SPECIAL ISSUE
THE YALE INFORMATION SOCIETY PROJECT & YALE JOURNAL OF LAW AND TECHNOLOGY DIGITAL PUBLIC SPHERE SERIES

RESPONSIBILITY FOR ALGORITHMIC MISCONDUCT: UNITY OR FRAGMENTATION OF LIABILITY REGIMES?

Anna Beckers and Gunther Teubner***

25 YALE J.L. & TECH. SPECIAL ISSUE 76 (2023)

When autonomous algorithms act within socio-digital institutions and take wrong decisions, what are the consequences for legal liability? Is a uniform liability regime required, or should fragmentation along sectoral rules prevail? The article argues for a middle path between the Scylla of one-size-fits-all and the Charybdis of situationism. For an appropriate diversity of liability regimes, this article draws on a typology of machine behavior developed in IT-studies and simultaneously on sociological and philosophical theories which suggest identifying the foundations for three emerging socio-legal institutions in (1) personification of non-human actors, (2) human-machine association as an emergent social system with the qualities of a collective actor, and (3) distributed cognition in the interconnectivity of algorithms. The liability regimes proposed in this article will have a considerable impact on the digital public sphere and its regulation. The differentiating approach will contribute significantly to the digital constitution that is currently emerging.

TABLE OF CONTENTS

I. THREE CASES: DIGITAL RESPONSIBILITY GAPS

A. *Robo-Advice*

Samathur Li Ki-kan, a Hong Kong tycoon, sues Raffaela Costa, an investment broker, for damages of $23 million for the failures of a robo advice computer. The supercomputer, named K1, was supposed to comb through online sources to gauge the emotional sentiment (!) of investors and make related predictions for US stock futures. Although the first simulations looked highly promising, large sums of money were regularly lost when the computer was used in real-life stock trading. On 14 February 2018, Li lost over $20million due to a stop-loss order.[1] This is the first known case in which a claim for damages was brought to the courts that concerned investment losses caused by the decisions of an autonomous algorithm. The case raises a black box problem: if humans cannot understand the algorithm's decisions, who is liable if something goes wrong? Under current law, there is no compensation for damages if the human actors involved have fulfilled their duties of conduct. No one is liable for mere machine failure. In our context, this is the first major responsibility gap.

B. *Panama Papers*

The second major responsibility gap looks completely different. We will illustrate it with the example of investigative journalism. It is common practice today in journalism to use algorithms for investigation and the production of content and news. This was also the case in this real-life case that we have partly amended. In a complex investigation to uncover illegal tax practices, an international consortium of journalists used software to analyze numerous documents.[2] The software was

---

* Associate Professor of Private Law and Legal Methodology, Maastricht University, The Netherlands

** Emeritus Professor of Private Law and Legal Sociology, Goethe-University, Frankfurt am Main, Germany. This article expands on arguments in ANNA BECKERS & GUNTHER TEUBNER, THREE LIABILITY REGIMES FOR ARTIFICIAL INTELLIGENCE: ALGORITHMIC ACTANTS, HYBRIDS, CROWDS (2021).

[1] See for details of the case, Thomas Beardsworth & Nishant Kumar, *Going to Court Over Losses When Robot Is to Blame*, INSURANCE JOURNAL (May 7, 2019), https://www.insurancejournal.com/news/national/2019/05/07/525762.htm; Nicholas Pratt, *HK Investor Sues Robo-adviser in Potential Landmark Case about AI Liability*, COMMERCIAL RISK (May 14, 2019), https://www.commercialriskonline.com/hk-investor-sues-robo-adviser-in-potential-landmark-case-about-ai-liability/.

[2] This is a fictitious case, but one that uses publicly available information on the Panama Papers research to illustrate the emergent properties of a human-algorithm association and its legal problems. For details: Von Ivonne Wagner, Wolfgang Jaschensky & Laura Terberl, *Panama Papers: The*

used to reduce for the immense difficulties of the investigative work, to analyze and make sense of an enormous number of complex technical documents. Algorithms were used for marking, categorizing and selecting the relevant texts. Humans were involved in their work in close interaction.[3]

Although such human-algorithm cooperation can be extremely beneficial for uncovering complex news stories—some of the journalistic investigations would have been impossible without the help of the technology—there is also a considerable potential for damage. Who is liable, for example, if during such an investigation persons or companies are accused of misconduct, that, in fact, were not involved? In this situation, a responsibility gap emerges when it cannot be clearly determined whether it was the algorithm that was at fault or it was the humans that erred. Current law does not provide for liability of a human-machine association.

C. Flash Crash

A third, again different, responsibility gap occurs when multiple algorithms act in interconnection. Algorithmic high-frequency trading is the most prominent case that has the potential to cause so-called "flash crashes". Such a flash crash happened in 2010 on the US capital market.[4] To assign responsibility, the US Department of Justice identified one trader, Navinder Saro, who was supposed to be responsible for causing the crash. Saro was sued for conducting so-called "spoofing": his algorithm allegedly placed false orders on the market for inducing other trading algorithms to follow his example. This allowed him to change his own strategy in the exact opposite direction to make profits. The investigation revealed that human-initiated spoofing had indeed caused the other algorithms' behavior and ultimately triggered the crash. However, the immense damage seemed to be caused primarily by algorithmic high-frequency trading involving algorithms that are programmed very similarly and thus mutually reinforce their actions.[5] This points to herd behavior in which individually programmed decisions accumulate in an interdependent process, triggering catastrophic consequences. In such cases, where

---

Journalists behind the Leak, SUDDEUTSCHE ZEITUNG (April 25, 2016), https://www.sueddeutsche.de/politik/panama-papers-the-journalists-behind-the-leak-1.2966929 .

[3] On hybrid journalism in general NICHOLAS DIAKOPOULOS, AUTOMATING THE NEWS: HOW ALGORITHMS ARE REWRITING THE MEDIA, 13-40(2019).

[4] U.S. COMMODITY FUTURES TRADING COMMISSION & U.S. SECURITIES & EXCHANGE COMMISSION, FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010 (2016), https://www.sec.gov/files/marketevents-report.pdf.

[5] Yesha Yadav, *The Failure of Liability in Modern Markets*, 102 VIR. L. REV 1031, 1080 (2016)

algorithms act correctly individually, but cause damage due to their mutual reinforcement, traditional liability law fails completely. This is the third major variant of the responsibility gaps.

II. LIABILITY REGIME: UNIFORMITY OR DIVERSITY?

How can liability law deal with those responsibility gaps? There are two options: uniformity, or fragmentation.

Several authors favor a uniform treatment of these three responsibility gaps. They neglect their differences and argue for a one-size-fits-all solution. They treat algorithmic failures indiscriminately in all three situations. Either, they declare algorithms as mere tools of human actors and apply strict liability principles.[6] Or, they treat them as agents of human principals and apply vicarious liability rules. [7] Or, they construct them as self-interested "e-persons" and make them directly liable—provided of course they have the necessary financial resources.[8]

In contrast to these positions we think that, as a response to different algorithmic risks, a differentiation of liability regimes is inevitable.[9] One needs to distinguish a distinct variety

---

[6] EWA HARASIMIUK & TOMASZ BRAUN, REGULATING ARTIFICIAL INTELLIGENCE: BINARY ETHICS AND THE LAW 122-__ (2021); Emiliano Marchisio, *In Support of "No-Fault" Civil Liability Rules for Artificial Intelligence*, 1 SN SOC. SCI. 54 (2021); ANDREA BERTOLINI, ARTIFICIAL INTELLIGENCE AND CIVIL LIABILITY, at §§ 5.1-5.3 (2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf; Christine Wendehorst, *Strict Liability for AI and other Emerging Technologies*, 11 J. EUR TORT L. 150, 161 (2020).

[7] Mihailis E. Diamantis, *Vicarious liability for AI, Cambridge Handbook of AI and Law in* CAMBRIDGE HANDBOOK OF AI AND LAW (Kristin Johnson & Carla Reyes eds., 2022)**;** Pinchas Huberman, *A Theory of Vicarious Liability for Autonomous Machine-Caused Harm*, 58 OSGOODE HALL L. J. 254 (2021); Anat Lior, *AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondent Superior Analogy*, 46 MITCHELL HAMLINE L. REV 1043, 1084 (2020); Ryan Abbott, *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, 86 GEO. WASH. L. REV. 1, 22 (2018); Karni A. Chagal-Feferkorn, *The Reasonable Algorithm*, UNIV. ILL. J. L. TECH & POL'Y 111, 115 (2018); JACOB TURNER, ROBOT RULES: REGULATING ARTIFICIAL INTELLIGENCE at 101 (2018).

[8] Alicia Lai, *Artificial Intelligence, LLC: Corporate Personhood as Tort Reform*, 2021 MICH. STATE L. REV. 597, 631 (2021); S.M. Solaiman, *Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy*, 25 A.I. & L. 155 (2017); Jessica Allain, *From Jeopardy! to Jaundice: The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems*, 73 LA. L. REV. 1049, 1078 (2013); ; Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 N.C. L. REV. 1231 (1992).

[9] Similarly against uniform solutions, Tobias D. Krafft, Katharina A. Zweig & Pascal D. König, *How to Regulate Algorithmic Decision-Making: A*

of responsibility situations according to the variety of liability gaps. The differences between these gaps explain the somewhat bewildering fact that algorithms appear in many guises; sometimes as mere objects or tools, sometimes as complex persons, sometimes as strange in-between entities, sometimes as depersonalized processes. There is no one right solution for attributing a social status to algorithms. These differences make it difficult, if not impossible, to provide a one-size-fits-all solution for liability, either product liability, strict liability, or liability of the e-person itself.

Instead, we encounter a whole variety of status attributions. These attributions do not just reflect legal scholars' preferences, but depend on the inner logic of a variety of social institutions involved. It is not society as such that attributes personhood in a collective act. Rather, each social context has its unique criteria of personhood; the economy is no different from politics, science, moral philosophy—or the law. Each one of the fragmented social systems attributes actions, decisions, assets, responsibilities, entitlements and obligations differently to individual actors, collective actors or algorithms as its 'persons' and equips them with capital, interests, and even intentions, goals or preferences. The variety of concrete social institutions, like exchange, association or principal-agent relations, excludes a uniform status ascription and requires different types of personification with specified properties.

A. False one-size-fits-all solutions

But why exactly are uniform solutions the wrong approach to take? The reason is that only very few situations exist where individual algorithms acting in isolation function as units of responsibility. Of course, these situations will continue to exist, and individual liability law will remain relevant for them. More often, however, liability law will have to develop solutions both for damages from collective acts of human-algorithm associations and for damages from comprehensive computer networks.[10]

It is true that a uniform liability regime offers the advantage of greater flexibility if new risks arise due to technical developments. But to generally rely on strict liability and thus

Framework of Regulatory Requirements for Different Applications, 16 REGUL. & GOVERNANCE 119 (2022); Bernhard Koch, *Product Liability 2.0 — Mere Update or New Version?, in* LIABILITY FOR ROBOTICS AND IN THE INTERNET OF THINGS 113 (Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer eds., 2019).

[10] Argyro Karanasiou & Dimitris Pinotsis, *Towards a Legal Definition of Machine Intelligence: The Argument for Artificial Personhood in the Age of Deep Learning*, ICAL'17: PROCEEDINGS OF THE 16TH EDITION OF THE INTERNATIONAL CONFERENCE ON ARTIFICAL INTELLIGENCE AND LAW 119.

treat algorithms as mere objects would unjustifiably disadvantage the operator of the algorithm because he is not always setting the specific risk involved. If other actors create their specific risks, i.e. programmers, producers, the entire network of actors behind the algorithm or the whole industry involved, then it is inappropriate to hold the operator exclusively liable. Conversely, treating algorithms as fully-fledged subjects makes sense only if they not only play the role of digital assistants, but become self-interested actors. Again, in the case of a human-algorithm association, complete personification would be irrelevant in liability law because, in the dense interactions, an individual responsible actor is not identifiable at all. And finally, in computer interconnectivity, it makes no sense to grant each of the algorithms involved the status of an autonomous e-person. How is one supposed to find the responsible e-person in the multitude of e-persons involved?

B. The fallacy of misplaced concreteness

At the same time, a plea for different liability regimes should not end up in the "fallacy of misplaced concreteness"[11] of a radically sectoral approach. It is true that a sectoral approach, which develops specific liability rules for each type of algorithm, would have some obvious advantages. It can count on the experience with existing liability law and can be better adapted to technological and social developments.[12] However, as it then very soon turns out, such an approach requires a myriad of "ad hoc regulations".[13]

Such ad hoc regulation is only superficially plausible. A radically situationist approach will get lost in countless specifics. It suffers from excessive contextualism that tries to respond to the infinite number of concrete circumstances with ever new regulations, instead of abstracting typical risk situations. The biggest problem, however, is that legislators are likely to develop ad hoc liability rules only for those digital actors whose negative externalities are a politically "hot" topic. But this blatantly violates the principle of equal treatment. In particular, it violates the principle of "technology neutrality". This principle prohibits a higher regulatory burden for one form of technology in comparison to others which are functionally equivalent.[14] Why

[11] ALFRED N. WHITEHEAD, SCIENCE AND THE MODERN WORLD 52 (1997))1925).

[12] See e.g. Georg Borges, *New Liability Concepts: The Potential of Insurance and Compensation Funds, in* LIABILITY FOR ROBOTICS AND IN THE INTERNET OF THINGS 145, 152 (Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer eds., 2019).

[13] BERTOLINI. 2020, *supra* note 6, 102.

[14] Technology neutrality requires a careful analysis "whether and how use of the technology impacts analysis under existing technology neutral laws or genuinely poses questions requiring the development of new legal

should far-reaching strict liability rules apply in the car industry while patients in hospitals remain unprotected from algorithmic errors? Does it really make sense to develop a specific liability regime for, say, lawnmowers, industrial robots, smart kitchen appliances, surgical robots or military and emergency robots, as it is currently being proposed?[15] Liability law would be at the mercy of the whims of local politicians and the varying lobbying power of different industries. The legal principle of treating equal cases equally and unequal cases unequally requires distinctions that are not based on random factual differences, but on normatively viable criteria. This does not exclude deviating from the principle of technology neutrality if there are overriding legal policies.[16] The opposite is the case. Adapting liability law principles to the inner logic of a variety of social institutions, as we argue, requires well-reasoned arguments in favor of "industry-specific goals that we may try to foster by distributing accident costs in a specific way (with strict liability, or negligence, or enterprise liability, or fund, etc.) rather than consisting of the imperatives of a normatively coherent 'liability law' per se."[17] But apart from these deviations, it seems most suitable to work out different digital risk types on the basis of different machine behavior, which provide a plausible basis for different liability regimes.

III. MACHINE BEHAVIOR, SOCIO-DIGITAL INSTITUTIONS, LIABILITY LAW

A. Machine behavior and socio-digital institutions

1. Against the technology-determinist short circuit

Many authors make an interdisciplinary short-circuit in their reform proposals. They draw far-reaching conclusions for liability from examinations of the technical properties of computers. "Technology determines legal liability" – with such an argument, they remain caught in simple causal models and equally simple normative conclusions. In contrast, we propose a more complex and fragmented model that places the different social contexts of computer use at the center of liability arguments and emphasizes the role of the social sciences in developing an appropriate liability regime.

---

principles", Carla L. Reyes, *Autonomous Corporate Personhood*, 96 WASH. L. REV. 1453, 1509 (2021); also 1507-1510.

[15] See the critique by Koch, *supra* note 9, at 114.

[16] But the burden of arguments is on those who favor the deviation. For details on this debate, see Reyes, *supra* note 14, at 1507.

[17] This has been expressed by Pinchas Huberman in the comments on this paper.

Our starting point is a typology developed in IT studies that distinguishes three types of machine behavior: individual, collective and hybrid.[18]

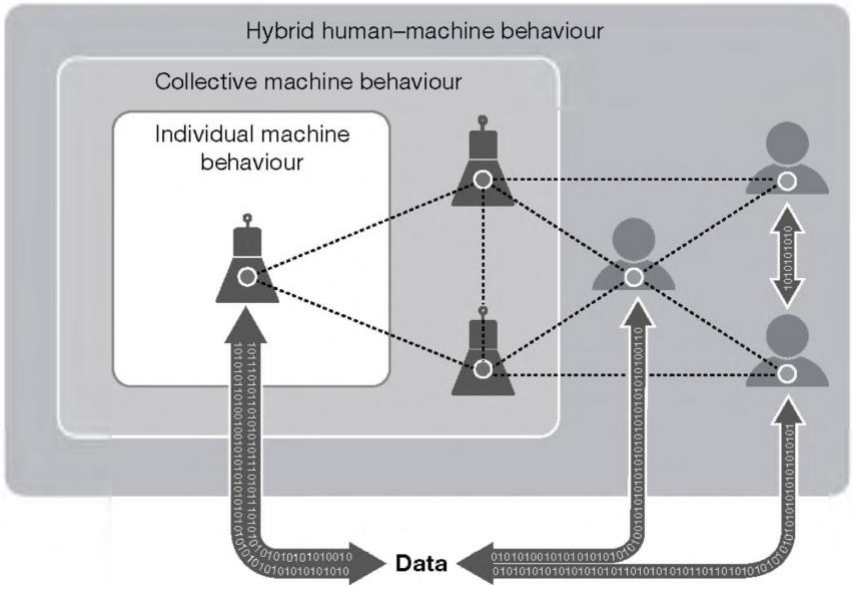

Fig. 1: Three types of machine behavior. Source: Rahwan et al. 2019, p. 482, Fig. 4.

This typology is likely to be highly relevant for liability law. In addition, however, to avoid the technology-determinist short-circuit, it is necessary to introduce "socio-digital institutions" as intervening variables between technology and law. By socio-digital institutions, we mean stabilized complexes of social expectations, in our case expectations regarding the behavior of algorithms in social contexts. Such institutions are neither identical with social systems, nor with formal organizations, nor with social relations. Rather, social systems, including formal organizations and interpersonal relations, produce expectations via their communications, which—to use a classical formulation—condense into institutions under an "idée directrice". Such expectations are institutionalized when consensus can be assumed to support them.[19] Moreover, because institutions consist of expectations, they have the ability to build bridges between different social systems and their expectations.[20] Their bridging to law is particularly striking because social norms and legal norms have the same if-then structure and differ only in their orientation to specific binary

[18] Iyad Rahwan et al., *Machine Behaviour*, 568 NATURE 477, 481 (2019).

[19] NIKLAS LUHMANN, A SOCIOLOGICAL THEORY OF LAW (Elisabeth King-Utz & Martin Albrow trans., 1985), ch.II.4.

[20] See in more detail Gunther Teubner, *Legal Irritants: Good Faith in British Law or How Unifying Law Ends Up in New Divergence*, 61 MOD. L. REV. 11, 21 (1998).

codes. In such bridging institutions, expectations of a legal, economic, political and technological nature meet, and it is often difficult to distinguish between the expectations of the systems involved.

Now, socio-digital institutions integrate diverse technical and social expectations about the opportunities and risks of using algorithms. This happens in a process of co-production.[21] These institutions thus serve as effective structural couplings between technical and social systems, including the legal system.

Only their embedding in different socio-digital institutions explains (as we said above) the thoroughly confusing fact that algorithms sometimes appear as mere objects or tools, sometimes as complex constructs of persons, sometimes as members of strange hybrids, sometimes finally as entirely depersonalized processes.[22] Different attributions of social status depend on the intrinsic rationality and normativity of the respective socio-digital institution.

2. The constitutive role of the social sciences

We thus argue for an "institutional turn" in the law of digitality.[23] Idiosyncratic socio-digital institutions structure the appropriate models of responsibility for the actions of autonomous algorithms.[24] For adequately understanding these contexts, the social sciences are needed. They serve as intermediaries between IT sciences and jurisprudence.[25] Their methods are able to analyze in-depth specific socio-digital institutions and their risks, and to interpret them with sufficient density. In such an institutional analysis,[26] the role of the social sciences is by no means limited to merely descriptive-empirical research of existing social norms, as lawyers often misunderstand it. Rather, their central contribution is to independently interpret the significance of socio-digital

[21] On the co-production of different social systems ANDREW FEENBERG, TECHNOSYSTEM: THE SOCIAL LIFE OF REASON 75 (2017); Sheila Jasanoff, *The Idiom of Co-Production'*, *in* STATES OF KNOWLEDGE: THE CO-PRODUCTION OF SCIENCE AND THE SOCIAL ORDER (Sheila Jasanoff ed. 2004).

[22] Reyes, *supra* note 14, at 1483.

[23] This follows the call for an institutional turn in contract interpretation, which becomes particularly relevant for emerging institutions in the digital sphere: Dan Wielsch, *Contract Interpretation Regimes*, 81 MOD. L. REV. 958, 959 (2018).

[24] Jack Balkin, *The Path of Robotics Law*, 6 CAL. L. REV. CIR. 45, 49 (2015).

[25] Reyes, *supra* note 14, at 1475.

[26] Comprehensively PHILIP SELZNICK, LAW, SOCIETY AND INDUSTRIAL JUSTICE (1969).

institutions and use "institutional imagination"[27] in a narrower functional or wider normative sense.

Socio-digital institutions correlate in their differences with the three types of machine behavior mentioned above: (1) Individual machine behavior is realized as agent's action in the institution of digital assistance. (2) Hybrid machine behavior produces affordances for the institution of a human-machine association that emerges in the dense interaction between humans and machines.[28] (3) Collective machine behavior occurs when interconnected algorithms remain only indirectly connected to the social sphere. Here, society is exposed to invisible machines and their interconnected operations. Each type of machine-behavior thus creates the technical preconditions for the unfolding of a specific socio-digital institution.

A. Socio-digital institutions and liability law

For each socio-digital institution, we propose a specific liability regime. Each socio-digital institution has its own novel risks of harm to which liability law must respond: The risk of *digital assistance* arises when tasks are delegated to autonomous algorithms instead of humans and their decisions can no longer be controlled. *Human-machine associations* create the risk of emergent collective decisions that cannot be traced back to individual decisions of the algorithms or humans involved. The risk of *digital interconnectivity* is related to society's exposure to an opaque network of uncontrollable interconnected algorithms.[29]

In choosing relevant social science theorems, liability law cannot rely exclusively on economic analyses, as many authors suggest.[30] While economic perspectives are certainly relevant when it comes to identifying incentives for appropriate standards of care and activity levels, they are relatively indifferent to broader societal problems, especially victims'

---

[27] Roberto M. Unger, *Legal Analysis as Institutional Imagination*, 59 MOD. L. REV. 1 (1996).

[28] Affordances are "opportunities or constraints of a technology that are co-shaped within the processes of material design and social interpretation", Christoph B. Graber, *How the Law Learns in the Digital Society*, 3 LAW, TECH. & HUMANS 12, 14 (2021).

[29] For details BECKERS & TEUBNER. 2021, *supra* note **, at 14-22, 45-86, 89-110, 111-137.

[30] E.g., GEORGIOS I. ZEKOS, ECONOMICS AND LAW OF ARTIFICIAL INTELLIGENCE: FINANCE, ECONOMIC IMPACTS, RISK MANAGEMENT AND GOVERNANCE (2021); Gerhard Wagner, *Robot, Inc.: Personhood for Autonomous Systems?*, 88 FORD. L. REV. 591 (2019); MITJA KOVAC, JUDGEMENT-PROOF ROBOTS AND ARTIFICIAL INTELLIGENCE: A COMPARATIVE LAW AND ECONOMICS APPROACH (2020).

compensation, encroachment of public institutions, or ecological damage. According to the principle of "transversality" developed in philosophy and sociology, we propose to gain relevant insights from other social sciences as well. In doing so, we refer in particular to theories on the social personification of algorithms, on emergent properties of human-algorithm associations and on distributed cognition in interconnected algorithms.

1. Digital assistance

Individual machine behavior refers to intrinsic properties of an individual algorithm whose dynamics are determined by source code or design in its interaction with the environment.[31] As suggested above, these technical properties alone cannot determine whether algorithms qualify as autonomous actors or not. Instead, socio-digital institutions determine whether algorithms assume the social status of mere instruments, whether they are agents in principal-agent relationships or whether—as a possible future development—they become self-standing socio-economic actors that act in their own interest ("e-persons").

Sociological analysis clarifies the conditions under which the institution of digital assistance emerges. If the delegation of tasks from a human actor (or an organization) to an algorithm creates two autonomous but interdependent chains of action, then a principal-agent relationship emerges between them.[32] Such relationships necessarily presuppose social agency for both the principal and the agent. Therefore, within digital assistance, a (partial) attribution of personhood to algorithms becomes necessary.

Personification of algorithms – for this complex process, several social theories provide the appropriate rationale. Economists contribute relatively little to this topic. When they observe the use of algorithms in markets, they implicitly perceive algorithms as rational actors. In contrast to narrow rational choice assumptions, sociological theory analyses personification as a performative act that institutes the social reality of an actor, which cannot be identified with a specific rationality, economic or else. Actor-Network Theory defines the interactive qualities that transform an algorithm into an 'actant'.[33] Information philosophy defines the conditions under

[31] Iyad Rahwan, et al., *Machine Behaviour*, 568 NATURE 477(2019)., *supra* note 18, at 481.

[32] e.g. Krafft et al., *supra* note 9, at 119.

[33] BRUNO LATOUR, POLITICS OF NATURE: HOW TO BRING THE SCIENCES INTO DEMOCRACY 62-__ (Catherine Porter trans., 2004)

which algorithmic actions can be considered autonomous.[34] Systems theory describes in detail how, in a situation of double contingency, emergent human-machine communication constitutes the social identity of the algorithm and its (limited) action capacities.[35] Each social context creates its own criteria of algorithmic personification, the economy no differently than politics, science, morality or law. Political philosophy describes in detail how the transfer of a "*potestas vicaria*" constitutes the personhood of algorithms in principal-agent relations, which opens up new productive potentials but at the same time "implies clear risks and dangers for modernity".[36]

As a result of social personification, technological risks are transformed into social risks. Causal risks stemming from the movement of objects are now conceived as action risks arising from the disappointment of Ego's expectations about Alter's actions. In digital assistance, no longer an instrumental subject-object relationship appears, instead, a subject-subject relation, more precisely a principal-agent relation with its typical communicative risks. The more the institution of digital assistance covers online transactions, the more the law is challenged to decide according to its own criteria the type of legal personhood that it grants to digital actors. In this constellation, special liability rules are necessary that react to the risks of digital actors' decision-making, which differ from the causal risks of dangerous objects. This is why legal policy proposals are inadequate that introduce a new strict liability regime or simply modify the product liability rules. Such proposals would treat algorithms wrongly as objects, as dangerous installations or as defective products and ignore what is new about algorithms: their autonomous decision-making ability. Instead, the rules of vicarious liability are to be applied to faulty decisions of algorithms in the context of digital assistance. The principal is bound when the algorithm enters into contracts as an agent, and the principal is liable when the algorithm decides incorrectly and causes damage.

2. Digital hybridity

Similar to their role in digital assistance, the social sciences contribute to an adequate understanding of hybrid human-machine associations, i.e. the closely interwoven interactions of algorithms and humans, yet in a slightly different manner. Human-machine associations develop collective risks

[34] Luciano Floridi & J.W. Sanders, *On the Morality of Artificial Agents*, *in* MACHINE ETHICS (Michael Anderson & Susan L. Anderson eds., 2011), 192.

[35] Elena Esposito, *Artificial Communication? The Production of Contingency by Algorithms*, 46 ZEITSCHRIFT FÜR SOZIOLOGIE 249(2017).

[36] Katrin Trüstedt, *Representing Agency*, 32 LAW & LITERATURE 195, 196 (2020).

that are qualitatively different from the individual risks of digital assistance. While, as shown, digital assistance creates the risk of algorithmic autonomy, digital hybridity generates risks based on the emergent properties of collective behavior. The social sciences play, again, the intermediating role between computer science and liability law. They determine the conditions under which human-machine associations are constituted in social practices.

Because they are unconditionally committed to methodological individualism, economists remain skeptical about the reality status of collective actors and legal persons. They understand them as mere "nexus of contracts" and see their personification, at best, as an abbreviation for complex interpersonal relations. At worst, they qualify such personification as dangerous "errors", "traps" or "fictions".[37] In the world of economics, only the behavior of individuals counts. In contrast, sociological analyses focus precisely on the various complex social relations that arise in the contacts between humans and algorithms and their potential personification.[38] These range from short-term individual interactions via loosely structured networks to collective human-algorithm associations, which are equipped with actorship, an internal division of labor, resource pooling and distribution of competences. In such condensed interaction, actions become attributed to the hybrid as a collective entity, and do no longer qualify as the individual actions of the algorithms or humans involved.[39] As a result, law must react to the emergent risk of the hybrid's collective capacity and develop forms of collective responsibility.

3. Digital interconnectivity

In contrast to digital assistance and digital hybridity, our third category, collective machine behavior, is a purely technological matter. It emerges in the interconnectivity of autonomous algorithms without human interference.[40] Interconnectivity is different from digital assistance because it is impossible to identify an individual algorithm as the responsible actor. The risk of interconnectivity is equally incomparable to

[37] Michael Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 306 (1976).

[38] e.g. ANDREAS HEPP, DEEP MEDIATIZATION: KEY IDEAS IN MEDIA & CULTURAL STUDIES (2020); BRUNO LATOUR, REASSEMBLING THE SOCIAL - AN INTRODUCTION INTO ACTOR-NETWORK-THEORY 159 (2005).

[39] Philip Pettit, *Responsibility Incorporated*, 117 ETHICS 171(2007). is relevant not only for human but also algorithmic action.

[40] If legal analysis identifies a human involvement, the case would qualify as vicarious liability in digital assistance or network liability in digital hybrids. More details on the delineation of the three liability regimes, see BECKERS & TEUBNER. 2021, *supra* note **, at 153-155.

the risk of hybrid human-machine associations. Here, we are dealing with interconnected algorithmic operations to which society is ultimately exposed without being able to influence them, let alone establish communicative relations. In collective machine behavior, there is no two-way communication between humans and algorithms, not to speak of an associative relation between them, but only an indirect structural coupling.

The interdependent algorithmic calculations can be qualified as a "restless collective" based on distributed cognition.[41] Such a "collectivity without a collective" cannot be described neither as a formal organization nor as a network. It is only a "swarm" of algorithms arising from chance encounters. Systems theory describes society's relationship to such algorithmic swarms as social contact to "invisible machines".[42] Their influence on society is difficult to grasp. Neither is there, as said above, genuine communication between humans and algorithms, nor does a communicative collective emerge from humans and algorithms. Instead of a direct influence mediated through communication, interconnected algorithms exert an influence on social relations that is only indirectly mediated through structural coupling. Therefore, it is not possible to apply the legal liability rules for individual algorithms acting in isolation, nor for human-machine associations. Instead, we propose fund solutions that require political and administrative decisions by regulatory authorities, which impose responsibility on the respective industry.

B. Subjects of liability

The threefold fragmentation of socio-digital institutions further affects the question of which actors are to be held responsible for algorithms going astray. Here, too, we propose a differential treatment depending on the institutional context.

1. User/operator: Liability for delegation risks

Digital assistance generates responsibilities only within the bilateral relation between algorithm and human user/operator (or organization). Principal-agent liability does not hold liable the multitude of actors involved in the computer use, i.e. programmers, manufacturers, traders etc. Instead, it exclusively targets the user who delegates a task to the technology and thus assumes the risk of autonomous decision-making by the

[41] Carolin Wiedemann, *Between Swarm, Network, and Multitude: Anonymous and the Infrastructures of the Common*, 15 DISTINKTION: SCANDINAVIAN J. SOC. THEORY 309, 313 (2014).

[42] 1 NIKLAS LUHMANN, THEORY OF SOCIETY, 66 (2012); similarly MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW, 40 (2015).

algorithm. Therefore, only the human user/operator (or organization) is responsible for the algorithmic failures.

In contrast, some authors argue that this unfairly shifts all the risks on the user/operator alone.[43] They also see other actors in the role of the responsible principal, in particular the manufacturer or producer, including the back-end operator who provides program updates and similar services in the background.[44] In doing so, however, they ignore that the specific risk of task delegation has been assumed by the operator. As a result, they arrive at an unfair distribution of risk between manufacturer, programmer and operator. All actors involved in the construction and operation of the algorithm create different types of risks. It is these risks that must be defined precisely in each case and then allocated exclusively to those actors who have assumed them. Principal-agent liability responds to the risks of the division of labor between user and algorithm. In contrast, product liability, which certainly remains applicable, responds to the specific risks of programming, manufacturing and monitoring the algorithms, but, as said above, leaves open considerable gaps in liability.

2. Network members: Liability for collective risks

In contrast to principal-agent liability that exclusively burdens the user/operator, digital hybridity involves different risks. Here, since it is impossible to identify any individual actors, the wrongful acts can be attributed only to the human-machine association itself. However, as long as the association does not have its own assets, it is necessary to channel the resulting liability to the multitude of actors who are "behind" the digital hybrid. A whole network of different actors is involved in and benefits from the human-machine association. As control in the network is dispersed across the network nodes, liability must also follow this specific risk structure. We consider "network liability" to be well-equipped to assign, in a fair manner, responsibility to the network participants for the digital hybrid's failures.[45]

The digital network liability we propose is modelled on the American "enterprise liability" and the German *Gesamthandshaftung*. It works in two steps: first, an attribution

[43] e.g., Pablo Sanz Bayón, *A Legal Framework for Robo-Advisors*, in 311 DATENSCHUTZ / LEGALTECH (Erich Schweighofer, Franz Kummer, Ahti Saarenpää & Burkhard Schafer,eds., 2019), sec. 7.

[44] Resolution on Civil Liability Regime for Artificial Intelligence, EUR. PARL. DOC. (Oct. 20, 2020), at para 8.

[45] David C. Vladeck, *Machines without Principles: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 149 (2014); Allain, *supra* note 8, at 1074.

of action, then an attribution of liability. In the first step, the wrongful act is attributed to the hybrid as a collective actor. This avoids having to identify the contributions of all humans and algorithms involved. In the second step, liability for the collective action is channelled to the network members. These members have built the network and control it, even if only indirectly. They profit from its activities. As a result of this attribution, all network nodes are liable according to their share. The share is determined by economic benefit from and control over the hybrid. In analogy to the well-known market-share liability, we propose a "network-share liability".[46] An exception is only the constellation in which a company centrally coordinates the network on the basis of contractual agreements. Here, primary liability should lie with the controlling company.[47] As a rule, this will be the producer, who will then have recourse to the other network nodes.

3. Industry sector: Liability for connectivity risks

Finally, in the case of interconnectivity, liability is determined differently again. Responsibility shifts from those directly involved to a larger social collective. The interconnectivity of "invisible machines" makes it impossible from the outset to determine an individually responsible algorithm. Since there is only an indirect "structural coupling" between algorithmic interconnectivity and society, no one-to-one responsibility relationship can be established either. Therefore, we propose that liability funds be established. The funds should be financed by the sector involved.[48] The contributions of the players involved are calculated on the basis of their market share and their specific problem-solving capacity. The U.S. Superfund for environmental damage can serve as a model here.[49] The Superfund aims not only at compensating individual affected parties, but also contains rules about remedying the wider social and ecological impact, including rules on clean-up and prevention. This idea should also be taken up for damage resulting from algorithmic interconnectivity. Restitution measures will serve as additional instruments of liability law. In the case of large-scale damage, the regulatory authority responsible for the fund should be empowered to select those actors who have a strong problem-solving capacity and impose the task of restitution and undoing

[46] For a general discussion of network liability, see: GUNTHER TEUBNER, NETWORKS AS CONNECTED CONTRACTS 264-268 (2011).

[47] Rory van Loo, *The Revival of Respondeat Superior and Evolution of Gatekeeper Liability*, 109 GEO. L. J. 141, 189 (2020).

[48] Olivia J. Erdélyi & Gabor Erdélyi, *The AI Liability Puzzle and a Fund-Based Work-Around*, AIES '20: PROCEEDINGS OF THE AAAI/ACM CONFERENCE ON AI, ETHICS, AND SOCIETY, 50 (2020).

[49] 42 US Code § 9601-9628.

adverse consequences. The actors involved are obliged to take measures that limit or even eliminate the negative externalities of interconnectivity for the future, such as reverseability[50], creation of firewalls or slowing down of interconnectivity or, ultimately, the shut-down of dangerous technological systems, described as the 'death penalty' for robots.[51]

C. Legal status of algorithms

Finally, the new socio-digital institutions – digital assistance, hybridity, interconnectivity – require different ascriptions of the legal status of algorithms. The solution cannot be a uniform legal personification of software agents, human-computer associations or interconnected multi-agent systems. Instead, in response to the three risks, we propose aligning the legal status of algorithms with the role they each play within the respective socio-digital institution.

Only in the case of digital assistance is it appropriate to grant algorithms the status of limited legal personhood. Such a partial legal capacity enables them to conclude contracts with third parties as agents with binding effect for their principals. As vicarious agents, algorithms must be provided with the necessary legal action capacity, so that the principals can be made liable for their misconduct.

In contrast, the appropriate response to the association risk of digital hybridity is to give the software agent involved the legal status of a full member of the human-machine association. A future-oriented solution for law could even be to attribute actions, rights and obligations as well as liability to the hybrid association itself – a solution that would break completely new ground in the rules on legal personhood. A less disruptive solution that can be realized under current law would merely refer to the legal concept of contractual purpose and make it usable for the interpretation of computer declarations and the determination of the rights and obligations of the participants. In contrast to both, we favor an intermediate solution that creates an analogy to the principles of network liability.[52] The algorithm is thus given the status of a network node.

---

[50] See on reversability Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics, EUR. PARL. DOC. (Oct. 20, 2020), Annex.

[51] Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 UNIV. CHI. L. REV. 1311, 1390 (2019).

[52] For an advanced concept of network liability, RÓNÁN CONDON, NETWORK RESPONSIBILITY: EUROPEAN TORT LAW AND THE SOCIETY OF NETWORKS 192-197 (2022); for network liability in digital configurations, Anat Lior, *The AI Accident Network: Artificial Intelligence Liability Meets Network Theory*, 95 TUL. L. REV. 1148-1152, 1160-1162(2021).

Finally, our answer to the risks of digital interconnectivity is called 'risk pool'. Liability law must delineate this risk pool in a binding way. The wrongful act is then attributed to the pool. The legal status of the algorithms then consists neither of their own personhood nor of the membership in a hybrid, but in being a mere part of a digital risk pool.

IV. THREE LIABILITY REGIMES

A. *Synopsis*

In order to illustrate the differences between the three liability regimes, their digital and social preconditions and their legal rules, we present here in tabular form a condensed version of our proposals. The (recursive) interrelationships of digital machine behavior, socio-digital institutions and liability norms look like this:

Machine behaviour	Socio-digital institution	Emerging risks (new actors)	Liability regime	Liable actors	Legal status of algorithm
Individual	Digital assistance	Autonomy risk (actant)	Principal-agent liability / vicarious liability	User/Operator • strict	Limited legal personhood
Hybrid	Human-machine-association	Collective action risk (hybrid)	Enterprise liability/ network liability	Network members • control • economic benefit	Membership in hybrid
Collective	Exposure to digital interconnectivity	Distributed cognition in invisible machines (swarm/crowds)	Collective funds	Industry sector • market share • problem-solving capacity	Part of risk pool

Table 1: Causal and normative relationships between machine behavior, socio-digital institutions and liability regimes.

A. *Liability rules*

We propose the following rules to concretize the liability regimes:

1. Principal-agent liability

Principal-agent liability for wrongful decisions by an algorithm applies if (1) a human principal (or an organization) delegates a task to an algorithm, (2) the delegation requires the agent to take autonomous decisions, (3) the agent acts wrongfully without it being foreseeable or explainable by a programmer, (4) the agent's action amounts to breach of a contractual or tortious duty of care, and (5) causation between the action and the damage can be proven.

(6) As a consequence, the user of the algorithm is exclusively liable as principal. (7) Compensation of damage is not limited to the narrow compensation principles of strict liability, but follows established compensation principles of contract and tort law, according to which, in particular, compensation must also be paid for damages exceeding bodily injury and property damage.

2. Enterprise liability

If the conditions of vicarious liability are not met, enterprise liability applies if (1) in the cooperation between humans and machines, (2) an unlawful decision was taken and (3) their activities are so densely intertwined that (4) the decision cannot be attributed to either the human or the algorithm and (5) causal links between the individual actions and damage cannot be established, while (6) it can be proven that the collective decision had caused the damage.

(7) As a consequence, the participants of the human-machine network are liable, i.e. producers, programmers, traders and the human members within the hybrid. (8) Enterprise liability primarily targets the producer as the hub of the networked enterprise. (9) The producer can take recourse against the other participants according to their network share. (10) The network share is determined by the criteria of economic benefit and control within the network.

3. Fund liability

If neither vicarious liability nor enterprise liability are applicable, compensation is only possible (1) through a fund or insurance that will be set up to provide compensation for algorithmic damages. Conditions for compensation by the fund are that (2) breach of a tortious or contractual duty can be attributed to interconnected algorithmic decisions, which (3) together cause damage.

(4) As a consequence, the fund shall be liable for the damages. (5) A regulatory agency is charged with the administration of the fund and shall decide on the compensation. The regulatory agency shall also determine (6) the actors in the industry that have to provide ex ante financing according to their respective market share and (7) the actors to be called upon in case of ex-post liability according to their problem-solving capacity.

V. DISCUSSION OF THE INITIAL CASES

What are the legal consequences under the proposed liability rules for the three cases presented in the introduction? We had first established that under the law in force today, no liability is provided for in all three cases and the damages are thus to be borne solely by the injured party. We have further established that those arguing for a uniform liability regime would solve all cases either by focusing on strict liability as a solution or consider the liability of the algorithms as e-persons. Proponents of radically situationist regimes would, in contrast, propose that a sectoral piecemeal approach would be in order. Accordingly, they would likely propose solutions for the financial sector that would apply to the case of robo-advisors and flash crashes and distinguish such solutions from those relevant for media, as in our case 2. According to our proposals, however, the cases are each to be related to one of three socio-digital institution and subjected to the corresponding liability rules.

A. Robo-Advice : Digital Actants

Legally, the first question in this case is whether Costa, an investment intermediary offering advice and guidance on stock futures through algorithms, breached its own duties. However, if the injured party Li cannot prove that Costa breached the duties of an investment intermediary, the success of his claim will depend on whether the wrongful decisions of the autonomously acting algorithm give rise to liability.[53]

The algorithm's stop-loss order was an unlawful decision by the algorithm. The relevant socio-digital institution here is digital assistance, where the algorithm acts as an agent in a principal-agent relationship. In this context, product liability is of no help, as Costa has not breached any obligation under product liability laws. Strict liability, which would first have to be mandated by the legislature, would again go much too far. It would open the floodgates to financial liability. As pure causal liability, it would make the principal liable for every action, whether illegal or not, of the algorithmic agent, insofar as it causes financial damage. This leaves only principal-agent liability as a basis for a claim.[54] If the principal Costa has entered into a financial brokerage agreement with Li and delegated his contractual duties of portfolio management to K1 as his

[53] Ben Hughes & Russell Williamson, *When AI Systems Cause Harm: The Application of Civil and Criminal Liability*, DIGITAL BUSINESS LAW (Nov. 8, 2019) https://digitalbusiness.law/2019/11/when-ai-systems-cause-harm-the-application-of-civil-and-criminal-liability/.

[54] Bret E. Strzelczyk, *Rise of the Machines: The Legal Implications for Investor Protection with the Rise of Robo-Advisors*, 16 DEPAUL BUS. & COM. L. J. 54 (2018).

vicarious agent, then he is liable for any breaches of contractual duties committed by K1. Under current law, however, the algorithm does not (yet) have the legal capacity that is mandatory for principal-agent liability. However, courts can grant legal subjectivity to autonomous algorithms, as they have done in the past with certain associations of human actors. For principal-agent liability, it is sufficient to endow algorithms with partial legal capacity, namely the capacity to fulfil the contractual obligations of the principal and to breach them accordingly.

B. Panama Papers: Digital Hybrids

If the algorithm that analyzed the multitude of documents in collaboration with the journalists operated according to its programming and the human journalists fulfilled their monitoring duties, no one can be held liable.[55] This is a situation of "collective moral responsibility" in which a group commits an unlawful act even though the individuals involved behaved correctly.[56] The algorithm worked as programmed and made decisions about labelling, classifying, selecting and preparing information for use by humans as intended, and the human journalists diligently reviewed this information based on their knowledge. It is not possible to identify a single wrongful act, although the collective work of algorithms and journalists led to the wrongful allegations. For these cases, enterprise liability as outlined above is appropriate. The wrongful conduct is attributable to the human-machine association as a collective of journalists and algorithms.

Provided the wrongful act can be attributed to the human-machine hybrid, it is possible to channel financial liability to the members of the network. The injured party can successfully sue the central node of the network. In the case of hybrid journalism, this can be either the controlling news organization or the producer of the algorithm. In the context of algorithmic news dissemination, it could be the manufacturing company of the algorithm, i.e. a news or social media company. Such liability would apply regardless of whether there are specific legal provisions for strict liability of news providers or platforms. Within the network, the internal proportional distribution of liability would be according to the economic benefit and control in the collaborative network.

---

[55] Seth C. Lewis, et al., *Libel by Algorithm? Automated Journalism and the Threat of Legal Liability,* 98 JOURNALISM & MASS COMMC'N Q. 60. 69 (2019).

[56] David Copp, *The Collective Moral Autonomy Thesis,* 38 J. SOC. PHIL 369 (2007).

C. Flash Crash: Digital Swarms

The damage caused by the networked algorithms in the financial market is a case of the interconnectivity risk. The damaging operations of the algorithms here were indeed triggered externally by the fraudulent behavior of a single trader, and incentivized by the infrastructure of the financial market itself, on which similarly programmed algorithms operate. The immediate causes of the collapse, however, are the interdependent operations of networked algorithms, whose speed by far exceeds human capabilities. Human intervention in the operations causing the damage was impossible. Foreseeability and individual fault, as would be required for negligence, cannot be demanded in such a context.

For such cases, instead of the futile search for a responsible actor (as attempted by the U.S. Treasury), we think that only a fund solution makes sense. The fund needs to be placed under the supervision of the financial market authorities.[57] It will be financed by a relatively small market access fee paid by the users and producers of financial market algorithms based on their market share.

This is where the criterion of illegality comes into play. Not every flash crash should open up access to the fund for the injured parties. A loss triggered by mere volatility in the financial markets is not per se a ground for liability. The access of injured parties to the fund capital after a flash crash should be limited to those cases in which a breach of law can be established by networked algorithms. On the basis of this criterion, damages caused by the normal volatility of the financial markets can be distinguished from crashes resulting from a breach of regulations or other rules of conduct that apply to financial market trading.

The supervisory authority for the financial market should also be empowered to instruct the actors involved in high-frequency algorithmic trading to take recovery and preventive measures. This could entail what can be called a "digital clean-up". The authority would order the firms involved to make systemic changes to the algorithmic trading infrastructure. For example, the risk of algorithmic swarming behavior could be mitigated by programming a slowdown of algorithmic decisions into the system.[58]

[57] Similarly Yadav, *supra* note 5, at 1095.
[58] *Ibid*., at 1097-1099.

VI. OUTLOOK: LIABILITY LAW IN THE DIGITAL PUBLIC SPHERE

The liability regimes that we are proposing have a considerable impact on the digital public sphere and its regulation. Two important aspects stand out.

First, our differentiating approach would contribute significantly to the digital constitution that is currently emerging.[59] Certainly, the purpose of liability law is seeking to control algorithmic activities via optimizing standards of care and levels of activity. But the constitutional requirements on digitality are not exhausted with legal-economic policies.[60] In the recursive dynamics of technology/social institutions/liability law, a mutual constitution of legal norms, legal subjects and social institutions takes place. Indeed, the emergence of autonomous algorithms as novel quasi-subjects confronts private law with a first-order constitutional question. The response may be to grant legal personality to algorithms acting in isolation and to human-algorithm associations, as well as create risk pools along with their liability consequences. As already mentioned, this development is neither determined only by technology nor by economics, but depends on various political decisions about the social responsibility of digital technologies. Insofar as the—only seemingly technical—liability law is used for closing responsibility gaps, for responding to opportunities and dangers of the personification of algorithmic processes, for formulating standards of care for algorithmic decisions, for protecting individual legal positions endangered by wrong algorithmic decisions, for compensating ecological damages and for reprogramming risky algorithms, it contributes considerably to an evolving digital constitution. The threefold differentiation of liability regimes will lead to recognize new digital actors populating the digital public sphere and help allocating risks for their uncontrollable behaviour.

Second, liability law as a central institution of private law, will itself be in need of assimilating public elements. Liability law will have to respond to the entrance of public actors into the digital sphere and react to new violations of the public interest, particularly fundamental rights. In this article, we exemplified our liability regimes with cases in which algorithms are employed by private actors and operate to serve private interests—advising on investments, creating journalistic content made for commercial use or trading on financial markets.

---

[59] EDOARDO CELESTE, DIGITAL CONSTITUTIONALISM: THE ROLE OF INTERNET BILLS OF RIGHTS 23-24 (2022).

[60] For a variety of constitutional requirements, Angelo Jr Golia & Gunther Teubner, *Digital Constitution: On the Transformative Potential of Societal Constitutionalism*. SYMPOSIUM: INDIANA JOURNAL OF GLOBAL LEGAL STUDIES (2023, forthcoming).

However, the use of algorithms is certainly not limited to only private and commercial purpose. As our second example of hybrid journalism demonstrates, when investigative journalists cooperate with algorithms, the outcome is never only a commercial content; necessarily, the public role of media in democratic societies is involved. Since journalism influences public opinion, its content impacts fundamental rights, and it shapes the function of media as an institution, the participation of algorithms has a significant influence on the public sphere. As for digital assistance, we not only observe the increasing use of robo-advisors and digital contracting agents by commercial actors; also, public actors—administrative and criminal enforcement agencies—make use of digital assistants. As our 'google auto-complete' case prominently shows, digital assistants have a massive potential to violate fundamental rights.[61] And digital interconnectivity certainly exists beyond financial markets. In particular, on digital platforms the interconnection of autonomous bots evolves into swarm behaviour to which humans are exposed.[62] This may influence public opinion on a large scale.

These examples show that public actors have entered the digital sphere through the use of algorithms. This poses for them similar questions of responsibility attribution. The three liability regimes may, after an adaption of public law rules on state liability, help constitute responsibility for algorithmic misconduct by public actors.[63] Similarly, the violation of the public interest by digital assistants, hybrids and interconnected algorithms requires liability law to respond. This can be achieved by creating new remedies for the violation of public law rules and by integrating fundamental rights aspects in private law arguments on standards of care and activity levels.

[61] For more details, BECKERS & TEUBNER. 2021, *supra* note **, at 163-166.

[62] See for a study of Wikipedia-editing bots, Milena Tsetkova, et al., *Even Good Bots Fight: The Case of Wikipedia*, 12 PLOS ONE 1(2017).

[63] For a convincing argument in that direction, arguing that networks require the linking of rules on private and public actors liability, CONDON. 2022, *supra* note 51, at 180-192.