# Internet Of Bodies: Digital Content Directive, And Beyond

by **Cristina Amato***

**Abstract:** "Internet of Bodies" (IoB) is the new frontier of digital technologies challenging our lives as individuals and as a society. The European Union has not yet set up a coherent and complete regulatory framework dealing with the "Internet of Everything". This paper aims at describing the possible implications of the new technologies in search for responsible legal reactions. After defining IoB and some uncomfortable problems raised by it, the paper faces the topic of what can law and policy do in order to provide a set of rules adequate for supporting sustainable data-driven technologies. The current legal framework is essentially designed by the Digital Content Directive, the Product Liability Directive and the product safety legislation framed into a multilevel layout, as set up by the New Legislative Framework and by the European Standardization System. The article argues that it is within this regulatory framework that new technologies should be controlled, although a substantial institutional revision of co-regulation in the light of plurality and transparency is still desirable.

Keywords: IoB; Digital Content Directive; Product liability Directive; NLF; ESS

© 2021 Cristina Amato

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8.

Recommended citation: Cristina Amato, Internet of Bodies:Digital Content Directive, and beyond, 12 (2021) JIPITEC 181 para 1.

## A. Introduction

**1** "... We are unquestionably entering a technological age where the line between the human body and the machine is beginning to blur. Many human bodies will soon become at least occasionally reliant on the Internet for some aspect of their functionality, and the energy of the human body is already being used experimentally to mine cryptocurrency. Just as the Internet of Things has networked our possessions into a 'cloud' of shared gadgetry, so too our bodies are slowly becoming networked into an "Internet of Bodies".[1] Science fiction movies like *The Matrix*[2] or *Brazil*[3] have already introduced humans to the possibility of melding with machines. Although the current representations do not correspond to a waste land picture, the relationship between humans and digital devices may open the curtain on dystopian scenarios. This paper aims at describing the possible implications of the new technologies, in search for responsible legal reactions. It is structured as follows: first, IoB is defined, and its most popular applications shall be listed (**B.**); at a second stage, some uncomfortable problems raised by Internet of Bodies ("IoB") but derived from unresolved questions with the Internet of Things ("IoT") shall be proposed, and related issues specifically linked to IoB shall be stressed (**C.**). Once the descriptive background has been settled, a third section shall deal with the topic of what can law and policy do in order to provide a set of rules for a sustainable technology. Having this goal in mind, the applicability of the Digital Content Directive ("DCD") to IoB will be checked, especially under the effectiveness perspective (**D.**). Because this regulatory solution does not seem to be completely satisfying, a fourth Section introduces

* Full Professor of Comparative Law – University of Brescia (Italy). This work was part of the research project PRG124 "Protection of consumer rights in the Digital Single Market – contractual aspects", funded by the Estonian Research Council.

1 Andrea M Matwyshyn, 'The Internet of Bodies' (2019) 61 Wm & Mary L Rev 90, who claims (at nt 45) the authorship of the phrase "Internet of Bodies".

2 1999, directed by The Wachowskis sisters.

3 1985, directed by T. Gilliam.

a wide definition of security to be found outside contract law and within products' safety legislation, linked to the Product Liability Directive ("PLD") but essentially framed by a multilevel layout, as set up by the New Legislative Framework and by the European Standardization System (**E.**). Final remarks shall underline why this multilevel layout is not completely adequate to the challenges launched by IoB and new digital technologies, rather it needs a substantial institutional revision in the light of plurality and transparency (**F.**).

## B. What is the IoB? A World of Fun or Dystopian Stories

### I. Functionalities

**2** Specialised literature defines IoB as "a network of human bodies whose integrity and functionality rely at least in part on the Internet and related technologies, such as artificial intelligence".[4] A varied scenario opens where chips and bodies stick or blend. The human body becomes the new technology platform depending on bits and the Internet, turning into a "cyborg": a being with both organic and bio mechatronic body parts.[5] The incorporation of technology into human bodies relies on: the widespread availability of high-speed interconnectivity; the faster computational capabilities permitting real-time analysis of Big Data (the so-called 3V's: high volumes, high velocity and high variety); and the lowering costs of chips and sensors with their increasing reliability at the same time.[6] In this scenario we may appreciate the evident advantages for health care and wellness; or we may catch a glimpse to dystopian episodes taken from the Netflix series "*Black Mirror*",[7] and even predict the commodification or thing-ified nature of the human body, where it may serve in a near future as fungible and rentable commodity for physicality or energy extrusion.[8]

**3** The "spectrum of technohumanity"[9] ranges from a simple model of the mechanically extended human where our existential nature is still preserved; to a sophisticated model of AI domain where human flesh and organs are permanently embedded into hardware and software. Our human essence thus turning into a semi-digital platform that needs on-going updating, subject to the new generation of hackers' attacks (biohacking and hackathons, or hacking senses; brain jacking).

**4** The IoB devices can be diachronically divided into three generations (at **B.II.1.**). Their functionality can be distinguished into: medical devices (e.g. robotic surgery, like in the case of prosthetics that the patient operates on his own from a mobile phone); general wellness (e.g. health monitoring tattoos, temporary tattoos to control various wireless devices, and wearable skin, like super-thin wearable that can record data through skin instead of sensor[10]); educational/recreations devices (e.g. fitness trackers, electronic skin with organic circuit, smart watches, connected glasses or helmets, in-ear translators, and eye-mapping); workers' environment devices (e.g. Amazon's wristband that conducts ultrasonic tracking of workers' hands to monitor performances, Microsfot Brain-Computer Interface that is a direct communication pathway between an enhanced or wired brain and an external device that allow users to operate computer with their thought,[11] and Brain-to-Vehicle (B2V), a new

4 Andrea M Matwyshyn, 'The Internet of Bodies' (2019) 61 Wm & Mary L Rev 77.

5 Manfred E Clynes and Nathan S Kline, 'Cyborgs and space' (1960) Astronautics, September, 26-27 ; S Navas Navarro and S. Camacho Clavijo, *El ciborg humano. Aspectos jurídicos* (Comares, 2018).

6 Scott J Shackelford, 'Governing the Internet of Everything' (2019) 37 Cardozo Arts & Ent LJ 701, 705.

7 Eleonore Pauwels and Sarah W Denton, 'The Internet of Bodies: Life and Death in the Age of AI' (2018) 55 Cal W L Rev 221, 227.

8 As in the case of Human Uber, developed by a Japanese researcher, Jun Rekimoto: it is a special screen strapped to a person's face paid to live on your behalf with your face and dresses: https://www.independent.co.uk/life-style/gadgets-and-tech/news/human-uber-telepresence-robot-ipad-face-carry-round-live-life-pay-service-researcher-a8189836.html; In 2015, the Institute of Human Obsolescence (a Dutch start up) has launched a very peculiar project which is also an art installation: a body suit that harvests excess human body heat to mine cryptocurrency: https://thenextweb.com/cryptocurrency/2017/12/12/startup-uses-body-heat-to-mine-crypto-for-when-robots-take-jobs/#:~:text=IoHO%20created%20a%20body%20suit,potential%20to%20grow%20in%20value.

9 See Andrea M Matwyshyn (2019, nt 1) 166, who identifies five steps on the "spectrum of technohumanity".

10 See "The verge": https://www.theverge.com/2017/7/17/15985940/wearable-electronic-skin-nanomesh-health-monitoring.

11 https://www.microsoft.com/en-us/research/project/brain-computer-interfaces/#:~:text=Brain%2DComputer%20Interface%20(BCI),its%20external%20or%20internal%20environment.

technology presented by Nissan, which connects driver's brain with the vehicle to anticipate the driver's intentions behind the wheel, creating more comfortable and safer driving experiences).[12]

## II. The Three IoB Generations

### 1. IoB Body External

5 The first generation of IoB that can be currently found in the market is "*body external*": technological devices connected to the Internet; they are not embedded in flesh or in organs. They are usually 'self-archival', which means that users stock their own data for their use (i.e. tracking). The most popular IoB devices are Fitbit, the Apple Watch (that identifies irregular heart rhythms, including those from potentially serious heart conditions like fibrillation)[13] and other connected fitness tracking devices, such as smart glasses and breast pumps. Even in the first generation of IoB there is a trend (defined as 'Quantified-Self Movement')[14] to accept, or foster third-party big data research, in health applications[15] as well as in educational settings.[16] Reflection, in addition to tracking, is so far becoming an added value for health care and general wellness. The marketing and use of these types of IoB devices raises the main issues of conformity and serviceability, as well as of data protection;[17] although security problems also appear at this level, as will be argued hereafter. The IoB privacy policy may imply a poor user's consent, especially when personal data are processed by third-party big data processors in the case of interoperational or tethered devices.[18] In such cases the exclusion of "entrusted persons" by users is often functionally impossible or inconvenient. This situation may disarm the DCD defence mechanism that expressly connects objective and subjective conformity to compliance with the requirements of "data protection by design" envisaged by the Regulation (EU) No. 679/2016 ("GDPR").[19]

12 https://global.nissannews.com/en/releases/180103-01-e?source=nng#:~:text=The%20company's%20Brain%2Dto%2DVehicle,trade%20show%20in%20Las%20Vegas.

13 https://www.apple.com/watch/.

14 "This movement promotes the use of devices that not only 'solve problems related to health' but also produce data ... as a way of knowing oneself:" Craig Konnoth, 'Health Information Equity' (2017) U PA L Rev. 1317, 1341-2.

15 Collecting human health data and processing them may generate a picture of our health through detailed information that we would not be able to disclose to a health care provider. Such processes of data collection may dramatically enhance the possibilities to cure human vulnerabilities: Kate Crawford & Jason Schultz, 'BigData and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 BC L Rev 93, 98; Frank Pasquale, 'Grand Bargains for Big Data: The Emerging Law of Health Information' (2013) 72 MDL Rev 682, 684.

16 E.g.: connected brain sensing headbands to monitor students' attention.

17 Andrea M Matwyshyn, 'Unavailable' (2019) 81 U PITT L Rev 349; Id., 'The Security Mistakes Big Companies Make When Buying Tech', WALL ST. J. (Mar. 13, 2017). The safe processing of data by design can be challenged even under the Regulation No 679/2016: the lawfulness of a data processing depends on the data subject consent, or on the legitimate interests pursued by the data controller (art. 6(1)(a) and (f)). As underlined in Recital 47 "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a *third party*, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where *the data subject is a client* or in the service of the controller".

18 Tethered goods or services "maintain[ing] an ongoing connection between a consumer good and its seller that often renders that good in some way dependent on the seller for its ordinary operation": Chris J Hoofnagle and Aniket Kesari and Aaron Perzanowski, 'The Tethered Economy' (2019) 87 G WASH L Rev 785.

19 DCD Recital 48 gives an example of objective non conformity of a digital device: "if the trader of data encryption software fails to implement appropriate measures as required by Regulation (EU) 2016/679 to ensure that by design personal data are not disclosed to unauthorised recipients, thus rendering the encryption software unfit for its intended purpose which is the secure transferring of data by the consumer to their intended recipient". As a matter of fact, in the IoB magic box the intended purpose of a data encryption software is not only the secure transferring of data, but interoperation with other devices that require de-encryption of the transmitted data: if this is the case, users shall be willing to give their consent to third-party processing.

## 2. IoB Body Internal

6 The second generation of IoB technologies is "*body internal*": it refers to devices where a portion of them resides inside the body or accesses the body by breaking the skin. Existing examples in the market mainly concern medical devices: pacemakers with digital components; Bluetooth cochlear implants; IoB artificial pancreas with an insulin delivery system for diabetes mellitus that is connected to software and smartphones; chips with cameras for heart surgeries; sensor–enabled sutures with data collectors for healing wounds. Other examples include prosthetics smart products (like bionics arms; electrodes array directly implanted on the brain enabling amputees to move prosthetic digits with their thoughts alone; brain implants to restore sight to the blind; brain implants with four sensor strips wirelessly connected to a computer interface that allows the patient to type out messages using their eyes and brain) and IoB devices hardwired into patients' nerves and muscles (like open-source-smart prosthetics for wounded veterans). When chips enter into human bodies, besides conformity and privacy protection, the slippage from health care to the promotion of wellness through the implant of non–medical devices[20] raises a delicate issue: security, which may affect both the human body as well as public safety.[21]

## 3. IoB Body Embedded

7 The third generation of interoperating digital technology refers to "*body embedded*" digital devices, like injected or implanted brain computer interfaces (direct cortical interfaces) that work in a bidirectional (read/write) manner externalizing portion of human mind. Current applications of these brain prosthetic components are limited to treating humans with Alzheimer's, Parkinson's, and epilepsy. They also help veterans recover from post-war memory loss and traumatic experiences. Slippage into non-medical uses of third-generation IoB directly leads to the cyborg human where brain enhancement and uploadable knowledge will become added values, thus raising more problematic issues like the loss of control on cognitive processes. This danger deserves deep reflections on private and public fallouts. Medical and non-medical body-embedded IoB raise not only conformity and data protection issues as described above (at. **B.II.1.**), but also serious security issues (at **B.II.2.**) legal questions related to body-property and its disposition,[22] the deterioration of autonomy and heautonomy processes necessary in our understanding of experience and in achieving knowledge and pleasure.[23] The private sphere of human values is not the only topic to be tackled. Tightly linked to the security threat and the loss/decline of reflective judgment is their public impact

20 Existing examples are: a self-implanted chip vibrating whenever the wearer is facing north; a fused implant to brain to have colours transformed into musical tones; digital pills with a 3D printed circuit and a transmitter inside the capsule, connected to a smartphone to monitor gas levels in the human intestinal tracts, and track variability driven from food consumption; swallowable pills patented by British Airways to monitor customer experiences on flights: https://www.independent.co.uk/travel/news-and-advice/british-airways-ba-digital-pill-patent-flight-services-cabin-crew-a7451771.html

21 Security involves mainly two sets of issues, usually separately dealt with by scholars: "pipes" issues, involving "network neutrality" (availability, access and design of high quality, stable Internet infrastructures); "people" issues (economic and social impact of Internet infrastructures on end users): Tim Wu, 'Network Neutrality, Broadband Discrimination (2003) 2 J ON TELECOMM & HIGH TECH L. 141, 145; Frank Pasquale, 'Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries' (2010) 104 NW U L Rev 105, 128; Andrea M Matwyshyn, 'Unavailable' (nt 17) 349; Jamie Condliffe, 'How to Get One Trillion Devices Online' MIT TECH Rev (Sept. 20, 2017), https://www.technologyreview.com/s/608878/how-to-get-one trillion-devices-online/; Eleonore Pauwels and Sarah W Denton, 'The Internet of Bodies: Life and Death in the Age of AI' (2018) 55 Cal W L Rev 230; Id., 'There's Nowhere To hide: Artificial Intelligence and Privacy in the Fourth Industrial Revolution' (2018). https://www.researchgate.net/publication/324451812_Nowhere_to_Hide_Artificial_Intelligence_and_Privacy_in_the_Fourth_Industrial_Revolution

22 Radhika Rao, 'Property, Privacy, and The Human Body (2000) 80 BULRev. 359, 406 f.; Devin Desai, Privacy – Property. Reflections on the Implications of a Post-Human World, 18 KAN. J.L. & PUB. POLY 174 f.

23 Immanuel Kant, *Critique of Judgment* (Nicholas Walkers, tr., Oxford World's Classics, Oxford 2007), *Introduction*, §§ 183-188. Understanding as laws is a (necessary) *a priori* in possession of universal laws of nature. It allows us to form a connected experience from given perception of a nature containing an endless multiplicity of empirical laws. Over and above the understanding as laws, it lays at the basis of all reflections a principle, a *reflective judgment* that attributes to nature a transcendental purposiveness. This judgment too is equipped with an *a priori* principle: it prescribes a law to itself as *heautonomy*, the law of the specification of nature, to guide its reflections upon nature (*autonomy)*, which cannot determine anything *a priori* on the basis of empirical and contingent objects. The law of specification of nature is not prescribed by nature nor by observation: only so far as that principle (heautonomy based on reflective judgment) applies, can we make any headway in the employment of our understanding in experience, or gain knowledge. While we do not gain any pleasure from the perception of categories, the discovery that two or more empirical heterogeneous laws of nature are allied under one principle is a ground for a very appreciable pleasure.

on values affecting the entire society that eventually results into dramatic attacks to deliberative democratic mechanisms.[24]

## C. The Dark Side of Interoperability and Tethered Devices

**8** Once they meet human bodies, interconnected devices clearly bring along questionable fallouts that have raised serious doubts.[25] Legacies[26] inherited from the IoT become much more threatening; the obsession for connectivity and the corresponding total trust in technology[27] may have disruptive effects on physical integrity of the human body as well as on public security. The "commodification of data" may turn the human body into a "platform" itself, broadcasting huge amounts of personal data and thoughts that – once connected to other body-embedded devices – may not only jeopardize the human bodies' physical integrity, but may facilitate third-party attacks or even the influence on our minds, thus undermining not only our health but even our deliberative internal processes.[28] On the other hand choosing to disconnect an internal or embedded device when an interconnected device is not working better implies a fully informed consent concerning the related obsolescence that shall affect the device. Nevertheless, free choice in a free market cannot be taken for granted.[29] It is doubtful that manufacturers would be willing to disclose updating costs or the prices of fungible goods or services with the same or higher level of interconnectivity, although the DCD prescribes for digital content or services delivered on the market at a "normal" level of conformity for items of the same type (art. 8(1)(a)(b): at **D.IV.**). In the end, the average consumer would suffer (physical) damages related to obsolescence and "digital dementia" by simply accepting to disconnect (or by accepting a poor updating) her device through general terms of use included in the sale agreement.[30] Interconnectivity, interoperability and tethering strategies present a dark side that deserves deep reflections on the private and public risks linked to the functionality of the digital tools we expect to break into the market and into our future. Medical, healthy lifestyle, employment, recreational or educational devices present different impacts on health and wellness that we may consider lead to ethically "tragic choices" in favour of recognised and protected human values by the Treaty and the EU Charter. It is also of the utmost importance that the IoB "cargo" may travel in regulated waters and land in safe harbours. Does the DCD represent the proper and unique toolbox able to steer the ship skilfully, or should we envisage a more complex regulatory system that may provide a responsible "security by design" for IoB future technology?

## D. The Current Legal Framework

### I. Law of Contract and Law of Tort for the IoB Magic Box

**9** The two Directives adopted on the 20th of May in 2019, 2019/770/UE on digital content and digital services ("DCD") and 2019/771/UE on sales of goods ("SGD") have finally completed a path started in 1999 by the European Commission (Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees and the aborted CESL), with the goal of creating a set of rules derived from sales law but bound to become a model for a new approach to contract law2.0.[31] Directive 2019/770/

24 Neil Richards, 'Intellectual Privacy: Rethinking Civil Liberties in the Digital Age' (Oxford University Press, Oxford 2015) 6; Andrea M Matwyshyn 'The Internet of Bodies' (nt 1) 159 f.

25 "Is the human body an existential construct to be protected and preserved, or is it merely an outdated 'operating system' or 'platform' awaiting an upgrade from new technologies"? Andrea M Matwyshyn, 'The Internet of Bodies' (nt 1) 165.

26 Andrea M Matwyshyn, 'The Internet of Bodies' (nt 1) 116 f.

27 The magic world of technology explains users' over-reliance on digital devices, even though they meld with our bodies. This trustworthiness phenomenon in turn generates a "vulnerability by design": manufacturers are not very much concerned with delivering the safest high tech products; they have much more incentives in delivering them as fast as the market demands.

28 "When we build technologies that allow for owing and pawning of (parts of) human bodies – regardless of whether those rights of access are controlled by the public or the private sector – we risk of undermining the process of 'self-self governance' that Kant highlighted as essential to autonomy and freedom": Andrea M Matwyshyn, 'The Internet of Bodies' (nt 1) 163-4.

29 A full informed consent can be envisaged when public figures are involved: Dick Cheney, G. Bush S. vice-President from 2001-2009, obtained technical changes to his interconnected pacemaker because he feared to be attacked and murdered via medical device.

30 Andrea M Matwyshyn, 'The Internet of Bodies (nt 1) 124 f.

31 Sebastian Lohsse and Reiner Schulze and Dick Staudemayer, *Data as Counter Performance - Contract Law 2.0?* (Baden-Baden: Nomos 2019); Cristina Amato, 'Dal diritto europeo dei

UE, in particular, aims to provide a first approach to technology regulation. My argument is that its scope and contents do not cover all the main issues raised by interconnected digital contents or services because on one side it is too detailed; while on the other side, it needs to be integrated by sector-specific regulatory provisions or standards. The contractual approach itself is not adequate to face the "Internet of Everything"[32], as the central notion of conformity in the DCD brings about a trader's liability restoring damages *to* digital devices, not injuries caused *by them*. In the latter case, the law of tort supplies, currently led by PLD, and completed by a multilevel layout concerning product safety that is intended to be superseded by a new regulatory framework facing the fallouts of artificial intelligence and machine learning.

## II. Policy and Goals of the DCD

**10** The first doubts of the DCD concern the policy to which it is subject to. Art. 1 and Recital 2 refer to regulatory measures establishing or ensuring the functioning of the internal market, protecting consumers, and striking the right balance between achieving a high level of consumer protection and promoting the competitiveness of enterprises. The IoB world is populated with users. "Consumers" is a term referring to a restricted category of users who do not need protection (as meant in consumers' *acquis communautaire* policy: levelling the playing field) but eventually a barrier against the commodification of their bodies. IoB discipline should thereforestrike the balance between protecting health and enhancing innovation.

**11** Harmonization is said to be the goal of the DCD in order to reach a genuine Digital Single Market (Art. 4 and Recital 3); while the future of IoB should look further on to the preservation of shared values, rights and freedoms carved into the Treaty and the EU Charter.[33] Body embedded IoB challenges human dignity (art. 1), physical and mental integrity (art. 3), the right to liberty and security (art. 6), freedom of thought and conscience (art. 10).

## III. Scope and Range of Application

**12** The second critical observation on the DCD concerns its scope and range of application. Squeezed among several general or specific regulatory instruments, the DCD applies to digital contents supplied by a platform provider that are exchanged for money *or* personal data,[34] independently of the medium used for the transmission of or for giving access to the digital content or service (Recitals 19, 41). Nevertheless, digital contents or services incorporated in or inter-connected with goods shall be covered by the sales of goods contract (art. 3(4)), as regulated by dir. 2019/771/UE, *unless* the good as tangible medium serves *exclusively* as a carrier (art. 3(3)). The DCD range of application (Recital 41) includes computer programmes, applications and also digital services that allow creating, processing, accessing, or storing data in digital form, including software-as-a-service (such as video and audio sharing and other file hosting), taylor-made software and 3D print, and typical IoB body external devices like fitness-trackers[35]. However, there is no certainty concerning chips. They are goods with digital elements and the tangible medium might be considered as an exclusive carrier' nevertheless, art. 3(4) presumes that the digital content or service is covered by the sales contract. The uncertainty in establishing what is covered by the DCD is further complicated by the different regimes applicable to similar digital contents. Medical devices, in particular, are covered by the DCD directive if they consist of health applications that can be obtained by the consumer without being prescribed or provided by a health professional; otherwise they will be covered by sector-specific provisions.[36] Another issue related to the DCD scope concerns data as tradable assets. As mentioned above, the DCD deals not only with digital contents and services paid with money, but also traded with personal data. Nevertheless, the application of the Directive is limited to data processed for *other* purposes than supplying digital contents or services. One example (provided by Recital 25) refers to registration required by traders for security or identification

contratti 1.0. agli *smart contracts'*, in Rossella Cerchia (ed.), Lezioni di dottorato, *forthcoming*.

32 Scott J Shackelford, 'Governing the Internet of Everything' (nt 6) 701 f.

33 COM (2019) 168 final 2.

34 In cases where consumers paid the price *and* gave personal data, no hierarchy of remedies should be in question, but they should all be available (Recital 67).

35 Piia Kalamees and Karin Sein, 'Connected Consumer Goods: Who is Liable for Defects in the Ancillary Digital Service'? (2019) EuCML 13. With reference to the proposals of Directives on digital contents and services, and on sales of goods the Authors underline the unclear liability regime for defective connected goods.

36 DCD Recital 29, which refers mainly to Directive 2011/24/EU and Directive 93/42/EEC (now superseded by Regulation (EU) 2017/745).

purposes. This distinction is questionable on two grounds: first, security in data-driven technologies should always remain a responsible purpose even though data represent the price exchanged for digital contents or services; second, the valid conclusion of a contract through the exchange of personal data is an issue left to Member States' national contract law (see Recitals 24, 25). This legislative choice jeopardizes not only certainty but also, the users' non-discrimination within the internal digital market. More controversial is the connection of personal data as counter-performance with the GDPR as this issue opens up to the consent dilemma. As argued above (at **B.II.1.**) it is difficult for users of digital contents or services to deny their consent to the processing of their data by third-parties, but it is even more problematic for them to withdraw it or restrict the personal data processing in compliance with arts. 7(3) and 18 GDPR. The DCD does not provide any answer, nor can it be inferred from it or the sales law system when the consent we are dealing with concerns interconnected health care devices as correct functioning may undermine the wearer's physical or moral integrity.

## IV. The Conformity Requirements: A Short Cover for IoB

**13** It is generally acknowledged that the essential feature of the DCD concerns the notion of conformity that - together with the obligation to supply in due time (art. 5) - defines the seller's liability and assigns consumers the corresponding remedies.[37] Within the limits of this intervention, subjective (art. 7) and objective (art. 8) requirements for conformity as well as integration of digital contents and services (art. 9) sketch a complete spectrum of the traders' obligations to comply not only with the *contractual* requirements (functionality[38], compatibility, interoperability[39], updating, fitness for a particular purpose and other features as required by the contract), but also with *statutory criteria,* involving the consumers' digital environment as well.[40] The objective definition of fitness for purpose for which digital content or digital services of the same type would normally be used takes into account any existing Union and national law, as well as technical standards[41] or applicable sector-specific industry codes of conduct (art. 8(1)(a)). By the same token, conformity consisting of accessibility, continuity and security normal for digital content and services of the same type that the consumer may reasonably expect refers to *legal notions* that can be found into Union or national sector-specific regulatory instruments (art. 8(1)(b)). Therefore, these provisions represent the necessary link between the contractual discipline set up in the DCD and a security multilevel system projected into the future of IoB. As a matter of fact, the DCD reveals gaps and inconsistencies that render its regulatory framework inadequate for the complexity of devices interoperating with human bodies. Three features in particular demonstrate this assumption and deserve further development: updating, contracting out and modifications aimed at maintaining conformity.

**14** Regarding the first, it is considered both as a subjective requirement for conformity and as an objective one (arts. 7(d), 8(2)); although the consumer remains *free* to install or not install updates (Recital 47). While the recognised freedom of the consumer may have limited impact where body external IoB non-medical devices are involved (like fitness trackers or smartwatches[42]), the same cannot be said when the updating concerns self-implanted healthy lifestyle chips, electronic skin with organic

37 Jorge Morais Carvalho, 'Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771 (2019) 5 EuCML 194 f.; Jozefien Vanherpe, 'White Smoke, but Smoke Nonetheless: Some (Burning) Questions Regarding the Directives on Sale of Goods and Supply of Digital Content' (2020) 2 ERPL 259 f.

38 Absence or presence of Digital Rights Managements (Recital 43).

39 Successful functioning could include, for instance, the ability of the digital content or digital service to exchange information with such other software or hardware and to use the information exchanged (Recital 43).

40 See Dirk Staudenmayer, 'The Directives on Digital Contracts: First Steps Towards the Private Law of the Digital Economy' (2020) 2 ERPL 236, according to whom conformity has essentially an objective meaning referred to statutory criteria, while subjective criteria required by the contract are provided in addition.

41 "When applying the rules of this Directive, traders should make use of standards, open technical specifications, good practices and codes of conduct, including in relation to the commonly used and machine-readable format for retrieving the content other than personal data, which was provided or created by the consumer when using the digital content or digital service, and including on the security of information systems and digital environments, whether established at international level, Union level or at the level of a specific industry sector. In this context, *the Commission could call for the development of international and Union standards and the drawing up of a code of conduct by trade associations and other representative organisations that could support the uniform implementation of this Directive*" (Recital 50).

42 The impact on body external devices may turn to be substantial, when security jeopardized by data breach is involved: see nt. 72.

circuit, wearable skin, or ingested digital pills. More dramatically, medical devices (e.g. pacemakers with digital components) provided by health care professionals and not covered by the DCD, as well as rules and prescriptions on updating and producer's liability should be found in sector-specific provisions and in the law of tort.

**15** Regarding contracting out, art. 8(5) of the DCD excludes the lack of conformity and the trader's liability in contract if the consumer expressly and separately accepted that a particular characteristic of the digital content or service was deviating from the objective requirements for conformity. This provision represents an easy way out for traders that may be accepted in (certain) situations where an IoB body external device has been purchased, like in the case of a fitness tracker;[43] but it casts serious doubts when the objective requirement of conformity waived by the consumer regards the security of self-implanted medical devices (like pills) or external healthy lifestyle devices (like pump breasts or wearable skins). On the other hand, security as well as functionality, compatibility, accessibility, and continuity affecting body internal or body embedded medical devices provided and implanted by health care professionals should be dealt with outside the law of contract.

**16** The third critical feature of the DCD concerns modifications aimed at maintaining conformity (art. 19, Recital 75). On one side, the trader is allowed - under certain conditions listed at art. 19(1) - to modify digital content or digital services provided that the contract gives a valid reason for such a modification (art. 19(1)(d)) and, unless the trader has enabled the consumer[44], to maintain (without additional costs) the digital content or service in conformity even without the modifications. Once again, this mechanism implies a high level of freedom and true informed consent on the side of IoB users, which is not necessarily the case in a high technology and data-driven market that may already have blurred individual heautonomy.

**17** A last but supportive thought on the DCD is devoted to the incorrect integration of the digital content or service into the consumer hardware and software environment. This requirement for conformity is particularly interesting in the IoB world, as it cannot be waived by consumers nor contracted out by traders. Together with a crucial subjective requirement for conformity that is interoperability, it positively affects IoB products that perform their functions with alternative hardware/software already possessed by the IoB user.

## V. The Effectiveness of Traditional Sales Remedies on IoB Devices

**18** The remedies mentioned by the DCD take over the remedies and their hierarchy already put forward by the Directive 1999/44/EC with the necessary adaptions required by the digital object of these products. Therefore, instead of repair or replacement, art. 14 entitles the consumer "to have the digital content or service brought into conformity" provided that it does not bring disproportionate costs, thus leaving the trader with the task of reaching the statutory goal regarding the nature and functionality of the digital content. As in Directive 1999/44/EC, consumers are entitled to the reduction of price (but only if the lack of conformity is not minor) and termination of the contract only when conformity cannot be achieved, as in the instances expressly provided by the law (art. 14(4)). In the IoB world, these remedies should be considered "a first step"[45] as in most cases, reduction of price or termination of the contract in particular may be at odds with the nature and functionality of non-medical internal or embedded devices (see nt 20)[46]. As already observed, IoB medical devices implanted by health care professionals are not covered by the DCD. Related remedies against producers' or distributors' liability shall follow sector-specific provisions and the law of tort.

43 It is doubtful that the user's acceptance of a deviation from objective requirements for conformity shall bring no injury to her when certain body external devices connected to human brain are involved, as in the case of Microsoft Brain-Computer Interface or the Brain-to-Vehicle (B2V) Nissan model (at **A.I.1.**).

44 This possibility may be given to users through Digital Rights Managements' codes, or "DRM". In truth, recourse to these technologies is usually made by producers on their own goods or services, in order to control and limit purchasers' usage of the digital product.

45 Dirk Staudenmayer, 'The Directives on Digital Contracts: First Steps Towards the Private Law of the Digital Economy' (nt 40) 222.

46 Whether technology itself, through specific software and codes – like blockchains - might replace the traditional remedies is a complex issue investigated by several representatives of civil law as well as in the common law tradition: Scott J Shackelford, 'Governing the Internet of Everything' (nt 6) 701, 724; Cristina Poncibò, *Il diritto comparato e la «Blockchain»*, ESI, 2020.

# E. The Safety and Product Liability Regulatory Framework Under Test.

## I. Preliminary Remarks

**19** The short insight into the DCD applications to the IoB digital contents or services reveals its poor effectiveness, as the most significant items belonging to the heterogynous and futuristic magic box of the interconnected IoB world either are not covered by the DCD (as it the case for medical devices, that deserve special legislation[47]), or the non-conformity in terms of safety may generate injuries to physical or mental human integrity traditionally not covered by contract law. Besides, the problem of drawing a line between sales of goods and product liability has already been faced by Directive 85/374/EEC at art 9(b), dealing with limiting damages to items of property other than the defective products itself. Together with the sales of goods Directive 2019/771/UE, the DCD "open[s] up the process of legislative adaptation of European private law in the transition towards a digital economy",[48] but it needs to be integrated into cross-sector regulatory instruments where data and technology converge in a responsible way. "The convergence of physical and digital worlds, in turn, blurs the boundaries between traditional sectors and industries, products and services, consumption and production, online and offline, and therefore challenges standard setting processes. Interoperable solutions based on open systems and interfaces keep markets open, boost innovation and allow service portability in the Digital Single Market".[49] As argued at **D.VI.**, conformity assessment seems to be a founding element of dir. 2019/770/UE and of the European Private Law 2.0. Nonetheless, the issue in the IoB world is not only serviceability, which is whether a product or a service works or not, but also fitness for the purpose. In the IoB world, the goals to be achieved through an innovative regulatory process are safety, which is protecting life and health, as well as desirability; these can all be included in a wider meaning of "security". In this perspective, the European layout set up to guarantee the quality chain of products within the single market may serve as the institutional framework of co-regulation where the cooperation between public regulators and private entities shall enhance innovation while protecting public interests.

**20** Where then can we find the proper regulatory framework for IoB? The portal to a sophisticated safety and product liability regulatory framework is represented by the PLD on liability for defective products. High technological products distributed on large scale are required to comply with technical standards. A modern construction of the PLD that can adapt to new technologies creates a link[50] between the product liability framework and the safety legislation by adopting a multilevel layout based on the dialogue involving public entities, private standardisations organisations and the relevant stakeholders. This current layout (defined as Consumer Safety Network) has been set up by safety legislation[51]. It works with expert groups (that include Member States' representatives and private stakeholders like industry and consumer associations) and is complemented by market surveillance conferred to national authorities.

**21** Although the current safety legislative framework can be considered highly sophisticated[52], it has

47 Scott J Shackelford and Michael Mattioli and Steve Myers and Austin Brady and Yvette Wang and Stephanie Wong, 'Securing the Internet of Healthcare' (2018) 19 MINN JL SCI & TECH 405 f.

48 Dirk Staudenmayer, 'The Directives on Digital Contracts: First Steps Towards the Private Law of the Digital Economy' (nt 40) 220.

49 COM (2016) 176 final "ICT Standardisation Priorities for the Digital Single Market" 3.

50 The link between safety and liability is provided by art. 7 let (d) of PLD, the compliance defence, according to which: 'The producer shall not be liable as a result of this Directive if he proves: (d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities': Cristina Amato, 'Product Liability and Product Security: Present and Future', in Sebastian Lohsse and Reiner Schulze and Dirk Staudermayer (eds.), *Liability for Artificial Intelligence and the Internet of Things. Munster Colloquia on EU Law and the Digital Economy* (vol. IV, Nomos 2019) 77-95.

51 Directive 2001/95/EC on general product safety; Directive 2006/42/EC, Machinery Directive; Directive 2014/53/EU on Radio Equipment.

52 A negative example of sophisticated co-regulation layout is represented by the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation founded in California in 1999 with a mandate to govern the technical architecture of the Internet and in particular to control the lucrative ".com" domains. The reason for its failure is apparently grounded on a complicated hybrid governance structure that includes representations from stakeholders' groups and national governments: Michael A. Froomkin, 'Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution' (2000) 50 DUKE L.J. 17, 29; John Palfrey, 'The End of the Experiment: How ICANN's Foray into Global Internet Democracy Failed' (2004) 17 HARV. J.L. & TECH. 409, 429, 460; Jonathan Weinberg, ICANN and the Problem of Legitimacy (2000) 50 DUKE L.J. 187, 210; Kevin Werbach, 'The Song Remains the Same:

been structured before AI and emergent technologies; therefore, it is necessary to evaluate its persisting safety and security-by-design effectiveness.[53] "AI systems should integrate safety and security-by-design mechanisms to ensure that they are verifiably safe at every step, taking at heart the physical and mental safety of all concerned".[54] Although a lively debate around regulating the digital environment has been raised years ago, a theory of (complete) Internet governance has not yet been fully developed. Within the limits of this intervention, I will not address the crucial issues concerning the role of traditional sovereigns, on one side, and of powerful market players, on the other side, nor the related issue of whether Internet users should govern their own interoperability in the cyberspace. Suffice it to recall the discussion started around the finding that governmental regulation is rigid, it takes long times for approval, and ends into an excess of bureaucratic rules. As argued above (at **D.**), dir. 2019/770/UE represents a clear example of this assumption. Such a regulatory process may negatively affect both innovation (which advances faster than regulation[55]) and public interests (the sovereign powers being captured by private interests[56]). The 'cyber libertarianism' movement dramatically expressed the mood of the first generation of cyber spacemen against state regulatory powers when in 1996, J.P. Barlow published the *manifesto* of the independence of the cyberspace. He addressed the Governments of the Industrial World as tyrannies and he stressed their lack of moral right to rule by methods of enforcement and of consent.[57] On the other hand, it is doubtful that the sovereignty of the private sector in the Internet world would be desirable. By the same token, it would be questionable to rebut cyber libertarians or supporters of private sectors regulatory power with the opposite argument of promoting the *prevalent* sovereign power and legitimacy of governments and legal systems to efficiently regulate cyberspace as the "cyber realist movement" attempted to do.[58]

What Cyberlaw Might Teach the Next Internet Economy' (2017) 69 FLA. L. Rev. 948 f.

53 COM (2020) 64 final "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics". While waiting for the proofs, the European Commission published a Proposal for a Regulation of the European Parliament and of the Council (COM(2021)206). The aim of this Proposal is to put forward a legislation for a coordinated European approach on the human and ethical implications of AI and the development of an ecosystem of trust, by proposing a legal framework for trustworthy AI. The option preferred in the Proposal is a regulatory framework for high-risk AI systems.

54 COM (2019) 168 final "Building Trust in Human-Centric Artificial Intelligence" 5.

55 I refer to the so-called "Collingridge dilemma": "Potential benefits of new technology are widely accepted before enough is known about future consequences or potential risks to regulate the technology from the outset, while by the time enough is known about the consequences and possible harms to enable regulating it, vested interests in the success of technology are so entrenched that any regulatory effort will be expensive, dramatic and resisted": Morag Goodwin, 'Introduction: A Dimensions Approach to Technology Regulation', in Morag Goodwin and Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing, 2010) 1, 2; David Collingridge, *The Social Control of Technology* (Pinter 1980) 11 defined it as the "dilemma of social control".

56 Public choice theorists have demonstrated in different ways that regulators pursue economic policies that press them into regulatory captures, a phenomenon that denounces the ability of self-interested regulated entities to have a substantial influence over policymaking. The result is that despite the desire of public officials to protect public interests, regulatory capture spoils the regulatory process that turns into a failure: George J. Stigler, 'The Theory of Economic Regulation' (1971) 2 BELL J. ECON. 3, 4; Alfred E. Kahn, *The Economics of Regulation: Principles and Institutions* (Vol. I-II, Cambridge-London 1970-71); Richard Posner, 'Theories of Economic Regulation' (1974) 5 BELL J. ECON. 335, 341; Stephen Breyer, *Regulation and its Reform* (Cambridge-London 1982) 15-20; Daniel A. Farber and Philip P. Frickey, *Law and Public Choice: A Critical Introduction* (Chicago-London 1991) 21-22.

57 Online self-governance was first proclaimed by John P. Barlow, *A Declaration of the Independence of the Cyberspace*, February 8th, 1996: https://www.eff.org/cyberspace-independence. For a previous elegy: Trotter Hardy, 'The Proper Legal Regime for "Cyberspace," (1994) 55 U. PIRR. L. REV. 993, 1004. Soon after the Declaration of the Independence, the 'cyberlibertarians' movement leaned over seeking for freedom in the cyberspace: David R. Johnson and David G. Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 STANF. L. Rev. 1367, 1388; David G. Post, 'Governing Cyberspace' (1996) 43 WAYNE L. Rev. 155, 166-67; Joel R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 EMORY L.J. 911, 919.

58 In contrast to the cyberlibertarians, 'cyber realists' appeared on the scene a short period after the Declaration of Independence: Jack L. Goldsmith, 'Against Cyberanarchy' (1998) 65 U. CHI. L. Rev. 1199, 1244; Neil Weinstock Netanel, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 CALIF. L. Rev. 395, 452. The Napster case (online music store created in 1999) is a clear demonstration of how legal action enforced by state power against copyright infringement may extinguish a business model (based on the sharing of digital audios), thus disproving the "cyberlibertarian" argument based on the absolute lack of state method of enforcement on the digital world. In the same perspective stands the request for network

**22** As implied in my scepticism over the current discipline applicable on IoB, I believe that a desirable regulatory European policy should choose a balanced framework. Werbach captures this sentiment: "Like a pendulum gradually narrowing its arc, extreme libertarianism and regulatory revanchism gradually gave way to practical solutions in the middle. This story describes the website-dominated era of Web 1.0 as well as the social/mobile/app world of Web 2.0. There is every reason to expect the pattern to continue".[59] In my view, therefore, a more feasible approach for a European responsible innovation agenda would rather consist in "bringing together public and private institutions and organisations in a collaborative dialogue process"[60] by improving the regulation policy within the current New Legislative Framework ("NLF"), the European Standardisation System ("ESS") as set up by Regulation (EU) No. 1025/2012 and Regulation (EU) No. 1020/2019[61] [62] and the product safety legislation (nt 51). My argument is that IoB technologies should be incorporated within the regulatory process of the NLF, essentially consisting of a multilevel layout that discards *ex ante* state approval, in favor of a double control system: a pre-market product safety control limited to certification process assigned to notified bodies (that is private institutions within Member States that are approved by the Commission) based on essential requirements (contained in directives or regulations) and standards;[63] a post-market product control based on market surveillance of products. We need a Better Regulation policy within the Regulation (EU) 1020/2019[64].

## II. The New Legislative Framework and the European Standardisation System

**23** The European Council Resolution from the 7th of May 1985 described a New Approach to technical harmonisation and standards grounded on four principles:[65] (1) legislative harmonisation is limited to the adoption of the *essential safety requirements*; (2) the task of drawing up the technical specifications needed for the production and placing on the market of products conforming to the essential requirements established by the Directives, while taking into account the current stage of technology, is entrusted

neutrality rules originated by governmental intervention, advocated by start-ups and academics in order to avoid discrimination by broadband access providers.

59 Kevin Werbach, 'The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy' (nt 52) 887, 945.

60 COM (2016) 358 3. It seems a rational approach between extremisms: John Palfrey, 'The End of the Experiment: How ICANN's Foray into Global Internet Democracy Failed' (nt 52) 409, 473; Kevin Werbach, 'The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy' (nt 52) 954, 957.

61 The European standardisation policy also includes the planned Joint Initiative on European Standardisation, the Rolling Plan for ICT standardisation and the Annual Union Working Programme: see COM (2016) 176 final 6.

62 A different approach that may deserve further inquiry as a possible and desirable legislative technique to be combined with the NLF and ESS described in the text is represented by the so-called 'experimental legislation' that has been mainly analysed within the collaborative economy models. It "... refers to statutes or, in the majority of cases, regulations enacted for a period of time determined beforehand, on a small-scale basis, in derogation from existing law, and subject to a periodic or final evaluation": Sofia Ranchordas, 'The Whys and Woes of Experimental Legislation' (2013) 1 THEORY & PRAC LEGIS 415, 419. See more recently: Id., 'Time, Timing, and Experimental Legislation' (2015) 3 Theory & Prac Legis 135; Id., 'Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation' (2015) 55 JURIMETRICS 201; Id., 'Sunset Clauses and Experimental Regulations: Blessing or Curse for Legal Certainty' (2015) 36 ST L REV 28; Id., 'Nudging Citizens through Technology in Smart Cities. Rediscovering Trust in the Datafied City' (2020) 34 Int ReOF LAW, COMPUTERS & TECH, 254; Id., 'Public Values, Private Regulators: Between Regulation and Reputation in the Sharing Economy' (2019) 13 LAW & ETHICS OF HUMAN RIGHTS 203.

63 The term 'standards' used in the text refers to 'ICT technical specifications' as "adopted by a recognised standardisation body for repeated or continuous application with which compliance is not compulsory in the fields of information and communication technology (art. 2(1)(4)(5) Regulation (EU) No. 1025/2012). In the same sense: COM (2016) final, "ICT Standardisation Priorities for the Digital Single Market" nt 1.

64 With reference to the particular issue of regulating robotics domain: "We are facing a new evolutionary step in regulation-the necessity to shift from a responsive regulation to a so-called 'smart regulation'. It means it is important to articulate a cross domain target or concern that unifies the regulatory approach to robotics": Giorgia Guerra, 'An Interdisciplinary Approach for Comparative Lawyers: Insights from the Fast-Moving Fields of Law and Technology' (2018) 19 GERMAN LJ 579, 609; see also: Ronald Leenes and Erica Palmerini and Bert-Jaap Koops and Andrea Bertolini and Pericle Salvini and Federica Lucivero, 'Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues' (2017) 9 LAW, INN AND TECH 1-44.

65 Resolution 85/C 136/01, Annex II.

to organisations competent in the standardisation area; (3) *these technical specifications are not mandatory* and maintain their status as voluntary standards; and, (4) at the same time, national authorities are obliged to recognise that products manufactured in conformity with harmonised standards (or provisionally with national standards) are presumed to conform to the "essential requirements" established by the Directives. The essential feature of this layout is to limit legislative safety harmonization to the essential requirements that are of public interest, such as the health and safety of users. The New Approach Directives provide a system based on double controls: conformity assessment modules (pre-market control) and market surveillance (post-market control). The goal is to strengthen the free movement of goods system.[66]

**24** Adopted in 2008 within the New Approach, the NLF'[67] consists of a complex, multilevel layout.[68] At a first stage, there is a mandatory general standard of safety (Directive 1992/59/EC of 29 June 1992 now superseded by Directive 2001/95/EC of 3 December 2001 on general product safety: 'GPSD') intended to ensure a high level of product safety throughout the EU for consumer products that are not covered by sector-specific EU harmonization legislation and mandatory specific safety standards contained into vertical directives (horizontal legislation).[69] At a second stage, technical harmonization is achieved through *general* regulatory rules concerning *specific products*, categories, market sectors and/or types of risks (vertical legislation: New Approach Directives), implemented by European[70] and national standards institutions.[71] GPSD complements the existing sector-specific (vertical) legislation and it also provides for market surveillance provisions.[72] In both horizontal and vertical legislation, the producers' duties to comply with standardized rules are still general (i.e. they provide the goal of safety to be achieved and the type of risks to be avoided). The wording of the *essential requirements*[73] contained in the sections of the acts or in their annexes[74] is intended to

66 "The New Approach (complemented by the Global Approach) is a legislative technique used in the area of the free movement of goods, widely recognised as highly efficient and successful": COM (2003) 240 Final "Enhancing the Implementation of the New Approach Directives" 2. A list of the New Approach Directives (now aligned to the NLF), and in particular to Decision 768/2008/EC can be found at: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en.

67 The NLF (<https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en> accessed 8 August 2018) consists essentially of a package of measures aimed at setting clear rules for the accreditation of conformity assessment bodies, providing stronger and clearer rules on the requirements for the notification of conformity assessment bodies, providing a toolbox of measures for use in future legislation (including definitions of terms commonly used in product legislation, procedures to allow future sectorial legislation to become more consistent and easier to implement), and improving the market surveillance rule through the RAPEX alert system for the rapid exchange of information among EU countries and the European Commission. These regulatory measures are: Regulation (EC) 765/2008 (setting out the requirements for accreditation and the market surveillance of products); Decision 768/2008 on a common framework for the marketing of products; Regulation (EC) 764/2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another EU country; and, Regulation (EU) 1020/2019 on market surveillance.

68 Enrico Al Mureden, 'La responsabilità del fabbricante nella prospettiva della standardizzazione delle regole sulla sicurezza dei prodotti' in Enrico Al Mureden (ed.), *La sicurezza dei prodotti e la responsabilità del produttore* (Giappichelli 2017) 2ff.

69 See the list of specific Directives and Regulations at <https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en> accessed 30 September 2018.

70 In Europe: European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC), European Telecommunication Standards institute (ETSI). See Annex I of Regulation (EU) No 1025/2012.

71 In Italy: Ente Nazionale di unificazione (UNI); Comitato Elettrotecnico Italiano (CEI).

72 See in particular: RAPEX, Rapid Alert System set up between Member States and the Commission; to certain conditions, Rapid Alert System notifications can also be exchanged with non-EU countries. The efficiency of this system has been recently demonstrated by a case detected by Rapex and occurred in Iceland, concerning a smartwatch for children: https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en. This product would not cause a direct harm to the child wearing it, but it lacked a minimum level of security: it could be easily used as a tool to have access to the child, thus jeopardizing his/her safety through localisation.

73 Essential requirements define the results to be attained, or the hazards to be dealt with, but do not specify the technical solutions for doing so. The precise technical solution may be provided by a standard or by other technical specifications or be developed in accordance with general engineering or scientific knowledge laid down in engineering and scientific literature at the discretion of the manufacturer: The 'Blue Guide' 38.

74 As an example, Regulation (EU) 2017/745 on medical devices (repealing Council Directives 90/385/EEC and 93/42/

"facilitate the setting up of standardization requests by the Commission to the European standardization organizations to produce harmonized standards. They are also formulated so to enable the assessment of conformity with those requirements, even in the absence of harmonized standards or in case the manufacturer chooses not to apply them".[75]

**25** So far, it is the public regulator that provides the *general framework* for safety and quality requirements of products as positive regulation of *all* safety aspects is impractical. Harmonized technical standards are focused on a third level of intervention; they are European standards adopted by recognized standardization organizations upon requests (*standardization mandates*) made by the European Commission for the correct implementation of the harmonization legislation. Such organizations have a private nature as they operate on mutual agreement that maintains their status of voluntary application, and their technical standards never replace the legally binding essential requirements. Regulation (EU) No 1025/2012 on European standardization defines the role and responsibilities of the standardization organizations and it gives the Commission the possibility of inviting, after consultation with the Member States, the European standardization organizations to draw up harmonized standards.[76] At the end of this complex process, standards are published on the European Official Journal[77]; from publication, they shall mandatorily be applied by national standards institutions or by national notified bodies that are authorized to issue marks or certificates of conformity,[78]although compliance with harmonized technical standards remains a voluntary action for producers who will benefit in the case of the "compliance defense" (Art. 7 let d) PLD).[79] The cross-reference method illustrated above is preferred to vertical, ossified legislation. First, it encourages flexibility. Safety assessment procedures must be flexible, above all, because the hazards to be assessed vary tremendously in nature and intensity. Secondly, it provides sustainability of the imposed standards that involves transparency and the participation of relevant stakeholders, including SMEs, consumers, environmental organizations and social stakeholders (see Regulation (EU) No 1025/2012, Art 5 ch II, in particular). This dialogue between public entities, private standardization organizations and relevant stakeholders provides sufficient guarantees[80] that the standardization

EEC), art 5, §2 runs: "A device shall meet the general safety and performance requirements set out in Annex I which apply to it, taking into account its intended purpose". In Annex I (*General Safety and Performance Requirements*), general safety requirements are then listed in three different Chapters, dealing with: general requirements (Ch I); design and manufacture (Ch II); information supplied with the device (Ch III). The same pattern is used as for directives and regulations on toys, cosmetics, machinery, etc.: <https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en>

75 Commission Notice 5 April 2016 C (2016) 1958 final "The Blue Guide" 37–38.

76 See the *Vademecum* on European standardization: SWD (2015) 205 final, 27 October 2015 available at <http://ec.europa.eu/growth/single-market/european-standards/vademecum/index_en.htm>. The Commission (assisted by a committee, consisting of representatives of national states: Art 22 of Regulation (EU) No 1025/2012) issues standardisation mandates (i.e. after consulting sectoral authorities at the national level), addressing the European standardisation organisations that will formally take a position on the request and finally start up the standardisation work.

77 About the content of the harmonised standards and their relationship with the essential requirements of the harmonised legislation, see more extensively the Blue Guide (nt 75) 4.1.2.2., 39ff. 'A specification given in a harmonized standard is not an alternative to a relevant essential or other legal requirement but only a possible technical means to comply with it', 40.

78 The list of notified bodies designated by the European Commission can be found at: https://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=notifiedbody.notifiedbodies&char=A

79 See for example, art. 8(1) Regulation (EU) 2017/745 on medical devices: "Devices that are in conformity with the relevant harmonised standards, or the relevant parts of those standards, the references of which have been published in the Official Journal of the European Union, shall be presumed to be in conformity with the requirements of this Regulation covered by those standards or parts thereof".

80 For a different view: Christian Joerges and Hans W Micklitz, 'Completing the New Approach Through a European Product Safety Policy (2010) 6 HANSE L. Rev. 381; Christian Joerges and Hans W Micklitz, 'The need to Supplement the New Approach to Technical Harmonization and Standards By a Coherent European Product Safety Policy' (2010) 6 HANSE L. Rev. 349 – Special issue. The Authors consider the Union product safety policy as a barrier to trade and plead for a Standing Committee on Product Safety (that includes private parties like CEN/CENELEC) before setting the special standards. On the ineffectiveness of several EU instrument to ensure and control the safety of products see: Christian Joerges, 'Product Safety, Product Safety Policy and Product Safety Law' (2010) 6 HANSE L. Rev. 115; Richard W Parker and Alberto Alemanno, 'A Comparative Overview of EU and US Legislative and Regulatory System: Implications for Domestic Governance & the Transatlantic Trade and Investment Partnership' (2015) 22 COLUM. J. EUR. L. 89 f., where the Authors argue for a more procedural approach of

requests are well understood in order to satisfy the essential requirements. On the other hand, public interests are taken into account in the process without completely delegating technical standards to industry representatives. Safety law is about social protection which no manufacturer nor single judge can determine unilaterally by laying down what "safety" is. "The alignment of corresponding decisions to technical standards specifying general safety duties is equivalent to setting a threshold value establishing the extent of permissible risks in general terms".[81]

**26** The multilevel layout promoted by the NLF and the ESS has been recently confirmed and completed by Regulation (EU) No. 1020/2019/EU on market surveillance whose objective is "to improve the functioning of the internal market by strengthening the market surveillance of products covered by the Union harmonization legislation [...], with a view to ensuring that only *compliant products* that fulfil requirements providing a high level of protection of public interests, such as health and safety in general, health and safety in the workplace, the protection of consumers, the protection of the environment and public security and any other public interests protected by that legislation, are made available on the Union market" (art. 1). This Regulation sets up a complex system consisting of: (a) a combination of regulatory tools involving producers (see Ch. II) and (b) rules on controls delegated to national market surveillance authorities and a single liaison office (Ch. IV). In particular, Ch. II Reg. N. 1020/2019/EU lays down rules assigning specific tasks to economic operators concerning conformity and risks of products subject to Union harmonization legislation (listed in Annex I). Among these products there are medical devices,[82] that is technological devices that so far can be listed among the most relevant IoB assets (at **A.**). Special attention is payed to emerging technologies and the digital environment which takes into account that consumers are increasingly using connected devices in their daily lives. Therefore, the regulatory framework addresses the new risks to ensure the safety of the end users (Recital 30) and market surveillance authorities are expected to bring non-compliance to an end quickly and effectively (Recital 41). The safety framework has eventually been completed by the connection of the standardization policy to the Digital Single Market Strategy[83] on the ground that common standards ensure the interoperability of digital technologies thus fostering innovation and lowering market entry barriers.[84]

## F. Final Remarks: Rethinking the European Product Safety Regulatory Scheme

**27** The dialogue between public European institutions and private organizations (and stakeholders) will contribute to answer several questions together with serviceability which are implied in a wider notion of security that concerns the correct edge between promoting technology and marketing useless technological risks. The implementation of a flexible, transparent, and open safety process would also reduce, in the long run, the placing on the market of unavoidable unsafe products (especially if they belong to the category of healthy lifestyle or recreational devices). Collectively, the safety regulatory framework set out by the European New approach, the NLF, the recent Regulation on market surveillance and product liability certainly represent a smart method to achieve an optimal safety level for medical, health lifestyle, educational or workers' environment devices.[85]

**28** Nevertheless, such a framework still needs rethinking in view of appropriately regulating the ICT new technologies.[86] In particular:

1. The NLF and the ESS should be coherently integrated with sales law so that *innovative* definitions of and rules on products' security and conformity shall give place to the present shattered legislative patchworks (at **D.IV.**).[87]

the EU consultation practices.

81 Christian Joerges, 'Product Safety, Product Safety Policy and Product Safety Law' (nt 80) 118.

82 Reg. (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

83 COM (2015) 192.

84 COM (2015) 550 final, "Upgrading the Single Market: more opportunities for people and business, para. 3; COM (2016) 176 final, ICT Standardisation Priorities for the Digital Single Market", para. 1.

85 Norbert Reich, 'Product Liability and Beyond: An Exercise in "Gap-Filling"' (2016) 3-4- ERPL 619, 626.

86 COM (2020) 64 final 16-17. For an AI regulatory model that takes into account the GDPR structure, see: Denise Amram, 'The Role of the GDPR in Designing the European Strategy on Artificial Intelligence: Law-Making Potentialities of a Recurrent Synecdoche' (2020) 1 OJC § 3.

87 In the ESS framework, the only reference to the law of sales can be found in Regulation No. 1020/2019/UE: art. 2(4)

Moreover, the current system of product liability needs adjustments at a European and national level, in the view of welcoming AI and new technologies.[88]

2. The NLF and the ESS should be significantly reformed by introducing key priority areas, stakeholders, and processes that guarantee the boost of competitiveness and innovation within the limits of desirability. At present,[89] explicit reference is made to an "ethical level playing field" and seven key requirements that AI applications in different settings should respect have been identified: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and, accountability. Regarding stakeholders and regulatory processes, public interests groups are represented by the ESS and they are expected to take part at all stages of developments of the European standards.[90] Nevertheless, the future of the IoB regulatory framework requires an institutional designing through: reviewing the agility of processes where dialogue between public entities and private stakeholders takes place, simplifying the current safety and liability layout to provide a well-structured regulatory process that is pluralistic and transparent,[91] and shaping the technology of the next future to be desirable. "The celebration of innovation should not obscure the principle that law exists to protect core societal values precisely because they do not change".[92]

which foresees that its provisions are without prejudice of arts 12-15 of Dir. 2000/31/EC on electronic commerce. This reference is made just to restate that no general obligation is imposed on information society service providers to monitor the information which they transmit or store, nor should a general obligation be imposed upon them to actively seek facts or circumstances indicating illegal activity. "Hosting service providers in particular shall be held liable as long as they do not have actual knowledge of illegal activity or information and are not aware of the facts or circumstances from which the illegal activity or information is apparent" (recital 16). This general principle on the ISS provider's liability is again re-stated by the Proposal for a Regulation COM (2020) 825 final 15.12.2020 on a *Single Market For Digital Services*.

88 SWD (2018) 137 final. See Giovanni Comandé, 'Multilayered (Accountable) Liability for Artificial Intelligence' in Sebastian Lohsse and Reiner Schulze and Dirk Staudermayer (eds.), *Liability for Artificial Intelligence and the Internet of Things. Munster Colloquia on EU Law and the Digital Economy* (vol. IV, Nomos 2019), 176 f., where the A. argues that whatever liability regime is chosen; AI requires a gradual layered approach to liability grounded on accountability principles, and it also requires the use of technology itself to unfold a multi-layered accountable liability system. The A. also recognises that the interconnectedness of algorithms also restricts the means of algorithms decision-makers to give an account of the decisions they make.

89 SWD (2019) 168 final 2-3: "There is a need for ethics guidelines that build on the existing regulatory framework and that should be applied by developers, suppliers and users of AI in the internal market, establishing an *ethical level playing field* across all Member States".

90 Art. 5(1) Regulation (EU) N. 1025/2012. The Commission has engaged in partnership agreements and financial agreements with four organisations (listed in Annex III, Regulation (EU) N. 1025/2012) representing consumers, environmental and social interests as well as the interest of SMEs in standardisation at European level. The four organisations are the following: European Association for the Coordination of Consumer Representation in Standardisation (ANEC); Small Business Standards (SBS) European Environmental Citizens Organisation for Standardisation (ECOS) Confédération Européenne des Syndicats (ETUC). A summary of their activities can be found in the SWD (2018) 15 final, 56 f. the recognition that working closely with stakeholders and public authorities is essential to achieve the ICT priorities is re-stated in: COM (2018) 26 final 8. Recently, the EU Commission has appointed a high level expert group on AI and set up an open multi-stakeholder platform with more than 2.700 members: COM (2019) 168 final 2-3. A significant participation of public interests' representatives and their financing may be deemed as effective which cures against capturing the regulator. They should be reinforced by promoting effective civil service through hiring expert and professional civil servants (not hired from industry); providing for them a brilliant career in the civil service; eliminating conflict of interest: Rachel E. Barkow, 'Insulating Agencies: Avoiding Capture Through Institutional Design' (2010) 89 TEX LRev 15, 43; Sidney A. Shapiro, 'The Complexity of Regulatory Capture: Diagnosis, Causality, and Remediation' (2012) 17 Roger Williams ULR 249 f.

91 The market surveillance set up in Regulation (EU) No. 1020/2019 is essentially based on checks conducted on a risk-based approach and on information required by society services providers (Ch. IV and V). A 'regulatory metric' designed for measuring agencies outputs would be much more effective: Michael E. Levine and Jennifer L. Forrence, 'Public Regulatory Capture, Interest, and the Public Agenda: Toward a Synthesis' (1990) 6 J. L. ECON. & ORG 167 offering a theory explaining public interest outcomes as the result of other-regarding behavior.

92 Werbach (2017) 948.