Dismantling Four Myths in AI & EU Law Through Legal Information 'About' Reality

Ugo Pagallo

Abstract The European Commission has recently proposed several acts, directives and regulations that shall complement today's legislation on the internet, data governance, and Artificial Intelligence, e.g., the AI Act from May 2021. Some have proposed to sum up current trends of EU law according to catchy formulas, such as (i) digital sovereignty; (ii) digital constitutionalism; (iii) a new Brussels effect; and, (iv) a human-centric approach to AI. Each of these narratives has its merits, but can be highly misleading. They must be taken with four pinches of salt. The aim of this paper is to dismantle these 'myths' through legal information 'about' reality, that is, knowledge and concepts that frame the representation and function of EU law. We should be attentive to that which current myths overlook, such as the open issues on the balance of power between EU institutions and member states (MS), a new generation of digital rights at both EU and MS constitutional levels, down to the interplay between new models of legal governance and the potential fragmentation of the system, e.g., between technological regulations and environmental law.

1 Introduction

Over the past few years, the European Commission has proposed several acts, directives and regulations that shall complement today's legislation on the internet, data governance, Artificial Intelligence, and more. The list of initiatives and proposals discussed at the European Union ('EU') level includes the *Digital Services* and *Digital Markets Act* from December 2020, the *Data Governance Act* from November of that year, the *Artificial Intelligence Act* (AIA) from May 2021, the *Cybersecurity Act* from July 2021, in addition to the initiatives for a Green Deal, the Open Science project, etc. By considering such legal complexity, scholars have proposed some catchy formulas that should help us setting the proper level of

U. Pagallo (✉)
Department of Law, University of Turin, Torino, Italy
e-mail: ugo.pagallo@unito.it

© The Author(s) 2024

H. Sousa Antunes et al. (eds.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, Law, Governance and Technology Series 58,
https://doi.org/10.1007/978-3-031-41264-6_13

abstraction, to address the intricacy of technological regulation and data governance in EU law. The aim of this paper is to examine four of these formulas: (i) digital sovereignty; (ii) digital constitutionalism; (iii) a new Brussels effect; and, (iv) a human-centric approach to AI ('HAI'). The overall assumption of the analysis is that each of these levels of abstraction has its merits, and still, the formulas can be misleading. Their use may suggest false problems, or problems taken for granted, missing at times the proverbial elephant in the room. The aim of this paper is thus to dismantle these 'myths' through the lens of legal information 'about' reality, that is, knowledge and concepts that frame the representation and function of EU law. The analysis is divided into five parts, each of which devoted to one of the myths under scrutiny in this paper, with its conclusions. The overall intent is to offer a soberer analysis of current trends of EU law and technological regulation.

2 Digital Sovereignty

Luciano Floridi has recently scrutinized the 'fight for digital sovereignty' occurred over the past few years, examining 'what it is' (a matter of control of data, software, standards, services, infrastructures, etc.); and 'why it matters' (the fight touches everyone) 'especially for the EU' (Floridi 2020). Although Floridi refers to a 'post-Westphalian world in which the territoriality of the law no longer applies automatically and may be irrelevant' (Floridi 2021), this new dimension of the old concept, that is, 'digital sovereignty' should still shed light on the current fight for control between the multiple regulatory systems in competition out there: the forces of the market, and of social norms, the legal powers of national governments and international organizations, the role of civic institutions and the financial sector, and more.

However, in EU law, since the ruling of the European Court of Justice in *Van Gend & Loos* from 1963, the principle of sovereignty and the current formula on 'digital sovereignty' remind us of the legal knot on who must have the 'last word' between the EU institutions and the Member States (MS). For better or for worse, 30 years ago, the compromise has been struck with the Maastricht treaty (1992), and the principle of subsidiarity pursuant to Art. 5 of the EU Treaty. Most of the regulatory initiatives and proposals of the Commission, mentioned above in the introduction, hinge indeed on the principle of subsidiarity due to the scale of the issues that are at stake with the regulation of crucial aspects of social interaction on the internet, data governance, or AI and other emerging technologies. So, it is misleading to refer to these trends of current EU law in terms of 'digital sovereignty' because the formula may suggest that regulations of EU look like federal law. They're not. Transferred by MS and their constitutional powers through the Treaties, EU powers are not 'original' as occurs with the constitutional powers of federal states, e.g. the USA.

This legal detail suggests that either the formula of 'digital sovereignty' misses the balance of power between EU institutions and MS, or the formula suggests that

some problems have been solved—or, at least, properly addressed—when they are not. Scholars still discuss that which was dubbed as the *Kompetenz-Kompetenz* issue in the saga of the German federal constitutional court, the *Solange* cases, since the 1970s. Dealing with the governance of the internet, of AI, or tackling the flow of data in current information societies, the formula 'digital sovereignty' does not help us solving this evergreen issue on who's sovereign in Europe. Moreover, if we are interested to what this formula means 'especially for the EU', 'digital sovereignty' does not help us shedding light on the kind of governance behind the recent proposals and initiatives of the Commission. Rather than searching for a sovereign, or a bunch of them in today's law, we should be more technical about today's EU governance and its case-law (Reeds and Murray 2018). Would the stance on 'digital constitutionalism' offer such a more technical analysis?

3 Digital Constitutionalism

Considering the EU approach to the current challenges of technological regulation and its governance, some claim that "in the last twenty years, the policy of the European Union in the field of digital technologies has shifted from a liberal economic perspective to a constitution-oriented approach" (De Gregorio 2021). This new digital dimension of EU constitutionalism is often illustrated with current attempts to oppose the powers of transnational corporations operating in cyberspace, with a new set of responsibilities and duties for such corporations, as providers of services on the internet, as designers and manufacturers of high-risk AI systems, as personal data controllers of complex digital environments, and more. This new set of duties and obligations goes of course together with the corresponding new rights. Starting with the right to de-listing set up by the Court of Luxembourg in the Google case from 2013, attention should be drawn to the new rights to erasure, to be forgotten, to data portability, etc. enshrined in the general data protection regulation, or 'GDPR' from 2016, or the new rights not to be profiled, nor recognized by AI systems, proposed by Art. 5 of the 2021 AI Act of the European Commission, down to its current policies on open access rights, open science rights, etc. Shouldn't we dub all this trend as the 'digital constitutionalism' of the EU institutions?

Interestingly, this stance on digital constitutionalism refers, on the one hand, to a tenet of the digital sovereignty viewpoint, such as the current fight for access, control, and protection over data and information in digital environments, between national and international governments and institutions, e.g. the EU, and the power of transnational corporations. The EU would have flexed its muscles, showing who's the digital sovereign today, by establishing new duties for the fat cats of Silicon Valley, and new rights for the EU citizens. Although the enforcement of such rights and duties appears now and then problematic, e.g., data portability, it seems fair to admit that this stance on digital constitutionalism, much as the overlapping stance of digital sovereignty, draw our attention to a game changer. Over the past 20 years and more, EU law has indeed attempted to complement the traditional framework

of basic constitutional (and human) rights associated with the physical body of the individuals and their *habeas corpus*, with a new principle of *habeas data*. The latter can be traced back to that which the German Constitutional Court has framed in terms of 'informational self-determination' since its *Volkszählungs-Urteil* ('census decision'), from 1983.

Yet, on the other hand, the formula of 'digital constitutionalism' can be misleading, once applied to EU law, because that which EU lacks is the core of traditional constitutionalism, that is, power over matters of public order, law enforcement, and national security in such crucial fields as criminal and administrative law (including procedural safeguards). By referring to the formula of EU digital constitutionalism, the risk is thus to overlook a black hole in such framework, namely, rights and safeguards for the digital body of individuals vis-à-vis law enforcement officers, public prosecutors, or secret services.

To understand how technology impacts on tenets of the rule of law, such as the principle of habeas corpus and notions of 'fair trial,' of 'equality of arms,' etc., attention must be drawn, first, to the national law level. For example, the double standard of protection for the physical body and the digital body of individuals, according to the case-law of both the Constitutional Court and the Court of Cassation in Italy, is deemed compatible with EU law and moreover, the general framework provided by the 1950 European Convention of Human Rights and its Court (ECtHR). This means that, dealing with the physical body and its protection in Italian constitutional law, a statute and the authorization of courts provide for a double level of legal protection (Art. 14 of the Constitution), whereas, in the case of the digital body in criminal proceedings, most powers are simply up to public prosecutors (Art. 2). Whether or not AI systems will reinforce this asymmetry of power between public prosecutors and suspects—also, but not only in Italy—remains of course an open question (Pagallo and Quattrocolo 2019). However, *pace* current claims of digital constitutionalism, this open question and, more in general, the informational counterpart of traditional principles of habeas corpus, fair trial, equality of arms, etc. does not revolve around trends of EU law, but mostly the powers of the Member States of the Union within the framework of the ECtHR. This is not to say that EU law has no role in shaping the legal framework for the protection of the individuals even before a criminal Court, e.g. data protection issues, and yet the whole set of sources, which every European digital constitutionalism must include—such as national powers and constitutions, the ECtHR, EU law and its treaties, international agreements, and more—begets a further question.

I admit that the role of EU law, although limited to certain areas of constitutional law, is especially relevant in some new fields of digital constitutionalism, such as personal data protection and the new set of rights in human-AI interaction set up e.g., by the AIA of the European Commission. This role of EU law in shaping today's digital constitutionalism in Europe and its complex legal governance, however, has now and then engendered further myths. Whilst, in EU law, the formula of digital constitutionalism overlooks the problems of national powers and the disrupting use of AI systems by law enforcement agencies, the plan of a new (and even desirable) digital constitutionalism in Europe often exaggerates the role of EU law. Next

section dwells on one of these popular exaggerations, which brings us back to the stance of digital sovereignty.

4 The Brussels Effect

Ten years ago, Anu Bradford's idea on a 'Brussels effect' went viral (Bradford 2012). In a nutshell, the idea was that, dealing with issues of technological regulation, data protection, environmental law, or antitrust, EU law had unilaterally exerted a legal extra-territorial effect. Recently, Bradford has refined this idea in a new volume (Bradford 2020), and some scholars guess whether we should expect a new Brussels effect due to the recent initiatives of the European Commission on AI, data governance, digital services and markets, etc. (Floridi 2021). In fact, so goes the argument of the Brussels effect, the non-divisibility of data and the compliance costs of multinational corporations, dealing with multiple regulatory regimes, may prompt most technological manufacturers and service providers to adopt and adapt themselves to the strictest international standards across the board, that is, the EU data protection and environmental framework (Pagallo 2018), and now, the proposals of the European Commission.

Once again, after the stances on digital sovereignty and digital constitutionalism, the 'Brussels effect' has its merits. I may dare to say that, for example, EU data protection law does represent a model for the rest of the world. Still, even on the basis of this common assumption, the Brussels effect must be taken with a pinch of salt. By insisting on the power unilaterally exerted by EU law, the thesis on the Brussels effect often overlooks the multiple ways in which EU regulations have to do with coordination and cooperation. First, the extra-territorial provisions of the GDPR, drawing on a long experience in consumer law, are complemented with bilateral agreements of mutual recognition at the international level, e.g. Japan. Second, dealing with technological regulation, the EU lawmakers have more often opted for co-regulatory solutions of legal governance, rather than top-down approaches. Art. 5 of the GDPR on the accountability principle provides an illustration of such co-regulatory model. Third, the analysis of such co-regulatory models adopted by EU law with the 2017 policy on better and smart regulation, some of the technical developments of the EU Better Regulation scheme for interoperability (TOGAF 2017), down to the 'Data Governance Act' from November 2020, converge with similar trends in other legal sectors. Co-regulatory approaches are at work with standardisation agencies, such as NIST-800-53 from 2013 and NIST-800-63C from 2016, together with ISO/IEC 27002 and 27,001 on security and privacy controls for Federal Information Systems and Organizations. Along the same lines, this co-regulatory approach is consistent with some governance models in the business field, such as the COBIT2019 framework launched by ISACA and the Enterprise Architecture model, which aims to align management information systems with business interests (Pagallo et al. 2019).

By insisting on current trends of legal governance and international law today, the aim is not to discard any Brussels effect. I already admitted the (unilateral) impact of EU data protection law on the rest of the world and am ready to concede that certain provisions of the AIA on the banning of AI uses are not only here to stay, but will similarly represent a reference point in international law.

However, once we embrace this scenario, attention should be drawn to the content of the effect, in other words, that which would exert unilateral extra-territorial effect across jurisdictions, representing a model for the rest of the world. Current debate on EU law and technological regulation has provided some myths and popular catchy formulas also in this case. Next section scrutinizes one of such formulas: the 'human-centric' approach to the normative challenges of AI, or 'HAI.' This stance summarizes the narratives of the previous sections, according to a threefold stance on:

(i) EU's HAI for AI regulation, as illustrated by the AIA proposal of the Commission, as an act of digital sovereignty in international law;
(ii) EU's new rights in human-AI interaction set up by the AIA as a further strengthening of EU digital constitutionalism;
(iii) A possible new Brussels effect due to (i) and (ii).

The aim of next section is to take sides on whether HAI, i.e. the 'human-centric' approach of EU law for the regulation of AI systems is robust, or alternatively, even misleading.

5 'HAI' (Human-Centric Artificial Intelligence)

'HAI' has an already long story. Since the mid 2010s, the European Parliament insisted on the 'European values' that should have guided the necessary regulation of AI systems and other emerging technologies. In 2018, the European Commission set up a High-Level Expert Group (HLEG), to elucidate the ethical principles of AI. The HLEG delivered its Ethical Guidelines in 2019. The guidelines include environmental robustness and the protection of societal and environmental well-being among the six requirements that AI systems must satisfy to be considered trustworthy.[1] From a philosophical standpoint, however, it is noteworthy that such Ethical Guidelines insist time and again on their 'human-centric' approach: "the common foundation that unites these rights can be understood as rooted in respect for human dignity – thereby reflecting what we describe as a 'human-centric approach' in which the human being enjoys a unique and inalienable moral status of primacy in the civil, political, economic and social fields."[2]

[1] See https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
[2] *Ibid.*, at 10.

At their best possible light, such claims, and similar declarations, may make sense. HLEG's ethical guidelines hinge after all on a previous document of another group of experts, in which my colleagues and I insisted on four risks of AI, i.e., (i) devaluing human skills; (ii) removing human responsibility; (iii) reducing human control; (iv) eroding human self-determination (Floridi et al. 2018). Against such risks, it is thus welcomed any clear understanding of these issues under scrutiny and what initiatives can be taken against the misuses of technology in a proactive way.

However, HAI raises two formidable problems. One is philosophical, the other practical. As regards the philosophical part of this story, the limits of every human-centric, or neo-Protagorean approach have been stressed time and again over the past decades, since the ecological movements in the 1950s and 1960s, down to current regulations and principles of EU environmental law. Bioethics and its onto-centric stance tell a lot about the normative challenges brought forth by AI and other emerging technologies: "The comparison should not be surprising. Of all areas of applied ethics, bioethics is the one that most closely resembles digital ethics in dealing ecologically with new forms of agents, patients, and environments" (Floridi et al. 2018). There is robust work on why an onto-centric, rather than anthropocentric viewpoint can help us tackling that which the European Commission, in the Explanatory Memorandum of the AIA, dubs as a 'twin challenge,' namely, the green and digital transformations of our societies (Pagallo and Durante 2009).

In addition, there is evidence of the practical shortcomings of HAI. In the AIA, for example, the European Commission fully endorses the human-centric approach: all new mandatory requirements for high-risk AI systems do not include any commitment against adverse environmental impacts, lest such AI systems pose a direct threat to "the health and safety, or a risk of adverse impact on fundamental rights." This approach of the European Commission has already been criticized. The Report of the European Parliament's special committee on Artificial Intelligence in a Digital Age (AIDA) reckons that such approach simply omits "any hazards related to the environment" (Gailhofer et al. 2021, p. 10). The claim is that the proposed set of rules on AI and data governance, transparency, human oversight and security simply overlook a governance system that shall prevent critical environmental impacts of technology. After all, most proposals on the "environmental sustainability" of technology, including AI, are left to voluntary initiatives put in place by providers of non-high-risk AI systems as regards, for instance, the formation of codes of conduct (EU Commission's AIA, whereas no. 81 and article 69.2).

The troubles of EU law with environmental protection, admittedly, are older than current issues about the digital transformation of our societies and its regulation. A human-centric understanding of the challenges of AI, however, makes the green transformation of our societies even messier. Only an onto-centric approach to the 'twin challenges' of our societies fits this task. To substantiate this assumption, the onto-centric stance must include the principles of bioethics—that is, beneficence, non-maleficence, autonomy, and justice—and complement them with a new principle, the principle of 'explicability.' The latter should incorporate both the intelligibility of AI and the accountability for its uses, to understand and hold to

account the decision-making processes of AI (Floridi et al. 2018). We don't need to be human-centric, to admit the risks for the misuses of AI and its impact on human skills, human responsibilities, human control, or human self-determination. Yet, it's likely that every human-centric approach to these risks will fall short in tackling how such human skills and responsibilities, control and self-determination should be further understood in connection with the challenges of environmental protection and the climate crisis. To say the least, the European Commission should complement its proposal of AIA with the assessment of the environmental impact of AI in the existing European regulatory framework (Gailhofer et al. 2021, p. 37).

On this basis, we may wonder about the metrics for the assessment of the environmental impact of AI, whether their footprint assessment should be compulsory for all high-risk AI systems, for example, or extended to certain low-risk AI applications. Likewise, focus should be on energy costs and carbon emissions (Lacoste et al. 2019; Anthony et al. 2020), e-waste and further conditions of sustainability as, for instance, working conditions, down to the metrics AI systems are optimized for, or further efficiency metrics for AI, as model training (Taddeo et al. 2021). Advanced AI technologies often require massive computational resources that hinge on large computing centers and these facilities have a very high energy requirement and carbon footprint. Some estimates suggest that the total electricity demand of information and communication technologies (ICTs) could require up to 20% of the global electricity demand by 2030, whilst today's demand revolves around 1% (Jones 2018). AI is likely to add growing concerns for the increasing volume of e-waste and the pressure on rare-earth elements generated by the computing industry (Alonso et al. 2012).

A final problem with the philosophical and practical posture of HAI has to do with its redundancy. Not only HAI is insufficient to properly tackle the onto-centric challenges of the green and digital transformations of our societies, but it does not even help to clarify the technicalities of our field. For example, there is a glorious tradition in robotics and AI devoted to the study of human-robot interaction (HRI). Interestingly, experts distinguish two sub-fields of the discipline. Some focus on a human-centred HRI approach: emphasis is here on whether and to what extent AI systems and robots fulfil their task specifications in a way that appears as comfortable and acceptable to humans (Dautenhahn 2007). Yet, there is also a robot-centred HRI approach: this does not mean that experts and scholars are devoted to diminishing human skills, or devaluing human responsibility. Rather, that which computer scientists and engineers aim to understand is an entity, such as a smart robot, that is pursuing 'its own' goals, based on such cues, as its motivations, drivers, or emotions (Pagallo 2013). These vibrant fields of technological development and innovation, e.g. the set up of 'moral machines' have been funded by EU research programs (and that's a good thing). Should we conclude that, in all projects of robot-centred HRI research, scholars should abide by a human-centric approach?

The question is either redundant or highly debatable. It is redundant, because AI researchers should abide by the law; it is highly debatable, because some laws, such as EU environmental law, hinge on an onto-centric basis, e.g. Art. 37 of the EU Charter of fundamental rights (CFR), and Art. 11 of the Treaty on the Functioning of

the European Union (TFEU). Therefore, as occurs with previous catchy formulas on digital sovereignty, digital constitutionalism, and the Brussels effect, also HAI must be taken with a pinch of salt. The pinch of salt we apply ourselves when asking when the sun sets, or will rise tomorrow, although we are no earth-flatters but Copernicans. AI raises unique challenges for human skills and responsibilities, human control and self-determination. Yet, this uniqueness does not entail any neo-Protagorean view, rather, it should be grasped in accordance with the onto-centric stance of digital ethics that properly complements the four principles of bioethics.

6 Conclusions

The chapter dwelt on current EU legal trends and the array of further proposals by the Commission, dismantling four popular narratives or 'myths' on digital sovereignty, digital constitutionalism, a new Brussels effect, and HAI. Four lessons were learnt because of this stance on legal information 'about' reality, namely, about knowledge and concepts that frame the representation and function of EU law:

(a) Against the tenets of digital sovereignty, attention was drawn to the principle of subsidiarity pursuant to Art. 5 of the EU Treaty and the complex governance of the EU institutions;
(b) Against the view on EU digital constitutionalism, the limits of EU law in criminal law, national security, public order and law enforcement were stressed, to offer a more realistic picture of current debate and trends on how the law should protect the digital body of the individuals (also but not only in criminal law and administrative law);
(c) Against advocates of a new Brussels effect, this view on unilateral exertion of extra-territorial legal effects was complemented with bilateral initiatives of mutual recognition at the international level and new models of co-regulation, coordination and cooperation within the EU;
(d) Against the assumptions of HAI, focus was on its philosophical and practical drawbacks and how the onto-centric approach of digital ethics provides a better lens for the twin challenge of the green and digital transformations of our societies.

This stance on current trends of EU law casts light on that which is still critical: the balance between EU powers and member states, a new generation of digital rights at both EU and MS constitutional levels, down to the interplay between new models of legal governance and the potential fragmentation of the system, e.g. between technological regulations and environmental law. Current myths on digital sovereignty, digital constitutionalism, a new Brussels effect, and HAI do not help us addressing these open problems. Rather, they may induce us to overlook them. Although some of these problems do not depend on EU law and its institutions, they contribute to shape current trends of EU law.

References

Alonso E, Sherman AM, Wallington TJ, Everson MP, Field FR, Roth R, Kirchain RE (2012) Evaluating rare earth element availability: a case with revolutionary demand from clean technologies. Environ Sci Technol 46:3406–3414

Anthony LFW, Kanding B, Selvan R (2020) Carbontracker: tracking and predicting the carbon footprint of training deep learning models. ArXiv200703051

Bradford A (2012) The Brussels effect. Northwest Univ Law Rev 107:1–68

Bradford A (2020) The Brussels effect: how the European union rules the world. Oxford University Press, Oxford

Dautenhahn K (2007) Socially intelligent robots: dimensions of human-robot interaction. Philos Trans R Soc B Biol Sci 362:679–704

De Gregorio G (2021) The rise of digital constitutionalism in the European Union. Int J Const Law 19:41–70

Floridi L (2020) The fight for digital sovereignty: what it is, and why it matters, especially for the EU. Philos Technol 33:369–378

Floridi L (2021) The European legislation on AI: a brief analysis of its philosophical approach. Philos Technol 34:215–222

Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, Luetge C, Madelin R, Pagallo U, Rossi F, Schafer B, Valcke P, Vayena E (2018) AI4People - an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds Mach 28:689–707

Gailhofer P, Herold A, Schemmel JP, Scherf CS, Urrutia C, Köhler AR, Braungardt S (2021) The role of artificial intelligence in the European green deal. In: Study for the special committee on artificial intelligence in a digital age (AIDA). Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg

Jones N (2018) How to stop data centres from gobbling up the world's electricity. Nature 561:163–166

Lacoste A, Luccioni A, Schmidt V, Dandres T (2019) Quantifying the carbon emissions of machine learning. ArXiv:1910.09700

Pagallo U (2013) The laws of robots: crimes, contracts, and torts. Springer, Dordrecht

Pagallo U (2018) Algo-rhythms and the beat of the legal drum. Philos Technol 31:507–524

Pagallo U, Durante M (2009) Three roads to P2P systems and their impact on business practices and ethics. J Bus Ethics 90:551–564

Pagallo U, Quattrocolo S (2019) The impact of AI on criminal law, and its twofold procedures. In: Barfield W, Pagallo U (eds) The research handbook of the law of artificial intelligence. Edward Elgar Publishing, Northampton, pp 385–409

Pagallo U, Casanovas P, Madelin R (2019) The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the web of data. Theory Pract Legis 7:1–25

Reeds C, Murray A (2018) Rethinking the jurisprudence of cyberspace. Elgar, Cheltenham

Taddeo M, Tsamados A, Cowls J, Floridi L (2021) Artificial intelligence and the climate emergency: opportunities, challenges, and recommendations. One Earth 4:776–779

TOGAF (2017) An introduction to the European interoperability reference architecture (EIRA©) v2.1.0. https://joinup.ec.europa.eu/sites/default/files/distribution/access_url/2018-02/b1859b84-3e86-4e00-a5c4-d87913cdcc6f/EIRA_v2_1_0_Overview.pdf. Accessed 3 Aug 2020

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.