The Regulation of Digital Reality in Nutshell

Mónika Nogel
Department of Criminal Sciences
Széchenyi István University
Győr, Hungary
nogel.monika@ga.sze.hu

Gábor Kovács
Department of Criminal Sciences
Széchenyi István University
Győr, Hungary
gkovacs@ga.sze.hu

György Wersényi
Department of Telecommunications
Széchenyi István University
Győr, Hungary
wersenyi@sze.hu

***Abstract*—Digital reality refers to the wide spectrum of technologies and affordances that include Augmented Reality, Virtual Reality and Mixed Reality that simulate reality in various ways. Current level of digital technology and future development towards improving user involvement, entertainment, and accessibility based on digital reality induces not only technological questions but also regulatory, policy and liability issues. The ever-growing market of services using public networks will offer new possibilities and dangers for the user, for the business and create place for criminal activity. Regulators try to follow and adjust laws according to the challenges. This paper briefly analyses the current level and status of regulations on Hungarian and EU level, directing the attention of developers, system engineers and software designers to the questions of responsibility. Based on literature review, this paper discusses issues that are currently in the focus of the regulation in Europe in this regard.**

Keywords—IoD, digital reality, virtual reality, legal aspects, Hungarian regulation for digital reality

I. INTRODUCTION

As the Internet was introduced and widely spread from the 1990s, public networks established connections and enabled data transfer between people. Users can communicate, share information in a blink of an eye. It also introduced criminal activity (cybercrime) under the anonymity of the technology provided. Authentication methods, data security solutions emerged, legislation and regulatory processes followed. New technology needed and needs new regulations. However, personal responsibility was usually maintained and users have to be responsible (and penalized) for their digital activity. A new era started, as machines and devices with a certain level of autonomy accessed the internet.

Internet of Things (IoT) deals with "things" and devices connected via the public internet [1, 2]. They communicate with each other and usually are some kind of sensors, actuators, higher level devices and machines providing data, information and receiving controlling instructions in order to execute certain actions partly or fully automated. Internet of Everything (IoE) includes "intelligent connections", decision making of some extent and thus, allowing more autonomy. Internet of Digital Reality (IoD) extends and levels this up by handling all digital entities that are present in the digital reality represented in a virtual space [3, 4].

Digital entities include virtual representations of physical entities (people, robots, machines), real-world entities (legal entities, institutions, corporations etc.), and also purely digital/virtual ones (AI, algorithms, avatars, chatbots etc.). These entities act, function and coexist in the same virtual world, having different rights and obligations.

Engineers, designers, programmers and developers constantly face the non-technical problem of "what they can do"" from the security and legal perspective as well [5, 6]. Especially liability and responsibility questions have to be answered and regulated. Autonomous driving is one of the most commonly discussed problem, where decisions and resulting actions made by a non-human entity (the vehicle and its software) has to be handled not only from a technical point of view, but on ethics and responsibility.

Artificial Intelligence (AI) comes in when real or virtual machines can do tasks that usually require human intelligence. It should be more than pure computational superiority. Even a simple pocket calculator surpasses human capabilities, without being an AI. Machine learning is where they can learn by experience and acquire skills without human involvement. Deep learning is part of machine learning where underlying neural networks and algorithms are inspired by the human brain. These algorithms perform tasks repeatedly to improve the outcome. Typical applications include translations, chatbots and virtual assistants, facial recognition or personalized advertisement based on our virtual behaviour.

Although, real AI is not common and lot of development is still needed on that field, capabilities of current systems can outperform our expectations, leaving us perplexed and asking "how do they do that?" [7].

Today, we will be advised by Google, influenced by Facebook ads, informed by Amazon Alexa, served by autonomous drones and chatbots. If we look at the future of internet, including smart networks, various digital entities, fully immersive virtual reality scenarios, safety, security, legal and regulatory aspects will become more important than ever [8, 9].

More intensive interfaces between different entities in the virtual environment and the fact that digital reality becomes a commonplace in everyday life, brings variety of legal issues and ethical challenges [10, 11, 12]. Obviously, stakeholder engagement is a crucial element of regulatory policy. However, as digital reality is by nature interdisciplinary - involving not only technology but also social sciences and design - developing the appropriate regulatory mechanisms is not a simple task. Our study argues that better understanding of human-value-technology entanglements can substantially contribute to a more responsible design and use of technologies used in digital reality. Therefore, we are committed to social engagement and values-sensitive design. Recently, human–computer interaction-related public policies applicable in digital reality cover a broad range of mandatory and voluntary rights, obligations, and activities and are implemented across a broad spectrum of institutions, legal and regulatory documents at the national and European Union (EU) level. There are some directly or indirectly applicable principles, as well. However, most of the latter do not have unitary definition. In some cases, we can also witness that the applicability of different principles is surrounded by controversy.

The purpose of the present study is to analyze the most emerging ethical and legal tasks of digital reality, a topic that is highly related to the field of Cognitive Infocommunications (CogInfoCom). Cognitive Infocommunications investigates the link between the research areas of infocommunications and cognitive sciences, as well as the various engineering applications which have emerged as a synergic combination of these sciences [13]. The primary goal of CogInfoCom is to provide a systematic view of how cognitive processes can co-evolve with infocommunications devices so that the capabilities of the human brain may not only be extended through these devices, irrespective of geographical distance, but may also interact with the capabilities of any artificially cognitive system. This merging and extension of cognitive capabilities is targeted towards engineering applications in which artificial and/or natural cognitive systems are enabled to work together more effectively [14].

Another aim of the study is to give a fundamental review of the current regulatory framework for developers (especially of Hungarian citizenship or based in Hungary) and also to point out issues that need to be addressed by policy-makers in the near future. Our starting point is that clear communication, cooperation and coordination between design and regulation is inevitable.

II. PRINCIPLES AND RULES OF DESIGN AND OPERATION OF IOD

There often remains a gap in real world between the prescriptions derived from general theories and the results of the prescriptions in the world of policy making and the practice. The biggest challenge is that it is unclear how to predict the impact of digital reality technologies and AI (i.e., foreseeable harm or risk, or even potential) and how to control them.

A. Collingridge's dilemma and the control of IoD

The task of the social control over digital reality and AI is a typical Collingridge dilemma. In 1980, in his book David Collingridge articulated the dilemma thus: *„attempting to control a technology is difficult…because during its early stages, when it can be controlled, not enough can be known about its harmful social consequences to warrant controlling its development; but by the time these consequences are apparent, control has become costly and slow*" [15]. Collingridge argues that keeping future options open facilitates the social control of technology by enhancing the flexibility of decisions. Having a range of technical options available avoids reliance on any one technology. For Collingridge, the choice of which nascent innovation pathways to pursue (or not) is a matter of societal and technological choice, implicated with competing visions of the purposes, benefits and limitations of technology and more or less effective processes for decision-making [15, 16]. Most current approaches to the Collingridge dilemma focus on anticipation: an attempt is made to make technology more predictable.

There are two different ways of anticipation: the **risk approach** and the **precautionary principle**. According to the risk approach, we must determine the risk of a new technology and decide, whether these risks are tolerable. Risk is here objectively understood as likelihood times severity. The problem we face with IoD, is that in a case of emerging digital reality technologies we often do not know, and it is beyond possibility to know the probabilities, which results in uncertainty. Sometimes we do not even know all possible consequences – and so end up in ignorance [17]. Therefore, we cannot actually determine the risks. In these cases, the possible right decision is following the "precautionary principle", that we will discuss later. It will be obvious then, that even this choice is not without difficulties and doubt.

Certainly, there are other quandaries, as well. For instance, as the European Commission stated, Europe must address the twin challenge of the green and digital transitions to become a modern, resource-efficient, and competitive economy [18].

B. Application of the precautionary principle for IoD

The precautionary principle has neither a commonly accepted definition nor a unified set of criteria to guide its

implementation. It can be interpreted, that decision-makers can adopt precautionary measures when scientific evidence about an environmental or human health hazard is uncertain and the stakes are high. It emphasizes caution, pausing and review before leaping into new innovations that may prove disastrous. Carol Raffensberger and Joel Tickner suggest: „*In its simplest formulation, the precautionary principle has a dual trigger: If there is a potential for harm from an activity and if there is uncertainty about the magnitude of impacts or causality, then anticipatory action should be taken to avoid harm*." [19].

Even the principle does not have a clear definition, there are several legal documents that advocates its application. The 1992 Rio Declaration on Environment and Development formulated this as follows: "*Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation*" [20]. In the EU, the principle has been adopted in the 1992 Maastricht Treaty. It aims at ensuring a higher level of environmental protection through preventative decision-taking in the case of risk [21]. However, in practice, the scope of this principle is far wider. It also covers consumer policy, legislation concerning food and human, animal and plant health. One area in which the EU has used the precautionary principle is to make decisions about genetically modified organisms [22]. The definition of the principle shall also have a positive impact at international level, so as to ensure an appropriate level of environmental and health protection in international negotiations.

However, the precautionary principle has been extensively criticized [23]. Major objections include that it is unscientific or impractical and that it does not take the costs of missed opportunity into account. Regarding to AI, Daniel Castro and Michael McLaughin go further. They state that if policymakers apply the precautionary principle to AI, they will limit innovation and discourage adoption - undermining economic growth, competitive advantage, and social progress. They suggest that policymakers should follow the "**innovation principle**," which holds that the vast majority of new innovations are beneficial and pose little risk, so government should encourage them [24].

Wolter Pieters and André van Cleeff indicate, that for the precautionary principle to apply, threats of serious or irreversible damage must be present, with no possibility of substitution. They argue that applying the precautionary principle to IT is justified, but several questions have to be answered. How the principle can be applied in an effective way? Which specific characteristics of IT demand adapting the principle for this domain [25]?

There is no unified regulation in Hungary to answer these questions. We acknowledge and support the scheme published by the Dutch Scientific Council for Government Policy (WRR) [26, 27], that distinguishes between different levels of risk:

- *Simple:* These problem types can be addressed by standard risk-assessment and -management procedures.
- *Complex:* These problem types occur when the relations between causes and effects are subject to scientific discussion.
- *Uncertain*: A lack of knowledge about possible effects arises when these problem types occur.
- *Ambiguous:* These problem types arise when the desirability of effects becomes subject to discussion.

In accordance with the resolution of the WRR, we argue, that if the risk is uncertain or ambiguous, the precautionary principle has to be followed. In other cases, following well-known risk-management procedures, keeping in mind principles of value-sensitive design and compliance with specific relevant legal rules is appropriate.

We do agree with the concept described by Pieters and van Cleeff, that is, the precautionary principle in software engineering should be interpreted differently than in "traditional" environment and health-related cases. They argue that in the case of digital security, we do not only face with unintentional harm: the harm can also result from intentional human misuse. Therefore, the focus of the application of the precautionary principle should be on anticipating human behavior [25]. The authors state, that if software engineers focus on the indirect consequences of their technology next to direct effects, many of the indirect impacts could be identified at an early stage. They also argue that conceptual tools must be developed to support reasoning about indirect consequences in terms of invitation, inhibition, amplification, and reduction.

We do support the view that the application of the precautionary principle in digital technology – including the Internet of Digital Reality – requires further research.

III. Responsible Research and Innovation & IoD

According to Rene von Schomberg, RRI is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society) [28]. The author argues, that the societal impacts of scientific and technological advances are difficult to predict, but early societal intervention may enable anticipation of positive and negative impacts and can help avoid technologies failing to embed in society [28]. It is likely, that mistrust of science and of emerging technologies (e.g., 5G technology, recombinant DNA technology) is often caused by lack of understanding of science by the public and the failure of science and scientists to communicate with the public. Therefore, adequate public information, education, and involvement of the society in decision-making, can help facilitate trust for science and the adoption of new technologies.

Jeroen van den Hoven states that responsible innovation is an activity or process which may give rise to previously unknown designs either pertaining to the physical world (e.g. designs of buildings and infrastructure), the conceptual world (e.g.

conceptual frameworks, mathematics, logic, theory, software), the institutional world (social and legal institutions, procedures and organization) or combinations of these, which — when implemented — expand the set of relevant feasible options regarding solving a set of moral problems [29].
Rome Declaration on RRI in Europe argues that decisions in research and innovation must consider the principles on which the EU is founded, i.e. the respect of human dignity, freedom, democracy, equality, the rule of law and the respect of human rights, including the rights of persons belonging to minorities [30]. RRI is also key action of the 'Science with and for Society' objective in Horizon 2020 program of the European Commission [31].
This paper argues that there is a need in Hungary for establishing best practices for the design of digital reality environments, which are based on common European values and serves common European goals, to ensure that two essential targets will be balanced: the need to share data widely to maximize its utility for ongoing scientific exploration, and the need to protect individual's and society's rights and interests. We need to explore policies that encourage policymakers and regulators to develop effective, necessary and proportionate legislation for the tasks of IoD.

A. Value-Sensitive Design (VSD) of IoD

Designers, developers, testers, and managers need to take a "value-sensitive" approach. An emerging multi-disciplinary field of VSD seeks to design technology that accounts for human values in a principled and comprehensive manner throughout the design process. VSD is primarily concerned with values that center on human wellbeing, human dignity, justice, welfare, and human rights [32]. Indeed, in the case of IoD, values need to be compared and ranked, especially when non-compatible values point in different directions for the development of new technologies. Considerable amount of literature has summarized VSD approach, regarding VR, MR, AR and AI [33-36].
This paper argues that the set of values also applies for the researcher in the context of IoD. Therefore, our recommendations for the design and operation of IoD is to keep the following values in mind:

- development should contribute to physical and mental well-being,
- do not pursue development that involves foreseeable harm,
- identification and minimization of potential risks are essential,
- the experimental work, design and operation should be transparent,
- beware of deception and ambiguous information,
- have a respect for human life and dignity,
- pay special attention to the interests of children and juvenile,
- require informed consent for experiments,
- have a respect for privacy,
- use safeguards against the manipulation and misuse,
- make a fair contribution.

B. Personal data protection

Privacy is a fundamental human right. The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity [37].
Hungary is a member of the Council of Europe, and its Article 8 of the European Convention on Human Rights provides a right to respect for one's "private and family life, his home and his correspondence". Hungary also ratified the International Covenant on Civil and Political Rights which in Article 17 provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation". Article 6 of the Hungarian Fundamental law recognizes the right to privacy and the right to protection of personal data. In Hungary, the current main national law on personal data protection is Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information. The Act was amended on 26 July 2018 to implement the changes of the GDPR [38]. The Act sets out the general framework for data protection. AI is not explicitly mentioned in the GPDR, but many provisions in the GDPR are relevant to AI, and some are indeed challenged by the new ways of processing personal data that are enabled by AI [39].
The core principles stipulate that all personal data must be:

- processed fairly and lawfully,
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed,
- accurate and, where necessary, kept up to date,
- kept in identifiable form for no longer than necessary for the purposes for which the data were collected or for which they are further processed.

Considering the fact, that digital reality technologies may collect body-tracking data, so they actually collect biometric data. If so, according to Article 9 of GDPR, their processing requires special attention as they are considered a special category of personal data. The GDPR states that the processing of biometric data (for the purpose of uniquely identifying a natural person) − except for some limited purposes, such as employment and social security law purposes of medicine, etc. − shall be prohibited, unless the data subject has given explicit consent to the processing. According to Article 7., conditions for consent are:

- Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the

other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of GDPR shall not be binding.

- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

As a written consent, sites can use clickwrap agreement, that is presented to the users, requiring them to state that they have read it and then agree to its terms by clicking on the "I Accept" button. Clickwrap can be used even if agreement does not pop up, download, or print. However, the reading, downloads and printing must be possible.

Another topic to consider is Article 25 of the GDPR. GDPR's requirement for "privacy by design" means that appropriate organizational and technical measures to ensure personal data security and privacy have to be embedded into the complete lifecycle of an organization's products, services, applications, and business and technical procedures.

According to the regulation, providers should minimize any potential data or information exposure. It is also necessary for providers to implement adequate procedures and security measures to protect children's personal data.

It is necessary to consider, that GDPR does not apply if the data subject is dead, however, Hungarian Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information does protect also personal data of deceased persons.

C. Information security

Hungary was one of the first countries in Central Europe to formulate its national cybersecurity strategy in 2013. In 2018, a new national strategy was published [40]. The strategy is in conformity with the recommendations of the European Parliament for the Member States included in Decision No. 2012/2096(INI) on cyber security and defense, adopted on 22 November 2012, and with the joint communication published by the European Commission and the High Representative of the Common Foreign and Security Policy of the European Union on 7 February 2013 under the title "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace".

The mail goals of the strategy declared are:

- critical information infrastructure protection;
- national cyber contingency plans;
- international cooperation;
- incident response capability;
- institutionalized form of cooperation between public agencies;
- baseline security requirements; incident reporting mechanisms;
- cybersecurity exercises; training and educational programs.

The Hungarian Parliament passed the Act on the Electronic Information Security of Central and Local Government Agencies on 15 April 2013 in line with the National Cyber Security Strategy. The basic concept of the Act is to ensure the security of national electronic data assets as a part of national assets, of the information systems managing such assets and of other vital information systems and system elements. In order to protect electronic information systems and data, proportionally to the risks, the Act states that the electronic information systems must be allocated to particular security classes. This classification is based on confidentiality, integrity and availability properties in a scale of 1 to 5 where 5 is the highest security level.

IV. CRIMINAL RESPONSIBILITY AND IOD

For now, there are way more questions regarding the criminal liability, if AI and immersive technologies causes harm, than the amount of answers we possess. There is no international or national consensus how to handle theoretical and practical challenges that come with these emerging technologies. However, professionals are laboring hard to work out appropriate solutions.

In Hungary, we must follow our traditional regulation [41]. We emphasize, that by virtue of Section 3 of the CC, Hungarian criminal law shall apply to any act of Hungarian citizens committed either in Hungary or abroad, if such an act is criminalized under Hungarian law, and even if the act is not regarded as a criminal offense in the place where it was committed. Also, it applies for every criminal offense committed in Hungary, even if in the offender's country of origin, the act in question does not constitute a criminal offense**.**

According to Section 4 of the CC, Criminal offense indicates any conduct that is committed intentionally or - if negligence also carries a punishment - with negligence, and that is considered potentially harmful to society and that is punishable under CC. Mens rea is one of the most important components of criminal responsibility. It is the mental element of a person's intention to commit a crime; or knowledge that one's action or lack of action would cause a crime to be committed.

In the case of crimes related to digital reality, criminal liability in general assumes that the conduct is punishable under the CC if the perpetrator

- has turned 14 years old,
- has not committed a criminal act in a state of impairment of the mind of a character such that it is impossible for the person so afflicted to understand the nature and consequences of his acts,
- was free to act (there was no coercion or threat),

- was aware of the circumstances that made his/her act a crime,
- the act is harmful for the society and he/she is aware of that,
- the conduct was committed intentionally or - if negligence also carries a punishment - with negligence,
- the action was not a justifiable defense or a last resort,
- the act was not authorized by law or was not exempted from punishment by law.

There are various solutions, how EU countries regulate AI. However, the starting point of the regulation is common, since they see it as a software. In Hungary, for all AI-based technologies applies, that it is considered as a software. Obviously, actions related to IoD can cause harm. These technologies mostly raise problems, when they interface with human actions and there is an unfavorable change in real world environment. Information provided to users may be false or misleading, that can cause harm, injury, property damage. Digital reality environments have a potential to distract the users from the real world, and that can result in an accident. The process of development may be accompanied by intellectual property infringement. The technology often relies upon recording and analyzing sensitive personal data, therefore privacy can be violated. The more we live our lives online and virtually, the more vulnerable we become to hackers and wrongdoers.

In 2020, the European Commission adopted a white paper [42]. In this white paper, as regards the issue of criminal liability the Commission recommends adjusting or clarifying existing legislation in this area, or even introducing new legislation specifically on AI, with mandatory requirements in high-risk AI applications, in order to ensure effective judicial redress for parties negatively affected by AI systems and to ensure legal certainty and competitiveness for companies marketing their AI-based products in the European Union. However, at present, there are no regional or international regulations on AI and criminal liability.

Speaking about national legislation, it is essential, that in Hungarian law, AI alone cannot currently be sanctioned by criminal law, there is always need for exploration of human criminal act behind it. We do not have even special regulation for actions when AI is involved. According to the study European Committee, Hungary belongs to the majority in this respect, since only a few EU countries have prepared or already adopted general legislation which may affect criminal liability when humans hand over the control to AI-driven technology [43]. However, even in those countries, where special rules applies when the AI has a role in an accident (for example in France), the exceptional regulation do not allow the punishment of the AI, but allow the human concerned to release of from criminal liability.

In Hungary, criminal liability of the person using AI would be established if the conduct were punishable according to CC, if there were a causal connection between the act and the adverse consequence, and the designer, operator or third party have acted intentionally or – in certain cases – by negligence [44]. However, in the case of deep learning systems, the causal relationship between human actions and the autonomous system's activity will be difficult to identify. It is also impossible to ascertain, whether there was guilty human intention or a reprehensible omission behind a given factual act. Therefore, the application of autonomous decision-making systems may blur direct human responsibility for adverse outcomes [45].

A. Criminal liability of developers

As it was already mentioned, criminal liability of developers is a hard task, due to difficulties to prove mens rea, causal relationship between the act and result, etc.

Another difficulty lies in a problem, that it is typical for these technologies: actions of all involved stakeholders together lead to a deleterious outcome and it is not possible, to pinpoint who is responsible for what. Then, especially harm caused by immersive technologies rise a question of sharing of liability between software and hardware developers. This phenomenon is called "the problem of many hands" and it is well-known for example from the literature about autonomous vehicles [46]. It is clear, that this topic will challenge lawyers in the following years. However, some may argue no reassuring solution will be necessarily found. An example of such a case in Hungarian criminal law is the question of criminal responsibility of a medical team.

Another potential party to which a portion of liability may be allocated is the one decided to employ autonomous or immersive solutions in the configuration. Last, but not least the question remains, whether, and if so then to what extent the responsibility should be taken by the person who relies on such technology and causes harm.

According to the current law position, there is no permissibility to allow for AI to make completely independent decisions. There is a requirement to ensure, that while operating AI there is a possibility (or in some cases obligation) of human intervention into automatic decision-making. For example, in the case of autonomous vehicles, Decree No. 6/1990 (IV. 12.) in its Annex 17 provides, that the sensor and control systems of the autonomous vehicle for development purposes must be sufficiently advanced to be able to respond safely to all environmental impacts and road users whom the vehicle may encounter during the test under the supervision or assistance of the test driver [47]. In the case of automated decision-making process this obligation is clear from the Article 22 of the GDPR: if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, or is based on the data subject's explicit consent, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. The Article 29 Working Party (Art. 29 WP) defines automated decision-making as "the ability to make decisions by technological means without human involvement." Art. 29 WP concluded

that guidance is needed on automated decision-making. It seems that an obligation of reasonableness – including normative and reliability aspects – should be imposed on controllers engaging in profiling, mostly, but not only when profiling is aimed at automated decision-making. Controllers should also be under an obligation to provide individual explanations, to the extent that this is possible according to the available AI technologies, and reasonable according to costs and benefits. The explanations may be high-level, but they should still enable users to contest detrimental outcomes [48]. Prescribing human intervention into processes is a logical step. However, in most cases it is not possible for a person to react preventively, since the necessity of the intervention becomes obvious only when the adverse consequences caused by AI have already (at least) started to manifest. The other problem is that even if a human recognizes his/her duty to act, he/she is not able to make it adequately, for example because of cognitive biases or due to lack of knowledge or time.

If jurisprudence finds answers to these general preliminary questions of criminal liability, developers can expect punishment for offenses, when their act resulted in a biological result (death, injury), a property disadvantage, violation of privacy, crimes against information systems and illicit access to data.

B. Crime in virtual world

Crimes in virtual world are committed using digital software, the internet and computers. After reviewing CC, we can conclude that some human actions can be punished even if they took place in a virtual world. We can also find arguments that there is no room for criminal law in virtual worlds, at all. However, the fact that the action took place in a virtual environment, sometimes remains a detail. Under certain conditions, the human behind the virtual character is responsible for everything his/her virtual character manifests. For example, if somebody uses his/her avatar to offer pornographic images of a real person under the age of eighteen years in the virtual world, his/her criminal liability is obvious. However, not every kind of real-life criminal offense can be committed in a virtual environment, e.g. rape of human in cyberspace, illegal use of human gametes in virtual world, driving under the influence of alcohol in cyberspace, etc. An act performed by an avatar that would be a crime in the real world, but the value protected by the CC is not violated in the real world, is not considered as a crime. Based on Bart J.V. Keupink's opinion, we argue, that there are three categories, when CC cannot be used to punish an act committed in cyberspace:

- there is no real human act: the action of the avatar is not directed by his owner,
- there is no real harm, which would manifest in the real world: for example, if one avatar kills another avatar,
- the situation is part of the game [49].

To keep digital spaces crime free, criminal justice professions should continue to work with industry and academia to ensure the greatest possible cooperation in trying to minimize any social harm resulting from these technological developments. We hope that the future will not go in the direction, that we have even consider employing virtual detectives to explore virtual crime, as China has introduced in 2007.

CRIMES AGAINST LIFE, LIMB AND HEALTH	**OFFENSES AGAINST PROPERTY**	**CRIMES AGAINST HUMAN DIGNITY AND FUNDAMENTAL RIGHTS**	**ILLICIT ACCESS TO DATA AND CRIMES AGAINST INFORMATION SYSTEMS**
Homicide (Section 160)	Theft (Section 370)	Misuse of Personal Data (Section 219)	Illicit Access to Data (Section 422)
Voluntary Manslaughter (Section 161)	Embezzlement (Section 372)	Misuse of Public Information (Section 220)	Breach of Information System or Data (Section 423)
Aiding and Abetting Suicide (Section 162)	Fraud (Section 373)	Harassment (Section 222)	Compromising or Defrauding the Integrity of the Computer Protection System or Device (Section 424)
Professional Misconduct (Section 165)	Economic Fraud (Section 374)	Invasion of Privacy (Section 223)	
	Information System Fraud (Section 375)	Degrading Treatment of Vulnerable Persons (Section 225)	

Table 1. Relevant criminal acts in Digital Reality with section numbers.

V. CONCLUSIONS

Hungary's Artificial Intelligence Strategy for 2020–2030 states, that it is necessary to explore legal constraints on and the regulatory needs of AI development and to make proposals regarding changes to be made to the general regulatory environment, along with improvements to the sector-specific regulatory environment in order to facilitate AI development [50]. For this purpose, it is essential to

- continuously monitor the relevant EU rules and soft law,
- develop AI registers and lie down requirements to be applied in the most important areas,
- establish responsibility system applicable for new technologies.

The Expert Group on Liability and New Technologies – New Technologies Formation published their report on Liability for Artificial Intelligence and other emerging digital technologies in 2019 [51]. They have concluded that the specific characteristics of new digital technologies and their applications – including complexity, modification through updates or self-learning during operation, limited predictability, and vulnerability to cybersecurity threats – make it difficult to design a fair and efficient liability system. On the basis of the work of the group the option of adopting a standard-setting

instrument addressing AI, which might take the form of a Council of Europe convention, will be considered [52].

The keywords of the program of establishing appropriate regulation for all platforms of the IoD are sustainability, democracy, necessity and proportionality, rule of law and transparency. Probably there is no simple one size fits all solution to liability issues which might arise. Rather, a balanced and nuanced approach tailored to the issue is likely to be called for.

The present background paper has provided an overview and an analysis of the ethical and legal issues raised by IoD. The results of this study indicate that when it comes to new developments, there are legally binding rules such as data protection and information security. We have also shown that certain human actions that cause a detrimental result in the real world, can be punished under the rules currently in force.

However, EU and the member states would be advised to establish harmonized detailed responsibility system applicable for the designers of new technologies of IoD, since the regulation is quite incomplete for now.

We argue, that starting point for this process should be application of ethical principles such as responsible innovation and precautionary principle. Therefore, as far as there is no clear regulation on this topic, when it comes to innovation, we suggest for designers, developers, testers, and managers to follow a "value-sensitive" approach and respect ethical principles mentioned above. In comparison to latest publications, the novel contribution of the paper consists in emphasizing ethical principles that should be followed by innovators, and in giving brief summary of legislation that is essential for the developers of IoD.

ACKNOWLEDGMENT

This research was supported by the Digital Development Center in the national framework GINOP-3.1.1-VEKOP-15-2016-00001 "Promotion and support of cooperations between educational institutions and ICT enterprises".

REFERENCES

[1] C.R. Srinivasan, B. Rajesh, P. Saikalyan, K. Premsagar, and E.S. Yadav, "A review on the different types of internet of things (IoT)," J. of Advanced Research in Dynamical and Control Systems, vol. 11, no. 1, pp. 154-158, 2019.

[2] J.H. Norda, A. Koohang, and J. Paliszkiewiczc, "The Internet of Things: Review and theoretical framework," Expert Systems with Applications, vol. 133, no. 1, pp. 97-108, Nov. 2019.

[3] P. Baranyi, Á. Csapó, T. Budai, and Gy. Wersényi, "Introducing the Concept of Internet of Digital Reality - Part I," Acta Polytechnica Hungarica, vol. 18, no. 7, pp. 225–240, 2021.

[4] Gy. Wersényi, Á. Csapó, T. Budai, and P. Baranyi, "Internet of Digital Reality: Infrastructural Background - Part II," Acta Polytechnica Hungarica, vol. 18, no. 8, pp. 91–104, 2021.

[5] W.K. Robinson, and J.T. Smith, "Emerging Technologies Challenging Current Legal Paradigms," Minn. JL Sci. & Tech, pp. 355-370, 2018.

[6] J.S. Spiegel, "The Ethics of Virtual Reality Technology: Social Hazards and Public Policy Recommendations," Sci Eng Ethics, vol. 24, pp. 1537–1550, 2018.

[7] M.R. Carrillo, "Artificial Intelligence: From Ethics to Law," Telecommunications Policy, vol. 44, no. 6, July 2020, 101937.

[8] E. Bastug, M. Bennis, M. Medard, and M. Debbah, "Toward Interconnected Virtual Reality: Opportunities, Challenges, and Enablers," in IEEE Communications Magazine, vol. 55, no. 6, pp. 110-117, June 2017.

[9] J.L. Rubio-Tamayo, M. Gertrudix Barrio, and F. García García, "Immersive Environments and Virtual Reality: Systematic Review and Advances in Communication, Interaction and Simulation," Multimodal Technologies and Interaction, vol. 1, no. 4, 21 pages, 2017.

[10] A. Czebe, and G. Kovács, "How cognitive infocommunications play a critical role in shaping the future of forensic sciences defining forensic cognitive infocommunications," in Proc. of 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), 2016.

[11] A. Beke, "Forensic speaker profiling in a Hungarian speech corpus," in Proc. of 9th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), 2018.

[12] M. Zichar, "Guidelines for cost-effective geovisualization in digital forensics," Landscape & Environment, vol. 10, no. 3-4, pp. 117-122, 2016.

[13] P. Baranyi, Á. Csapó, Gy. Sallai, Cognitive infocommunications (CogInfoCom), Springer, 2015.

[14] P. Baranyi, Á. Csapó "Definition and Synergies of Cognitive Infocommunications," Acta Polytechnica Hungarica, vol. 9, no. 1, pp. 67-83, 2012.

[15] D. Collingridge, The Social Control of Technology, Pinter, London, 1980.

[16] H. Sutcliffe, A report on Responsible Research & Innovation, Brussels: Matter, 2011.

[17] J.G. Kormelink (Ed), Responsible Innovation: Ethics and risks of new technologies, TU-Delft, 2019.

[18] European Commission, "Science, Research and Innovation Performance of the EU 2020 - A fair, green and digital Europe," Luxembourg, 2020.

[19] C. Raffensperger, and J. Tickner, "Introduction: to foresee and to forestall," in C. Raffensperger and J. Tickner (Eds), Protecting Public Health and the Environment: Implementing the Precautionary Principle, Washington D.C., 1999, pp. 1-11.

[20] United Nations,"Agenda 21, Rio Declaration, Forest Principles, New York, 1992.

[21] Treaty on European Union OJ C 191, 29.7.1992.

[22] A. Anyshchenko, "The Precautionary Principle in EU Regulation of GMOs: Socio-Economic Considerations and Ethical Implications of Biotechnology," Journal of Agricultural and Environmental Ethics, vol. 32, pp. 855–872, 2019.

[23] J. Hughes, "How Not to Criticize the Precautionary Principle," Journal of Medicine and Philosophy, vol. 31, no. 5, pp. 447-464, 2006.

[24] D. Castro, and M. McLaughlin, Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence. ITIF, 2019. https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence.

[25] W. Pieters, and A. Cleef, "The Precautionary Principle In A World Of Digital Dependencies," Computer, vol. 42, no. 6, pp. 50–56, 2009.

[26] O. Veiligheid, Scientific Council for Government Policy.: Verantwoordelijkheden voor Fysieke Veiligheid, Amsterdam Univ. Press, 2008.

[27] WWR - Scientific Council for Government Policy, Physical Safety, a matter of balancing responsibilities, Amsterdam University Press, 2012.

[28] R. Schomberg, "A vision of responsible innovation," in: R. Owen, M. Heintz, and J. Bessant (Eds.), Responsible Innovation, London, John Wiley, 2013.

[29] J. van de Hooven, "Ethics for the Digital Age: Where Are the Moral Specs?" in H. Werthner, and F. van Harmelen (Eds), Informatics in the Future, Springer, 2017.

[30] European Commission, Rome Declaration on Responsible Research and Innovation in Europe, 2014. https://digital-strategy.ec.europa.eu/en/library/rome-declaration-responsible-research-and-innovation-europe.

[31] Communication from The Commission to the European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Horizon 2020 - The Framework Programme for Research and Innovation /* COM/2011/0808 final, 2011. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52011DC0808.

[32] B. Friedman, Human Values and the Design of Computer Technology, Cambridge University Press, New York, 1997.

[33] M. Madary, and T.K. Metzinger, "Real Virtuality: A Code of Ethical Conduct - Recommendations for Good Scientific Practice and the Consumers of VR-Technology," Frontiers in Robotic AI, vol. 3, no.3, pp. 1-23, 2016.

[34] D. Hosfelt, "Making Ethical Decisions for the Immersive Web," {USENIX} Conference on Privacy Engineering Practice and Respect 19, pp. 1-9, 2019.

[35] B. Friedman, and P.H. Kahn, "New Directions: A Value-Sensitive Design Approach to Augmented Reality," in: Proceedings of DARE 2000 on Designing Augmented Reality Environments, ACM: New York, USA, pp. 163–164, 2000.

[36] L. Floridi, J. Cowls, T.C. King, and M. Taddeo, "Designing AI for social good: seven essential factors," Science and Engineering Ethics, vol. 26, pp. 1771–1796, 2020.

[37] R.R. Romansky, I.S. Noninska, "Challenges of the digital age for privacy and personal data protection," Mathematical Biosciences and Engineering, vol. 17, no. 5, pp. 5288–5303, 2000.

[38] The General Data Protection Regulation (EU) 2016/679 (GDPR).

[39] European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Brussels, 2020.

[40] Department of Defense Cyber Strategy, 2018.

[41] Act C of 2012 on Criminal Code.

[42] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, 2020. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[43] Council of Europe European Committee On Crime Problems, Feasibility Study on a FutureCouncile of Europe Insturment on AI and Criminal Law, 2020. https://rm.coe.int/cdpc-2020-3-feasibility-study-of-a-future-instrument-on-ai-and-crimina/16809f9b60.

[44] D. Eszter. ,"A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései," Infokommunikáció és jog (in Hungarian), 2015/12.

[45] Z. Szathmáry, "A mesterséges intelligencia hatása a büntetőjogi felelősségre," (in Hungarian), Ügyészek Lapja, 2020/6.

[46] L. Royakkers, S.D. Zwart, and I. Poel, Moral Responsibility and the Problem of Many Hands, Routledge, 2018.

[47] Decree No. 6/1990 (IV. 12.) KöHÉM of the Minister of Transport, Communications and Construction on Technical Requirements for Placing into, and Maintaining in Circulation of Road Transport Vehicles, 1990.

[48] Council of Europe, Responsibility and AI. DGI(2019)05. https://rm.coe.int/responsability-and-ai-en/168097d9c5

[49] B.J.V. Keupink, "Virtual criminal law in boundless new environments," International Journal of Technology Transfer and Commercialisation, vol. 6, no. 2/3/4, pp. 160–170, 2007.

[50] Hungary's Artificial Intelligence Strategy for 2020 – 2030, 2020 https://ai-hungary.com/files/e8/dd/e8dd79bd380a40c9890dd2fb01dd771b.pdf.

[51] Directorate-General for Justice and Consumers (European Commission), Liability for artificial intelligence and other emerging digital technologies, 2019.

[52] A. Renda, "Artificial Intelligence. Ethics, governance and policy challenges," Report of a CEPS Task Force, pp. 82-90, 2019. www.ceps.eu/ceps-publications/artificial-intelligence-ethics-governanceand-policy challenges/