes more and more prevalent. In the area of cybercrime, this tendency is even more evident, as regulation now takes place primarily on the federal level.[15]

Specifically, the question of distributing power to regulate cybercrime between the federal and the State level essentially hinges on two factors, namely the interpretation of pertinent constitutional provisions, and the wording of each statute introducing a substantive offense.[16] As regards the former, it is to be noted that the bulk of offenses committed in cyberspace are being regulated by Congress based on the Commerce Clause.[17] Indeed, the Internet has repeatedly been classified as an "instrumentality of interstate commerce",[18] thus falling squarely within the ambit of congressional power.[19] In the post-*Lopez* era,[20] certain issues have arisen with

[13] See, e. g., D. Halberstam, Comparative Federalism and the Issue of Commandeering, in K. Nicolaïdis and R. Howse (eds.), *The Federal Vision: Legitimacy and Levels of Governance in the US and the EU*, Oxford University Press, 2001 [pointing out certain comparative advantages of the US federal model]; C. Friedrich, *Trends of Federalism in Theory and Practice*, New York: Praeger, 1969, *passim*.

[14] For an overview of case-law concerning the relationship between State and federal authority in criminal law matters in the US see C. Bradley, 'Federalism and the Federal Criminal Law', Maurer School of Law: Indiana University, Faculty Publications, available online at: http://www.repository.law.indiana.edu/facpub/185 [last visited on 20 August, 2013].

[15] F. Mendez, 'The European Union and Cybercrime: Insights from Comparative Federalism', 12:3 Journal of European Public Policy 509 (2005), at 513 [noting, at the same time, the limited number of federal prosecutions of cybercrime cases].

[16] O. Kerr, *Computer Crime Law*, West: American Casebook Series, 2nd ed., 2009, pp. 545 *et seq*. [hereinafter cited as O. Kerr, *Computer Crime Law*[2]]

[17] Article I, Section 8, Clause 3 of the US Constitution reads: "[The Congress shall have power] … to regulate commerce with foreign nations, and among the several states, and with the Indian tribes".

[18] See, e. g., *United States v. Mitra*, 405 F.3 d 492, 496 (7th Cir. 2005) [concerning "computer-based" communications systems]; *United States v. Hornaday*, 392 F.3 d 1306, 1311 (11th Cir. 2004) [concerning the Internet as such]; *United States v. Carnes*, 309 F.3 d 950 (6th Cir. 2002) [concerning telecommunications]; *United States v. Gilbert*, 181 F.3 d 152 (1st Cir. 1999) [concerning telephone lines].

[19] O. Kerr, *Computer Crime Law*[2], at 546; D. Carucci, D. Overhuls and N. Soares, "Computer Crimes", 48 Am. Crim. L. Rev. 375 (2011), at 386.

[20] The decision of the Supreme Court in *Lopez* reignited the debate on State *versus* federal power in the field of criminal law after almost six decades of seemingly limitless congressional activity: see *United States v. Lopez*, 514 US 549, 558 (1995), delineating the types of conduct that are within the reach of congressional authority under the Commerce Clause ['channels of interstate commerce'; 'instrumentalities of interstate commerce, or persons or things in interstate commerce'; and, finally, 'activities having a substantial relation to interstate commerce']. A lot has been written on this decision (as well as its 'progeny', *United States v. Morrison*, 529 US 598) and its impact on federal power: see indicatively C. Dral and J. Phillips, ÄCommerce by another Name: The Impact of United States v. Lopez and United States v. MorrisonÄ, 68 Tenn. L. Rev. 605 (2001); A. Kolenc, "Commerce Clause Challenges after United States v. Lopez", 50 Fla. L. Rev. 867 (1998); A. Laurent, "Reconstituting United States v. Lopez: Another Look at Federal Criminal Law", 31 Col. J. L. & Soc. Probs. 61 (1997). For the purposes of the present discussion, suffice it to note that activities carried out on the Internet fall squarely within the ambit of congressional power as per *Lopez*. On the question of whether activities involving "stand-alone" computers can also be classified as activities related to interstate commerce see *infra*.

respect to offenses not directly involving the Internet, such as the offense of "producing visual depictions of sexually explicit conduct with a minor"[21] by means of a "stand-alone computer".[22] Even in these cases, however, courts have been rather deferential towards Congress.[23] In *United States v. Jeronimo-Bautista*,[24] for instance, the US Court of Appeals for the 10th Circuit combined the Supreme Court's reasoning in *Gonzales v. Raich*[25] with the so-called 'standard four-factor *Lopez/Morrison* test'[26] to the effect of acknowledging some "federal interest" in eliminating commercial transactions that indirectly affect interstate commerce.[27] This *prima facie* broad federal power may be confined based on the wording of a particular statute. In *United States v. Schaefer*,[28] for instance, the Court of Appeals for the 10th Circuit noted the following with respect to the offense of receipt and possession of images involving the sexual exploitation of minors under 18 U.S.C. §§ 2252(a)(2) and (a)(4)(B):[29]

'It is apparent that Congress elected not to reach all conduct it could have regulated under § 2252(a). Congress's use of the 'in commerce' language, as opposed to phrasing such as 'affecting commerce' or a 'facility of interstate commerce', signals its decision to limit federal jurisdiction and require actual movement between states to satisfy the interstate nexus'.

Accordingly, the Court found that the government's evidence "was insufficient to satisfy the jurisdictional requirement" under the applicable statutes.[30] Although

---

[21] See 18 U.S.C. § 2251(a). Similar language is employed in 18 USC § 2252(a)(4)(B) ["Certain activities relating to material involving the sexual exploitation of minors"] and § 2252A(a)(5)(B) [Certain activities relating to material constituting or containing child pornography].

[22] A "stand-alone" computer would comprise any "non-networked" computer, i.e. one that is not connected to a modem or fax server: see E. Sinrod and W. Reilly, Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Computer & High Tech. L.J. 177 (2000), at 220.

[23] Some reservations have been expressed as to the absence of a 'limiting jurisdictional factor' concerning congressional power: see, e.g., *United States v. McCoy*, 323 F.3d 1114, 1125 (9th Cir. 2003), cautioning that 'the limiting jurisdictional factor is almost useless here, since all but the most self-sufficient child pornographers will rely on film, cameras, or chemicals that traveled in interstate commerce'.

[24] *United States v. Jeronimo-Bautista*, 425 F.3d 1266 (10th Cir. 2005).

[25] In *Gonzales v. Raich* [545 US 1 (2005)], the Supreme Court ruled that Congress has the authority to criminally proscribe the production and use of home-grown cannabis even in the face of State legislation endorsing its use for medicinal purposes. In *United States v. Jeronimo-Bautista* [*ibid.*], the US Court of Appeals for the 10th Circuit essentially analogized between the illicit market in marijuana found to exist in *Raich* with the illicit (and extremely profitable) industry of child pornography. The Court also cited *Wickard v. Filburn* [317 US 111 (1942)], where the Supreme Court upheld the 1938 Agriculture Adjustment Act, which had enabled Congress to regulate purely intrastate production which was not *per se* 'commercial' in nature. Regardless of 'New Deal' politics involved in this latter decision, it should be noted that the interpretation adopted in *United States v. Jeronimo-Bautista* brings virtually every computer-related activity within the reach of congressional power under the Commerce Clause.

[26] See T. Odom, *Federal Constitutional Law: Introduction to the Federal Legislative Power*, vol. 3, LexisNexis, 2009, p. 181.

[27] Needless to say, no need to establish 'federal interest' is present in those fields over which Congress possesses inherent powers by virtue of specific constitutional clauses. One such example is the Copyright Clause. Specifically, Article I, Section 8, Clause 8 of the US Constitution reads: '[The Congress shall have power] … to promote the progress of science and useful arts, by securing for limited times to Layouters and inventors the exclusive right to their respective writings and discoveries'. See R. Graves III, 'Private Rights, Public Uses, and the Future of the Copyright Clause', 80 Neb. L.Rev. 64 (2001), esp. at 80 *et seq*. [containing an analysis of issues pertaining to digital copying as they emerged in the beginning of the 21st century].

[28] *United States v. Schaefer*, 501 F.3d 1197, 1201 (10th Cir. 2007).

[29] See *supra*, n. 21.

[30] *Cf. United States v. Kammersell*, 196 F.3d 1137 (10th Cir. 1999), decided under the provision 18 USC § 875(c), according to which: '*Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any*

interpretative ambiguities often arise,[31] it is clear that substantive statutory provisions[32] can actually pose jurisdictional limitations to federal power.[33]

On the procedural level, federal power has steadily expanded ever since the 9/11 attack on the World Trade Center.[34] The Office for Homeland Security and the Critical Infrastructure Board were created by virtue of executive orders (issued by President Bush) to address, *inter alia*, cyber-threats.[35] The enactment of the 'PATRIOT Act'[36] was a decisive step toward the direction of enhancing federal power:[37] among other things, it gave the federal government authority to intercept electronic communications relating to computer fraud and abuse offenses;[38] it allowed the government to share electronic information;[39] and it provided the government with the ability to intercept computer communications.[40] These initiatives were subsequently supplemented by the creation of the Department of Homeland Security,[41] the enactment of the 'PROTECT' Act,[42] as well as a number of executive measures aimed at consolidating authority in the area of cybercrime.[43]

---

person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both'. The court distinguished the case at hand from *Lopez* on the grounds that § 875(c) requires the use of a channel of interstate commerce. Since the provision was not 'subject to the same limiting interpretation as *Lopez*', it upheld it.

[31] The court relied on, *inter alia*, *United States v. Carroll* [105 F.3 d 740 (1st Cir. 1997)], as well as *United States v. MacEwan*, 445 F.3 d 237 (3rd Cir. 2006). See some criticism of the court's line of reasoning in C. Fieman, 'Defending Internet Pornography Cases by Challenging Interstate Jurisdictional Elements Under U. S. v. Schaefer', available online at: http://www.nacdl.org/champion.aspx?id=4952 [last visited on 20 August, 2013].

[32] *Cf. United States v. Lewis*, 554 F. 3 d 208 (1st Cir. 2009) [interpreting 18 USC § 2252(a)(2) as it stood at the time of the defendant's conduct, notwithstanding subsequent expansion of the 'jurisdictional coverage' (the statute was found to cover the conduct in question even under its original construction). The court's decision was thus in line with the non-retroactivity of substantive criminal law provisions].

[33] For an overview of *procedural* statutory limits see O. Kerr, *Computer Crime Law*², at 562 *et seq*. [discussing limitations imposed by statutory privacy laws, e. g. in *United States v. Scarfo*, 180 F. Supp.2 d 572 (D.N. J. 2001), or arising in the context of the conflict between national and local authorities, e. g. in *United States v. Rodriguez*, 968 F.2 d 130 (2nd Cir. 1992)].

[34] See A. Parker and J. Fellner, "Above the Law: Executive Power after September 11 in the United States", Human Rights Watch, World Report 2004, available online at: http://www.hrw.org/legacy/wr2k4/8.htm [last visited on 20 August, 2013].

[35] See F. Mendez, *op. cit.*, at 515, referencing Executive Order 13228 (setting up the Office for Homeland Security), and Executive Order 13231 (setting up the Critical Infrastructure Protection Board). Contrast the absence of similar executive bodies on a European level (of which see *infra*, in the next chapter).

[36] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT Act), P. L. 107-56, 115 Stat. 272 (2001). The USA PATRIOT Act originated as H. R. 2975 in the House and S. 1510 in the Senate.

[37] For an overview of the Act's provisions see C. Doyle, 'The USA PATRIOT Act: A Legal Analysis', CRS Report for Congress, April 15, 2002. The Report is available online at: http://www.fas.org/irp/crs/RL31377.pdf [last visited on 20 August, 2013].

[38] Section 202 ["Authority to Intercept Wire, Oral, and Electronic Communications Relating to Computer Fraud and Abuse Offenses"].

[39] Section 203 ['Authority to Share Criminal Investigative Information', including 'grand jury information' (a), 'electronic, wire, and oral interception information" (b), and "foreign intelligence information' (d)].

[40] Section 217 ["Interception of Computer Trespasser Communications"].

[41] For an overview of key documents describing the procedure leading to the creation of the Department of Homeland Security [DHS] in 2003 see the Department's website: http://www.dhs.gov/xabout/history/gc_1297963906741.shtm [last visited on 20 August, 2013].

[42] P.L. 108-21, 117 Stat. 650 (2003). 'PROTECT' stands for 'Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today'.

[43] Legislative initiatives are ongoing to this day. See, e. g., a discussion on the upcoming Cyber Crime Protection Security Act (S. 2111) [currently on the Senate calendar] in C. Doyle, 'Cybersecurity: Cyber Crime Protection

In the aggregate, there seem to be two forces at play, which have been exerted in the field of cybercrime for over a decade:

(i) On a 'vertical' level, authority has been shifting from the local (State) government to the federal government, attaining a more 'centralized' form. This tendency, which remains largely unaffected by the tendency to reserve some power to the States in the post-*Lopez* era, is being justified either on the basis of the cross-border nature of cybercrime or on account of its actual or potential transformation into a national security threat.

(ii) On a 'horizontal' level, the tendency has been to focus more on Presidential authority than Congressional or even Judicial power. In fact, a closer look at the application of federal legislation reveals that the number of federal prosecutions is disproportionately low compared to the amount of federal legislation enacted. This shows that the actual (and significant) effect of centralization of authority in the US is the expansion of federal *executive* power, exercised by the FBI, the Department of Justice, and so forth.

This structure of authority seems to accord with the very nature of the federal system in the US, which has favored a strong center. Under these circumstances, one might indeed argue that consolidating power in the way exercised above is an inevitable outcome of a 'dualist' federal system.[44] Regardless of the impact of such an arrangement on civil liberties, there is something to be said about the system's increased efficiency.[45] The question then arises as to whether this centralization is equally predictable –or even desirable- in a system that consists of a weak center surrounded by strong peripheral 'hubs', such as the one that has evolved in the European Union.[46]

2. 'Shadows' of federalism – Centralizing powers in the EU

Europe's institutional framework is of course quite different from the one existing in the US, and this has obvious implications also in the field of cybercrime. Although the European Union is a major supranational entity with the ability to implement policies over a broad spectrum of subject areas, it is by no means the only one. In fact, it is the Council of Europe that has been the most active 'player'

Security Act (S. 2111) – A Legal Analysis', CRS Report for Congress, March 12, 2012. The Report is available online at: http://www.fas.org/sgp/crs/misc/R42403.pdf [last visited on 20 August, 2013].

[44] For a comparison between 'dualist' federalism and 'interactive' federalism see R. Schapiro, 'Justice Stevens's Theory of Interactive Federalism', 74 Fordham L. Rev. 2133 (2006) [arguing that "dualist federalism does not seek to enforce strict borders between state and federal power", since it 'acknowledges substantial areas of concurrent jurisdiction' (*id*., at 2134)]. *Cf*., however, the decision of the Supreme Court in *Printz v. United States*, 521 US 898 (1997), at 918, insisting that the local and the national 'sovereigns' must be divided by a clear line 'policed' by the Court.

[45] See R. Schapiro, *id*., at 2139 *et seq*. [speaking of "the values of dualism"]; F. Barry, 'Valuing Federalism', 82 Minn. L. Rev. 317 (1997), at 389 *et seq*. [arguing that federalism fosters political participation]; B. Weingast, 'The Economic Role of Political Institutions: Market-Preserving Federalism and Economic Development', 11 J. L. Econ. & Org. 1 (1995) [discussing financial arguments in favor of federalism].

[46] The institutional arrangement in the EU may not even justify the use of the term 'federalism'. For the purposes of the present analysis, the term will be used so as to describe the EU in a functionally analogous way to the US system.

in the field of cybercrime during the last two decades.[47] As far back as 1989, the Council of Europe adopted Recommendation 89(9), emphasizing the need for intergovernmental cooperation in the field of what it termed "computer-related crime".[48] Six years later, Recommendation 95(13) laid out a set of measures to enforce the dictates of Recommendation 89(9), thus complementing substantive provisions with procedural mechanisms.[49] These efforts in the context of the Council of Europe culminated in 2001, with the Convention on Cybercrime.[50] This Convention was prepared not only by European experts, but also with the active participation and support of third States, including the United States.[51] The Convention came into effect in 2004,[52] and constitutes the most important international instrument in the field.

All EU member-States (though not the European Union *itself*) are currently signatory parties to the Cybercrime Convention, while most of them have already ratified it.[53] Yet a multilateral convention only functions on an intergovernmental level, creating international obligations that have to be implemented by virtue of *domestic* legislation.[54] In addition, the Council of Europe lacks a mechanism that might ensure compliance on the part of State parties. It soon became apparent that a multilateral convention would be *per se* inadequate to address cybercrime issues on the European continent. Some argued that, in contrast, the European Union seemed better positioned to bring about real changes in the way member States dealt with cybercrime.[55]

To be relatively better positioned compared to a 'loose' intergovernmental organization such as the Council of Europe does not necessarily mean that the European Union is institutionally capable of dealing with cybercrime with the

[47] For an overview of initiatives adopted by the Council of Europe concerning cybercrime see: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp [last visited on 20 August, 2013].

[48] Recommendation No.R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (Adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies).

[49] Recommendation No.R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies).

[50] Convention on Cybercrime, ETS No. 185, Budapest, 23.XI.2001, available online at: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm [last visited on 20 August, 2013].

[51] The United States signed the treaty on November 23, 2001, and ratified it on September 29, 2006. Upon signature, the US had made six reservations and four declarations.

[52] According to the terms of the Convention, entry into force required a minimum of five ratifications, including three by members of the Council of Europe. This requirement had been satisfied by 1 July, 2004.

[53] To date, thirty-nine States have ratified the Convention on Cybercrime (including thirty-five member-States of the Council of Europe plus Australia, the Dominican Republic, Japan, and the United States), while an additional twelve States have signed but not ratified the Convention (including ten member States of the Council of Europe plus Canada and South Africa). See CoE Treaty Office, online at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [last visited on 20 August, 2013].

[54] Of course, there are certain provisions of the Convention that are self-executing, and thus do not require implementation by virtue of domestic legislation. These would include provisions on extradition and mutual assistance: see D. Robel, International Cybercrime Treaty: Looking Beyond Ratification, Report, SANS Institute, 15 August, 2006, pp. 13-14 [also available online at: http://www.sans.org/reading_room/whitepapers/honors/international-cybercrime-treaty-ratification_1756 (last visited on 20 August, 2013)].

[55] For the sequence of initiatives between the CoE Convention on Cybercrime and the EU Framework Decision on attacks against information systems see P. Csonka, 'The Council of Europe's Convention on Cyber-crime and other European Initiatives', 77 Revue Internationale de Droit Pénal 473 (2006).

efficiency of a full-fledged federal government. The history of cybercrime legislation in the European Union is a good example of the deficiencies of the European structural arrangement.[56] One might discern three stages in the evolution of EU power to deal with cybercrime, corresponding to successive expansions of its criminal law authority in general.[57] Specifically:

(i) During the initial stages of European integration, criminal law –especially cybercrime- was not among the priorities of the European Communities. The Maastricht Treaty of 1993 launched a new era by introducing "justice and home affairs" as the third pillar of the newly-formed European Union.[58] Such an arrangement was very similar to the type of cooperation achieved through intergovernmental organizations like the Council of Europe or the Organization for Economic Cooperation and Development (both of which were already promoting their own agendas in the field of cybercrime).[59] This was an inefficient system, as member States were jealously reserving power for themselves, while it also smacked of lack of transparency, since there was no monitoring mechanism in place to assess 'legislative' initiatives.[60] It is no wonder, then, that no significant steps were taken during that period towards the direction of combating cybercrime on an EU level.

(ii) A significant development occurred after the entry into force of the Amsterdam Treaty in 1999.[61] For the first time in European history, a common area of "freedom, security and justice" was created, coupled –shortly thereafter- with the notion of "mutual recognition".[62] Most notably, the EU was now equipped with

---

[56] S. Mercado Kierkegaard, EU Tackles Cybercrime, in L. Janczewski and A. Colarik, *Cyber Warfare and Cyber Terrorism*, Information Science Reference, 2008, p. 437.

[57] On European criminal law as it has evolved through the various developmental stages of the EU see, *inter alia*, A. Klip, *European Criminal Law: An Integrative Approach*, Intersentia, 2nd ed., 2012, pp. 13 *et seq*.; M. Fletcher, EU Criminal Justice: Beyond Lisbon, in C. Eckes and T. Konstantinides (eds.), *Crime within the Area of Freedom, Security and Justice: A European Public Order*, Cambridge University Press, 2011, pp. 10 *et seq*.; B. Hecker, *EuropäischesStrafrecht*, Springer, 3rd ed., 2010, pp. 77 *et seq*.; H. Satzger, *Internationales und EuropäischesStrafrecht*, 2nd ed., 2010, pp. 100 *et seq*.; M. Fletcher, R. Lööf and B. Gilmore, *EU Criminal Law and Justice*, Edward Elgar, 2008, *passim*.

[58] E. Baker and C. Harding, 'From Past Imperfect to Future Imperfect? A Longitudinal Study of the Third Pillar', 34 European Law Review 25 (2009); S. Douglas-Scott, 'The Rule of Law in the European Union: Putting Security into the "Area of Freedom, Security and Justice"', 29 European Law Review 219 (2004).

[59] On these initiatives see S. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, Greenwood Publishing Group, 2010, pp. 173 *et seq*.

[60] In addition, the 'third pillar' of the EU structure was considered less than an 'ideal counterpart' to the first pillar (i.e. the EC): see S. Lavenex and W. Wallace, Justice and Home Affairs, in H. Wallace and M. Pollack, (eds.), *Policy-Making in the European Union*, Oxford University Press, 2005, ch. 18.

[61] For a discussion of the changes brought about by the Treaty of Amsterdam see, *inter alia*, P. Craig and G. de Búrca, *EU Law: Text, Cases and Materials*, Oxford University Press, 4th ed., 2008, pp. 20 *et seq*.; A. Moravcsik and K. Nicolaïdis, 'Explaining the Treaty of Amsterdam: Interests, Influence, Institutions', 37 Journal of Common Market Studies 59 (1999); I. Pernice, 'Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitution-Making Revisited?', 36 Common Market Law Review 703 (1999); F. Dehousse, 'Le Traité d' Amsterdam: Reflet de la Nouvelle Europe', 33 CDE 265 (1997); J. Shaw, 'The Treaty of Amsterdam: Challenges of Flexibility and Legitimacy', 4 ELJ 63 (1998).

[62] See A. Gibbs, *Life and Europe's Area of Freedom, Security and Justice*, Ashgate Publishing, 2011, p. 114 [citing the judgment of the German Constitutional Court in *Re Constitutionality of German Law Implementing the Framework Decision on a European Arrest Warrant*, 18 July 2005, 1 CMLR 16 (2006), demonstrating certain limits of mutual recognition]; F. Calderoni, *Organized Crime Legislation in the European Union: Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decision on the Fight Against Organized Crime*, Springer, 2010, p. 14; V. Mitsilegas, "The Transformation of Criminal Law in the Area of Freedom, Security and Justice", 26 Yearbook of European Law 1 (2007).

novel legislative tools (alongside traditional instruments such as Regulations, Directives, and Decisions), including 'Framework Decisions', which could be adopted to address issues pertaining to criminal law.[63] These changes spawned an array of documents regulating cyberspace, which included:

- The 2000 Directive on Electronic Commerce, which aspired to create a "common market" environment for businesses and individuals engaging in commercial activities on the Internet;[64]

- The 2002 Directive on Privacy and Electronic Communications, which served as a 'complement' to the Data Protection Directive of 1995,[65] in that it extended the protection afforded by the latter to activities carried out in cyberspace;[66]

- The 2004 Framework Decision on Combating Child pornography on the Internet, which, among, other things, introduced broad definitions of what constitutes prohibited 'pornographic material', including any visual depiction (real or imaginary) of sexually explicit conduct involving minors or persons pretending to be minors;[67]

- The 2005 Framework Decision on Attacks against Information Systems, proscribing a number of types of conduct on the Internet and calling for the 'approximation' of national legislations so as to strengthen mutual judicial cooperation in the field;[68]

- The 2006 Directive on the Retention of Data, requiring the storage of data for a period of up to two years.[69]

Admittedly, this legislative activity marked a new era in which a common European approach to cybercrime became a realistic prospect. However, there were

---

[63] See P. Craig and G. de Búrca, *The Evolution of EU Law*, Oxford University Press, 2nd ed., 2011, p. 377 [citing Case C-105/03 *Pupino* (2005) ECR I-5285]; D. Chalmers, G. Davies and G. Monti, *European Union Law*, Cambridge University Press, 2nd ed., 2010, p. 300; A. Hinarejos, 'On the Legal Effects of Framework Decisions and Decisions: Directly Applicable, Directly Effective, Self-Executing, Supreme?', 14 ELJ 620 (2008).

[64] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L 178, 17. 7. 2000, pp. 1–16, full text available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT [last visited on 20 August, 2013].

[65] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23. 11. 1995 pp. 31-50, full text available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [last visited on 20 August, 2013].

[66] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L 201/37, 31. 7. 2002, pp. 37-47, full text available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF [last visited on 20 August, 2013].

[67] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, Official Journal L 13, 20. 1. 2004, pp. 44-48, online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML [last visited on 20 August, 2013].

[68] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Official Journal L 69, 16. 3. 2005, pp. 67-71 [hereinafter '2005 Framework Decision'], full text available online at: http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/203.pdf [last visited on 20 August, 2013].

[69] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13. 4. 2006, pp. 54-63, available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [last visited on 20 August, 2013].

still a number of problems. As the EU did not have autonomous power in the field of criminal law, these instruments had to be 'transposed' into the domestic legal order of each member State.[70] The respective deadlines were rarely –if ever- observed, while certain member States openly questioned their commitment to Union objectives, which were delineated absent of any democratic legitimization of the pertinent organs. These deficiencies made it imperative[71] that the European Union assume additional powers to regulate cross-border crime, including cybercrime, which in turn led to the Treaty of Lisbon.[72]

(iii) The amendments brought about by the Lisbon Treaty have admittedly engendered a qualitatively different structure of EU authority in relation to criminal law.[73] Under the newly-inserted Article 83 of the Treaty on the Functioning of the European Union (TFEU),

'the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, ***establish minimum rules concerning the definition of criminal offenses*** *and* ***sanctions*** *in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis'*. [emphasis added][74]

'Computer crime' is explicitly enumerated among the "particularly serious" criminal offenses triggering such legislative process on a European level.[75] This is a qualitatively different framework than the one which existed prior to the Lisbon Treaty. For the first time in its history, the European Union possesses *legislative* power in the field of criminal law, and cybercrime in particular, that it can exercise by

[70] On the effect of 'pre-Lisbon' EU legislative instruments see S. Peers, *EU Justice and Home Affairs Law*, Oxford University Press, 3rd ed., 2011, pp. 24 *et seq*.

[71] Of course, there are those who argue that the EU could have followed a different path: see, among several others, B. Schünemann, "Alternative-Project for a European Criminal Law and Procedure", 18 Criminal Law Forum 227 (2007).

[72] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, Official Journal C 306, 17. 12. 2007, available online at: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML [last visited on 20 August, 2013].

[73] See, *inter alia*, E. Herlin-Karnell, EU Competence in Criminal Law after Lisbon, in A. Biondi, P. Eeckhout and S. Ripley (eds.), *EU Law after Lisbon*, Oxford University Press, 2012, pp. 331 *et seq*.; J.-C. Piris, *The Lisbon Treaty: A Legal and political Analysis*, Cambridge University Press, 2010, pp. 177 *et seq*.; M. Heger, "Perspektiven des Europäischen Strafrechts nach dem Vertrag von Lissabon", 4 ZIS 406 (2009).

[74] According to the German Constitutional Court, the "cross-border" character of a specific type of criminal conduct is not merely a 'label' that can be attached at will by the competent organs of the EU; rather, affirmation of the EU's competence in each specific area of criminal law shall depend on concrete criteria demonstrating that criminal law measures –and indeed on a European level- are necessary to address the problem: see *Bundesverfassungsgericht Lissabon-Urteil*, 2 BvE 2/08 – 2 BvE 5/08 – 2 BvR 1010/08 – 2 BvR 1022/08 – 2 BvR 1259/08 – 2 BvR 182/09, NJW 2009, at 2267. On the implications of the "Lisbon decision" by the German Constitutional Court see K. Ambos and P. Rackow, "Erste Überlegungen zu den Konsequenzen des Lissabon-Urteils des Bundesverfassungsgerichts für das Europäische Strafrecht", 4 ZIS 397 (2009); A. Fischer-Lescano, C. Joerges and A. Wonka (eds.), *The German Constitutional Court's Lisbon Ruling Legal and Political Science Perspectives*, ZERP – Discussion Paper 1/2010, available online at: http://www.mpifg.de/people/mh/paper/ZERP%20Discussion%20Paper%201.2010.pdf [last visited on 20 August, 2013].

[75] It should be noted that the EU retains the competence to enact 'legislation' with a direct binding effect when it comes to crimes of fraud against its own interests. Such competence is based on Article 325 of the TFEU, and would probably cover fraudulent conduct against EU interests carried out in cyberspace. On the 'enhanced' competence of the EU in this area see H. Satzger, supra n. 57, at 100 *et seq*. [discussing the possibility of the EU enacting Regulations to proscribe fraud under article 325 TFEU]; also see U. Sieber, "Die Zukunft des Europäischen Strafrechts", 121 ZStW 1 (2009).

means of directives.[76] Directive 2013/40/EU on attacks against information systems,[77] which quite recently replaced the 2005 Framework Decision on Attacks against Information Systems following a much debated proposal by the European Commission,[78] is one of the first directives to be adopted under the new regime. The only way for member States to exempt themselves from the application of the definitions and sanctions imposed by EU organs would be to invoke the so-called 'emergency brake clause', i. e. to contend that a given directive would have an adverse impact on 'fundamental aspects of its criminal justice system'.[79] Invocation of this provision is indeed not expected to occur very often in actual practice.

The pattern described above has one similarity and one notable difference in comparison with the structure of authority that exists in the US federal system. It is similar to the latter in that the vertical flow of power appears to be moving in the same direction, i. e. from the periphery to the 'center'. To be sure, this transfer of authority has been taking place in other sectors; however, criminal law authority has always been associated with the 'hard core' of State power, and ceding part of that power to a supranational organization like the European Union meets with a certain degree of reluctance, which is, of course, understandable.[80]

The striking difference between the US federal system and the EU 'quasi-federal' system is to be traced in the 'horizontal' allocation of power within the central structure. In contrast to the US federal government, which has leaned towards strengthening the executive, the European Union appears to refrain from extending any apparent executive 'arm' that might autonomously enforce its legislative initiatives. At a first glance, this may seem as an 'innocuous' attempt at a progressive unification. In reality, however, such 'reticence' is but a symptom of the 'democratic deficit' that has characterized the European Union ever since the early '90s.[81] The

[76] On the nature of EU competence in the field of criminal law under article 83(1) and (2) TFEU, as well as the attributes of the new 'breed' of directives created by the Treaty of Lisbon see A. Klip, *supra* n. 57, at 49 *et seq*.

[77] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal L 218, 14. 8. 2013, pp. 8-14, available online at:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF [last visited on 20 August, 2013].

[78] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM (2010) 517 final, 30. 9. 2010. The full text of the proposal, along with its accompanying 'explanatory memorandum', is available online at: http://ec.europa.eu/home-affairs/policies/crime/1_EN_ACT_part1_v101.pdf [last visited on 20 August, 2013].

[79] For a discussion of 'emergency brake' procedures after the Treaty of Lisbon see S. Peers, 'EU Criminal Law and the Treaty of Lisbon', 33 European Law Review 507 (2008).

[80] Any transfer of sovereignty to an international organization would, predictably, engender some resistance on the part of national authorities. In the case of the EU, however, an additional problem is the so-called 'democratic deficit' that was accentuated alongside the exponential expansion of the Union's powers during the '90s. For an interesting discussion of the pertinent issues see A. Føllesdal and S. Hix, "Why there is a Democratic Deficit in the EU: A Response to Majone and Moravcsik", 44 JCMS 533 (2006); A. Moravcsik, "Is there a 'Democratic Deficit' in World Politics? A Framework for Analysis", 39 Government and Opposition 336 (2004); G. Majone, 'Europe's Democratic Deficit', 4 European Law Journal 5 (1998).

[81] Truth be told, there are some scholars who argue that the European Union should *not* subscribe to democratic principles, lest it lose the ability to integrate: see, e. g., G. Majone, *ibid*. Under this approach, a 'democratic deficit' is by definition necessary in order to attain consolidation of sovereign power on a supranational level (this would presumably be true *a fortiori* in the case of 'cross-border' threats, such as cybercrime, terrorism, and organized crime). Also see A. Føllesdal and S. Hix, *ibid*.

organs retaining the initiative, i. e. the European Council and the European Commission, are comprised either by members of each national government (as in the case of the former) or by individuals appointed by their respective national governments (as in the case of the latter). Thus, by convening in Brussels, national governments have managed to advance their agendas without meaningful 'checks' by their national Legislatures (i.e. the local Parliament in each member State). The decisions thus made would then have to be implemented by local *enforcement* agencies, thus strengthening the Executive in each Member State. Needless to say, this practice has favored stronger States within the European Union, which are naturally better positioned to exercise control over the Union's legislative processes, which they can subsequently put into effect at their own will and pace. Confining oneself to the observation that executive power has not increased on an EU level would therefore be deceiving: in reality, European integration has thus far been about the increase of *local* executive power at the expense of *local* legislatures. Admittedly, this tendency is susceptible to the same criticism waged against the strengthening of Presidential powers in the United States, without being able to display the latter's effectiveness.

A recent proposal by the European Commission to establish a European Cybercrime Center[82] with the declared goal of protecting European citizens and businesses against "mounting cyber-threats"[83] can hardly be considered to constitute a substitute for an effective consolidation of executive power on a 'high level' (meaning in a genuinely 'centralized' fashion comparable to what has been happening in the United States). This center will be established as a branch of Europol (which is itself lacking in actual enforcement authority),[84] and will primarily focus on combating organized crime groups involved in a whole range of activities, from attacks against critical infrastructure and information systems to child pornography.[85] However, it will be confined to alerting member States of potential cyber-threats, providing some sort of operational support in investigations carried out by *local*

[82] See the pertinent Press Release by the European Commission, available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317&format=HTML&aged=0&language=EN&guiLanguage=en [last visited on 20 August, 2013].

[83] The creation of a center to combat cybercrime had been envisaged as part of the 'Internal Security Strategy' of the EU laid out in 2010. Specifically, raising levels of security for citizens and businesses in cyberspace was deemed to require three 'actions": (i) building capacity through law enforcement and the judiciary (by, *inter alia*, fostering cooperation between the cybercrime center, the European Network and Information Security Agency ['ENISA'], and a network of national Computer Emergency Response Teams ['CERTs']); (ii) working with industry to empower and protect citizens (with a view to, among other things, encouraging the reporting of cybercrime incidents); and (iii) improving capability for dealing with cyber-attacks (by putting together, *inter alia*, a European Information Sharing and Alert System ['EISAS']). See Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Brussels, 22. 11. 2010, COM (2010) 673 final, at pp. 9-10. The full text of this document is available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF [last visited on 20 August, 2013].

[84] Admittedly, Europol's mandate has been considerably expanded ever since the agency's creation: see, indicatively, House of Lords: European Union Committee, *Europol: Coordinating the Fight against Serious and Organised Crime [Report with Evidence]*, 2008, *passim*.

[85] For more information on the mandate of the new European Cybercrime Center see MEMO/12/221 of 28 March 2012 containing some preliminary remarks, available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221&format=HTML&aged=0&language=EN&guiLanguage=en [last visited on 20 August, 2013].

agencies, and serving as a hub of information for both the public and the private sector.[86] It becomes evident that this center will not be able to discharge executive authority independently from the law enforcement agencies of each member State, but will essentially act as an advisor to them.

Thus, the European Union is currently moving towards a new vertical arrangement of authority despite the absence of a structure capable of accommodating executive action. At the same time, the implementation of former policies –e. g. under the 2005 Framework Decision- is still underway, and obligations under the Council of Europe Convention on Cybercrime have not been fully met or even undertaken by all State parties.[87] Such order of doing things is prone to the criticism of putting the cart before the horse, and that is even before looking at the provisions of the newly-adopted directive.

III. Defining cybercrime on a substantive level

1. The 'utility' of tradition

Much of the debate concerning cybercrime regulation on both sides of the Atlantic revolves around a central question: should crimes committed in cyberspace be treated as being 'qualitatively' different than other forms of crime?[88] If this question were answered in the affirmative, it would only be natural to concede that departure from traditional principles underlining criminal legislation in general is justified, at least to some extent. A negative answer, on the other hand, would mean that such departure is hardly justified, at least in certain cases, which would in turn make it much easier to draw analogies from 'ordinary' criminal law cases.

A case could be made (and indeed *is* made) that the presumed idiosyncratic nature of cybercrime is somewhat exaggerated.[89] Indeed, cybercrime tags develop-

[86] See Communication from the Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, Brussels, 28. 3. 2012, COM (2012) 140 final. The document is available online at: http://ec.europa.eu/home-affairs/doc_centre/crime/docs/Communication%20-%20European%20Cybercrime%20Centre.pdf [last visited on 20 August, 2013].

[87] Although all 27 EU member-States have signed the Convention on Cybercrime, not all of them have ratified it to date. It is noteworthy that, in its proposal for a directive on cybercrime, the EU Commission actively encouraged the remaining EU member-States to ratify the Convention as soon as possible, considering that the latter "is regarded as the most complete international standard to date, since it provides a comprehensive and coherent framework embracing the various aspects relating to cybercrime": see Proposal, *supra* n. 78, at 2.

[88] For a discussion of this question (illustrated through the use of pertinent examples and including further citations) see S. Brenner, 'Cybercrime Metrics: Old Wine, New Bottles?', 9 Va. J. L. & Tech. 1 (2004).

[89] Brenner concludes that 'cybercrime is different with regard to the methods that are used in its commission and the tangential harms that result from its commission', and, therefore 'it eludes the scope of the metrics we use for crime' [*id.*, at p. 52]. The position adopted in this paper does not necessarily conflict with the above conclusion; however, it will be argued that, since the differentiating attribute is essentially the 'method' being used, no departure is justified from the relationship between the proscribed conduct and the harm caused (including 'tangential harms' as per Brenner). In other words, the argument is *not* that specific legislation on cybercrime is not required; rather, the position of the paper is that such legislation –which is called for- should abide by the same principles underlining legislative practices in relation to 'ordinary' crime. If 'ordinary' fraud is proscribed in a manner conforming to the 'harm principle' (e.g. by requiring 'damage', as well as proof of the existence of a causal link between the fraudulent conduct and the result), there is no reason in law or logic why fraud committed in cyberspace should be proscribed in a different manner (e.g. as a 'crime of conduct' as opposed to a "result crime").

ments in computer and Internet technology, and is therefore no more different from 'common crime' than cyberspace is from the 'real world'. During the last two decades, technological developments on the Internet have largely consisted in replicating the real world in cyberspace.[90] Accordingly, cyber-applications imitate social forums, ordinary mail, actual games, and so forth. It is only natural, then, that cybercrime has evolved to be a replica of known forms of criminality, only in digital form.[91] That is not to say that there are no qualitatively different elements underlying it: one of these, for instance, is the ease with which crime crosses borders in the digital world (admittedly, the Internet has made it easier to commit traditional crimes across greater distances). However, the essence of criminal conduct –at least as regards a significant number of offenses against property and against the person- has remained the same, even though the means to carry it out are different.

It would *prima facie* appear that both US and European criminal law are on the same path when it comes to substantive law definitions of criminal offenses in cyberspace. For instance, there seems to be an increasing number of inchoate offenses, in which the link between the conduct and any perceived harm is tenuous at best.[92] This is partly due to the fact that definitions in one system are frequently modeled after those adopted in the other. Nonetheless, it is the overall legal environment in which these definitions are applied that makes a difference. Once put in context, substantive law enacted in one system seems a less plausible candidate for 'transfusion' to the other.

Criminal law in the US has traditionally been less attached to the 'harm principle' compared to European criminal law.[93] This is evident both in the 'general' and in the 'special' part: for instance, case-law has subscribed to a rather expansive construal of attempt, thereby attenuating the link to any perceived result,[94] while the Model

[90] Word is often made of a 'technological plateau' these days: see, e. g., T. Cowen, 'Innovation is Doing Little for Incomes', NY Times, 29 January, 2011, available online at: http://www.nytimes.com/2011/01/30/business/30view.html [last visited on 20 August, 2013]. For a geopolitical perspective of this phenomenon see G. Friedman, *The Next Decade: Empire and Republic in a Changing World*, Anchor Books, 2011, p. 229 [arguing that "we are now at an extrapolative and incremental state in which the primary focus is on expanding capacity and finding new applications for technology developed years ago"]. Similar claims put forward in the past have usually been followed by significant advances in technology. For the purposes of the present discussion, however, what is important to note is that, regardless of what the future has in store, the present seems to indeed coincide with the reality described above, and this is what matters with a view to adopting appropriate legal responses to cybercrime.

[91] In fact, the very term 'cybercrime' is frequently misplaced, as it is used to describe conduct that is *per se* unrelated to cybercrime (even though cyberspace may have had something to do with the motive of the crime or the opportunity to carry it out). See, e. g., the reporting of the so-called British 'cyber-murder' case by the London Times: "Gory Details as British Cyber-Murder Trial Opens", 29 April, 2009, available online at: http://www.foxnews.com/story/0,2933,518359,00.html [last visited on 20 August, 2013] (concerning the stabbing of a British student by a German man, motivated by hatred caused by the fact that the perpetrator was obsessed with the victim's girlfriend, whom he had met on an Internet gaming website). That is not to say that 'cyber-murder' is inconceivable: see, e. g., BBC's story on the possibility of malicious action targeted against medical implants such as pacemakers: M. Ward, 'Warning over Medical Implant Attacks', BBC News, 9 April 2012, available online at: http://m.bbc.co.uk/news/technology-17623948 [last visited on 20 August, 2013].

[92] Note that the Convention on Cybercrime also requires that State parties criminally proscribe inchoate offenses under Article 6(1).

[93] See B. Harcourt, "The Collapse of the Harm Principle", 90 J. Crim. L. & Criminology 109 (1999).

[94] See R. Duff, *Criminal Attempts*, Oxford University Press, 1997 [attempting to delineate the notion of attempt based on objective criteria]; A. Bierschbach and A. Stein, "Mediating Rules in Criminal Law", 93 Va. L. Rev. 1197 (2007), at pp. 1234 *et seq*. [leaning towards broadening the scope of attempt based on, *inter alia*, policy arguments].

Penal Code has also expanded the array of acts that might be regarded as a 'substantial step' towards the commission of the crime.[95] In terms of the 'general part' of criminal law, the theory of accomplice liability also reveals some distance from resulting harm: the *Luparello* criteria blur the line between the participatory act and the resulting harm.[96] The Model Penal Code, on its part, has adopted a largely subjective test,[97] which tends to punish the accomplices for what they intended as opposed to punishing them for what they actually contributed in. Coming to the special part, case-law seems to expand such notions as conspiracy in order to prevent harm before it materializes. Abuses are thus inevitable, as in the *Padilla* case, in which prosecutors and judges ended up fabricating perceived threats (short of actual harm) to justify what would otherwise have been unjustifiable detention.[98] In addition, Anglo-American criminal law has traditionally kept distances from the harm principle in the way proscribed offenses are classified (in contrast to such jurisdictions as Germany or Sweden, where offenses are strictly classified based on the type and/or extent of harm they bring about), which has an impact in such fields as concurrence between offenses, properly applying the lesser offense doctrine, the merger rule, and so forth. Last but not least, sentencing is not linked to resulting harm. Pieces of legislation such as the three-strikes statute reveal that the law in the US is sometimes more preoccupied with punishing persons for who they *are* (not for what they have *done*).[99]

In many respects, Anglo-American criminal law (and US criminal law in particular) reflects utilitarian considerations. Cybercrime regulation is no exception in this regard: even when the court decides in favor of the defendant, as in the recent case of *United States v. Nosal* decided by the Court of Appeals for the 9th Circuit,[100] it does so based on utilitarian arguments. Indeed, Judge Kozinski – writing for the majority- focused on the fact that the government's interpretation would effectively turn the CFAA into a 'sweeping' statute,[101] and would drastically and unjustifiably alter the nature of employer-employee relationships (which are "traditionally governed by tort and contract law") by turning them into criminal law disputes.[102] A harm-based approach would rather be focused on the 'fundamental interest(s)' protected under the applicable provisions of the CFAA, and

[95] There are cases in which courts have adopted a more balanced approach [such as *People v. Rizzo*, 158 N.E. 888 (N.Y. 1927), adopting the so-called "physical proximity test"], but they are in the minority.

[96] *People v. Luparello*, 231 Cal. Rptr. 832 (Cal. Ct. App. 1986) [recognizing that the criterion for accomplice liability is the 'foreseeability' of the principal's act on the part of the accomplice]; *cf.* M. Moore, 'Causing, Aiding, and the Superfluity of Accomplice Liability', 156 U. Pa. L. Rev. 395 (2007) [attempting to link accomplice liability with some version of the 'harm principle'].

[97] See section 2.06 of the Model Penal Code.

[98] *Padilla v. Rumsfeld*, 124 S. Ct. 2711 (2004) [stopping short of dealing with the question whether the defendant had been lawfully detained].

[99] For a criticism of California's three-strikes statute from the angle of international human rights law see A. Goldin, 'The California Three Strikes Law: A Violation of International Law and a Possible Impediment to Extradition', 15 Sw. J. Int'l L. 327 (2009).

[100] *United States v. Nosal*, No. 10-10038 (9th Cir. 10 April 2012), available online at: http://www.ca9.uscourts.gov/datastore/opinions/2012/04/10/10-10038.pdf [last visited on August 20, 2013].

[101] *Id.*, at 3863.

[102] *Id.*, at 3864, 3867.

whether such interests have been undermined by a mere violation of terms of service.[103]

Three pertinent examples attest to the above-described orientation of cybercrime regulation. These relate to: (i) damage as a requirement for ascertaining a felony under the CFAA; (ii) issues pertaining to causation; and (iii) special skills as an aggravated circumstance affecting sentencing. Specifically:

(i) In its current form,[104] 18 USC § 1030(c)(4) provides for a criminal penalty to be imposed for computer damage offenses contained therein, if the defendant's conduct caused ("or, in the case of an attempted offense, would, if completed, have caused"), *inter alia*, "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value".[105] The inclusion of such a threshold for the ascertainment of a felony under the CFAA smacks of retributivism; yet the application of the threshold in actual practice indicates otherwise.[106] In *United States v. Middleton*,[107] which set the pace for the interpretation of the said provision, damage was broadly construed so as to include –in the aggregate- all "natural and foreseeable" results of the defendant's conduct, including the cost of repairing and re-securing the system against future similar acts.[108] Such an interpretation in effect renders the $5,000 threshold moot,[109] and is only one step away from recognizing that 'unauthorized access' itself constitutes sufficient damage for the purposes of this provision.[110] Even when it is upheld that damage has to consist in something "more than mere unauthorized use", the decisive factor was the defendant's intent (or lack thereof) as opposed to an assessment that actual harm had not been caused based on *objective* indicia: in *United States v. Czubinski*,[111] for example, the Court acquitted based on the government's failure to establish that the defendant "intended anything more than to satisfy idle curiosity".[112]

---

[103] The absence of 'harm-based' arguments is also apparent in legal scholarship. See, e. g., P. Murray, "Myspace-ing is Not a Crime: Why Breaching Terms of Service Agreements Should Not Implicate the Computer Fraud and Abuse Act", 29 Loy. L. A. Ent. L. Rev. 475 (2009), esp. at 482 *et seq*. [laying out a number of other arguments ranging from the plain statutory language to constitutional prohibitions].

[104] Subsequent to successive amendments (especially those that were enacted in 1996, 2001, and 2008, respectively).

[105] See use of the '$ 5,000 threshold' in other provisions of the statute, including those under § 1030(a)(2)(B)(iii), and (a)(4).

[106] See a discussion of possible justifications for the introduction of this 'threshold' in R. Skibell, 'Cybercrimes and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act', 18 Berkeley Tech. L. J. 909 (2003), esp. at pp. 913 *et seq*.

[107] *United States v. Middleton*, 231 F.3 d 1207 (9th Cir. 2000). The subsequent amendment of 18 USC § 1030(a)(5) by virtue of the 'PATRIOT ACT' in essence "codified" the holding of this case: see O. Kerr, *Computer Crime Law*[2], at 88.

[108] See, *inter alia*, *B & B Microscopes v. Armogida*, 532 F.Supp.2 d 744 (W.D. Pa. 2007); *United States v. Millot*, 433 F.3 d 1057 (8th Cir. 2006); *Nexans-Wires S. A. v. Sark-USA, Inc.*, 319 F.Supp.2 d 468 (S.D. N. Y. 2004).

[109] Not to mention the fact that the assessment of any cost in the event of an attempt would inevitably be purely hypothetical.

[110] *Cf. Carpenter v. US* [484 US 19 (1987)], in which the Supreme Court ruled that fraud does not *perforce* require actual monetary damage.

[111] *United States v. Czubinski*, 106 F.3 d 1069 (1st Cir. 1997).

[112] *Id*., at 1078.

(ii) The fact that cybercrime regulation is not 'result-driven' also creates certain complications in terms of applying the law to specific types of conduct. A case in point would be 18 USC § 1030(a)(5)(A)(i), which proscribes "knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer".[113] Aside from the problematic feature of recognizing 'dual' *mens rea* ("knowledge" as regards the transmission itself and "intent" as regards the damage),[114] problems have also arisen with respect to delineating the requisite *actus reus* for this offense, and specifically what constitutes a "transmission" within the meaning of the said provision.[115] In *United States v. Citrin*,[116] the court mulled over whether merely pressing the 'delete' key on the keyboard suffices *in lieu* of transmission, or whether additional acts might be required, such as installing a secure-erase program.[117] In a harm-based system, these issues would be dealt with in the context of the causation requirement, which would, among other things, also help in allocating liability between principals and accomplices in situations which entail the involvement of multiple actors.[118] In US case-law, causation hardly –if ever- comes up as a tool for properly delineating the proscribed conduct. On certain occasions, this has had the inevitable effect of construing the *actus reus*

[113] In the context of this particular provision, 'without authorization' refers to 'causing damage', not to the 'transmission' as such or obtaining access to a 'protected computer'. At first sight, it seems bizarre that the statute would allude to "damage without authorization", since authorized damage sounds like an unlikely occurrence. The drafters of the statute probably aimed at excluding cases of innocuous 'impairment' of data, such as encryption carried out by an employee upon authorization by the employer [absent authorization, the encryption *per se* would constitute prohibited 'damage' within the meaning of 18 USC § 1030(a)(5)(a)(i)]: see example in O. Kerr, *Computer Crime Law*[2], at 80.

[114] The term 'dual *mens rea*' is usually employed in the case of accomplice liability [see, e. g. T. Robinson, "A Question of Intent: Aiding and Abetting Law and the Rule of Accomplice Liability Under § 924(c)", 96 Mich. L. Rev. 783 (1997), at 788]. In the context of the present discussion, it is used to indicate that different parts of the *actus reus* are accompanied with a varying degree of requisite *mens rea*: specifically, the 'transmission' must be carried out 'knowingly', while the 'damage' (including the lack of authorization) must be intentional. See *United States v. Carlson*, 209 Fed. Appx. 181 (3rd Cir. 2006) [rejecting the defendant's claim that 'damage' was not caused intentionally].

[115] See O. Kerr, *Computer Crime Law*[2], at 95-96.

[116] *International Airport Centers v. Citrin*, 440 F.3 d 418 (7th Cir. 2006).

[117] See a characteristic part of the opinion written by Judge Posner: 'Pressing a delete or erase key in fact transmits a command, but it might be stretching the statute too far (especially since it provides criminal as well as civil sanctions for its violation) to consider any typing on a computer keyboard to be a form of 'transmission' just because it transmits a command to the computer.[…] If the statute is to reach the disgruntled programmer, which Congress intended by providing that whoever "*intentionally accesses* a protected computer without authorization, and as a result of such conduct, recklessly causes damage" violates the Act, it can't make any difference that the destructive program comes on a physical medium, such as a floppy disk or CD'.

[118] A pertinent category of cases would be those in which the person carrying out a *prima facie* unlawful 'hacking attack' does not coincide with those potentially benefiting from the act: a case in point would be the 'MBTA Case', where three students at the Massachusetts Institute of Technology (MIT) exposed a vulnerability in 'Charlie Card', i. e. the automated fare collection system used by the Massachusetts Bay Transportation Authority [MBTA]. The question that arose was whether disclosure of security flaws of a 'computer system' falls within the scope of the CFAA, and, if so, whether such conduct should be regarded as protected speech under the First Amendment. See the complaint filed on 8 August, 2008: *Massachusetts Bay Transportation Authority [plaintiff] v. Zack Anderson, RJ Ryan, Alessandro Chiesa, and the Massachusetts Institute of Technology [defendants]*, United States District Court, District of Massachusetts [available online at the EFF website: https://www.eff.org/sites/default/files/filenode/MBTA_v_Anderson/mbta-v-anderson-complaint.pdf (last visited on 20 August, 2013)]. The case was ultimately resolved through an out-of-court settlement.

very broadly, so as to bring within its ambit conduct that would have more effectively been dealt with in the context of 'indirect perpetratorship' or 'accomplice liability'.[119] In the *Eisenberg* Case,[120] for instance, the defendants mailed a floppy disk to the plaintiffs containing a program that damaged the plaintiffs' software. In view of the fact that the plaintiffs themselves had inserted the floppy disk into the disk drive and installed the program (unaware of its harmful nature), the Court came up with a broad interpretation of the notion of 'transmission': specifically, it held that the act of physically mailing the floppy disk amounted to 'transmission' within the meaning of 18 USC § 1030(a)(5), since it was accompanied with the intent to cause harm.[121] Thus, *mens rea* was effectively put to use as a substitute for the *actus reus* as opposed to an additional requirement being affirmed alongside the latter.[122]

(iii) A third example would be the position of courts *vis-à-vis* the so-called "special skill enhancement".[123] In a system fully subscribing to the 'harm principle', use of a special skill "in a manner that significantly facilitates the commission or concealment" of an offense would justify an adjustment of the sentence upwards on account of the increased dangerousness of the defendant (and the respective 'enhanced' risk to fundamental interests posed by the special skills possessed by the defendant).[124] US courts, on their part, have laid emphasis on the 'abuse of trust' inherent in situations entailing 'special skills'. In *United States v. Lee*,[125] for example, the Court of Appeals for the 9th Circuit –echoing previous case-law- associated the requisite "special skill" with some form of 'public trust' placed on the defendant.[126] Although certain scholars tend to classify this rationale as "retributive" because it insinuates some notion of 'special harm',[127] this is not the kind of retributivism

[119] The notion of 'indirect perpetratorship' has been developed in civil law systems [see T. Weigend, Germany, in K. Heller and D. Dubber (eds.), *The Handbook of Comparative Criminal Law*, Stanford University Press, 2011, pp. 265 *et seq.*], but traces thereof can be found in the Anglo-American criminal law system, in cases involving 'innocent agents'.

[120] *North Texas Preventive Imaging v. Eisenberg*, 1996 U. S. Dist. LEXIS 19990 (C.D. Cal. Aug. 19, 1996), SA CV 96-71 AHS (EEx).

[121] See *id*., part A and part C (Conclusion).

[122] One does not need to be a European 'formalist' to realize that this amounts to 'putting the cart before the horse' (and then letting the horse go!). Contrast that to *United States v. Morris*, 928 F.2 d 504 (2nd Cir. 1991), which in fact did the exact opposite, by affirming that the release of an internet worm was in breach of the CFAA despite the absence of an intent to cause harm.

[123] The 'special skill enhancement' is also referred to sometimes as 'special skill adjustment'.

[124] This would in turn mean that the affirmation of the 'special skill enhancement' in a particular case, and the attendant aggravation of the sentence, shall hinge on proof of a causal link between the skill and the unlawful result. In other words, unless the prosecution is able to prove that the special skill contributed in the harm (or at the very least the extent thereof), the 'special skill enhancement' will not apply (even in the presence of a special skill possessed by the defendant). This is a clear distinction between a 'harm-based' model and a system focusing on 'abuse of trust'.

[125] *United States v. Lee*, 296 F.3 d 792 (9th Cir. 2002).

[126] See, e. g., *United States v. Mainard*, 5 F.3 d 404 (9th Cir. 1993): 'In a sense, abuse of a special skill is a special kind of abuse of trust. It is a breach of the trust that society reposes in a person when it enables him to acquire and have a skill that other members of society do not possess. That special societal investment and encouragement allows a person to acquire *skills that are then held in a kind of trust for all of us*. When the person turns those skills to evil deeds, *a special wrong is perpetrated upon society*, just as other abuses of trust perpetrate a special wrong upon their victims'. [emphasis added]

[127] See O. Kerr, *Computer Crime Law*2, at 276.

associated with the 'harm principle' strictly construed.[128] In that regard, it is important to note that abuse of special skills is viewed from the defendant's –not the victim's- perspective.

One might be left with the impression that substantive criminal law in the US is –by virtue of its defining attributes- not fully aligned with fundamental principles aimed at protecting rights of the defense. Such an assumption would not be entirely accurate (although there is some truth in it).[129] It is important to note that 'deficiencies' arising out of imperfect substantive definitions are to a great extent counterbalanced by a number of safeguards traced in the criminal justice system viewed as a whole, including prosecutorial discretion, the ability of courts to in effect discharge quasi-regulatory duties, as well as certain constitutional guarantees, of which some word will be made in the next chapter.[130] Criminal prosecution of cybercrime offenses is thus less 'invasive' than one might conclude simply by looking at the way in which these types of conduct are proscribed.

2. The new EU Directive on Cybercrime

In contrast to the Anglo-American model, European criminal law has traditionally subscribed to theories of criminal punishment that take retributivism more seriously into account, influenced by the *Kantian* conception of punishment.[131] Intrinsically, then, the harm principle has always lain at the core of continental European criminal justice systems, as evidenced in such doctrinal concepts as the 'fundamental interest' ('*Rechtsgut*'), which has posed limitations on what States can criminally proscribe.[132] According to this approach, the mere fact that a certain type of conduct does not seem to carry any social or moral value is insufficient *per se* to justify resort to criminal legislation. Instead, the Legislature would have to identify –in a concrete fashion- the harm that a specific piece of legislation purports to avert, as well as explain that other means have proved (or would be) futile in addressing such harm (based on the so-called *ultima ratio* principle).[133] Even when resort to criminal law means is deemed necessary, the proportionality principle ensures that punitive response shall not be disproportionate to the harm. In many situations, European doctrine would arrive at the same solution as American pragmatism, but not necessarily based on the same

[128] One might indeed contend that the reasoning reflected in the passage from *United States v. Mainard* cited above almost smacks of 'communitarianism', since harm to the victim is identified with harm to society in a manner that has nothing to do with the victim's own interests.

[129] For a critique of the American criminal justice system through a historical account see W. Stuntz, *The Collapse of American Criminal Justice System*, Belknap Press of Harvard University Press, 2011, esp. at pp. 196 *et seq*., 244 *et seq*.

[130] *Infra*, under IV.

[131] That is not to say that every country in Europe has adopted a 'purely' retributivist criminal justice system. In fact, this is not even the case in Germany, which is the cradle of modern retributivism. See M. Dubber, "Theories of Crime and Punishment in German Criminal Law", 53 Am. J. Comp. L. 679 (2005) [discussing the merging of retributivist and consequentialist theories in German criminal law].

[132] The notion of '*Rechtsgut*' as a limiting factor of criminal law norms was analyzed by K. Binding, *Handbuch des Strafrechts*, vol. I, Leipzig, 1885 (for a definition of the notion see, e. g., at p. 169).

[133] For a discussion of the fundamental principles which should underline European legislation in the field of criminal law see European Criminal Policy Initiative, 'A Manifesto on European Criminal Policy', 4 ZIS 707 (2009), available online (in English) at: http://www.zis-online.com/dat/artikel/2009_12_383.pdf [last visited on 20 August, 2013].

line of reasoning: a case in point would be 'thought crimes' in the form of dissemination of ideas over the Internet. In the US, such conduct would be off-limits as regards criminal law, mainly based on arguments revolving around freedom of expression as enshrined in the 1st Amendment to the US Constitution.[134] In Europe, on the other hand, the same conduct would escape the ambit of criminal legislation due to the lack of apparent (and concrete) resulting harm, based on the principle *cogitationis poenam nemo patitur*.[135] This latter approach –if faithfully applied- tends to protect more effectively against over-criminalization. Indeed, the lack of requisite harm would preclude criminalization even when it comes to conduct that falls within the ambit of one of the exceptions to the 1st Amendment (such as obscenity).[136] Moreover, strict adherence to the proportionality principle would ensure that criminal conduct in cyberspace does not receive harsher sentences compared to the same type of conduct when committed in the 'real world'.[137]

One can easily understand that, by adhering to these principles, European *substantive* criminal law is less 'expansive' than its US counterpart. Whereas the reach of the criminal justice system in the US is confined by the procedural guarantees mentioned above, the 'limiting principle(s)' in European criminal law is factored into the substantive part. Removing such factor would expose the defendants to potential abuses, absent any meaningful procedural safeguards. This is precisely why it is imperative to preserve the 'harm-based' character of substantive criminal law in Europe.

Yet EU legislation on cybercrime seems to distance itself from these time-honored principles underlining criminal law across the continent. Regrettably, criminalization seems to rely less on substantive criteria and more on 'procedural' needs, such as the approximation of domestic laws for the purpose of facilitating mutual legal assistance and extradition between member States.[138] While there is nothing wrong about enhancing judicial cooperation in the above sense, the absence of a principled method of sorting out conduct that deserves criminal punishment is bound to lead to a 'least common denominator' in terms of safeguarding civil liberties. This tendency, which first emerged in the context of EU legislation on terrorism and organized crime,[139] is now being transferred to the

[134] See, *inter alia*, S. Gellman, 'Sticks and Stones Can Put You in Jail, But Can Words Increase Your Sentence? Constitutional and Policy Dilemmas of Ethnic Intimidation Laws', 39 UCLA L. Rev. 333 (1991), esp. at 362 *et seq*.

[135] See, *inter alia*, C. von Bar *et al*. [transl. by T. Bell], *A History of Continental Criminal Law*, The Lawbook Exchange, 1999, p. 522.

[136] Admittedly, there have been voices calling for a new approach on 'obscenity standards' in the US ever since the advent of the worldwide web. See, *inter alia*, D. Burke, 'Cybersmut and the First Amendment: A Call for a New Obscenity Standard', 9 Harv. J. L. & Tech. 87 (1996).

[137] For an outline of the various ways to assess harm caused by cybercrime see S. Brenner, *supra* n. 88, esp. at pp. 32 *et seq*. [distinguishing between 'individual harm', 'systemic harm', and 'inchoate harm' cybercrimes].

[138] See P. Caeiro, Commentary on the 'European Touch" of the Comparative Appraisal, in A. Klip (ed.), *Substantive Criminal Law of the European Union*, Maklu Publishers, 2011, pp. 123 *et seq*. Interestingly, the European Court of Justice [ECJ] has upheld the need for mutual recognition even in the absence of prior approximation: see Joined Cases C-187/01 and C-385/01 *Hüseyin Gözütok and Klaus Brügge*, [2003] ECR I-1345, at § 32.

[139] See, e. g., W. de Bondt and G. Vermeulen, Appreciating Approximation: Using Common Offence Concepts to Facilitate Police and Judicial Cooperation in the EU, in M. Cools, S. de Kimpe, B. de Ruyver and M. Easton (eds.), *Readings on Criminal Justice, Criminal Law & Policing*, Maklu Publishers, 2009, pp. 15 *et seq*.

combating of cybercrime, as demonstrated in the pertinent newly-adopted directive.[140]

The European Commission brought its proposal for a new directive on cybercrime because it considered that the 2005 Framework Decision on Attacks against Information Systems was insufficient to address large-scale cyber-attacks, even coupled with the Convention on Cybercrime.[141] To a large extent, those 'deficiencies' were deemed to arise out of the lack of adequate *substantive* definitions.[142] Accordingly, directive 2013/40/EU brings about changes as regards a number of aspects pertaining to substantive criminal law: the special part, through the broadening of existing definitions as well as the introduction of new offenses under Articles 6 and 7;[143] the general part, through the broadening of accomplice liability under Article 8;[144] and sentencing, through the recognition of new aggravating circumstances under Article 9.[145] Five points should be made in that regard. Specifically:

(a) Directive 2013/40/EU mandates the introduction of a novel offense entitled "illegal interception of computer data".[146] It is quite striking that the directive –just like the Convention on Cybercrime- stops short of delimiting the notion of 'interception'. Moreover, it goes even beyond the scope of the Convention on Cybercrime, as the latter only proscribed 'illegal interception' committed "with dishonest intent" or in relation to computer systems that are part of a network.[147] Of course, the use of vague terms is not infrequent in the context of international conventions. Nonetheless, the 'new generation' of directives introduced by virtue of Article 83 of the TFEU have to include "minimum elements" adequately describing the *actus reus* and *mens rea* of each criminal offense.[148] Apparently, expanded authority comes with increased responsibility that the EU does not seem prepared to discharge.

(b) Perhaps the most controversial provision in the directive is Article 7, proscribing "the production, sale, procurement for use, import, distribution or otherwise making available of tools used for committing offenses" included in the

[140] See discussion *infra*.

[141] See Proposal for a Directive on Cybercrime, at 4.

[142] According to the European Commission, the reason for the adoption of a new directive is 'the emergence of large-scale simultaneous attacks against information systems and the increased criminal use of the so-called "botnets"' since the enactment of the 2005 Framework Decision: see *id*., at 2.

[143] In addition, that is, to those already proscribed under existing legislation, namely 'illegal access to information systems' under Article 3; 'illegal system interference' under Article 4; and 'illegal data interference' under Article 5.

[144] Such 'broadening' in essence occurs because of the fact that Article 8(1) requires member States to extend accomplice liability so as to cover even the inchoate offense proscribed under Article 7.

[145] Articles 10 and 11 relate to the liability of legal persons (the latter contains penalties to be assessed against legal persons that have engaged in the activities proscribed under the directive).

[146] See Article 6.

[147] The Presidency's Proposal to the Council [8795/11 DROIPEN 27 TELECOM 43 CODEC 609 of 8 April 2011 (hereinafter 'Presidency's Proposal')] narrowed the scope of the proposed provision by excluding so-called "minor cases" from its ambit (at 27). Such exemption has thus made its way into the text adopted.

[148] That the *lex certa* requirement shall underline directives issued under Article 83 TFEU has been emphasized by, *inter alia*, the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament: see C. de Jong, Draft Report on an EU Approach in Criminal Law [2010/2310 (INI)], 8 February 2012, at 3 [*cf*. Preamble, pts. H and I].

directive.[149] These so-called 'hacking tools' include (i) "a computer program, designed or adapted primarily for the purpose of committing any of the offenses referred to in Articles 3 to 6 [of the directive]; and (ii) "a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed".[150] The EU seems to be less cautious than the Council of Europe in this respect.[151] Specifically, there are at least three differences between the Council of Europe Convention on Cybercrime and the provisions in question: first of all, the Convention on Cybercrime allows State parties to insert a 'minimum gravity' requirement in criminally proscribing conduct related to hacking tools;[152] secondly, it provides that criminal liability shall not be imposed where "the production, sale, procurement for use, import, distribution or otherwise making available or possession of tools is for the purpose of authorized testing or protection of a computer system";[153] thirdly, it permits State parties to exclude 'tools' which are non-threatening *per se* from the ambit of criminalization.[154] None among these limitations have been adopted by the European Commission, leaving the interpretation of this new offense susceptible to entirely subjective criteria.[155] That being noted, there are two limitations that –albeit absent from the Commission's proposal- were introduced in the final text of the directive: (a) mere "possession" of hacking tools is not proscribed; (b) the enumeration of hacking tools as such is confined to computer programs, passwords, access codes, or similar data, as opposed to the potentially limitless array of devices that were included in the proposal (which would have rendered article 7 a 'sweeping' provision).

(c) Even with respect to already existing offenses, the directive seems to be exceeding the limits of judicious lawmaking. With respect to the offense of "illegal access to information systems" (i.e. the equivalent of "unauthorized access" under the CFAA),[156] it divests member States of any discretion in introducing limiting factors of their own choice,[157] such as the requirement of infringement of security

[149] As noted above, this offense is not proscribed under either the Convention on Cybercrime or the 2005 Framework Decision.

[150] The lack of a consensus on the proposed directive was largely due to the 'sweeping' character of this provision. See some pertinent preliminary comments on Article 7 of the proposed directive in the Presidency's Proposal, at 17.

[151] See a critical appraisal of the provision (as included in the Commission's proposal) in M. Kaiafa-Gbandi, "Criminalizing Attacks against Information Systems in the EU: The Anticipated Impact of the European Legal Instruments on the Greek Legal Order", 20 European Journal of Crime, Criminal Law and Criminal Justice 59 (2012), pp. 67 *et seq*.

[152] See Article 6(1)(b) *in fine* of the Cybercrime Convention: 'A Party may require by law that *a number of such items be possessed* before criminal liability attaches'.[emphasis added]

[153] See Article 6(2) of the Convention on Cybercrime.

[154] *Id*., Article 6(1).

[155] As noted above [*supra* n. 150], this is the primary reason for the lack of consensus on this particular provision: see Presidency's Proposal, at 6.

[156] See O. Kerr, *Computer Crime Law*², pp. 26 *et seq*.

[157] During the debate on the Commission's proposal, it was argued that the exclusion of 'minor cases' from the ambit of the directive could serve as a substitute for other limiting factors. On this argument see D. Brodowski, 'Strafrechtsrelevante Entwicklung in der Europäischen Union – ein Überblick', 5ZIS 753 (2010). *Contra*, however, M. Kaiafa-Gbandi, *supra* n. 151, at 65 [noting that the clause excluding 'minor cases' is also present in the 2005 Framework Decision, alongside the limiting clause concerning 'infringement of security measures', which signifies the distinct character of the two clauses].

measures.[158] This is not only in stark contrast to both the Convention on Cybercrime[159] and the 2005 Framework Decision,[160] but is also bound to create some confusion, as several member States already have pertinent definitions in place, which they will now be hard-pressed to amend. In addition, the new directive eliminates the requirement of 'dishonest intent', thus proscribing even 'harmless' conduct, such as intrusions meant to expose weaknesses in a given computer system.[161] Last but not least, the notion of committing every pertinent offense under the directive "without right" is now defined as "access […] not authorized *by the owner* or by *another right holder of the system* or of part of it, or not permitted under national law" (emphasis added).[162] It becomes evident that the said provision opens a window of opportunity for the *contractual* delimitation of the substantive content of criminal law provisions, at a time when US case-law seems to be moving in the exact opposite direction, namely to leave mere breaches of terms of service outside the scope of the CFAA.[163]

(d) Amendments pertaining to the 'general part' of criminal law also attest to the distance between the directive and the harm principle. Article 8 § 1 concerning accomplice liability is overly broad, and proscribes aiding and abetting even to the offense of Article 7. Considering that the procurement of hacking tools is *itself* a preparatory act, unconnected to actual harm, it becomes clear that recognition of complicity thereto stretches criminal liability in such a manner as to cover even ordinary commercial activity.[164] Moreover, Article 8 § 2 mandates the criminalization of attempt in the event of an offense referred to in Articles 4 and 5.[165] Thus, member States will no longer retain discretion to introduce 'qualified' attempted liability, which was the case under both the Convention on Cybercrime and the 2005 Framework Decision.[166] These changes are indications of a 'fragmentation'

---

[158] See the Presidency's Proposal, at 26 [recommending that the said requirement be inserted in the directive].

[159] See Article 2 of the Convention on Cybercrime, entitled 'Illegal access'.

[160] See Article 2 of the Framework Decision, entitled 'Illegal access to information systems'.

[161] This problem had been identified in the Explanatory Report by the Council of Europe (accompanying the Convention on Cybercrime). The Explanatory Report is available online at: http://conventions.coe.int/treaty/en/reports/html/185.htm [last visited on 20 August, 2013]. Specifically, paragraph 49 reads: 'Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the *detection of loopholes and weaknesses of the security of systems*. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the OECD Working Party in 1985'. [emphasis added]

[162] See Article 2(d) of the directive.

[163] See *United States v. Nosal*, *supra* n. 100.

[164] Note an interesting discussion of the practical significance of 'sweeping' statutory provisions proscribing even routine Internet usage in O. Kerr, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes', 78 NYU L. Rev. 1596 (2003), p. 1617, esp. at n. 87. Kerr notes that the mere existence of a statutory provision "on the books" does not necessarily mean that actual prosecutions based thereupon will occur in practice, as prosecutors are not likely to bring charges for 'innocuous' Internet use. This may be true in a criminal justice system based on prosecutorial discretion, such as the US one; however, European criminal justice systems generally do not know of prosecutorial discretion. Therefore, the existence of a sweeping provision 'on the books' is much more likely to bring about criminal prosecutions in actual practice.

[165] Unlike the Commission's proposal, the final text of the directive does not require member States to criminalize attempt when it comes to the offenses proscribed under Articles 3 and 6. Criminally proscribing attempt of an inchoate offense such as that introduced by Article 7 of the directive was considered farfetched even by the drafters of the initial proposal.

[166] See Article 11(2) and (3) of the Convention on Cybercrime; *cf.* Article 5(2) and (3) of the 2005 Framework Decision.

trend developing in EU criminal law: unlike traditional criminal law, according to which all offenses were subject to the same norms when it came to the general part, the way in which the EU legislates creates distinct 'clusters' of rules depending on each offense. Thus, certain types of crime –including terrorism, organized crime, and cybercrime- are being subjected to special rules concerning attempt, accomplice liability, and other aspects of the general part of criminal law.[167]

(e) Finally, the directive's provisions on sentencing are incompatible with the European model of criminal sentencing. For the first time, the EU is making use of its newly-acquired authority to determine sentences by setting a minimum of a two-year imprisonment (leaving member States free to determine stricter sentences at their discretion).[168] Such minimum sentences are imposed indiscriminately, without regard to the extent of harm brought about by each cyber-attack. This is at odds with the principle of proportionality, which would require a varying assessment of the sentence based on each particular offense.[169] It is noteworthy that the lack of flexibility in sentencing is also demonstrated in the sections concerning aggravated circumstances,[170] which mandates a minimum sentence of five years regardless of the underlying offense and the particular aggravating circumstance in each case.

IV. On the significance of 'constitutional' restraints

1. The practicalities of free speech

Evidently, the harm principle, which has always served as a limiting factor in European criminal law, does not seem to have a meaningful impact on the way in which the EU is approaching criminal activity in cyberspace. One might argue that this would bring the European approach "on a par" with US regulation of cybercrime. However, such a position would fail to take into account the central role played by fundamental rights in the US legal system. For the purposes of substantive law, it is in order to explain the limiting role played by freedom of expression.

Free speech has always occupied a central position in the US legal system, including criminal law. The United States Supreme Court has construed freedom of expression very broadly under the First Amendment, in a manner that elevates it to a cornerstone of the Constitution prevailing over other democratic values (including equality).[171]

---

[167] See J. Vervaele, Special Procedural Measures and the Protection of Human Rights, General Report for the Third Section of the XVIII[th] International Congress on Criminal Law of the AIDP [discussing the matter from a human rights perspective]. The Report is available online at: http://www.utrechtlawreview.org/index.php/ulr/article/viewFile/103/103 [last visited on 20 August, 2013].

[168] See Article 9(2) of the Directive.

[169] The principle of proportionality is explicitly enshrined under Article 49(3) of the EU Charter of Fundamental Rights. See M. Böse, 'The Principle of Proportionality and the Protection of Legal Interests', 1 European Criminal Law Review 34 (2011) [identifying the protection of 'legal' (fundamental) interests and the *ultima ratio* principle as 'sub-principles' of proportionality].

[170] See, e. g., Article 9(4) of the Directive.

[171] See R. Sedler, "An Essay on Freedom of Speech: The United States Versus the Rest of the World", Mich. St. L. Rev. 377 (2006), p. 379.

This treatment of the right is unique to the American environment, and distinguishes US law from both the domestic law of other countries and international instruments recognizing freedom of expression.[172] Certainly, there are historical and cultural reasons explaining the US attitude *vis-à-vis* freedom of expression, which have found their way into the legal realm.[173] 'Content neutrality' has become central to US case-law on the First Amendment, based on the idea that society must encourage the free development of a "marketplace of ideas", which will enable users to sort out benign and malicious content for themselves.[174] This is clearly a culture favoring open criticism over government-imposed "silence", and it seems to fit with the exigencies of cyberspace.

First Amendment protection has a substantive as well as a procedural prong.[175] An example of the First Amendment's substantive reach is the absence of a general rule allowing for the prohibition of 'hate speech', owing to the fact that even offensive speech is protected under the First Amendment.[176] Therefore, unlike most parts of the world, the fact that certain groups of people (whether ethnic, racial or religious) claim to be offended by instances of hate speech would *per se* be inadequate to limit speech.

In terms of the judicial process, the procedural prong is equally –if not more- important than the substantive one, since it has 'endowed' legal practice with the tools to stop censorship in its tracks. One of these tools is the 'prior restraint' doctrine,[177] which effectively precludes the *a priori* imposition of censorship.[178] The said doctrine applies even in the event of prior restraints to *prima facie* illicit content. In *Center for Democracy and Technology v. Pappert*,[179] for instance, it was held that the Pennsylvania Internet Child Pornography Act, which required ISPs to block access to websites allegedly hosting child pornography, was unconstitutional.[180] Clearly, then, the legal environment has created a presumption in favor of freedom of expression[181] (hence against the validity of any statute that restricts freedom of expression). In contrast to this picture, several legal systems around the world effectively impose an opposite presumption on ISPs: since the dissemination of

[172] See D. Nunziato, "How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide", 42 Geo. J. Int'l L. 1123 (2011).

[173] See a pertinent analysis by R. Krotoszynski, Jr., *The First Amendment in Cross-Cultural Perspective: A Comparative Legal Analysis of the Freedom of Speech*, NYU Press, 2009, esp. at pp. 12 *et seq*., 214 *et seq*.

[174] The metaphor of a 'marketplace of ideas' was coined by Justice Holmes, in his famous dissent [in which he was joined by Justice Brandeis] in *Abrams v. United States*, 250 US 616 (1919), at 630.

[175] See D. Nunziato, *supra* n. 172, at 1125-1126 [arguing that foreign legal systems would be more conducive to the adoption of the 'procedural' safeguards of the First Amendment as opposed to the 'substantive' ones].

[176] In *Texas v. Johnson*, 491 US 397, 414 (1989), the Supreme Court proclaimed, in no uncertain terms, the following: 'If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable.'

[177] See, *inter alia*, M. Redish, "The Proper Role of the Prior Restraint Doctrine in First Amendment Theory", 70 Va. L. Rev. 53 (1984).

[178] But for the presence of very strict requirements, such as precise definition of regulated speech; transparency; and providing a right to an appeal [see D. Nunziato, *supra* n. 172, at 1128-1129].

[179] *Center for Democracy & Technology et al. v. Pappert*, 337 F.Supp.2 d 606, 655 (E.D. Pa. 2004).

[180] Especially in view of the fact that no meaningful judicial review was allowed under the statute in question [*ibid*.].

[181] See R. Dworkin, "Is There a Right to Pornography?", 1 Oxford Journal of Legal Studies 177 (1981).

information is regarded as a 'public function' (*ergo* a privilege as opposed to a right), it only seems 'natural' to request some form of public certification of the content's legality.[182] It is no wonder, then, that even Western European States have consistently engaged in preventive censorship with the declared goal of preventing the use of the Internet for the dissemination of illicit content.[183]

Another procedural restraint that is unique to the American legal system is the "State action" doctrine,[184] which prevents the government from delegating its powers to nominally private entities so as to evade its responsibilities under the First Amendment.[185] The application of this doctrine in actual practice creates a number of problems, and there have been many critics of the concept itself.[186] However, even a 'thin' version of the doctrine –were it available in Europe- would suffice to outlaw comprehensive filtering systems such as the "Cleanfeed" system,[187] which blocks access of British users to any website that has been added to a black list compiled by the Internet Watch Foundation (IWF).[188]

All in all, one might conclude that the way in which courts have applied the 1st Amendment in cybercrime cases has effectively had an equivalent 'limiting' impact compared to the 'harm principle' as reflected in European criminal statutes.[189] Even the interpretation of exceptions to free speech under the 1st Amendment seems to neatly accommodate such limiting effect. In *United States v. Alkhabaz*,[190] for instance, the Court of Appeals for the 6th Circuit defined the notion of "true threat"

[182] The allocation of the burden of proof in defamation cases appears to reflect this 'reverse' presumption. See, for instance, the case of *Herrera Ulloa v. Costa Rica*, 2004 Inter-Am. Ct. H. R. (Ser. C) No. 107, 135 (Jul. 2, 2004): the case concerned a Costa Rican journalist who was convicted for defamation because he had published allegations against a public figure in a newspaper. Publishing this sort of information entailed bearing the attendant burden of proof, even if the journalist had published both sides of the story. Such burden of proof derives from the 'privileged' nature of public speech. See J. Pasqualucci, "Criminal Defamation and the Evolution of the Doctrine of Freedom of Expression in International Law: Comparative Jurisprudence of the Inter-American Court of Human Rights", 39 Vand. J. Transnat'l L. 379 (2006).

[183] Member States of the Council of Europe have gone as far as to 'filter' Internet content that they deem harmful for society (or the government). In the past, Switzerland has restricted access to websites featuring political content: see http://www.edri.org/edrigram/number2/censor [last visited on 20 August, 2013]. Turkey, on its part, has repeatedly restricted access to YouTube because certain users uploaded content targeted against the founder of the Turkish State: see http://opennet.net/research/profiles/turkey [last visited on 20 August, 2013].

[184] See W. Huhn, "The State Action Doctrine and the Principle of Democratic Choice", 34 Hofstra Law Review 1379 (2006).

[185] P. Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation', 71 U. Co. L. Rev. 1263 (2000).

[186] See, *inter alia*, M. Phillips, 'The Inevitable Incoherence of Modern State Action Doctrine', 28 St. Louis U. L. J. 683 (1984); also see C. Black's famous aphorism, characterizing State actions as a 'conceptual disaster area': C. Black, 'The Supreme Court, 1966 Term – Foreword: "State Action", Equal Protection, and California's Proposition 14', 81 Harv. L. Rev. 69 (1967), at 95.

[187] 'Cleanfeed' is a filtering system operated by British Telecom, which is formally a private corporation. For a description of how it operates see D. Nunziato, *supra* n. 172, at 1136 *et seq*.

[188] Although 'Project Cleanfeed' started off as an effort to regulate child pornography on the Internet, it has been expanded so as to filter hate speech, including racist content, and even (legal) adult pornographic material. The State action doctrine would not allow this in the US, notwithstanding the nominally private character of the entity operating the system [see, e. g., *Marsh v. Alabama*, 326 US 501 (1946), setting aside the 'formal' distinction between the public and the private sphere, and looking at the ability of the entity in question to exercise 'power' for the purpose of applying First Amendment protection].

[189] See *supra*, under III/2.

[190] *United States v. Alkhabaz*, 104 F.3 d 1492 (6th Cir. 1997).

with reference to both the *actus reus* and the *mens rea* of the offense proscribed under 18 USC § 875(c) in the following words:[191]

'To achieve the intent of Congress, we hold that, to constitute "a communication containing a threat" under Section 875(c), a communication must be such that a reasonable person (1) would take the statement as a serious expression of an intention to inflict bodily harm (the mens rea), and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the actus reus)'

To be sure, this line of reasoning has been more prevalent in offenses against persons (threats, harassment, etc.) as opposed to 'obscenity' crimes, such as those proscribed under 18 USC § 1462[192] or 18 USC § 1465.[193] Even in this latter category, however, the analytical approach adopted by courts consistently takes into account the need to *justify* limitations on free speech, whether based on the "patently offensive" character of the material in question or a proper construction of "community standards".[194]

2. A European 'privilege'

In continental Europe, on the other hand, freedom of speech is generally easier to 'override', which reduces its limiting effect on criminal law. Indeed, most European jurisdictions criminalize not only 'harmful speech' in the strict sense understood by US courts, but extend criminal prohibitions so as to cover 'offensive speech' in more general terms, including such cases as Holocaust denial, xenophobic speech, and so forth.[195] A number of reasons have been suggested to explain this approach: first of all, bitter experience from World War II has instilled fear of 'incendiary words' in the European 'collective sub-conscious';[196] secondly, 'rights discourse' in Europe has traditionally favored the natural origin of rights or entitlements which are in conflict with free speech (to the detriment of the latter): a case in point would be author's rights (*droits d' auteur*), which have been construed so as to encourage very tight copyright regulations, unmitigated by the utilitarian concerns raised in the Anglo-American environment;[197] thirdly, European courts have generally been reluctant to apply freedom of speech "horizontally", i. e. in the relations between citizens.[198] This approach does not leave much room for the use of freedom of speech as an analytical tool in adjudicating criminal offenses against individuals or copyright infringements.

---

[191] *Id*., at 1495.

[192] 'Importation or transportation of obscene matters'.

[193] "Production and transportation of obscene matters for sale or distribution".

[194] See, e. g., *United States v. Extreme Associates, Inc.*, 2009 US Dist. LEXIS 2860 (W.D. Pa. Jan. 15, 2009).

[195] For an overview of the typology of prohibited speech see I. Hare and J. Weinstein, *Extreme Speech and Democracy*, Oxford University Press, 2010 [see, e. g., pp. 511 *et seq*. on issues pertaining to 'Holocaust denial'].

[196] F. Schauer, Social Epistemology, Holocaust Denial, and the Post-Millian Calculus, in M. Hertz and P. Molnar (eds.), *The Content and Context of Hate Speech: Rethinking Regulation and Responses*, Cambridge University Press, 2012, p. 129.

[197] P. Hugenholtz, Copyright and Freedom of Expression in Europe, in R. Dreyfuss, H. First and D. Zimmerman (eds.), *Expanding the Boundaries of Intellectual Property*, Oxford University Press, 2001, pp. 343 *et seq*.

[198] *Ibid*.

The diverging approach *vis-à-vis* free speech on the two sides of the Atlantic becomes demonstrable in situations like the one which arose in the *Yahoo!* Case.[199] Two organizations dedicated to the fight against racism and anti-semitism sued both "*Yahoo!, Inc.*" and "*Yahoo! France*", alleging that the two companies had violated French criminal law by facilitating the auction of Nazi propaganda items through their web service.[200] In its initial judgment, the French Court found that the two Internet Service Providers had violated French law, and ordered them, *inter alia*, to block promotion of Nazi-related products via their online service, as well as warn users of the potential dangers arising out of the act of logging on to pertinent websites.[201] The ISPs argued that such judgment would have a chilling effect on the users' freedom of expression, and could in any event not be enforced in the US, i. e. the country where the services were primarily provided (at least as far as "*Yahoo!, Inc.*" was concerned).[202] However, the Paris Court found that the question of enforcement did not have any bearing whatsoever on the question of jurisdiction, and asserted that freedom of expression as understood under the US Constitution was irrelevant, as US law was not controlling in this case.[203] Rather, limiting free speech to preserve "French public order" (*ordre public*) was regarded as the optimal solution.

The backlash brought about because of the *Yahoo!* Case did not seem to modify the attitude of French courts. More recently, in the case of *UEJF et al. v. Free, AOL et al.*,[204] the French *Tribunal de Grande Instance* upheld the claim made by the plaintiffs to the effect of enjoining a number of ISPs from providing access to a website featuring "racist, anti-Semitic and revisionist" content. The court deemed the measure imposed to be proportionate to the goal it purported to serve, as it would only affect French users, while access would be restricted to just one website.[205]

Court decisions are not the only source of friction between divergent approaches to freedom of expression. The difference in attitude became apparent during the discussions leading to the adoption of the Cybercrime Convention. Negotiating parties were divided as to whether the Convention should proscribe the dissemination of racist or xenophobic material over the Internet.[206] In the end, a compromise

---

[199] *LICRA and UEJF v. Yahoo! Inc. and Yahoo France*, Tribunal de Grande Instance de Paris, Order of November 20, 2000: see unofficial English translation of the order online, at http://www.lapres.net/yahen11.html [last visited on August 20, 2013].

[200] Specifically, the provision allegedly violated was Section 645-1 of the French Penal Code.

[201] For a complete account of the facts of this case see C. Ku and P. Diehl (eds.), *International Law: Classic and Contemporary Readings*, Lynne Rienner Pub., 3rd ed., 2008, pp. 457 *et seq*.

[202] See M. Greenberg, 'A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market', 18 Berkeley Tech. L. J. 1191 (2003), at pp. 1231 *et seq*.

[203] See H. Muir-Watt, 'Yahoo! Cyber-Collision of Cultures: Who Regulates?', 24 Mich. J. Int'l L. 663 (2003), at p. 685.

[204] *UEJF et al. v. Free, AOL et al.*, Tribunal de Grande Instance de Paris Ordonnance de référé 13 juin 2005, available online (in French) at: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1443 [last visited on 20 August, 2013].

[205] *Ibid*.

[206] See I. Guardans, Report of the Committee on Legal Affairs and Human Rights, 5 September 2002, explicitly stating the irreconcilable views. The document is available online at: http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc02/EDOC9538.htm [last visited on 20 August, 2013].

was arrived at, leading most European State parties to sign and ratify an Additional Protocol to the Cybercrime Convention,[207] which encompassed provisions on hate speech, racism and xenophobia. Predictably, the US did not sign this Protocol (nor did the United Kingdom and Ireland).[208] The Protocol came into effect in 2006.[209]

The cases cited above have been widely criticized as unfortunate examples of European States attempting to impose their own cultural values on a global medium, paying no heed to the reasonableness –or even the practicability- of such endeavor.[210] For the purposes of this discussion, this serves as a reminder that broad criminal provisions are much more likely to have a chilling effect in Europe (compared to the US), due to the absence of adequate 'constitutional' safeguards of free speech.

3. Two versions of 'balancing'

To a greater or lesser extent, the difference between the European and the American approach to freedom of expression can be explained based on the historical and cultural reasons mentioned above.[211] For the purposes of the present discussion, however, it is important to conceptualize the issue on somewhat different terms.

To begin with, there is a notable difference in the way in which the right itself is being phrased. Under the First Amendment to the US Constitution, "Congress shall make no law […] abridging the freedom of speech".[212] Thus worded, freedom of expression seems to be almost absolute in nature, unqualified by competing rights. Although practice shows that the right is not absolute,[213] the language employed to frame it engenders –as stated above- a clear presumption that is very difficult to override.[214]

On the contrary, the recognition of freedom of expression in Europe is much more 'reserved' to begin with. Most European Constitutions contain 'built-in' limitations or even concrete exceptions to free speech, usually based on some competing right that is thus elevated to a superior status. The language of Article 10 of the European Convention on Human Rights[215] is quite representative of the

[207] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, available online at: http://conventions.coe.int/Treaty/en/Treaties/html/189.htm [last visited on 20 August, 2013].

[208] The only non-European countries to have signed this Protocol are Canada and South Africa (in 2005 and 2008, respectively).

[209] Also see J. Clough, *Principles of Cybercrime*, Cambridge University Press, 2010, pp. 108 *et seq*.

[210] See M. Greenberg, *supra* n. 202. The dispute was subsequently brought before US courts, which dealt, among other things, with constitutional issues arising under the First Amendment: see *Yahoo! I*, 145 F. Supp. 2 d, 1168 (N. D. Cal. 2001); *Yahoo! II*, 169 F. Supp. 2 d 1181 (N.D. Cal. 2001).

[211] *Supra*, under IV/2.

[212] The Supreme Court has clarified that the prohibition applies equally to States: see, e. g., *Gitlow v. New York*, 268 US 652 (1925).

[213] See H. Cohen, 'Freedom of Speech and Press: Exceptions to the First Amendment', CRS Report for Congress, October 16, 2009. The Report is available online at: http://www.au. af.mil/au/awc/awcgate/crs/95-815.pdf [last visited on 20 August, 2013].

[214] *Supra*, under IV/1.

[215] European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, available online at: http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7 a/0/englishanglais.pdf [last visited on 20 August, 2013].

European approach. Clearly, this latter provision does not merely confine itself to recognizing the right; rather, it proceeds to a 'balancing'[216] that immediately enfeebles it.[217] Such balancing takes place on three levels in the context of paragraph 2: first of all, the provision states the form of the limitations that may be imposed to free speech ("formalities, conditions, restrictions or penalties");[218] secondly, it sets the conditions under which such limitations shall apply (they have to be "prescribed by law", have a "legitimate aim", and be "necessary in a democratic society");[219] last but not least, it juxtaposes freedom of expression with its competing rights and interests ("the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary").[220]

Needless to say, some of the competing interests outlined in Article 10 of the European Convention on Human Rights (though not very many of them) are also present in the discourse taking place before US courts.[221] Note, however, the methodological difference: in the US, these competing interests will be taken into account in order to delimit the right *in the first place*. For instance, the dissemination of child pornography is not regarded as an expression of free speech within the meaning of the First Amendment for reasons related to crime prevention and public morals.[222] However, once the delimitation has taken place –a process that is based on clear rules refined by case-law over a period of decades- the right as such is unyielding, regardless of the exigencies of a given situation.[223] In contrast, the European approach requires that 'balancing' take place each and every time in light

[216] On the role of the 'margin of appreciation' (as recognized by the European Court of Human Rights) see *infra*, in this chapter.

[217] Also note the presence of an 'abuse clause' in the European Convention on Human Rights [article 17], which may further limit freedom of expression in cases that can be classified as an '*abus de droit*'. On this issue see H. Cannie and D. Voorhoof, 'The Abuse Clause and Freedom of Expression in the European Human Rights Convention: An Added Value for Democracy and Human Rights Protection?', 29 Netherlands Quarterly of Human Rights 54 (2011) [arguing *against* the application of the abuse clause in order to limit freedom of expression under article 10 ECHR].

[218] For instance, criminally proscribing the dissemination of specific content on the Internet would amount to a "penalty" within the meaning of Article 10 ECHR.

[219] The bulk of legal issues arising before the European Court of Human Rights relate to whether these three (cumulative) conditions have been met.

[220] 'Prevention of disorder or crime' *prima facie* appears to be very open-ended, or even a 'self-serving' clause (since the State can classify any type of conduct as criminal so as to invoke it). This is why applying a 'proportionality test' is indispensable to safeguard the hard core of the right: see, *inter alia*, L. Bachmaier Winter, "The Role of the Proportionality Principle in Cross-Border Investigations Involving Fundamental Rights", in S. Ruggeri (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, Springer, 2013, p. 85.

[221] See, e. g., *Miller v. California*, 413 US 15 (1973) [discussing obscenity].

[222] One of the explanations offered is the so-called 'proxy rationale' [see O. Kerr, *Computer Crime Law*², at 216 *et seq*.]; see an attempt at a rationalization of the receipt/possession distinction by Judge Posner in *United States v. Richardson*, 238 F.3 d 837 (7th Cir. 2001), at 839 ["receivers increase the market for child pornography and hence the demand for children to pose as models for pornographic photographs; possessors, at least *qua* possessors, as distinct from receivers, though most of them are that too, do not"].

[223] F. Schauer, Freedom of Expression Adjudication in Europe and the United States: a case study in comparative constitutional architecture, in G. Nolte (ed.), *European and US Constitutionalism*, Cambridge University Press, 2005, pp. 49 *et seq*.

of the circumstances of the case before the court. This has been aptly described as a two-tier process:[224] during the first stage, the right is delimited; subsequently, it is weighed up against its competing interest(s) in order to determine whether a given limitation (e.g. in the form of a criminal sentence) is warranted. At the outset of this process, freedom of expression will be placed on an equal footing with its competing interest at best, making it no more likely that it will prevail than the latter. In sum, courts are given two opportunities to restrict the right, and practice shows they do not hesitate to make ample use thereof.

Needless to say, it is virtually impossible to unilaterally impose restrictive rules over cyberspace activity without having an impact on individuals abroad. However, such extraterritorial effect does not seem to be of particular concern to European courts either. This became apparent in the case of *Perrin v. United Kingdom*,[225] decided by the European Court of Human Rights. A British court had convicted a French national for publishing obscene material on a US website. After exhausting local remedies, the defendant submitted an application to the ECHR, claiming that the UK had violated his rights under Article 10 of the European Convention on Human Rights. The Court rejected the arguments by making a number of important observations: *first of all*, it noted that the defendant should have anticipated that British law would be enforced against him despite the fact that he committed the impugned acts while on US soil; *secondly*, and most notably, it rejected the assertion that the UK could not prescribe its own standards of conduct on activities originating abroad. Given the dissemination of illicit content within its own territory, the UK was afforded the usual 'margin of appreciation' afforded to cases entailing freedom of expression; *thirdly*, the fact that the content was available on the website's free preview page, coupled with the inadequacy of parental control software programs to prevent access to the website, meant that the measures adopted by UK authorities were not disproportionate to their stated goal, particularly in view of the need to protect younger users against accessing the material in question.[226]

The *Perrin* Case is one among many expressions of what has evolved to become a rather deferential "margin of appreciation" conferred to national systems by the European Court of Human Rights.[227] In fact, the Court tends to be even more deferential when the provision *itself* invites limitations. It is no wonder then that a good portion of cases brought under Article 10 ECHR (concerning freedom of expression) have been resolved in a manner favoring State interests.[228] While the margin of appreciation started off as a 'procedural' mechanism ensuring respect for

[224] *Ibid*.

[225] *Perrin v. United Kingdom*, no. 5446/03, 18 October 2005 [declared the application inadmissible].

[226] *Ibid*.

[227] Y. Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Intersentia, 2002, esp. at 100 *et seq*.

[228] J. Brauch, 'The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law', 11 Col. J. Eur. L. 113 (2004) [arguing against the 'margin of appreciation' doctrine]. In fact, the 'definitive' case concerning the margin of appreciation involved freedom of expression: *Handyside v. the United Kingdom*, 5493/72 [1976] ECHR 5 (7 December 1976).

the sovereignty of member States, it has turned into a 'substantive' tool for restricting the scope of rights recognized by the European Convention on Human Rights.[229] Although it is unclear how future case-law will deal with freedom of speech on cyberspace, it is clear that the Court does not yet have a mechanism of overcoming 'particularism' within the European continent.

It follows from the above that freedom of expression as enshrined in the First Amendment to the US Constitution functions much in the same manner as substantive criminal law functions in Europe, in the sense that the protective scope of the right is a 'built-in' feature of the provision, leaving courts with considerable less space for 'manoeuver' to limit it. On the other hand, the European 'model' has produced a right that is vulnerable *by definition*, susceptible to limitations based on interests utterly extraneous to the reasons that dictated its recognition in the first place. The claim here is not necessarily that the 'architecture' of freedom of expression is flawed in the European system. Rather, the point is that, *given* such architectural structure of the right, it is unfit to contain prosecutorial excesses once you remove the substantive law guarantees that were the object of the previous theme.

4. Side note: 'Dignity' *versus* 'liberty'

This paper has focused on substantive law, which has left the right to privacy outside its core. When it comes to cybercrime regulation, however, the right to privacy is to procedure what freedom of speech is to substantive law, hence a brief note is in order. Courts on both sides of the Atlantic have invoked privacy so as to assess the admissibility of evidence, whether such evidence be retrieved through surveillance, handed over by a third party, or collected by other means.[230] Unlike freedom of speech, however, there is no obvious answer to the question whether European or US law is more deferential to national governments as opposed to the users' privacy expectations. US case-law –drawing essentially from the protective scope of the Fourth Amendment- focuses on restricting governmental authority,[231] whereas European practice prioritizes limitations to private parties handling personal information.[232] A pertinent example would be the non-recognition of the 'third party doctrine' in Europe, which dispenses with a number of thorny issues often arising in the context of litigation in the US.[233]

[229] See G. Letsas, 'Two Concepts of the Margin of Appreciation', 26 Oxford Journal of Legal Studies 705 (2006).

[230] See R. van den Hoven van Genderen, Cybercrime Investigation and the Protection of Personal Data and Privacy, Discussion Paper prepared in the context of the Project on Cybercrime of the Council of Europe, 25 March 2008, available online at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study5-d-provisional.pdf [last visited on 20 August, 2013].

[231] Nonetheless, there have been cases where governmental authority was preserved in the face of breaches of privacy. See, e. g., a discussion of the 'Invita' case in S. Graydon, "Jurisdiction Issues in Cybercrime", 59 Consumer Fin. L. Q. Rep. 99 (2005), p. 100,where it was held that the Fourth Amendment does not protect against search and seizure beyond US.

[232] Although both leaned towards less privacy after 9/11: see J. Klosek, *The War on Privacy*, Praeger Publishers, 2009, pp. 13 *et seq*., 77 *et seq*.

[233] O. Kerr, 'The Case for the Third-Party Doctrine', 107 Mich. L. Rev. 561 (2009) [in defense of the 'third party doctrine'].

That being noted, one would have to concede that the bulk of issues entailing privacy concerns arise in the relation between individuals and their respective government.[234] It is precisely in these kinds of cases that European law appears less protective (i.e. more deferential to governmental authority).[235] The very manner in which privacy is construed attests to this: European law treats privacy more as a 'societal interest' and less in the vein of purely 'individual rights'.[236] Such a 'paternalistic' view may appeal to those who advocate for more guarantees against dominant Internet Service Providers (such as Google),[237] but it also comes at a certain cost. This becomes apparent when it comes to balancing privacy concerns against other societal interests, including suppression of certain forms of crime. The nature of privacy as a 'societal interest' often means that it is easily overridden in the name of a 'safer' or 'cleaner' Internet.[238] As aptly put by a commentator, "European law often regards privacy as *what we tell you it is*", in contrast to US law, according to which "privacy is *what you think it is*".[239] With all its deficiencies, 4th Amendment discourse in the US has had a solid starting premise at least since Justice Harlan's concurrence in *Katz v. United States*.[240] Rather than recognize a "reasonable expectation of privacy" to the individual, European courts are often more willing to allow unreasonable government invasions to privacy.[241]

V. Conclusion: Three lessons for the EU

The new EU directive on cybercrime *prima facie* follows in the footsteps of cybercrime regulation in the US. The main purpose of this paper has been to demonstrate that this is by no means the only path to follow. That is not to say that the path *as such* is the wrong one. Instead, the real issue at stake is that achieving functional equivalence in terms of regulating any field of the law is an intricate process that has to take into account multi-dimensional considerations. This is *a fortiori* true of cybercrime, which is by definition a complex field, in which traditional problems meet with modern-day intricacies.

---

[234] Although, admittedly, that is gradually beginning to change in Europe –just like in the United States- since private entities have begun to infiltrate virtually every aspect of users' private lives.

[235] *German 'Census' Case*, Bundesverfassungsgericht, 15 December 1983, EuGrZ 1983, pp. 171 *et seq*. [though considered a great victory for the plaintiffs at the time, the census was merely "delayed", since certain additional requirements were imposed by the Constitutional Court that had to be fulfilled prior to it being carried out].

[236] S. Warren and L. Brandeis, 'The Right to Privacy', 4 Harv. L. Rev. (1890); *cf.* J. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty", 113 Yale L. J. 1151 (2004).

[237] One practical effect of this approach (other than the 'opt-in' / 'opt-out' divide) is that waivers of privacy rights on the part of European citizens are often liable to be declared void.

[238] G. Hornung and C. Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination', 25 Computer Law & Security Report 84 (2009).

[239] O. Tene, Privacy in Europe and the United States: I Know It When I See It, CDT, 27 June, 2011, available online at: https://www.cdt.org/blogs/privacy-europe-and-united-states-i-know-it-when-i-see-it [last visited on 20 August, 2013].

[240] *Katz v. United States*, 389 U. S. 347 (1967).

[241] Ironically, privacy is viewed not only as a negative fundamental right, but also as a 'precondition' of democratic participation. See S. Simitis, "Datenschutz – Rückschritt oder Neubeginn?", 34 NJW 2473 *(*1998), at p. 2475.

Three pertinent dimensions were explored in the preceding pages: the structure of authority through which cybercrime regulation is channeled; substantive law choices made in defining offenses committed in cyberspace; and the role of fundamental rights as limiting factors to governmental power. Accordingly, three respective lessons can be drawn:

First, federalism is an effective way of arriving at an effective regulatory regime, as long as there is an effective structure of authority in place. This is the case in every federal system, including the US, as well as certain member-States of the EU, such as Germany and Austria. However, the EU *itself* is *not* a federation, and legislating as if it were one will do little in addressing real challenges posed by cross-border crime. What is required instead is a reconfiguration of both legislative and executive authority so that they coincide both on a national and on the EU level.

Second, there is no 'magic recipe' to create effective substantive law provisions. Each set of rules operates best in an environment that is most receptive to its particular traits. European criminal justice systems have long functioned based on specific principles, reflected both in the definitions of offenses in the special part and in the general part of criminal law. Emulating bits and pieces drawn from cybercrime regulation in another system is thus not only unproductive, but bound to cause more problems than the ones it purports to solve. What is called for instead is the adoption of substantive norms compatible with the system's inherent principles. Central among these are the 'harm principle' and proportionality, which have always underlined criminal lawmaking in Europe, and they should be employed in the field of cybercrime regulation as well.

Third, overly broad definitions can be narrowed down interpretatively by means of 'constitutional rights' in the broad sense, derived both from national Constitutions and from international human rights instruments. This has been reaffirmed time and again in the United States, where courts routinely resort to constitutional guarantees so as to restrict what would otherwise be 'sweeping' statutes. Nonetheless, the European Union has yet to adopt a constitution of its own, and therefore 'checks' to its power can only come from national constitutions or international instruments such as the European Convention of Human Rights. This is yet another reason why substantive definitions must remain narrow in scope, so that guarantees to civil liberties are incorporated therein.

The fact that the challenges posed by cybercrime are common in both the United States and Europe does not necessarily mean that identical rules are equally effective in both systems. The above analysis aimed at demonstrating that imitating US legislative practices is far from a panacea, and the European Union had better follow its own path towards addressing cybercrime, taking into account the principles European criminal justice systems have always adhered to. Coordination with the United States and other countries will always be called for, mainly in terms of jurisdictional matters, but it cannot be attained at the cost of abandoning one's own tradition. The two systems will eventually approximate each other out of a need to

adjust to the new reality brought about by the gradual development of a 'global community'. Until then, it is useful to keep in mind that their respective points of departure were an ocean apart.