Editorial

by **Golnaz A. Jafari, David Roth-Isigkeit and Ronny Thomale***

Recommended citation: Golnaz A. Jafari, David Roth-Isigkeit and Ronny Thomale, Editorial, 12 (2021) JIPITEC 241 para 1.

1 Digitalisation and automation is becoming increasingly embedded in the societal sphere and infrastructure, a process largely enabled and facilitated by technological advances in the fields of Information and Communication Technology (ICT) and informatics in general. The resulting catch-up process in the existing legal and regulatory landscape requires establishing a level playing field for different actors and stakeholders. A fair balance has to be struck between the interests of the public and private sectors in favour of innovation and digital transformation, and the need for a clear pattern of legal and regulatory standards that would safeguard the rights and interests of individuals and communities within the well-established values of economic and democratic diversity and equality.

2 Based on the flux of novel business, governance and economic models being defined and put in practice underscoring the prevalence of the data-driven economy, a collaborative discourse between the disciplines of law and informatics is (inevitably) required allowing for a better understanding of the associated implications and repercussions, affecting individuals in particular. The associated implications on individuals are predominantly the consequence of processing their personal data[1] on a large scale using algorithms, Artificial Intelligence (AI) or machine learning. Here, the effects become even more potentially detrimental when algorithms are utilised in order to detect correlations between separate datasets, which would in turn set the grounds for patterns from behaviour prediction[2] to the exercise of control over access to a service, to name a few. Algorithms as the core element of AI entailing machine learning have seen a rapid evolution, from automated sets of instructions with mathematical logic -based execution triggers to rule-based expert systems and neural networks.

3 In this context, the concept of automated decision making, the varying levels and scope of human intervention throughout these processes and the counterbalancing of associated risks and benefits have in recent years been subject of regulatory scrutiny in various jurisdictions, including the European Union (EU) legal and regulatory landscape. These decisions form and impact an integral part of daily lives of the public, yet in practice remain largely unnoticed. In principle, a decision facilitated by an automated pro-

[*] Golnaz A. Jafari, LL.M., doctoral researcher at Lucernaiuris, University of Lucerne, Switzerland; David Roth-Isigkeit, PhD, head of a junior interdisciplinary research group "SOCAI centre for social implications of artificial intelligence", JMU, Würzburg, Germany; Ronny Thomale, PhD, full Professor at the chair for Theoretical Physics I (TP1), JMU, Würzburg, Germany.

[1] The terms 'personal data' and 'personally identifiable information (PII)' are used interchangeably, with former given preference in the EU regulatory landscape. Under the General Data Protection Regulation (EU) 2016/679 (GDPR), Art. 4(1) the term 'personal data' means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"; Under Art. 4(2) the term 'processing' means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[2] GDPR, Art. 4(4) refers to the term 'profiling' as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"; Note: automated decision making does not always and by default involve profiling.

cessing would need to protect the individuals' rights, freedoms and legitimate interests, which ought to be achieved via implementation of safeguarding measures. Of course, in practice, this would not in itself suffice to render and strengthen individuals' stance, which would in addition require providing for legal certainty and effective judicial recourse.

4 Questions then arise, among others, as to *system transparency* on the one hand, and the levels of *intelligibility* of complex software systems on the other. In this regard, various (implied) individual rights become relevant, such as the information and explanation requirements of the GDPR[3] or the constitutional *right to informational autonomy or self-determination.*[4] The latter is primarily conceived from national constitutions as well as from Article 8 of the Charter of the Fundamental Rights of the EU, which in essence empowers individuals to decide themselves about issues of collection, disclosure and use of their personal data, albeit in the form of a non-absolute right.

5 A modern perception of privacy must take account of individuals' existence within their societal surroundings. In this context, it is rightly argued[5] that "privacy as a legal right, should be conceived essentially as an instrument for fostering the specific yet changing *autonomic capabilities* of individuals that are, in a given society at a given time, necessary for sustaining a vivid democracy." Such capabilities are increasingly threatened by technological tools that provide for vast possibilities of, among others, surveillance and monitoring both for the public and private sectors. Here, in order to strike a balance between competing interests and the right to privacy, and whether legitimate and sufficiently compelling reasons exist for allowing interferences with that right, a normative inquiry would be required on the basis of Article 8 of the European Convention on Human Right (ECHR).

6 Questions also emanate concerning fairness and bias of algorithms, and the quality of input and output datasets in terms of e.g. accuracy and balance, with direct implications for potential risks associated with discrimination in automated decision making systems against individuals and the targeted audience at large.

7 On the other hand, emerging developments in ICT have allowed for distribution in network participation, communication and governance in given contexts. Peer to peer (P2P) network infrastructures are no longer seen as exclusively embedding 'technical distribution' among network participants, while maintaining centralised governance, risking a *single point of failure.* Instead, varying levels of decentralisation in governance could in principle be enabled through the deployment of algorithmic protocols. Distributed Ledger Technology (DLT)[6] denotes a distributed record (ledger) of databases shared among computer nodes outside jurisdictional boundaries, run and maintained according to defined algorithmic consensus protocols. Depending on the form a DLT architecture would take, i.e. public, private, permission-less, permissioned or hybrid, network participation and governance rules as well as the definition of actors and stakeholders and their respective roles, next to network security and scalability would greatly vary. Therefore, legal uncertainty exists, in particular as to the attribution of liability and responsibility which would in turn have an impact on the establishment of *public trust* in these network infrastructures.

8 The present special edition has been put together as a collective effort and team work between the two academic research centres at the University of Würzburg in Germany, namely the Würzburg Centre for Legal and Social Implications of AI (SOCAI) and the CT.QMAT Cluster of Excellence which deals with topics related to complexity and topology in quantum matter. The joint effort includes a conference venue, bringing together academic scholars predominantly from the disciplines of law, computer science and business informatics, and a collaborative publication with the Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC).

9 The SOCAI centre has been founded in 2019 with the intention to foster interdisciplinary dialogue between law and technical disciplines to assess the legal framework of cutting-edge developments in

[3] See the contribution by LK Kumkar & D Roth-Isigkeit in this volume.

[4] See an early reference to the German Federal Constitutional Court Decision of 1983, BVerfG, judgment of the First Senate of December 15, 1983 - 1 BvR 209/83 - Rn. 1-215, for non-authoritative English summary <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html;jsessionid=8EE69329DD3CC934B0D1321957DB249D.1_cid386>; see also A Rouvroy & Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S Gutwirth et al. (eds.), *Reinventing Data Protection?* (Springer Netherlands, 2009) ch.2, 45-76; see also C de Terwangne (on behalf of European Commission JRC), 'The Right to be Forgotten and the Informational Autonomy in the Digital Environment' (2013) 4ff; see also the contribution by F Thouvenin in this volume.

[5] Ibid Rouvroy (2009) 46.

[6] The terms 'blockchain' and 'distributed ledger technology (DLT)' may be utilised interchangeably throughout this draft.

hardware and software technology. Such a focus can potentially prove fruitful since – as has become clearly visible in the EU regulatory efforts on AI or data protection – law making procedures come with a considerable backlog that makes it practically difficult to orient legislation on the newest technological advancements. Yet, it is precisely this knowledge about possible legislative directions that could provide certainty to businesses and individuals and thereby accelerate and direct technological progress.

10 In this context, previous projects in cooperation with the CT.QMAT Cluster of Excellence[7] have focused on the joint development of legal norms and latest advancements in hardware. Contemporary progress towards applications of AI, deep learning and digital transformation predominantly necessitates the processing of a vast amount of data. This constitutes a major challenge, given that the steady growth of computing efficiency and higher integrated circuitry for central processing unit (CPU) power has reached its physical boundaries. As such, the prospective unfolding of the digital transformation in society will not only decisively depend on technological progress at the software, but also at the hardware level. For any useful societal support and regulation of the digital transformation, the availability and cost efficiency of future material platforms for next generation computing and data processing are thus the crucial parameters that will impact the scope of applications and the actual user group.

11 Therefore, the frame would need to be extended beyond the dimension of software. We believe that only an integrated perspective of law, hardware and software development would be fit to provide an understanding of the complex societal challenges that are embodied in technological progress. Largely speaking, social science research on digital transformation addresses the question of how we can use the technology-driven transformational uprising to create a state that is beneficial for humanity from a long-term perspective. In order to succeed, both crucial aspects of technical progress would need to be taken into account. In other words, awareness would need to be raised as to the inherent volatility of digital transformation mostly due to the fundamental uncertainties in hardware and software innovation.

12 Following this background, the idea behind our present conference has been to embed a number of central themes providing for a platform for further discourse. These include, but are not limited to, a) technical concept of 'distributed by design' and legal uncertainties as to jurisdictional boundaries, b) attribution of liability in DLT-based networks in the absence of a clear definition of roles and responsibilities among actors and stakeholders, c) digitisation of the state and potential consequences on fundamental rights of individuals, d) growing dominance of corporate entities in big data analytics and implications on the concepts of individual consent and control, e) data inaccuracy and bias in automated decision making processes and possible technical tools for detection and mitigation thereof, and f) identity management systems and individuals' control over all matters related to processing of personal data.

13 Contributions to this edition have mostly taken an interdisciplinary approach addressing, directly or indirectly, a combination of any of the above themes or more, synopses of which could be encapsulated as follows, without any particular order.

- With reference to automated decision making, in particular methods that are enabled by machine learning, a first paper acknowledges increased threats to the fundamental rights of data subjects. In doing so, the authors Kumkar and Roth-Isigkeit take the view that *explanation* requirements are merely a necessary starting point for a human review, arguing that the subjective legal asset discussed under the term *right to explanation* actually turns out to be a preparatory *right to justification*. On the one hand, this viewpoint would allow the law to reflect the general opacity of intelligent decision making systems in order to provide for a practical way of dealing with the limited explicability. On the other hand, law recognises the *autonomy* of intelligent decision making systems to the extent that the procedural and deterministic explanation of decision making is replaced by the subsequent substantive legality test. Law thus finds its mode of dealing with the non-explicability of machine decisions in converting its procedures to the model of justification adapted to human decisions.

- *Informational self-determination* is seen as the underlying rationale of the fundamental right to the protection of personal data as enshrined in Article 8 of the Charter of Fundamental Rights of the EU. The author Thouvenin adopts the stance that acknowledging informational self-determination as a fundamental right would mean that the state may not require citizens to provide information about themselves and government agencies may not use such information without a sound legal basis, leaving out any obligation on the part of the private actors. Contrary to a widespread assumption, the author stipulates that most data processing of private actors is not based on data subjects' consent but on the legitimate interests of the controller. The

[7] Reference to the research group coordinated by Ronny Thomale and Giorgio Sangiovanni, Lehrstuhl für Theoretische Physik 1, JMU, Würzburg.

relation between data subjects and private actors, namely businesses that process personal data about their customers, is therefore hardly ever based on exercising informational self-determination. This factual finding is supported by a normative analysis which demonstrates that the idea of informational self-determination can hardly be reconciled with the principle of private autonomy and the resulting need to provide a justification for the granting of a right that allows one private actor to control the activity of another. Thus, while informational self-determination may be acknowledged as a fundamental right, the author concludes that the concept cannot serve as a convincing rationale for an all-encompassing regulation of the processing of personal data by private actors.

- Over the last two decades, the number of organisations, both in the public and private sector, which have automated decisional processes, has grown notably. The phenomenon has been enabled by the availability of significant amounts of personal data and the development of software systems that use those data in order to optimise decisions with respect to certain optimisation goals. Today, software systems are involved in a wide realm of decisions that are relevant for the lives of people and the exercise of their rights and freedoms. The approach taken in this paper by the author Vetrò shifts the focus away from the outcomes of automated decision making systems and instead concentrates on inputs and processes. The foundations of a risk assessment approach are then laid based on a measurable characteristic of input data, i.e. *imbalance*, which can lead to discriminating automated decisions.

- A significant opportunity to engage in greater scrutiny of the digital transformation of the state, and its impact on fundamental rights, presented itself in a landmark judgment from the Netherlands. In the said case, the automated welfare-fraud detection system called *Systeem Risico Indicatie* (SyRI) was considered, allowing for the linking and analysis of data from an array of sources in order to generate fraud-risk reports on the public. In its judgment, the Court held that the legislation underpinning SyRI violated *the right to private life*, guaranteed under Article 8 ECHR. Taking a case study approach, the authors Appelman, Ó Fathaigh and van Hoboken highlight an important principle taken into account by the Court, namely the *special responsibility* that would need to be assumed by the government when applying new technologies to strike the right balance between the benefits the use of such technologies brings, and the potential interference with the exercise of *the right to private life*.

- By definition, blockchain[8] platforms offer secure and reliable data exchange between stakeholders without a trusted third party. Private and consortium blockchains implement access restrictions, so that private data would in principle be kept from the public. However, due to its distributed structure, only by means of one node all blockchain data could risk being leaked, due to a faulty configuration. This study by authors Hofmann, Gwinner, Winkelmann and Janiesch depicts ways in which confidential information could be revealed from blockchains, which should not be exposed to the public and which would potentially include identities, contract data as well as legal data. Thereby, the legal and social implications of data leakage by this distributed and supposedly secure technology are illustrated. In summary, the paper concludes that the large attack surface of private or consortium blockchains poses a threat to the security of the networks, raising the question whether (private) blockchain networks can reach a consensus without sharing all data between nodes and what data distribution strategies defend best against weak links in the chain.

- Blockchain technology is associated with the emergence of Decentralised Autonomous Organisations (DAO) as sovereign and software-based agents. A blockchain-based peer to peer vending machine as a physical marketplace, governed by a DAO, serving as both a testing ground and a speculative artefact is posited and analysed from a *de lege lata* perspective, taking into account the foremost liability questions from both Swiss private law (tort and contractual) and public law (criminal and tax law) perspectives. For this, the authors Schuppli and A. Jafari propose a hypothetical case study upon which the legal analysis is applied. As a result of the analysis the paper highlights where the current Swiss legal framework produces unsatisfactory results. From a private law perspective, the fact that contracting parties have little to no factual recourse in case of a purchase of counterfeit goods is an undesirable state from a public policy perspective. In other words, neither consumer protection nor good faith in commercial dealings would be viably upheld in this scenario. From a public law perspective, on the other hand, it is depicted that the state faces insurmountable challenges in taxing and collecting the taxable transactions involving a blockchain-based vending machine. Also, perpetrators of criminal offences, i.e., members of a DAO or unidentifiable

[8] See n 6.

associates of a DAO, could likely not be brought to justice – an outcome which directly infringes on the public good of legal protection and undermines trust in government. The authors take the position that Swiss substantive law currently does not offer a satisfactory framework to deal with such novel decentralised market infrastructures. Individuals interacting with the proposed infrastructure, be it as vendors, buyers or members of the DAO, would face uncertainty related to both private and public law enforcement. Thus, the overall functioning of the legal economy and the rule of law would be infringed upon.

- The ultimate contribution puts Facebook's Diem[9] project under scrutiny. On the one hand, many critics have recognised dangers to state currency sovereignty and the stability of the financial system; on the other hand, they fear negative developments regarding money laundering and the financing of terrorism. In addition, there are considerable concerns about an ever deeper erosion of privacy, consumer and data protection, which reaches a new dimension by linking such world currencies with already existing social networks governed and controlled by private entities. Under these circumstances, the chance of success of the Diem project clearly depends on the extent to which the aforementioned concerns can be dispelled and whether *public trust* can be established. Moreover, it is argued that the level of control by end users over their digital representations and online footprints remains untested in the context of a worldwide digital financial infrastructure as proposed by Diem. The authors A. Jafari and Gruber further elaborate and put data protection and privacy of end users under scrutiny, outlining the need for a self-sovereign identity (SSI) management system in order to address the risks associated with correlation and profiling of individuals concerning their behaviour in payment systems. The paper then concludes that for Diem to experience a realistic mass adoption and to serve as a complementary infrastructure to the established monetary systems, it must itself prove to be a constitutive part of the *lex digitalis*. Evolving into the *lex cryptographia*, it will depend on the *pouvoir constituant* of the digital world whether it succeeds in further developing a digital civil constitution in the medium of DLT. Such a constitution, not least with its respective identity management, will determine what human life will be like in a truly *vibrant ecosystem*.

14 Lastly, we would like to take the opportunity to forward our special regards to everyone who has contributed and provided us with support throughout this process, in particular special thanks to the SOCAI team members, Alina Machert, Sarah Eisert, Jason Coombe, Ruben Maass and Dominik Klaus as well as each and every one of the contributors to the SOCAI/JIPITEC special edition. Further thanks extend to Thomas Dreier and Gerald Spindler for accepting this volume as a special edition of the *Journal of Intellectual Property, Information Technology and E-Commerce Law* (JIPITEC) and Lydia Förster for her support of the editorial work at JIPITEC. The publication of this edition was supported by the Würzburg-Dresden Cluster of Excellence on Complexity and Topology in Quantum Matter — ct.qmat (EXC 2147, project ID 390858490).

[9] Diem is formerly known as Libra.