Liability For Artificial Intelligence And EU Consumer Law

by **Martin Ebers**[*]

Abstract: The new Directives on Digital Contracts – the Digital Content and Services Directive (DCSD) 2019/770 and the Sale of Goods Directive (SGD) 2019/771 – are often seen as important steps in adapting European private law to the requirements of the digital economy. However, neither directive contains special rules for new technologies such as Artificial Intelligence (AI). In light of this issue, the following paper discusses whether existing EU consumer law is equipped to deal with situations in which AI systems are either used for internal purposes by companies or offered to consumers as the main subject matter of the contract. This analysis will reveal a number of gaps in current EU consumer law and briefly discuss upcoming legislation.

Keywords: Digital Content and Services Directive; Sale of Goods Directive; Artificial Intelligence; AI; EU Consumer Law; Liability

Recommended citation: Martin Ebers, Liability for Artificial Intelligence and EU Consumer Law, 12 (2021) JIPITEC 204 para 1.

A. Introduction

1 The new Directives on Digital Contracts – the Digital Content and Services Directive (DCSD) 2019/770[1] and the Sale of Goods Directive (SGD) 2019/771[2] – are widely seen as crucial first steps in adapting European private law to the requirements of the digital economy.[3] Both directives – although based on the principle of full harmonization[4] –

* Professor of IT Law at the University of Tartu (Estonia) and permanent research fellow at the Humboldt University of Berlin. This work was supported by Estonian Research Council grant no PRG124. This paper was submitted to jiptec in February 2021 and has not been updated since, apart from all internet sources which were last accessed in April 2021. Therefore, this paper could not take into account the European Commission's proposal for a "Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts", COM(2021) 206 final, presented on April 21, 2021.

1 European Parliament and Council Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 (DCSD 2019/770).

2 European Parliament and Council Directive 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28 (SGD 2019/771).

3 Staudenmayer, 'The Directives on Digital Contracts: First Steps Towards the Private Law of the Digital Economy' (2020) 28 European Review of Private Law (ERPL) 217-247. For an extensive analysis of the DCSD 2019/770 see Sein and Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1' (2019) 15 European Review of Contract Law (ERCL) 257, 269ff; Sein and Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Conformity Criteria, Remedies and Modifications – Part 2' (2019) 15 ERCL 365.

4 Cf Art 4 DCSD 2019/770; Art 4 SGD 2019/771. As to the concept of "full harmonization" or "targeted full harmonization" see Ebers, *Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht* (Tübingen, Mohr Siebeck 2016) 269ff and 742ff; Riehm, 'Die überschießende Umsetzung vollharmonisieren-

cover only certain legal aspects in the private law relationship between a business and a consumer. Moreover, in line with the principle of technology neutrality,[5] neither directive contains tailored rules for specific digital technologies.[6] Instead, both directives are generalized to "any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer"[7] or to "sales contracts between a consumer and a seller" including "goods with digital elements".[8] Therefore, new technologies such as Artificial Intelligence (AI) are not subject to any special rules.

2 These limitations raise concerns over whether existing EU consumer law (as well as other areas of EU law such as data protection and antidiscrimination law) is equipped to deal with the current challenges posed by AI systems. The following article explores this question by looking at the trader's liability for AI systems vis-à-vis the consumer. In this respect, two different constellations must be strictly delineated from each other: (i) the internal use of AI systems by a business during the "life cycle" of a contract and (ii) AI systems as the subject-matter of contracts.[9]

3 Accordingly, this paper is structured as follows: Section B gives an overview of the use of AI technologies in consumer markets, the problematic features of AI systems, and the specific risks these systems pose for consumers; section C addresses the trader's liability for AI during the life cycle of a contract, including the pre-contractual phase, the conclusion of contract and algorithmic decision making phase, and the performance phase; section D focuses on constellations in which an AI system is the subject matter of the contract, examining the trader's liability for non-conforming AI applications; and the final part of the paper looks toward the future, asking whether current reform projects (especially at the European level) can close the gaps that currently exist in European consumer law as it applies to AI.

4 That said, a disclaimer is in order: the purpose of this article is not to provide a detailed analysis of the numerous legal issues that arise in the business-consumer relationship when AI systems are used. Such an analysis would go far beyond the scope of this paper and must necessarily be left to later studies. Rather, the focus is on providing an initial overview of the numerous consumer law issues related to the use of AI, in particular highlighting the limits of the current European legal framework.

B. The Use of AI in Consumer Markets

I. The (Missing) Universal Definition of AI

5 Although the term "artificial intelligence" has been in use for nearly 70 years, no universally accepted definition of AI has emerged. *John McCarthy*, who famously coined the term in 1956, opined that since there is no "solid definition of intelligence that doesn't depend on relating it to human intelligence ... we cannot yet characterize in general what kinds of computational procedures we want to call intelligent."[10] Later, he is said to have cynically remarked: "As soon as it works, no one calls it AI anymore".[11]

6 This observation no longer holds true today. AI has become a buzzword applied to a variety of technologies available on the market. In reality, however, the term is mainly used for a specific sub-discipline of artificial intelligence, namely machine learning (ML).[12]

der EG-Richtlinien im Privatrecht' (2006) 21 JuristenZeitung (JZ) 1035-1045.

5 The principle of technology neutrality aims to ensure equal treatment and sustainable rules; Reed, 'Taking Sides on Technology Neutrality' (2007) 4(3) SCRIPTed 263; Greenberg, 'Rethinking Technology Neutrality' (2016) 100 Minnesota Law Review 1495.

6 Cf recital (10) DCSD 2019/770: "Both the scope of this Directive and its substantive rules should be technologically neutral and future-proof".

7 Art 3(1) DCSD 2019/770.

8 Art 3(1) and 2(5)(b) SGD 2019/771.

9 Grundmann and Hacker, 'Digital Technology as a Challenge to European Contract Law. From the Existing to the Future Architecture' (2017) 13(3) ERCL 255–293, at 264.

10 <http://www-formal.stanford.edu\jmc\whatisai.pdf> accessed 31 January 2021.

11 Meyer, 'John McCarthy' (*CACM* 28 October 2011) <https://cacm.acm.org/blogs/blog-cacm/138907-john-mccarthy/fulltext> accessed 30 January 2021.

12 As to the various forms of machine learning, cf Anitha, Krithka, and Choudhry, 'Machine Learning Techniques for learning features of any kind of data: A Case Study' (2014) 3(12) International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 4324 <http://ijarcet.org/wp-content/uploads/IJARCET-VOL-3-ISSUE-12-4324-4331.pdf> accessed 30 January 2021; Buchanan and Miller, 'Machine Learning for Policymakers. What It Is and Why It Matters' (June 2017) Harvard Kennedy

7 Today's widely used ML-based systems are fundamentally different from earlier AI systems. In the past, many AI systems, especially expert systems, relied on rule-based conditional logic operations. Such systems typically break down complex human intellectual tasks into a set of computational steps or algorithms. In order to transform inputs into outputs, experts extract the knowledge from sources and convert them into a logical computational model using *symbolic rules* to represent and infer knowledge. Whereas symbolic systems have particular strengths in transparency and interpretability, one major flaw is their limited capacity to deal with complex situations. Most symbolic systems are only useful for narrow applications and cannot cope with uncertainty well enough to be useful in practical applications.[13]

8 By contrast, the current wave of successful AI applications is based on *data-learned knowledge*, which relies less on hand-coded human expertise than the knowledge learned from data. Instead of programming machines with specific instructions to accomplish particular tasks, ML algorithms enable computers to learn from "training data". Self-learning systems are not directly programmed; instead, they are trained with millions of examples so that the system develops by learning from experience.

II. The Seven Patterns of AI

9 Looking at concrete use-cases, we can distinguish seven patterns of AI, which are listed as follows in no particular order:[14]

10 *Autonomous Systems*: First, AI is the underlying technology for many autonomous systems which can accomplish a task or a goal with minimal human interaction. Such systems require the use of ML which can independently perceive the outside world, predict future behavior, and plan how to navigate changes. The most common applications are self-driving machines such as cars, trains, airplanes, etc.

11 *Patterns and Anomalies*: AI/ML also plays a role in the recognition of patterns and anomalies. ML and cognitive systems can learn patterns from data and check for anomalies by connecting data points. These techniques are most prominently used for fraud and risk detection, for example by insurance companies or tax offices.

12 *Hyperpersonalization*: Particularly in consumer markets, AI systems are used to personalize advertisements, prizes, and contracts. To this end, ML algorithms are applied to develop a profile of each individual in order to display and recommend to the consumer relevant advertisements or other content.

13 *Recognition*: To design and improve the accuracy of recognition technology, ML (especially deep learning) techniques are used for identifying and determining objects within image, audio, text, and other media formats. Examples include all manner of recognition systems, such as biometric (facial) recognition, object recognition, text recognition, audio, and video recognition.

14 *Human Interaction*: AI systems may also serve as conduits for conversation and human interaction. Here, the objective is to enable machines to interact with humans through voice, text, and image. These forms of AI systems are used for chatbots and voice assistants, as well as for the analysis of sentiment, mood, and intent.

15 *Predictive Analytics*: AI systems can also be employed to predict future outcomes based on patterns in order to help humans make better decisions. Examples include inter alia, assisted search, predicting behavior, and giving advice.

16 *Goal-driven system*: Finally, ML in the form of reinforcement learning can also be used to find the optimal solution to a problem. In practice, these goal-driven systems are used most frequently in game playing, resource optimization, and real-time auctions.

III. Use of AI Systems in the Business-Consumer Relationship

17 Many of the above-mentioned AI systems are used by companies in consumer markets. In this regard, we have to distinguish, as already mentioned, between (i) the internal use of AI systems within a company and (ii) cases in which AI is the subject of a contract.

School Cyber Security Project Paper <https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf> accessed 30 January 2021; Mohri, Rostamizadeh, and Talwalkar, *Foundations of Machine Learning* (Cambridge/London, MIT Press 2012).

13 Cf Kahneman and Tversky, 'Variants of uncertainty' (1982) 11(2) Cognition 143-157; Li and Du, *Artificial Intelligence with Uncertainty* (2nd edn, Boca Raton/London/New York, CRC Press 2017); Brill and Mooney, 'Empirical Natural Language Processing' (1997) 18(4) AI Magazine 13-24, at 16.

14 Cognilytica, 'The Seven Patterns of AI' (4 April 2019) <https://www.cognilytica.com/2019/04/04/the-seven-patterns-of-ai/> accessed 31 January 2021.

1. Internal Use of AI Systems

18 AI techniques are used by many companies during the "life cycle" of a contract to make contracting more efficient. At the *pre-contractual stage*, AI-driven profiling techniques provide better insights into consumers' behavior, preferences, and vulnerabilities. Companies can tailor their advertising campaigns[15] but also their products and prices specifically to the customer profile,[16] credit institutions can use the profiles for credit ratings,[17] and insurance companies can better assess the insured risk.[18] In addition to these applications, AI-driven big-data profiling techniques give companies the opportunity to gain superior knowledge about customers' personal circumstances, behavioral patterns, and personality, including future preferences. These insights enable companies to tailor their advertisements (so called "online behavioral advertising") and contracts in ways that maximize their expected utility by exploiting the behavioral vulnerabilities of their clients.

19 AI contracting tools and chatbots can also be used to govern the *contracting process* itself, especially for algorithmic (automated) decision making and formation of contracts.[19] Nowadays, such systems can be found not only in financial markets (e.g. for algorithmic trading), but also in consumer markets (e.g. for consumer sales, where an algorithmic system – and sometimes even a self-learning AI system – is contracting on behalf a company).

20 During the *performance phase*, AI systems facilitate and automatize the execution of transactions, assisting and simplifying real-time payments and managing supply chain risks. They also play a crucial role in contract management and due diligence.[20]

21 Finally, at the *post-contractual phase*, AI systems can help to litigate legal disputes by handling customer complaints, resolving online disputes, or predicting the outcome of court proceedings.[21]

2. AI Systems as the Subject-Matter of a Contract

22 Apart from their internal use by companies, AI systems may also be included in the subject-matter of a contract. Nowadays, many smart products and services offered to consumers are AI-based, e.g. self-driving cars, vacuum cleaners, surveillance equipment, health apps, voice assistants, and translation apps. For all these products and services, an unresolved question arises as to what requirements should be placed on contractual conformity when a lack of conformity exists, and under what preconditions the trader is then liable to the consumer.

15 Cf Calo, 'Digital Market Manipulation' (2014) 82(4) The George Washington Law Review 995, 1015ff; Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' in Schulze and Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Baden-Baden, Nomos 2016) 135ff.

16 Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy 34.

17 Cf Citron and Pasquale (2014) 89 Washington Law Review 1; Zarsky, 'Understanding Discrimination in the Scored Society' (2014) 89 Washington Law Review 1375.

18 Cf Swedloff, 'Risk Classification's Big Data (R)evolution' (2014) 21(1) Connecticut Insurance Law Journal 339; Helveston, 'Consumer Protection in the Age of Big Data' (2016) 93(4) Washington University Law Review 859.

19 From the technical perspective, cf (in a chronological order) especially the following books: Ossowski (ed), *Agreement technologies* (Amsterdam, Springer 2013); Rovatsos, Vouros & Julian (eds), *Multi-agent systems and agreement technologies - 13th European Conference, EUMAS 2015, and Third International Conference, AT 2015, Athens, Greece, December 17-18, 2015, Revised Selected Papers* (Cham, Springer 2016); Criado Pacheco, Carrascosa, Osman, Julian (eds), *Multi-agent systems and agreement technologies - 14th European Conference, EUMAS 2016, and 4th International Conference, AT 2016, Valencia, Spain, December 15-16, 2016, Revised Selected Papers* (Cham, Springer 2017); Lujak (ed), *Agreement technologies - 6th International Conference, AT 2018, Bergen, Norway, December 6-7, 2018, Revised Selected Papers* (Cham, Springer 2019). As to the legal perspective cf below at 3.2.

20 Schuhmann, 'Quo Vadis Contract Management? Conceptual Challenges Arising from Contract Automation' (2000) 16(4) ERCL 489-510.

21 The most prominent example is eBay's ODR Resolution Center, which reportedly handles (automatically) over 60 million disputes annually; Schmitz & Rule, *The New Handshake: Online Dispute Resolution and the Future of Consumer Protection* (Chicago, ABA 2017) 53; Rule & Nagarajan, 'Leveraging the Wisdom of Crowds: The eBay Community Court and the Future of Online Dispute Resolution' *ACResolution Magazine* (Winter 2010).

IV. Risks for Consumers

23 The (*internal*) *use of AI systems* by companies vis-à-vis consumers raises a number of ethical and legal concerns.[22] These include:

- intrusion into privacy;
- growing information asymmetries;
- inability of the consumer to understand businesses' behavior;
- risks surrounding exploitation of a consumer's vulnerabilities through profiling and targeting;
- risks of algorithmic decision making due to the opaqueness of automated decisions, potentially leading to biased or discriminatory results;
- risks surrounding consumer safety and property;
- risks involved in due process and fair trial rights, considering that the consumer might be hindered in enforcing his or her rights due the opaqueness of algorithmic procedures and decisions.

24 From the perspective of consumer contract law, one of the most troubling developments is the growing *asymmetry of information* between businesses and consumers. The use of AI in consumer markets leads to a new form of power and information asymmetry. Usually, the consumer remains unaware that advertising, information, prices, or contract terms have been personalized according to his or her profile. If, for example, a business refuses to conclude a contract or makes an offer with unfavorable conditions because of a certain score, consumers are usually barred from understanding how this score was achieved in the first place. This asymmetry arises not only because the algorithms used are well-guarded trade secrets, but also because the specific characteristics of many AI technologies[23] – such as opacity ("black box effect"), complexity, unpredictability and semi-autonomous behavior – can make effective enforcement of EU Consumer legislation difficult, as the decision cannot be traced and therefore cannot be checked for legal compliance.

25 The *use of AI in products and services* also raises a number of questions, such as when an AI system is in conformity with the contract and under which conditions the business is liable if the autonomous system causes damage. The latter point is contentious, as AI applications entail new risks and liability issues due to their connectivity and high degree of automation – aspects which are at present not explicitly covered by EU legislation.[24] Finally, there is the well-known black box problem[25] and the issue that software is often updated after purchase: how can the consumer even determine that the product or application he purchased was not in conformity with the contract at the time of purchase if the underlying system is opaque and may evolve after purchase?

26 The following analysis will show that European Union law has not yet found satisfactory answers to most of these questions.

C. Liability for AI Systems During the Life Cycle of Contracts

I. Pre-Contractual Duties

27 Over the past 35 years, the European Union has enacted a vast number of directives in order to protect the consumer,[26] who is commonly defined as a natural person acting for purposes which are outside

22 Cf also Jabłonowska, Kuziemski, Nowak, Micklitz, Pałka, and Sartor, 'Consumer law and artificial intelligence. Challenges to the EU consumer law and policy stemming from the business's use of artificial intelligence. Final report of the ARTSY project' (2018) European University Institute (EUI) Working Paper LAW 2018/11; Sartor, 'New aspects and challenges in consumer protection. Digital services and artificial intelligence' (April 2020) Study requested by the IMCO committee of the European Parliament PE 648.790.

23 European Commission, 'White Paper on AI' COM(2020) 65 final, 14.

24 Cf European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics' COM(2020) 64 final.

25 The term "black box" refers to the problem that automated decisions or predictions do not provide any reason or explanation for this decision or prediction; cf Burrell, "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms" (2016 January-June) Big Data & Society 1; Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, Harvard University Press 2015).

26 On development of EU Consumer law cf Ebers, *Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht* (n 4) 737ff; Howells and Wilhelmsson, *EC Consumer Law* (Aldershot, Routledge 1997) 9ff; Stuyck, 'European Consumer Law After the Treaty of Amsterdam: Consumer Policy in or beyond the Internal Market?' (2000) 37 Common Market Law Review (CMLR) 367-400, at 377ff; Weatherill, *EU Consumer Law and Policy* (2nd ed, Cheltenham, Elgar 2005) 1ff.

his or her business, commercial, or trade activity.[27] Many directives establish pre-contractual duties of the business – by prohibiting unfair commercial practices, such as misleading advertisements or by establishing information duties – in order to allow the consumer to make an informed decision before concluding a contract.

1. Dark Patterns and Online Behavioral Advertising as Unfair Commercial Practices?

28 A particular concerning business practice can be found in so-called "dark patterns" and online behavioral advertising techniques. The expression "dark patterns"[28] is a catch-all term for how user interface design can be used to adversely influence users and their decision-making abilities online.[29] The term has recently found its way into legal texts, for example the Californian Civil Code, as amended by the Privacy Rights Act of 2020, which defines "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation."[30] Online behavioral advertising, on the other hand, refers to the practice of targeting consumers based on their behavior and their cognitive biases, in order to influence consumers to take decisions that may go against their best interests.

29 The use of these practices poses the question of how EU law, especially the Unfair Commercial Practices Directive (UCPD) 2005/29,[31] can prevent (and remedy) situations in which the trader takes advantage of consumers' vulnerabilities.[32]

30 Many legal studies show that the UCPD 2005/29 insufficiently addresses the problem of dark patterns and other ways of online behavioral advertising,[33] highlighting two points in particular. On the one hand, the definition of "aggressive practices" seems to be too narrow, as all forms of aggressive behavior require the presence of pressure, which is normally absent in subtle forms of nudging. On the other hand, many scholars rightly argue that the benchmarks of "average" and "vulnerable" consumer are too narrow and static, as neither definition sufficiently reflects that traders in the age of AI and big data analytics have the technological capacity to exploit

27 For an overview of the various definitions of "consumer" in EU directives and the respective case-law, cf Ebers in Schulte-Nölke, Twigg-Flesner and Ebers, *EC Consumer Law Compendium. The Consumer Acquis and its transposition in the Member States (*München, Sellier European Law Publishers 2008) 453ff.

28 The term was coined by Brignull in 2010; Brignull, 'Dark Patterns: Deception vs. Honesty in UI Design' A List Apart (1 November 2011) <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/> accessed 31 January 2021.

29 In the context of data protection law, the Norwegian Consumer Council defines "dark patterns" as "techniques and features of interface design meant to manipulate [and] to nudge users towards privacy intrusive options", including "privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users"; Forbrukerrådet, 'Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy' (27 June 2018) Norwegian Consumer Council report <https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2020/12/deceived-by-design.pdf> accessed 31 January 2021.

30 Section 1798.140 (l) Californian Civil Code, as amended by section 14 of the California Privacy Rights Act 2020.

31 European Parliament and Council Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22 (Unfair Commercial Practices Directive).

32 See, for example, European Parliament, Parliamentary questions, Answer given by Ms Jourová on behalf of the European Commission, E-000774/2019, 11 April 2019.

33 Ebers, "Beeinflussung und Manipulation von Kunden durch 'Behavioral Microtargeting'" (2018) MultiMedia und Recht (MMR) 423; Galli, 'Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD' in Ebers and Cantero (eds), *Algorithmic Governance and Governance of Algorithms* (Cham, Springer 2020) 109-135; Helberger, 'Profiling and targeting consumers in the Internet of Things – a new challenge for consumer law' in Schulze and Staudenmayer (eds), *Digital revolution: challenges for contract law in practice* (Baden-Baden, Nomos 2016); Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8(1) Law, Innovation and Technology 1 <http://ink.library.smu.edu.sg/sol_research/1736> accessed 30 January 2021. However, see also Leiser, "'Dark Patterns': The Case for Regulatory Pluralism" (12 June 2020) <https://ssrn.com/abstract=3625637> accessed 31 January 2021, who argues that, although the European Union's consumer protection regime has been underutilized, "it is ripe for shining light on malicious and manipulative dark patterns".

temporary vulnerabilities and not just those caused by age, mental infirmity or credulity, as foreseen by Art. 5(3) UCPD.[34]

31 Contract law also fails to provide satisfactory answers to dark patterns and online behavioral advertising. As I have explained elsewhere,[35] it is difficult to subsume online behavioral advertising and subtle forms of nudging under any of the traditional protective doctrines – such as duress, mistake, undue influence, misrepresentation, or *culpa in contrahendo* – as there is a very fine line between informing, nudging, and outright manipulation.

32 Accordingly, the possibilities to protect consumers from dark patterns, nudging and subtle forms of manipulation are currently – *de lege lata* – rather limited.

2. Pre-contractual Information Duties

33 Pre-contractual information duties primarily serve the purpose of rectifying existing information asymmetries between the trader and the consumer. Accordingly, they could also serve to correct new power imbalances in the B2C relationship stemming from companies' use of opaque algorithmic systems. One way to realize this level of accountability could be to require that traders inform consumers before the conclusion of contract about the use of algorithmic systems, their main characteristics, and their underlying logic.

34 The EU Consumer Rights Directive 2011/83/EU, as amended by the "New Deal for Consumers", includes such an obligation, however, only to a very limited extent; according to Art. 6(1) (ea) Consumer Rights Directive (CRD) 2011/83/EU[36] as amended by Directive 2019/2161/EU,[37] the trader may be obliged to inform the consumer "that the price has been personalised on the basis of an automated decision making process". Moreover, the so-called P2B (platform-to-business) Regulation 2019/1150 requires providers of online search engines to "set out the main parameters, which individually or collectively are most significant in determining ranking and the relative importance of those main parameters, by providing an easily and publicly available description".[38]

35 Additionally, many consumer law directives require traders to disclose a list of information – for example, about the main characteristics and total price of the goods or services and the functionality of digital content – before the conclusion of a contract.[39] However, the relevant disclosure requirements are formulated too generally to determine how they can be concretized with regard to AI systems.

36 Therefore, considering the current legal situation, only limited pre-contractual information obligations can be leveraged to regulate the use of AI systems.

II. Formation of Contract and Algorithmic Decision Making

1. Formation of Contract under EU Private Law

37 Traditionally, formation of contract is not a subject of EU (Private) Law Directives.[40] Hence, the question of whether a contract has been concluded must be determined under the applicable national law. Accordingly, the heated debate[41] over whether

34 Critically, Duivenvoorde, 'The Protection of Vulnerable Consumers under the Unfair Commercial Practices Directive' (2013) 2 Journal of European Consumer and Market Law 69-79. See also Leczykiewicz and Weatherhill (eds), *The Images of the Consumer in EU Law* (Oxford/Portland, Hart Publishing 2018).

35 Ebers, "Beeinflussung und Manipulation von Kunden durch 'Behavioral Microtargeting'" (n 33).

36 European Parliament and Council Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64.

37 European Parliament and Council Directive 2019/2161 of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules [2019] OJ L328/7.

38 Art 5(2) Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57 (P2B Regulation).

39 Art 5(1)(a) CRD 2011/83; Art 6 of the Directive 2011/83/EU on consumer rights, etc.

40 Cf Art 3(5) CRD 2011/83; Art 3(10) DCSD 2019/770; Art 3(6) SGD 2019/771. For more details on this harmonization technique see the papers in Schulze/Ebers/Grigoleit (eds), *Information Requirements and Formation of Contract in the Acquis Communautaire – Informationspflichten und Vertragsschluss im Acquis Communautaire* (Tübingen, Mohr Siebeck 2003).

41 Cf Allen and Widdison, 'Can Computers Make Contracts?'

automatically generated declarations of an AI system can be attributed (e.g. as an offer or acceptance) to a natural or legal person depends on the applicable national law.[42]

2. Art. 22(1) GDPR and EU Private Law

38 Whether Art. 22 of the General Data Protection Regulation (GDPR) changes the national rules of formation of contract remains unclear. According to Art. 22(1) GDPR, "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Since this provision can be interpreted as a prohibition,[43] a breach of Art. 22(1) GDPR could result in the nullity of a contract, or, if interpreted as a right not to be subject to automated decision-making,[44] as a right to avoidance.

39 However, both views cannot be adopted. The GDPR does not intend to harmonize the national laws of obligations. In general, violations of the regulation do not affect the general contract law of Member States such as the rules on the validity, formation, or effect of a contract.[45] By the same token, EU secondary law clarifies that consumer contract law directives are without prejudice to the GDPR.[46] Hence, the GDPR and (partially harmonized) national laws of obligations are applicable alongside each other.[47]

40 Apart from this, Art. 22(1) GDPR has little significance in practice, as Art. 22(2) GDPR establishes numerous exceptions and only covers decisions "based solely on automated processing" of data (Art 22(1) GDPR). Since most algorithmically prepared decisions still involve a human being, the majority of algorithmic decision-making procedures are therefore not covered by the prohibition of Art 22(1) GDPR.[48]

(1996) 9 Harvard Journal of Law & Technology 26; Sartor, 'Agents in Cyber Law' in Cevenini, *Proceedings of the Workshop on the Law of Electronic Agents (LEA02)* (Bologna, CIRSFID 2002) 7; Turner, *Robot Rules. Regulating Artificial Intelligence* (Cham, Palgrave Macmillan 2019) 106ff; for German law cf Wendehorst/Grinzinger, '§ 4 Vertragsrechtliche Fragestellungen beim Einsatz intelligenter Agenten' in Ebers et al (eds), *Künstliche Intelligenz und Robotik – Rechtshandbuch* (München, CH Beck 2020) 139ff, at 149ff.

42 There have already been some attempts to create special laws to account for the role of computers in concluding contracts. Cf eg Art 12 of the UN Convention on the Use of Electronic Communications in International Contracts 2005 ("A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract"); section 14 of the Uniform Electronic Transactions Act ("A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.").

43 Sancho, 'Automated Decision-Making under Article 22 GDPR: Towards a More Substantial Regime for Solely Automated Decision-Making' in Ebers and Navas (eds), *Algorithms and Law* (Cambridge/New York, Cambridge University Press 2020) 147; see also Wachter, Mittelstadt, and Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law (IDPL) 94ff; Mendoza and Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' (2017) University of Oslo Faculty of Law Legal Studies Research Paper Series, 7ff, 9ff.

44 Sancho (n 43) 148.

45 This is expressly clarified for child consent in Art 8(3) GDPR, but it applies in principle to all breaches of the Regulation.

46 See Art 3(8) DCSD 2019/770.

47 For attempts to harmonize data protection law with the law of obligations in order to create a "Datenschuldrecht" or "data-related law of obligations", cf Langhanke/Schmidt-Kessel, 'Consumer Data as Consideration' (2015) 1 Journal of European Consumer and Market Law (EuCML) 218; Schmidt-Kessel, 'Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten' (2017) Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW) 84; Lohsse/Schulze/Staudenmayer (eds), *Data as Counter-Performance - Contract Law 2.0?* (Baden-Baden, Nomos 2019); Wendland, 'Sonderprivatrecht für Digitale Güter' (2019) 118 Zeitschrift für Vergleichende Rechtswissenschaft (ZVglRWiss) 191.

48 Wachter, Mittelstadt and Floridi (n 43) 92. Bygrave, on the other hand, is of the opinion that decisions formally attributed to humans but originating "from an automated data-processing operation the result of which is not actively assessed by either that person or other persons before being formalised as a decision" would fall under the category of "automated decision-making": Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Review 17.

3. Algorithmic Discrimination and EU Private Law

41 Another problem in the context of algorithmic decision making is the risk of discriminatory decisions. In fact, many examples show that algorithmic decisionmaking procedures are by no means neutral, but can perpetuate and even exacerbate human bias in various ways. For example, data mining and machine learning techniques which are used to select job applicants might discriminate against minorities, simply because the training data reflect existing social biases against a minority.[49] Despite these findings, a number of legal studies draw the conclusion that neither EU anti-discrimination law[50] nor EU data protection law[51] can tackle this problem.[52]

III. Contractual Liability for a Breach of Contract Caused by AI Systems

42 If, in using an AI system, the trader breaches the contract,[53] the question arises as to whether he is responsible for non-performance or other damages caused by the "misconduct" of such a system.

43 Currently, EU private law contains few provisions in this regard. When it comes to *non-conforming goods* or *non-conforming digital content/services*, the consumer's claim for repair/replacement (or other measures to bring the good/digital content into conformity), price reduction, or termination of contract does not require the seller to be at fault.[54] According to both the DCSD 2019/770 and the SGD 2019/771, the business's liability is, as a matter of principle, strict. Therefore, the consumer is not required to establish that the trader was aware or should have been aware that the AI system was likely to act in a way that led to a breach of contract and a damage.

44 However, this form of strict contractual liability applies only to the above listed remedies. The regulation of damages is, on the other hand, left to Member States.[55] As a consequence, Member States[56] remain free to maintain or introduce systems in which liability in damages is based on fault[57] or on

49 Lowry and MacPherson, 'A Blot on the Profession' 296 British Medical Journal 657–658 (1988).

50 Cf especially Race Equality Directive 2000/43/EC; Gender Equality Directive 2004/113.

51 Some scholars suggest that the GDPR should be used to mitigate risks of unfair and illegal discrimination; cf Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) 55 CMLR 1143. Cf also Mantelero, 'Regulating Big Data' (2017) 33(5) The Computer Law and Security Review 584; Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2018) 34(3) The Computer Law and Security Review 436; Wachter and Mittelstadt, 'A Right to Reasonable Inferences: Rethinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review 494 <https://ssrn.com/abstract=3248829> accessed 31 January 2021.

52 Ebers, 'Regulating AI and Robotics: Ethical and Legal Challenges' in Ebers and Navas (eds), *Algorithms and Law* (Cambridge/New York, Cambridge University Press 2020) 78ff. For the problems of applying EU anti-discrimination law, see also Hacker (n 51); for the limits of EU Data protection law to deal with algorithmic discrimination cf Zuiderveen Borgesius, 'Discrimination, artificial intelligence, and algorithmic decision-making' (2018) Study for the Council of Europe, 24ff <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> accessed 31 January 2021.

53 Example: The trader does not deliver the ordered good or does not provide the promised service because of a malfunction of the AI system.

54 Riehm/Abold, 'Mängelgewährleistungspflichten des Anbieters digitaler Inhalte' (2018) 2 Zeitschrift für Urheber- und Medienrecht (ZUM) 82–91, at 88; Rosenkranz, 'Article 10 - Third-party rights' in Schulze and Staudenmayer (eds), *EU Digital Law – Article-by-Article Commentary* (Baden-Baden/Oxford, CH Beck/Nomos/Hart 2020) 196, para 55.

55 Art 3(10) DCSD 2019/770; Art 3(6) SGD 2019/771. Additionally, recital (73) DCSD 2019/770 and recital (61) SGD 2019/771 state as a principle that the consumer should be entitled to claim compensation for detriment caused by a lack of conformity with the contract. At the same time, the recitals also stress that such a right already is ensured in all Member States and therefore the directives are without prejudice to national damages rules.

56 For a comparison between different legal systems, see Ebers, Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht (n 4) 941ff; Schwartze, *Europäische Sachmängelgewährleistung beim Warenkauf* (Tübingen, Mohr Siebeck 2000) 249ff, 331ff; von Bar, Clive and Schulte-Nölke et al (eds), 'Draft Common Frame of Reference (DCFR), Principles, Definitions and Model Rules of European Private Law, Full Edition' (2009), prepared by the Study Group on a European Civil Code and the Research Group on EC Private Law (Acquis Group) vol 1, 774ff.

57 This is, for example, the case in Germany; cf § 280(1) BGB. By contrast, under English and Irish law, contract liability is strict liability, and will occur in most cases of non-performance unless the failure to perform is excused; Treitel, *Remedies for Breach of Contract* (Oxford, Clarendon Press 1989).

force majeure as a defense.[58]

45 If the consumer's right to damages for breach of contract is subject to these conditions, it is doubtful whether the trader can be held liable in cases where the specific error and thus the behavior of the AI system was unforeseeable and in the specific situation unavoidable.

46 National contract law might come up with different answers.[59] According to a predominant view, computer programs – including AI systems – are seen as mere tools which are used by human agents.[60] Therefore, in order to hold a human accountable, what matters is not the damaging "behavior" of the software, but the behavior of the human actor involved. However, such an approach is problematic when it comes to autonomous systems. The higher the degree of automation, the less the human can be blamed for the specific behavior of the AI system that led to a breach of contract and damages. If the trader can prove that the occurrence of damage was neither predictable nor avoidable in accordance with the state of the art, he cannot be held liable.

47 In light of these considerations, a growing number of scholars want to treat AI systems as "agents" for which the human operator is liable according to the rules on vicarious liability.[61] Indeed, such an analogy leads in most cases to strict contractual liability of the human operator for breaches of contractual obligations caused by machines, regardless of whether such conduct was planned or envisaged. Others even call for autonomous AI systems to be granted limited legal capacity in order to close possible liability gaps in contract and tort law.[62]

48 In any case, contractual clauses might limit or exclude a business's liability for damages caused by AI systems. The question then becomes a matter of whether such clauses are valid. Since neither the DCSD 2019/770 nor the SGD 2019/771 regulate the right to damages, the validity of such disclaimers must be determined first and foremost by national (consumer) contract law. Additional requirements could result from the Unfair Contract Terms Directive (UCTD) 93/13.[63] While the Court of Justice of the European Union (CJEU) emphasized in earlier rulings that the list contained in the Annex to the directive is only of "indicative and illustrative value",[64] the Court has underlined since the Invitel case[65] that the Annex is "an essential element on which the competent court may base its assessment". At the same time, the CJEU gradually specified, in a number of cases, the abstract criteria listed in the Annex for reviewing whether a term is unfair.[66] Accordingly, the CJEU

58 Eg French law, see Beale, Fauvarque-Cosson, Rutgers and Vogenauer, *Ius Commune Casebooks for the Common Law of Europe: Cases, materials and text on Contract Law* (3rd edn, Oxford, Hart 2019) ch 28.3.

59 For an overview on the different theories cf Koops, Hildebrandt, and Jaquet-Chiffelle, 'Bridging the Accountability Gap: Rights for New Entities in the Information Society?' (2010) 11(2) Minnesota Journal of Law, Science & Technology 497.

60 Cerka, Grigiene, Sirbikyte, 'Liability for damages caused by artificial Intelligence' (2015) 31 Computer Law & Security Review 376-389, at 384ff. For Germany, cf Horner/Kaulartz, 'Haftung 4.0: Rechtliche Herausforderungen im Kontext der Industrie 4.0' (2016) Innovations- und Technikrecht (InTeR) 22-27, at 23; Hanisch, 'Zivilrechtliche Haftungskonzepte für Robotik' in Hilgendorf (ed), *Robotik im Kontext von Recht und Moral* (Baden-Baden, Nomos 2014) 27-61, at 32.

61 For the international debate cf fn 41 and 62. For Germany, cf Hacker, 'Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz' (2018) 9 Rechtswissenschaft (RW) 243–288, at 284ff; Schirmer, 'Rechtsfähige Roboter?' (2016) 71 JZ 660–816, at 665; Teubner, 'Digitale Rechtssubjekte' (2018) 218 Archiv für die civilistische Praxis (AcP) 155-205, at 186; Wendehorst/Grinzinger, 'Vertragsrechtliche Fragestellungen beim Einsatz intelligenter Agenten' (n 41) 168ff, para 82ff.

62 Solum, 'Legal Personhood for Artificial Intelligence' (1992) 70 North Carolina Law Rev 1231; Karnow, 'Liability for Distributed Artificial Intelligence' (1996) 11 Berkeley Technol Law Journal 147; Allen and Widdison, 'Can Computers Make Contracts?' (1996) 9 Harvard Journal of Law & Technology 26; Sartor, 'Agents in Cyber Law' in Santor and Cevenini (eds), *Proceedings of the Workshop on the Law of Electronic Agents (LEA02)* (Bologna, CIRSFID 2002) 7; Teubner, 'Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law' (2006) 33 Journal of Law & Society 497, 502; Matthias, 'Automaten als Träger von Rechten. Plädoyer für eine Gesetzesänderung' (PhD Thesis, University of Berlin 2007); Chopra and White, *A Legal Theory for Autonomous Artificial Agents* (Ann Arbor, University of Michigan Press 2011).

63 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.

64 Case C478/99 *Commission v Sweden* ECLI:EU:C:2002:281, [2002] ECR I-4147 [22].

65 Case C472/10 *Invitel Távközlési* ECLI:EU:C:2012:242 [26]; confirmed by case C488/11 *Asbeek Brusse and de Man Garabito* ECLI:EU:C:2013:341 [55]; case C342/13 *Sebestyén* ECLI:EU:C:2014:1857 [32]. In Case C143/13 *Matei* ECLI:EU:C:2015:127 [60] the Court refers to the Annex even as a "grey list".

66 For more detail cf Ebers, *Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht* (n 4) 887ff; Micklitz and Reich, 'The Court and the Sleeping Beauty: The Rival of the Unfair Contract Terms Directive (UCTD)' (2014) 51 CMLR 771-808,

could develop Europe-wide fairness requirements for clauses that limit the traders' liability for AI systems.

IV. Non-Contractual Liability for Defective AI Systems

49 Consumers who are harmed by an AI system may also have an extra-contractual claim against the producer or the operator of the AI system. So far, there is currently no specific legislation on civil liability for damage caused by AI either at European level or in any national jurisdictions.[67]

1. Product Liability Directive 85/374

50 In the European Union, product liability has been fully harmonized in all Member States through the Product Liability Directive (PLD) 85/374/EEC,[68] which establishes a system of strict liability – that is, liability without fault for producers when a defective product causes physical or material damage to the injured person.[69]

51 Whether the PLD can adjust effectively to the challenges posed by AI systems is currently unclear. Both the "Expert Group on Liability and New Technologies[70] and the European Commission in its report on "liability implications of Artificial Intelligence"[71] as well as other reports[72] point out various shortcomings of the PLD in this regard:[73]

52 First, it is unclear whether software is a product and thus covered by the PLD.

53 Second, the directive only applies to products and not to services.[74] Companies providing services such as (real-time) data services, data access, data-analytics tools, and machine-learning libraries are therefore not liable under the PLD,[75] so that national (non-harmonized) law decides whether the (strict) liability rules developed for product liability can be applied accordingly to services.

54 Third, the concept of defect remains unclear, because in the PLD, the determination of defect is linked to the level of safety that consumers are entitled to expect. However, with AI systems it becomes increasingly difficult for consumers and courts to establish the expected level of safety.

---

at 789 (judge-made "grey list").

67 According to a comparative report, Estonia and France are expected to develop and potentially propose either revision of the existing national legislation or adoption of the new legislation with a specific focus on liability issues; Evers, 'European Parliamentary Research Service, Civil liability regime for artificial intelligence. European added value assessment' (2020) EPRS Study PE 654.178, 46. However, the Estonian Ministry recently decided to refrain from reform projects in this regard, until the European Commission publishes its proposals on the regulation of AI; Liisi Jürgen, Tea Kookmaa, Tanel Kerikmäe, 'Jürgen, Kookmaa, Kerikmäe: kratiseadus pandi ootele' *ERR* (1 December 2020) <https://www.err.ee/1192069/jurgen-kookmaa-kerikmae-kratiseadus-pandi-ootele> accessed 2 February 2021.

68 European Parliament and Council Directive 1999/34/EC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products 1999 OJ L 141/20.

69 Art 9(b) PLD 1985/374 states that this claim does not relate to the defective product itself, but only to "damage to, or destruction of, any item of property other than the defective product itself". In other words, the PLD only provides compensation for "consequential loss", ie, economic loss that is connected to damage to a person or property of the claimant; For the term "consequential loss" as distinguished from "pure economic loss" cf Bussani/Palmer, 'The notion of pure economic loss and its settings' in Bussani/Palmer (eds), *Pure Economic Loss in Europe* (Cambridge, Cambridge University Press 2003) 3, 5ff.

70 European Commission, 'Liability for Artificial Intelligence and other emerging technologies' (2019) Report from the Expert Group on Liability and New Technologies - New Technologies Formation doi:10.2838/573689.

71 European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics' COM (2020) 64 final.

72 See especially Evers (n 67) 9.

73 See also Luzak, 'A Broken Notion: Impact of Modern Technologies on Product Liability' (2000) 11(3) European Journal of Risk Regulation 1; de Meeus, 'The Product Liability Directive at the Age of the Digital Industrial Revolution: Fit for Innovation?' (2019) 8 EuCML 149; Rott, 'Produkthaftung im Zeitalter der Digitalisierung' in Hentschel, Hornung and Jandt (eds), *Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft, Festschrift für Alexander Roßnagel* (Baden-Baden, Nomos 2020) 639; von Westphalen, 'Produkthaftungsrechtliche Erwägungen beim Versagen Künstlicher Intelligenz (KI) unter Beachtung der Mitteilung der Kommission COM(2020) 64 final' (2000) Verbraucher und Recht (VuR) 248-254.

74 Cf Case C-495/10 *Centre hospitalier universitaire de Besançon v Thomas Dutrueux and Caisse primaire d'assurance maladie du Jura* ECLI:EU:C:2011:869.

75 Service providers could only be liable if they manufacture the product as part of their service.

55 Moreover, there is the problem that, under Art 4 PLD, the injured party must prove the damage, the defect, and the causal relationship between defect and damage. This is precisely what is difficult with AI systems. The specific characteristics of many AI technologies – including opacity ('black box-effect'), complexity, unpredictability, and partially autonomous behavior,[76] as well as the (global) interconnectivity ("many hands problem")[77] – may make it hard for the victim to show that the AI system was defective when it was put into circulation and caused a damage.

56 Finally, the PLD provides for a number of exceptions in which producers can limit their liability, as for example the "development risks defence" admitted by Art 7(e) PLD.[78]

57 For all these reasons, the European Commission is currently examining possible amendments to the PLD.

2. National Tort Law

58 Liability for AI systems can arise not only from harmonized product liability law, but also from national liability systems, especially tort law. National tort law plays a crucial role especially when it comes to a claim of the injured party (consumer) against the operator of the AI system (e.g. against the trader).[79]

59 A recently published comparative legal analysis[80] of the national liability regimes of 19 Member States provides an interesting overview of the complexity and diversity of approaches and their degree of flexibility to adjust to the new challenges related to AI. By and large, all legal systems contain a regulatory mix between fault-based liability (as a rule) and strict liability systems (as a narrow set of exceptions).

60 Fault based systems usually do not provide satisfactory results when it comes to AI systems, because the high degree of automation/autonomy makes it increasingly difficult to trace damages back to negligent human behavior. If the operator can show that he/she has always taken all necessary safety precautions, it will be impossible to hold him/her liable for non-predictable actions of the AI systems.[81]

61 As a result, operators can only be held accountable if there is strict liability. However, in most member states, provisions on strict liability only apply in pre-determined cases – as, for example, with damages caused by things, dangerous activities, animals, and vicarious liability – and it is in all legal systems currently unclear whether these provisions can be applied to AI directly or by analogy.[82]

D. Liability for Non-Conforming AI Applications

62 In practice, AI systems are not only used by companies for internal purposes, but also offered to consumers as an essential part of smart goods or services, as for example in the form of automated translation services, surveillance technology, intelligent health apps, intelligent vacuum cleaners, or self-driving cars.

63 In these cases, the question arises as to what kind of quality consumers can expect from AI-driven goods, digital contents, or digital services. In other words: when is such a good, content, or service not in conformity with the contract? And what remedies are consumers then entitled to?

76 Cf European Commission, 'White Paper On Artificial Intelligence - A European approach to excellence and trust' COM(2020) 65 final, 12.

77 Yeung, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework' (2019) Council of Europe- Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), 11.

78 Cf thereto Cemre Polat, 'Defectiveness of Autonomous Systems and Development Risk Defence' (*RAILS-Blog*, 5 January 2021) <https://blog.ai-laws.org/defectiveness-of-autonomous-systems-and-development-risk-defence/> accessed 4 February 2021).

79 National tort law also plays a role in producers' liability insofar as it deals with situations that are not covered by the national laws transposing the PLD 85/374. For Germany, cf Ebers, 'Autonomes Fahren: Produkt- und Produzentenhaftung' in Oppermann/Stender-Vorwachs (eds), *Autonomes Fahren. Rechtsfolgen, Rechtsprobleme, technische Grundlagen* (München, CH Beck 2017) 93-125, at 102, available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192911> accessed 4 February 2021.

80 Evers (n 67).

81 This does not exclude in general the liability of operators. A person using AI systems should still be required to abide by duties to properly select, operate, monitor, and maintain the technology in use and – failing that – should be liable for breach of such duties if at fault.

82 Cf again Evers (n 67) 32.

I. Scope of the Directives on Digital Contracts

1. DCSD 2019/770 vs. SGD 2019/771: Which Directive Applies?

64 Since the DCSD 2019/770 and the SGD 2019/771 are mutually exclusive in their scope of application,[83] the first question is under which conditions each directive applies to AI-driven applications.

65 For the consumer, the demarcation of the scopes of application for both directives is of great importance. Although the two directives follow the same structure with almost identical rules on conformity and remedies, there are still some differences between them. The most notable point in this regard is the addressee of potential remedies.[84] The SGD 2019/771 establishes a one-stop mechanism: if the provision of digital content or service forms part of the contract, the seller is responsible for their functioning, even if this content or service is not supplied by the seller itself but by a third party. In other words, the consumer does not need to deal with different suppliers.[85] This situation changes if the consumer acquires a smart good separately from digital content or services. In that case, the SGD 2019/771 applies to the good only, whereas the DCSD 2019/770 applies to additional digital content and services with the consequence that the consumer has different contract partners to turn to, i.e. the seller and also the digital content/services provider.

66 The decisive factor in determining which of the directives applies is, at the end of the day, the content of the contract.[86] The SGD 2019/771 applies to goods with digital elements only if two cumulative conditions are met: a) first, the digital content or service must be incorporated or inter-connected with the good in such a way that "the absence of that digital content or digital service would prevent the goods from performing their functions" (Article 2(5)(b) SGD 2019/771); and b) second, the digital content or service must be "provided with the goods under the sales contract" (Article 3(3) SGD 2019/771).

2. Liability of Platform Providers?

67 Another issue is whether the new directives on digital contracts also apply to platforms. If a consumer and a business conclude the contract via an online platform, the platform is usually not a party to this contract. Rather, in such a "triangular" situation, there are normally three different contractual relationships, i.e. between the consumer and the business, the platform and the consumer, and the platform and the business.[87]

68 Accordingly, both the DCSD 2019/770 and the SGD 2019/771 clarify that platform providers are to be considered as sellers or traders only if they act "as the direct contractual partner of the consumer".[88] This could be the case, for example, when apps based on AI systems are offered by an operator of a platform which certifies and controls the apps,[89] or when a platform offers consumers directly "AI as a Service" (AIaaS).[90]

69 If, on the other hand, a platform acts as a mere intermediary, there is no obligation under EU law to apply the (nationally transposed) provisions of the directives to them. However, according to the

83 Cf Art 3(4) DCSD 2019/770; Art 3(3) SGD 2019/771.

84 Cf thereto Rott, 'The Digitalisation of Cars and the New Digital Consumer Contract Law' jipitec, in this issue. See also Tonner, 'Die EU-Warenkauf-Richtlinie: auf dem Wege zur Regelung langlebiger Waren mit digitalen Elementen' (2019) 10 VuR 363, 369.

85 See also Staudenmayer, 'Kauf von Waren mit digitalen Elementen – Die Richtlinie zum Warenkauf' (2019) Neue Juristische Wochenschrift (NJW) 2889; Staudenmayer, 'Die Richtlinie zu den digitalen Verträgen' (2019) 4 Zeitschrift für Europäisches Privatrecht (ZEuP) 663, 672ff.

86 Cf Sein and Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Part 1' (n 3) 269ff.

87 See Wendehorst, 'Platform Intermediary Services and Duties under the E-Commerce Directive and the Consumer Rights Directive' (2016) 5 EuCML 30-33; Busch et al, 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2016) 5 EuCML 3-4.

88 Recital (18) DCSD 2019/770 and recital (23) SGD 2019/770.

89 Cf Sein and Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Part 1' (n 3) 277ff.

90 Typically, AIaaS providers offer their customers access to pre-built AI models and services via APIs (application programming interfaces). Usually, however, AIaaS is offered only to commercial organizations and public sector bodies, and not to consumers. Cf Parsaeefard, Tabrizian, Leon-Garcia, 'Artificial Intelligence as a Services (AI-aaS) on Software-Defined Infrastructure' (AIES 2020, New York, 11 July 2019) arXiv:1907.05505v1 [cs.LG]; Javadi, Cloete, Cobbe, Lee and Singh, 'Monitoring Misuse for Accountable 'Artificial Intelligence as a Service'' (AIES 2020, New York, 7-8 February 2020); Berberich/Conrad, '§ 30 Plattformen und KI' in Ebers et al (eds), *Künstliche Intelligenz und Robotik – Rechtshandbuch* (München, CH Beck 2020) 930ff, at 938ff.

recitals of the directives,[91] even in this case Member States remain free to extend the directives' rules to these platform providers.

II. The Conformity Criteria

1. Overview

70 The new directives oblige the business to comply both with subjective as well as objective conformity criteria.[92] However, a closer look reveals that – in contrast to earlier proposals[93] – both Directives follow an approach under which goods, digital contents, and digital services have to respect mainly objective conformity criteria, i.e. statutory criteria.

71 As a matter of principle, subjective and objective conformity criteria apply cumulatively; in other words, both categories need to be respected.[94]

72 Whereas the parties to a contract can always agree to subjective conformity criteria that go beyond the objective conformity criteria (thereby establishing higher conformity standards), they cannot simply establish a lower standard than the objective conformity criteria in Art. 8 DCSD 2019/770, Art. 7 SGD 2019/771. According to both Directives, this is only possible if the consumer (i) was specifically informed that a particular characteristic of the good, digital content, or digital service was deviating from the objective requirements for conformity, and the consumer (ii) expressly and separately accepted that deviation when concluding the contract.[95]

73 As a result, consumers can rely on the objective criteria to establish non-conformity. Since compliance with objective conformity is mandatory for the business[96] and deviation is only possible by express and separate agreement,[97] (pre-formulated) standard contract terms cannot deviate from the objective conformity. Accordingly, it is not permissible for the business to attempt to exclude or limit its liability for AI systems through contract clauses defining the contractual performance in a way which is below the objective conformity, for example by pointing out that the AI system is "beta software" or a completely unpredictable system whose behavior cannot be predicted.

2. Objective Conformity, Art. 8(1) DCSD 2019/770 and Art. 7(1) SGD 2019/771

74 When digital goods, content, or services are based on AI-systems, the question arises as to which features, qualities, and performance these systems must comply with in order to meet the objective criteria for conformity. In this regard, Art. 8(1) DCSD 2019/770 and Art. 7(1) SGD 2019/771 contain a list of different objective conformity criteria, starting with the well-known "fit-for-purpose test", followed in Art. 8(1)(b) DCSD 2019/770 by a list of other objective conformity elements such as functionality, compatibility, accessibility, and security the consumer can reasonably expect.

75 Arguably, identifying objective criteria for AI systems is a complicated endeavor. How can we determine whether AI systems are fit for the purposes for which systems of the same type would "normally" be used? How do we measure whether AI systems possess the quality and performance features which are "normal" for systems of the same type and which the consumer may "reasonably" expect?

76 Obviously, such standards should not be defined by the courts on the basis of mere empirical findings. What is necessary, instead, is a normative standard that is not based on arbitrary subjective expectations, but on objective criteria. In this vein, Art. 8(1)(a) DCSD 2019/770 and Art. 7(1)(a) SGD 2019/771, in particular, refer to existing Union and national law

91 Cf again recital (18) DCSD 2019/770 and recital (23) SGD 2019/770.

92 Art 6 DCSD 2019/770; Art 5 SGD 2019/771.

93 The original proposal of a Digital Content Directive had taken a subjective approach; cf Art 6(1) of the European Commission, 'Proposal for a Directive on the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM(2015) 634 final. This approach encountered a lot of criticism; cf Loos, 'Not Good but Certainly Content' in Claeys and Terryn (eds), *Digital Content and Distance Sales* (Mortsel, Intersentia 2017) 18ff; Mak, 'The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content' (2016) Policy Department C in-depth analysis PE 536.494, 15ff; Twigg-Flesner, 'Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law' in Franceschi (ed), *European Contract Law and the Digital Single Market* (Cambridge/Antwerp/Portland, Intersentia 2016) 45.

94 Staudenmayer, 'Article 6 – Conformity of the digital content or digital service' in Schulze and Staudenmayer, *EU Digital Law: Article-by-Article Commentary* (Baden-Baden/Oxford, CH Beck/Nomos/Hart 2020) 107ff, at 115, para 29.

95 Art 8(5) DCSD 2019/770; Art 7(5) SGD 2019/771.

96 Art 22 DCSD 2019/770, Art 21 SGD 2019/771.

97 Art 8(5) DCSD 2019/770; Art 7(5) SGD 2019/771.

as well as technical standards.[98]

77 However, these criteria do not contribute significantly to concretizing the concept of objective conformity. Currently, there are neither legal rules specifically designed for AI systems nor international or national technical standards in that field. While it is true that both international[99] and national standardization organizations[100] are in the process of developing such technical standards, it will take a long time before they have emerged.

78 Even if technical standards for AI were available, two more related issues must be considered. First, standards in the field of AI can quickly become obsolete due to technical progress, updates, and upgrades. And second, there is a fundamental problem with learning AI systems in that the performance of such a system is not static, but constantly changing during operation. A characteristic feature of these systems is that they are not based on "locked" algorithms[101] that provide the same results each time the same input is applied to it. Instead, these algorithms rely on machine learning, so that they can change and adapt over time due to their real-world experience. As a consequence, the performance and quality of learning AI systems cannot be determined at a single point in time.

79 Considering these circumstances, one might indeed wonder whether it would be better if the DCSD had used a subjective notion of conformity "to promote innovation in the Digital Single Market and cater for technological developments reflected in the fast changing characteristics of digital content".[102]

3. Proof of Non-Conformity

80 Another important issue is the burden of proving a lack of conformity. In principle, both Directives reverse the burden of proof. According to Art. 12(2) DCSD 2019/770 and Art. 11(1) SGD 2019/770, if the lack of conformity becomes apparent within the period of one year, it is to be presumed that the lack of conformity existed at the time of delivery or supply.

81 However, this presumption only applies to an existing lack of conformity. The crucial question is therefore who must prove the lack of conformity itself. As both Directives are silent in this regard, this question is left to national law.[103] Usually, the

98 Additionally, both articles refer, in the absence of such technical standards, to applicable sector-specific industry "codes of conduct". However, it remains unclear from which guidelines objective conformity standards can be derived. At the end of day, codes of conducts primarily set out organizational structures. Usually, they do not state how a specific product must be manufactured but rather which organizational requirements as well as methods and procedures must be observed with regard to design and production processes, and how these prerequisites are put into practice. It is therefore doubtful whether conformity criteria can be derived from codes of conduct at all.

99 In 2017, the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) became the first international standards development organizations to set up a joint committee (ISO/IEC JTC 1/SC 42) which carries out standardization activities for AI; <https://www.iso.org/committee/6794475.html> accessed 4 February 2021.

100 In Germany, the Deutsches Intitut für Normung (DIN) published recently a roadmap for standards and specifications in the field of artificial intelligence; DIN/DKE, 'German Standardization Roadmap on Artificial Intelligence' (November 2020) <https://www.din.de/resource/blob/772610/e96c34dd6b12900ea75b460538805349/normungsroadmap-en-data.pdf> accessed 4 February 2021. See also DIN/DKE, 'Whitepaper: Ethik und Künstliche Intelligenz: Was können technische Normen und Standards leisten?' (October 2020), <https://www.din.de/resource/blob/754724/00dcbccc21399e13872b2b6120369e74/whitepaper-ki-ethikaspekte-data.pdf> accessed 4 February 2021.

101 The term "locked algorithms" is used in particular by the US Food and Drug Administration (FDA) for medical devices based on AI. To date, the FDA has cleared or approved only medical devices using "locked" algorithms; cf FDA, 'Artificial Intelligence and Machine Learning in Software as a Medical Device' (12 January 2021) <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device> accessed 4 February 2021; Benjamens, Dhunnoo, Meskó, 'The state of artificial intelligence-based FDA-approved medical devices and algorithms: an online database' (11 September 2020) NPJ Digit Medicine <https://doi.org/10.1038/s41746-020-00324-0> accessed 4 February 2021.

102 Thus, recital (24) of the original proposal for a Digital Content Directive (n 41) in order to justify the dominance of the subjective conformity criteria.

103 Zoll, 'Article 12 - Burden of proof' in Schulze and Staudenmayer (eds), *EU Digital Law– Article-by-Article Commentary* (Baden-Baden/Oxford, CH Beck/Nomos/Hart 2020) 217, para 17. In my opinion, nothing else follows from the CJEU judgment in Faber; Case C478/99 *Froukje Faber v Autobedrijf Hazet Ochten BV* ECLI:EU:C:2015:357. It is true that in the underlying case the car was completely destroyed, so that it could no longer be determined whether this fire was caused by a defect. Also, the CJEU ruled that according to Art 5(3) Consumer Sales Directive 1999/44, the consumer "does not

burden of proof concerning the appearance of the lack of conformity will be on the consumer, since he derives beneficial consequences from this fact.[104]

82 This raises the difficult question of how the consumer can prove a lack of conformity. First, AI systems are often embedded in an intelligent environment (Internet of Things) with contributions from multiple people and machine components, making it extremely difficult to determine why something is not working (the so called "many hands problem"). Second, proving a lack of conformity might be difficult if a system is constantly changing its features and performance due to its learning capabilities. And third, the lack of transparency (opaqueness) of many AI system might also make it difficult to attribute liability (the black box problem).

83 For all of these reasons, it can be assumed that consumers will have significant problems in practice enforcing their rights with AI systems.

4. Remedies

84 Regarding remedies, reference can be made to what has been said before.[105] For specific performance, price reduction, and termination, the liability of the business is strict. By contrast, contractual (and non-contractual) claims for damages caused to the consumer by a defective AI system are not governed by the Directives, so that Member State law decides, for example, whether compensation is linked to fault, how the fault requirement should be applied to AI systems, and who bears the burden of proof.

85 Clearly, the absence of any harmonization vis-à-vis damages is hardly compatible with the directives' objectives to provide a high level of consumer protection and to create a proper functioning of the internal market. Therefore, scholars correctly point out that there is still need for future European legislation to harmonize the law of damages in relation to the supply of digital content.[106]

E. Outlook

86 The *tour de horizon* through the lifecycle of contracts – in which AI is either used for internal purposes by companies or offered as an essential part of the main subject matter to consumers – reveals, as a result, a number of gaps in current EU consumer law. This concerns in particular (i) dark patterns and online behavioral advertising, (ii) growing information asymmetries, (iii) risks of algorithmic decision making, (iv) liability for defective AI systems, (v) missing standards for assessing whether AI systems comply with the objective conformity criteria, (vi) difficulties for the consumer to prove non-conformity of AI systems, and (vii) the lack of harmonization of the law of damages in relation to the supply of digital content.

87 An important question is, therefore, whether the current EU reform projects have the potential to close these gaps. In this respect, two main reform efforts are worth highlighting.[107]

88 First, the EU Commission's White Paper on AI,[108] in which the Commission considers possible adjustments to existing EU legislative frameworks,[109]

have to prove the cause of that lack of conformity or to establish that its origin is attributable to the seller". At the same time, however, the CJEU underlined that Art 5(3) only applies if "the consumer furnishes evidence that the goods sold are not in conformity with the contract". Therefore, it does not suffice to show that the item or a specific feature does not work; the consumer must still prove the lack of conformity itself.

104 Zoll (n 103). For Germany, Koch, 'Anmerkung zum Urteil des EuGH vom 4. Juni 2015 - C-497/13' (2015) JZ 834-837, at 834.

105 Cf above, 3.3. and 3.4.

106 Schulze, 'Article 5 - Supply of the digital content or digital service' in Schulze and Staudenmayer (eds), *EU Digital Law–Article-by-Article Commentary* (Baden-Baden/Oxford, CH Beck/Nomos/Hart 2020) para 35.

107 Additionally, the European Commission presented in December 2020 two proposals. First, the proposal for a Digital Services Act, which aims to introduce mechanisms for removing illegal content, possibilities for users to challenge platforms' content moderation decisions, and transparency measures for online platforms; European Commission, 'Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final. And second, the proposal for a Digital Markets Act, which aims to ensure that large online platforms (so called "gatekeepers") behave in a fair way vis-à-vis business users who depend on them; European Commission, 'Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act)' COM(2020) 842 final.

108 Cf thereto Ebers/Cantero, 'Algorithmic Governance and Governance of Algorithms: An Introduction' in Ebers/Cantero (eds), *Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges* (Cham, Springer 2020) 1-22, at 12ff.

109 European Commission, 'White Paper - On Artificial Intelligence – A European approach to excellence and trust'

and additionally, a new legal instrument for "high-risk AI applications". And second, the current efforts to modernize the civil liability regime for AI – discussed inter alia[110] in the report of the Expert Group on Liability and New Technology,[111] the European Commission's Report on the safety and liability implications of AI,[112] and the European Parliament's resolution with recommendations to the Commission on a civil liability regime for AI.[113]

89 Both initiatives as well as forthcoming guidance documents by the European Commission on the application of current consumer law[114] could make an important contribution to consumer protection. Nevertheless, it seems too early to evaluate these initiatives. In the AI White Paper, the Commission does not elaborate on possible consumer protection instruments with regard to AI applications.[115] And in the Liability Report, the Commission only states in general terms that "certain adjustments to the Product Liability Directive and national liability regimes through appropriate EU initiatives could be considered on a targeted, risk-based approach, i.e. taking into account that different AI applications pose different risks."[116]

90 In addition, some Member States have already voiced strong opposition to the plans of the European Commission. In a position paper published in October 2020, 14 EU countries called on the Commission to incentivize the development of next-generation AI technologies, rather than put up barriers, urging the Commission to adopt a "soft law approach".[117]

91 European consumers seem to disagree with this opinion. According to an AI consumer survey conducted by consumer groups in nine EU countries,[118] consumers have confidence in AI's potential; however, many of them doubt that they are sufficiently protected under current consumer law from the negative consequences of AI. Indeed, the foregoing analysis has shown that there is still much to be done.

COM(2020) 65 final, 14.

110 For a short overview cf de Bruyne, Dheu, 'An EU Perspective on Liability and Artificial Intelligence' (*RAILS-Blog*, 14 May 2020) <https://blog.ai-laws.org/an-eu-perspective-on-liability-and-artificial-intelligence/> accessed 2 February 2021.

111 European Commission, 'Liability for Artificial Intelligence and other emerging technologies' (2019) Report of the Expert Group on Liability and New Technologies- New Technologies Formation doi:10.2838/573689.

112 European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics' COM(2020) 64 final.

113 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). Cf moreover, European Parliament, Committee on Legal Affairs, Rapporteur: Axel Voss, 'Report with recommendations to the Commission on a civil liability regime for artificial intelligence' A9-0178/2020. For a critical discussion of this resolution see Sousa Antunes, 'Civil Liability Applicable to Artificial Intelligence: A Preliminary Critique of the European Parliament Resolution of 2020' (5 December 2020) <https://ssrn.com/abstract=3743242> accessed 4 February 2021; Etzkorn, 'Die Initiative des EU-Parlaments für eine EU-Verordnung zur zivilrechtlichen Haftung beim Einsatz von KI' (2020) 36 Computer und Recht (CR) 764-768.

114 The European Commission is planning to publish guidance documents on the application of the UCPD 2005/29 and the CRD 2011/83 to problematic practices observed in e-commerce that prevent consumers from obtaining important information and abuse their behavioural biases. This refers especially to the use of 'dark patterns' (user-interface designs aimed at manipulating consumers), profiling, hidden advertising, fraud, misleading information and manipulated consumer reviews; cf European Commission, 'New Consumer Agenda. Strengthening consumer resilience for sustainable recovery' COM(2020) 696 final, 10.

115 Cf Ebers, 'Künstliche Intelligenz und Verbraucherschutz: Das KI-Weißbuch der Europäischen Kommission' (2020) VuR 121-122; Ebers/Navas, 'Artificial Intelligence and Consumer Protection' (*fifteeneightyfour*, 10 September 2020) <http://www.cambridgeblog.org/2020/09/artificial-intelligence-and-consumer-protection/>.

116 European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics' COM(2020) 64 final, 17.

117 Stolton, 'EU nations call for 'soft law solutions' in future Artificial Intelligence regulation' *Euractiv* (8 October 2020) <https://www.euractiv.com/section/digital/news/eu-nations-call-for-soft-law-solutions-in-future-artificial-intelligence-regulation/> accessed 4 February 2021. The position paper was signed by Denmark (initiator), Belgium, the Czech Republic, Estonia, Finland, France, Ireland, Latvia, Luxembourg, the Netherlands, Poland, Portugal, Spain and Sweden.

118 BEUC, 'Artificial Intelligence: What consumers say. Findings and policy recommendations of a multi-country survey on AI' (2020) <http://www.beuc.eu/publications/beuc-x-2020-078_artificial_intelligence_what_consumers_say_report.pdf> accessed 4 February 2021.