robotics

MDPI

Review

Siri 2.0—Conversational Commerce of Social Bots and the New Law of Obligations of Data: Explorations for the Benefit of Consumer Protection

Dagmar Gesmann-Nuissl * and Stefanie Meyer

Faculty of Economics and Business Administration, Chemnitz University of Technology, 09111 Chemnitz, Germany

* Correspondence: dagmar.gesmann@wiwi.tu-chemnitz.de

Abstract: The possibilities and reach of social networks are increasing, designs are becoming more diverse, and ideas more visionary. Most recently, the former company "Facebook" announced the creation of a metaverse. With these technical possibilities, however, the danger of fraudsters is also growing. Using social bots, consumers are increasingly influenced on such platforms and business transactions are brought about through communication, i.e., conversational commerce. Minors or the elderly are particularly susceptible. This technical development is accompanied by a legal one: it is permitted by the Digital Services Directive and the Sale of Goods Directive to demand the provision of data as consideration for the sale of digital products. This raises legal problems at the level of the law of obligations and data protection law, whose regulations are intended to protect the aforementioned groups of individuals. This protection becomes even more important the more gullible consumers are influenced by communicative bots. We show that there is a lack of knowledge about what value objective data can have in business transactions. The sufficient transparency of objective data value can maintain legal protection, especially of vulnerable groups, and ensure the purpose of the laws.

Keywords: conversational commerce; data protection; law of obligations of data

Citation: Gesmann-Nuissl, D.; Meyer, S. Siri 2.0—Conversational Commerce of Social Bots and the New Law of Obligations of Data: Explorations for the Benefit of Consumer Protection. *Robotics* **2022**, *11*, 125. https://doi.org/10.3390/robotics11060125

Academic Editors: Laura Kunold and Linda Onnasch

Received: 16 August 2022
Accepted: 8 November 2022
Published: 14 November 2022

1. Introduction

The company long known as "Facebook" announced on 28 October 2021, at its *Facebook Connect* augmented and virtual reality conference, that it was changing its corporate name to "Meta." The new name is also meant to reflect the company's growing ambitions beyond social media [1].

"Today we're considered a social media company, but in our DNA we're a company that builds technology to connect people, and the metaverse is the next frontier, just like social networks were when we started", Meta CEO Mark Zuckerberg said.

While this new digital revolution has been positively received by users eager to communicate and by the company's investors, there are just as many skeptics who are particularly critical of the way social bots communicate, some of them anonymously. Social bots are already being used on simple social media platforms to engage in conversation with users. The use of these software agents is criticized not only from a moral point of view but also raises numerous legal issues related in particular to the method of communication. Unlike, for example, the first social bot ELIZA [2], which was developed by Weizenbaum in 1960 and could only draw on a set of text modules, modern social bots are able to conduct unpredictable conversations through their algorithms and programs, which can have a manipulative effect on their human partner. Particularly susceptible to such manipulation are minors and vulnerable groups who lack sufficient reflection (the elderly, addicts, etc.).

In the following, we therefore discuss the application scenarios of social bots that address this target group and, specifically, their protection as consumers. The considerations refer both to classic social media (e.g., Facebook Messenger or WhatsApp) and to the

visionary ambitions of leading companies—the metaverse. Narrowing down the scope of our consideration, we focus on the use of social bots in the area of conversational commerce. This type of commerce poses legal challenges, which have also been exacerbated by a recent change in legislation at the European level and are being incorporated into everyday contractual transactions through national implementation. Therefore, in our paper, we illustrate the difficulties that arise from the communicative behavior of social bots when paying with data.

2. Methods

First, we conducted a comprehensive and detailed investigation of the legal implications of conversational commerce using social robots in metaverse and searched for relevant sources in a variety of disciplines. Thereby, we conducted research using the snowball principle primarily through search engines such as Google Scholar, Web of Science, beck-online, juris, and the Social Science Research Network. We restricted the articles to the languages German and English. In this way, we obtained a total of N = 66 articles, books, commentaries, and case law reports. These essays or book chapters provided us with an overview of the basic definitions, technical requirements, and legal discussions in the literature and case law on the currently relevant legal acts. The studies of the technically possible developments enable us to consider the legal implications of the future.

3. Social Bots and Their Occurrence

To investigate the legal implications, we need a specific starting point in relation to the conversational agents, namely social bots. Therefore, we first consider the definitions, scopes, and prerequisites of these communication agents.

3.1. Social Bots

Social bots are a subgroup of so-called conversational agents. These are software applications that process natural language and automatically respond verbally or in writing in human language [3]. Conversational agents play an important role in the field of conversational commerce. This keyword is used to convey sales, ratings, and customer service in direct dialog, e.g., via Facebook Manager or WhatsApp, in order to address customers in their familiar communication sphere [4]. This allows customers to select products without leaving the social network space. The conversational agents used for this purpose in the area of conversational commerce are known as social bots [4]. Accordingly, social bots ("bot" derives from robot, the term "social" indicates that these are algorithms and programs that preferably have effects within social media, see [5,6]) are computer programs that pretend to have a human identity and are used for manipulative purposes by communicating like humans on the internet [7]. Essentially, social bots consist of three elements: user accounts in social networks, programming interfaces, and software written in any programming language with the behavioral logic of the social bot [6,8–10]. Social bots differ from other internet phenomena, such as assistance bots, spam emails, trolls, and cyberattacks, by combining three main features:

(1) an algorithm implemented in software,
(2) an algorithm that impersonates a person, and
(3) an algorithm that attempts to influence opinion formation (depending on their field of application, certain bots are also referred to as "Twitter bot" or "political bot", see [11]).

The use of social bots ranges from latent influence (e.g., use of a sympathetic voice) to targeted manipulation (e.g., through the automatic writing of posts or algorithmic interaction with third-party content) [4]. In general, two types can be distinguished [12]:

(1) Social bots that pursue (exclusively) commercial purposes by faking customer reviews, spreading alleged likes for products, or engaging consumers in automated sales dialogs [8,13];
(2) Social bots that are used to influence public discourse, especially political opinion formation [14,15].

In the following discussion, we will focus on the first type only. The focus of the considerations presented in this article will be solely on consumer protection as it applies to the area of the new law of obligations of data. Further considerations concerning the second type go beyond the scope of the civil law of obligations and are therefore reserved for a future publication.

3.2. Areas of Application

As described, social bots operating on social media in the area of conversational commerce make use of the platform's possibilities. They either act using the options to give likes or recommendations or make direct contact with the users of the platform. For this purpose, they use the integrated messengers, such as Facebook Messenger or the WhatsApp service. This familiar communication environment and human-like presence prevents the actual human communication partners from making rational (purchasing) decisions. Direct communication leads users to react more positively to such offers [8,13]. In addition to communication with social bots in the "real world", using technical tools and applications, conversations are increasingly taking place entirely in digital worlds. Since the specific details, scope, and possibilities of a metaverse cannot be determined across the board, as it is currently still more of a vision than a legally secure space, we therefore look to the field of the gaming industry. The first step in the development towards a metaverse was certainly taken in the gaming industry. While in the field of gaming the virtual world offers narrowly limited possibilities determined by the developer, the metaverse is endless.

However, the first approaches have already been apparent for more than 20 years. In particular, the game "Second Life", which was launched globally in June 2003, can be considered an important milestone in metaverse research. The technical director of this game, Cory Ondrejka, described it as an online world created by its users. The users of this game navigate with virtual characters called avatars, create content, and interact with other users or bots [16]. Users can also personalize many details of the virtual environment in this game (e.g., buildings, artwork, clothing, or cars) and sell or rent them to other users within the game setting by paying a game currency [17–19]. However, this currency can be exchanged for U.S. dollars on exchange platforms provided by the game operator, so that a legally relevant purchase contract exists here.

The manipulation of users by social bots in this environment is reinforced by the human-like representation of social bots as avatars: in such a virtual world, the social bot not only adopts a human-like language but can also manipulate the user through virtual gestures and appearance in the virtual world and thus conclude a sales contract (for virtual or real objects). Communication on such platforms detaches from a purely technical level and takes the user into a fictitious real world. Avatars face each other in artificially created business premises or market stalls as buyers and sellers just like in a real sales situation. Communication in this virtual world seems even more authentic than communication via messenger services can ever be and is therefore even more manipulative. At this point, the morally problematic circumstances also become relevant on a legal level. Due to family circumstances, consumers (especially vulnerable groups, such as minors or the elderly) are more easily induced to close contracts and commit to promising consideration (whether money, objects, or data) that would not have been closed or promised in more businesslike circumstances. It is precisely in this situation that the particular danger of using social bots in the conversational commerce environment arises.

3.3. Interim Conclusion

The technical developments of the environments in which communicative social bots operate clearly show that the possibilities for manipulating users are increasing and will continue to increase. While communicative agents in the realm of social networks already appear human-like, using speech tools to manipulate users to recommend products or even make sales pitches, this is amplified in the visible virtual world where the user is fully embedded as an avatar. The use of an avatar amplifies the influence of anthropomorphic

appearance and signals emotion, empathy, and understanding beyond the human voice. Research has shown that physical-looking avatars attract users' attention more than other social bots [20]. This external, more anthropomorphized appearance reduces user rationality and facilitates deception [21,22]. This tendency will increase as metaverses evolve and move beyond mere gaming environments, including arranging services, signing brokerage contracts, or providing advocacy services in these virtual worlds [23].

4. Legal Issues

Legal issues related to conversational commerce using social (chat) bots are almost infinite and—as the aforementioned areas of application make clear—encompass all areas of law. These include criminal law issues of fraud, tax law issues of sales tax on sold virtual goods, intellectual property law issues of created components, property law issues of virtual goods, and in particular, purchase and data protection law issues when concluding a purchase as a result of a conversation with a social bot. However, further questions may arise beyond the scope of the mere conclusion of a contract. For example, due to the morally precarious and manipulative use, the legal area of unfair competition can be mentioned. Due to the fact that the objective of the laws on unfair competition is not primarily consumer protection, reference is made here to further sources: [24,25]. Since selling and advertising (digital) products is an essential aspect of conversational commerce, the focus in the following is on the regulations governing purchase law, which, however, also have an impact on data protection law aspects due to recent changes in the legal framework.

4.1. Commercialization of Data

One of the main aspects of conversational commerce is to accelerate trade and, accordingly, to conclude legally binding contracts rapidly and thus generate revenue. The principle of freedom of contract or the superior principle of private autonomy applies to these civil law contracts. Freedom of contract is explicitly recommended in the Principles of European Contract Law or Lando-Principles (PECL) [26]. The PECL are a non-legally binding collection of common contract law principles to which EU member states can refer when drafting legislation, parties can refer to when drafting contracts, and courts can refer to when interpreting the law. Although they are not legally binding, they provide a clear direction of practice for European member states. Germany has constitutionally enshrined this freedom of contract in Article 2 (1) of the German Basic Law (Grundgesetz-GG) [27–30]. It establishes the freedom to conclude and dissolve contracts within the framework of the civil law system [31]. Private autonomy complies with the constitutional concept of freedom of action but is assigned to civil law. According to this concept, individuals are supposed to be able to define their legal relationships according to their will and on their own responsibility [32,33]. The individual can claim to determine independently, without state interference, paternalism, or even coercion, how to adequately balance their conflicting interests [34].

"Private autonomy is necessarily limited and requires legal elaboration. Private law systems therefore consist of a sophisticated system of coordinated rules and organizational instruments [...]", according to the German Federal Constitutional Court (BVerfG) in its famous guarantee decision [32].

Limits are set in this regard not only by factual circumstances, such as a lack of resources but above all by simple law, which has a protective function in addition to its regulatory function. Civil law regulations in particular are based on the need for the protection of the contracting parties [35]. For example, the law considers minors to be particularly worthy of protection. They are legally incapacitated or have only limited legal capacity and have notably limited experience in business transactions, which is why German legislation has established special protective provisions in sections 104 et seq. of the German Civil Code (Bürgerliches Gesetzbuch, BGB). For their protection, the

legislator either prevents them from participating in business activities at all or only to a limited extent.

In general, the entire contract law is based on a superordinate concept of protection and, in particular as a result of European legislation, increasingly including consumer protection regulations (e.g., special regulations on the purchase of goods, personal credit transactions, transactions conducted outside business premises, etc.). This concept of consumer protection, based on European law, needs to be taken into account in any interpretation, including newly introduced standards in contract law. Looking at the civil law framework of the purchase contract law and thus at Section 433 of the BGB (in other European legal systems, however, corresponding norms can be found, cf. e.g., Art. 1582 Code Civil (FR), Art. 1445 Código Civil (ESP)), this legislative approach becomes clear in the recently implemented regulations on "payment with data". To ensure the highest possible level of consumer protection, the previous obligation to pay a purchase price in money as consideration for a (virtual) item is changed. The legislator permits—as part of the implementation of a European consumer protection regulation—the "payment with (personal) data".

4.1.1. Legislative Change: Law of Obligations of Data

The conventional purchase for money and its legal structure have been modified in some respects to comply with current requirements by the implementation of the Digital Services Directive (Dir. (EU) 2019/770) [36] and the Directive on the Sale of Goods (Dir. (EU) 2019/771) [37]. The Digital Services Directive (Dir. (EU) 2019/770) is intended to support the Digital Single Market Strategy for Europe, which holistically aims to remove the main barriers to the development of cross-border e-commerce in the European Union in order to unleash this potential. The Consumer Sales Directive (Dir. (EU) 2019/771) aims to ensure a balance between a high level of consumer protection and the promotion of business competitiveness, while respecting the principle of subsidiarity. This reformulation or alignment is accompanied by a change in the civil law provisions in the national civil codes. In Germany, in particular, Section 312 (1a) in conjunction with Section 327 (3) of the BGB has given legal substance to a practice that has been common for quite some time (and was permitted under the concept of "private autonomy"): the so-called payment with data. With these regulations, it is possible to pay in digital business transactions, i.e., for digital goods, both by paying money (Section 327 (1) of the BGB) and by providing personal data (Section 327 (3) of the BGB). This implies that the payment of a monetary amount is equivalent to the provision of personal data or the obligation to provide it. However, this only applies to the scope of services of "digital products", for which the law provides a legal definition in Section 327 (1) p. 1 of the BGB: the provision of digital content or digital services. This also includes digital games (as defined in recital 19 of the Digital Services Directive). Due to the proximity of gaming applications to other digital environments, such as the metaverse (especially since these are to be considered a preliminary stage in development), it can be assumed that transactions concluded by means of social bots in the metaverse are also covered by this definition.

4.1.2. Privacy Paradox

However, this development should also be considered critically: the business model of conversational commerce is also successful because social bots exhibit human behavior and address the user or consumer in a way that is convenient for them by occurring in the world of social networks. The same applies to a gaming environment or any other virtual world that serves as a marketplace. Especially in these business environments, users are more willing to provide their personal data, frequently in a situational and unreflective manner, due to the convenience aspect [38]. For example, email addresses are passed on in conversation, location data, or health data are shared without considering the further (data protection) consequences. Vulnerable groups, i.e., minors, the elderly or those who are not attentive enough are particularly susceptible to this unreflective

behavior. Particularly on social media platforms, personal data are shared despite the legal obligation of providing information, as consent is given without reading it. In some situations, user interfaces are deliberately designed (so-called dark patterns) so that users do not deactivate pre-activated consents (e.g., by checking consent boxes) (so-called default bias) [39]. Admittedly, there has been a recent increase in privacy awareness among digital content users. They also request a higher level of privacy in their respective online environments [40]. Nevertheless, these (supposedly critical) consumers are willing to provide the required personal data and also to consent to the processing of these data. This effect is reinforced further if a previous conversation conveys the perception that this is the right decision or that this is a free option. It is evident that the discrepancy between supposedly observed and actually practiced data protection is increasing, a process known as the "privacy paradox" [41–43]. The previously appreciated data sovereignty through personal choice is neglected when, from the consumer's perspective, disclosure is required to add additional applications or functionalities. Evidently, the willingness to provide data will increase further if the individuals concerned can no longer distinguish between the "real world" and the "fictitious world". If, as avatars in a perfectly simulated environment, they are seduced into providing data by the appearance and gestures of their interlocutors or in group dynamic processes, it will become increasingly difficult for individual users to resist such a request. The ability of users to be cautious will diminish with the degree of simulation, and the privacy paradox will become even more exacerbated in virtual worlds.

4.2. Legal Challenges: Privacy vs. Economic Good

Precisely such scenarios illustrate the existing discrepancy between the freedom of informational self-determination guaranteed by fundamental rights (recommendations of the PECL, implementation in Germany by Article 1 (1) in conjunction with Article 2 (1) of the GG) on the one hand and the situation-specific restricted freedom of decision on the other. Resistance to encroachments on data sovereignty and decision-making authority is limited, even in the case of responsible consumers—despite their better knowledge. In particular, due to the communicative impact of conversing with a social bot, measures to prevent such intrusions are usually abandoned quickly or not even considered. Therefore, consumers cannot always be expected reasonably weigh the right to their data and the value of the data they are disclosing. To make matters worse, it is currently not possible for consumers to (a) know the value of their data and (b) negotiate that value in a self-determined manner.

In addition to the implications for secure and sovereign use of their own data, the pressure on consumers' freedom of choice thus generated—and now widespread—may have not only pathological (e.g., internet/gambling addiction) but also financial implications [44,45].

The development of a virtual world and the communication with human-like social bots therein will add more scenarios and business models in the future, as the new law of obligations of data in the BGB equates the provision of data with a monetary payment (Section 327 para. 3 BGB). In such scenarios, the deceived person (especially as a member of a vulnerable group) may even be more likely to recklessly disclose their data and thus an essential part of their personality due to the supposed gratuitousness of the service, instead of perceiving the "true value" of their data and consciously using it as consideration.

4.2.1. Data Protection

In this "payment transaction", the legal act is subject to the conflict between the law of obligations, circumscribed by civil law, and data protection law. If the user discloses personal data, this information has to comply first and foremost with the requirements of data protection law, in particular the GDPR (General Data Protection Regulation) (regulations with similar provisions can also be found in other legal systems outside Europe. For an example of a legal comparison with data protection regulations in China, see [46]). Personal data is protected by the GDPR, cf. Art. 4 (1) GDPR. These initially refer to a natural person, the so-called "data subject". This refers without limitation to all information that is in any way related to the data subject, i.e., this term is to be understood very broadly in

principle [47]. The regulation refers to personal data used in context, such as identifying characteristics external characteristics or internal conditions, see [48,49]. This indicates—to anticipate the conclusion—that the data disclosed in the context of a sales conversation and ultimately as consideration for a digital product is personal data within the scope of the GDPR.

The operator or user of the social bot processes this data in a legally relevant manner. The term "processing" is also legally defined in the GDPR (cf. Art. 4 No. 2 GDPR and see [50]. In any case, in order to be able to appropriately accept the data provided, the data controller has to collect and arrange the data so that they can conduct a legally relevant processing of the data.

The processing of the data is generally prohibited according to the regulatory content of the GDPR, which is designed as a prohibition with a requirement of permission. An exception exists if there is a justifying circumstance. Since in the described case of the conclusion of a contract by way of conversational communication the data is consciously provided, the consent to the data processing, which is described in Art. 6 (1) p. 1 lit. a) GDPR, has to be taken into account. However, this consent has to be considered valid, as regulations on the validity of consent as an element of permission can be found in various places in the GDPR, therefore it is worth looking at Art. 4 No. 11; Art. 6 (1) p. 1 lit. a); and Art. 7 GDPR in conjunction with the recitals of the Directive to obtain a full idea of which conditions for the validity of consent have to be fulfilled regularly [51].

In our context, transparency (i.e., definiteness), informedness, and voluntariness are of particular importance. Art. 7 (2) p. 1 GDPR requires both design and content transparency. This means that the user who provides his data has to be informed about the fact of the processing but also about the scope of the processing [49]. The voluntary nature of consent has always been one of the central prerequisites for valid consent according to data protection law. At the same time, its interpretation is characterized by ambivalence: an excessively liberal understanding is accused of accepting a mere "fiction". However, if voluntariness is understood too restrictively, the ability to control informational self-determination is called into question [52]. The provision links to the definitional standard of Art. 4 No. 11 GDPR, which defines consent as a declaration that has to be given "voluntarily". For consent to be considered voluntary, the individual needs to have a free choice and be able to refuse or withdraw consent without suffering any disadvantages as a result. Finally, consent has to be given "in full knowledge of the facts."

Article 7 (4) GDPR clarifies that particularly strict requirements are to be placed on these effectiveness requirements, especially with regard to any consideration. The element described there is referred to as the prohibition of coupling. Coupling in data protection law occurs when the conclusion of a contract or the provision of a service is dependent on the data subject's consent to further collection or processing of their personal data, which is not necessary for the transaction [53]. Such a request typically serves to generate data sets that are suitable for promotional use. The prohibition of coupling is intended to protect the free and independent expression of the user's will when giving consent and thereby prevent the emergence of a factual compulsion to consent to data use [54,55]. Admittedly, this regulation does not contain an "absolute" prohibition of coupling—this would also contradict informational self-determination [56]. This coupling can be a strong indication of the involuntariness of consent ("utmost account shall be taken") but does not have to be (the literature is divided in this regard. Cf. [53,57,58]). Nevertheless, this is imprecise. However, a look at recital 43 makes it clear that "Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance." There are voices in the literature that argue that if the legislator had intended such an absolute wording, this should also be expressed in the text of the regulation [56]. Since this is not the case, this prohibition of

coupling should, however, be applied to a particularly stringent extent when assessing "voluntariness" within the meaning of Art. 4 No. 11; Art. 6; and Art. 7 of the GDPR.

4.2.2. Law of Obligations of Data

The aforementioned law of obligations of data, which the German Civil Code (BGB) has implemented, is based to a significant extent on the Digital Services Directive (Dir. (EU) 2019/770) and the Directive on the Sale of Goods (Dir. (EU) 2019/771). Considering the terminology and legal effects of a contract of purchase, it is doubtful whether we can really speak of payment with data. Thus, a payment transaction is generally understood to be a consideration within the framework of an exchange situation in the context of a mutual contract [59]. In German law of obligations, the term "Synallagma" (meaning reciprocity) is used to describe this mutual situation. In the context of payment with data, such reciprocity relationship is rejected by a large number of opinions in the legal literature [43,60]. Recitals 24 and 25 of the Digital Services Directive, in particular, are used as justification. These considerations are based on the opinion of the European Data Protection Supervisor [61], according to which, the possibility to pay with data in the meaning of a consideration should be avoided. Personal data should not be used to objectify and subjugate as a commodity, as this ultimately constitutes a direct interference with the fundamental rights of data subjects. Moreover, consumers are also not in a position to dispose of their personal data as if it were a commodity. After all, they lack the ability to even comprehend the respective value and significance attached to their data. The disposition of personal data should be governed exclusively by the regime of the GDPR, avoiding any confusion with private law regimes [61]. Accordingly, it would be sufficient for the provision of data if there was a causal link between the service and the payment with data, but a reciprocal relationship in the sense of a "synallagma" would not be required. However, the reservations expressed have so far been ignored—on the contrary, it can be assumed that there will be further business models that enable consideration by providing data.

A number of legal questions arise in this context, e.g., how "payment with data" is to be legally classified. On the one hand, the wording of the law explicitly permits the provision of data as consideration for the provision of digital products or goods with digital content, which equates the provision of personal data on an equal basis with the provision of monetary units (Section 327 (3) of the BGB). On the other hand, however, the connection between service and consideration in the conceivable scenarios is to be a legally different one than in the case of a monetary payment. How exactly to draw the distinction here leads to considerable legal uncertainty, which needs to be clarified as quickly as possible in order to ensure the best possible consumer protection.

Crucial is the question of private autonomy on the one hand and the protection of consumers with regard to their right to informational self-determination on the other. Here, a balance has to be struck between consumers' private autonomy with the possibility of paying with data (especially since data can also have a financial value) and the scope of protection of the GDPR, which also has an impact on private legal relationships. In this context, the aspect of the voluntary nature of consent according to data protection law, for instance, becomes the focus of consideration, since it may no longer be merely a matter of data processing "on occasion".

5. Discussion

A detailed examination of the requirements under contract law and also data protection law shows that it is rather difficult to reconcile the interest of contract law in an equivalent consideration for a digital good and the interest of data protection law in an informal, self-acting provision of personal data.

5.1. Existing Legal Approaches

According to Art. 4 No. 11, Art. 6, and Art. 7 GDPR, informal and explicit consent requires that the data subjects are aware of the actual consequences of the provision of data.

This aspect could be restricted in the area of "conversational commerce". The social bots used in this field of business are predestined by their humanity to exert a manipulative influence on the actual human interlocutor. In communication, individuals are pressured into disclosing certain personal data. Users are often not aware of the actual consequences. This problem is exacerbated when considering that consent also has to be given voluntarily. Precisely because of the manipulative influence on consumer behavior, users sometimes feel compelled to disclose the requested data and carelessly give their consent to data processing. However, this also eliminates the requirement that the legislator imposes on the voluntary nature of consent to data processing. Consent is voluntary if the data subject has a "real choice" whether or not to give consent [62]. In the area of disclosure of data as a result of communication with social bots, this real choice is considered highly doubtful due to perceived pressure. In addition, the GDPR provides for a prohibition of coupling, Art. 7 (4) GDPR. This provision requires that particular strict attention is paid to whether consent is voluntary. As a consideration, this is to be doubted already based on the interpretation of the regulation. These doubts are strengthened when considering the further circumstances in which the consent occurred.

However, the disclosure of data as a result of conversation with social bots is not just problematic on the level of data protection law. It is also problematic with regard to the newly introduced regulation that consumers can also fulfill their obligation arising from the purchase contract for digital goods by providing data (Section 312 (1a) in conjunction with Section 327 (3) BGB). Consumers who provide their personal data in this case are hardly aware-irrespective of the problem of valid consent within the meaning of the GDPR just described—of the value that these data (may) have for the other party. However, it is expected and supported by the current draft legislation [63] that the consumer should recognize this value of the data exactly. Any consent to share personal data should require a reflective and informed decision. However, such a "perception of value" needs to be objectively ascertainable so that users can build their own subjective opinions of the consequences. Consumers need to be sensitized to the value of their personal data and their right to informational self-determination needs to be strengthened.

Accordingly, consumers need to be able to realistically assess the value of their data, although a distinction has to be made here: a particular personal datum may be more valuable to the individual consumer than to others—it is always related to the context in which it is used. The profitable data market needs to be detached from the responsibility of the data-processing companies and subjected to effective competition in order to ensure the fairness intended by the legislator. Consumers ultimately affected need to be able to assess what value the personal data they provide (or sell) actually has in the context of its use. This can be achieved, for example, by setting up a so-called "data stock exchange". Here, a subjective opinion about the value of data in the context of conversational commerce could be objectified using a large-scale survey of various users of virtual worlds, and transparency about the objectified value of data in relation to such sales models could be established in the form of a digital twin. A corresponding research proposal is currently under review by the German Federal Ministry of Education and Research (BMBF) headed by the authors. Second, it is necessary to recognize the property of personal data as a commodity. A denial of this property, also with reference to the special influence resulting from the fundamental rights of the respective person, has simply been outdated by reality. Nevertheless, it should be recognized that these are not just any goods but goods whose transactions require special protection. An appropriate control system, comparable to that for other sensitive goods, needs to be put in place. The GDPR can be a key in this respect, but it needs to be complemented by appropriate technical, but also legal, instruments. It should be noted that the numerous references and recommendations on application interfaces already pose a particular challenge to consumers' frustration tolerance, so more innovative alternatives (e.g., linking to incentive systems, incentives) need to be tested for their appropriateness.

5.2. Legal Basis for Design, Certification, and Construction

New technical developments always entail new legal regulations. This applies all the more to developments, such as artificial intelligence (AI) or digital products. Social bots, as used in conversational commerce, are predominantly based on AI technology, as they build their conversations on the implemented algorithms and evolve through machine learning systems, thus improving the quality of the conversation. However, this improved quality poses a particular risk to specific consumer groups, making them especially vulnerable to premature contracting. Because of the particular risk posed by new technologies, European legislators have taken action and recently issued a number of regulations, recommendations, and directives. In addition to the aforementioned Digital Services Directive (Dir. (EU) 2019/770) and the Sale of Goods Directive (Dir. (EU) 2019/771), there exists, in particular, the draft AI Regulation (COM/2021/206 final) [64], the proposal for a Directive of the European Parliament and of the Council on liability for defective products (COM(2022) 495) [65] or Regulation (EU) 2017/2394 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws [66]. For example, the AI Regulation provides risk ratings for AI systems in terms of fundamental rights, security, and privacy, thus taking a risk-based approach. The riskier an AI-powered product is, the more restrictions it is subject to, up to and including an outright ban. This idea supports consumer protection by implementing the much-discussed buzzword of "privacy by design."

Even though this draft AI regulation has a different focus than the Digital Services Directive (Dir. (EU) 2019/770) and the Sale of Goods Directive (Dir. (EU) 2019/771), which are the basis for transposition into national law and thus for our considerations, the idea of privacy by design is helpful to shape consumer protection as well. Therefore, in the area of payment with data, the perception of value through the design of the business partner—and thus of the social bot—should be designed to protect consumers.

6. Conclusions

Our research has shown that the use of social bots in social media has increased significantly in recent years. This may be due to the various possibilities and designs of the platforms but also because the platforms are constantly evolving. The use of manipulative social bots that entice users of such platforms to purchase (virtual) items by way of conversational commerce exacerbates the legal problems. Communicative influence in the supposedly safe virtual world is assuming dimensions that many users—especially vulnerable user groups—can no longer keep track of.

This substantive problem is being exacerbated by a further legal development. As a result of the implementation of the Digital Services Directive and the Sales of Goods Directive, it is now legally permissible to require the provision of data for the purchase of digital products or services. This raises the problem of valid consent in terms of data protection law on the one hand, and the problem of the nature and value of the consideration in terms of contract law on the other. Furthermore, the value of data as an equivalent of a purchase consideration is unclear. The value varies—depending on whether one takes the perspective of the consumer or the platform operator.

To provide the necessary transparency, it is therefore necessary to inform the user what the value of personal data is. In order to determine this objectively, however, a large number of subjectively shaped circumstances have to be examined and placed in the broader context. As long as this transparency cannot be established, the legal implementation of these data obligation regulations can only be to the detriment of consumers who are worthy of protection. However, it is precisely because of this uncertainty that conversational commerce business models are becoming increasingly successful and consumers are being increasingly manipulated. Especially in supposedly safe environments, communication with virtual bots then leads to serious financial, but above all also personal, disadvantages. This is one of the reasons why developments should be approached with caution and circumspection.

Author Contributions: Conceptualization, formal analysis, and writing, D.G.-N. and S.M. in equal measure; supervision, D.G.-N. All authors have read and agreed to the published version of the manuscript.

Funding: The publication of this article was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation)—Project-ID 416228727—CRC 1410 and was funded by Chemnitz University of Technology and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation)—491193532.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rodriguez, S. Facebook Changes Company Name to Meta. 2021. Available online: https://www.cnbc.com/2021/10/28/facebook-changes-company-name-to-meta.html (accessed on 5 August 2022).
2. Weizenbaum, J. *Die Macht der Computer und die Ohnmacht der Vernunft*, 1st ed.; Suhrkamp: Berlin, Germany, 1978.
3. Micklitz, H.-W.; Namyslowska, M.; Jablonowska, A. §6 KI und Verbraucherrecht. In *Künstliche Intelligenz und Robotik*, 1st ed.; Ebers, M., Heinze, C., Krügel, T., Steinrötter, B., Eds.; C.H.Beck:: München, Germany, 2020; pp. 202–241.
4. Jülicher, T.; Röttgen, C. Bots im Kontext von Wirtschaftsrecht und Cybercrime. *Z. Zum Innov.-Tech. InTeR* **2018**, *1*, 15–19.
5. Ferrara, E.; Varol, O.; Davis, C.; Menczer, F.; Flammini, A. The rise of social bots. *Commun. ACM* **2016**, *59*, 96–104. [CrossRef]
6. Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. The socialbot network: When bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'11), Orlando, FL, USA, 5–9 December 2011.
7. Woolley, S.C.; Howards, P.N. Political Communication, Computational Propaganda, and Autonomous Agents. *Int. J. Commun.* **2016**, *10*, 4882–4890.
8. Kind, S.; Jetzke, T.; Weide, S.; Ehrenberg-Silies, S.; Bovenschulte, M. *Social Bots*; TAB-Horizon-Scanning Nr. 3; Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB): Berlin, Germany, 2017.
9. Guilbeault, D. Growing Bot Security: An Ecological View of Bot Agency. *Int. J. Commun.* **2016**, *10*, 5003–5021.
10. Murthy, D.; Powell, A.B.; Tinati, R.; Anstead, N.; Carr, L.; Halford, S.J.; Weal, M. Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital. *Int. J. Commun.* **2016**, *10*, 4952–4971.
11. Kollanyi, B. Where Do Bots Come From? An Analysis of Bot Codes Shared on GitHub. *Int. J. Commun.* **2016**, *10*, 4932–4951.
12. Dankert, K.; Dreyer, S. Social Bots—Grenzenloser Einfluss auf den Meinungsbildungsprozess? *Kommunikation und Recht (K&R)* **2017**, *2*, 73–78.
13. Spiegel. Zalando-Marke Manipulierte Likes. 2017. Available online: https://www.spiegel.de/netzwelt/web/zalando-marke-mint-berry-nutzte-like-bots-fuer-instagram-profil-a-1153302.html (accessed on 5 August 2022).
14. Spiegel. 470.000 Trump-Retweets kamen von russischen Bot-Accounts. 2018. Available online: https://www.spiegel.de/politik/ausland/donald-trump-erhielt-470-000-retweets-von-russischen-bot-accounts-a-1190130.html (accessed on 5 August 2022).
15. Lischka, K.; Stöcker, C. *Digitale Öffentlichkeit—Wie algorithmische Prozesse den gesellschaftlichen Diskus beeinflussen*; Bertelsmann Stiftung: Gütersloh, Germany, 2017. [CrossRef]
16. Ondrejka, C. Escaping the Gilded Cage: User Created Content and Building the Metaverse. *N. Y. Law Sch. Law Rev.* **2005**, *49*, 81–101.
17. Dietsch, D.R. Leistungen im Metaverse nach dem Urteil des BFH v. 18.11.2021—V R 38/19 zu Second Life. *Z. Für Gesamte Mehrwertsteuerrecht (MwStR)* **2022**, *10*, 378–383.
18. German Federal Fiscal Court (BFH), judgment of 18.11.2021—V R 38/19. *Z. Für Gesamte Mehrwertsteuerrecht (MwStR)* **2022**, *10*, 391–397.
19. Judgment of the Cologne Fiscal Court of 13.08.2019—8 K 1565/18. *Z. Für Gesamte Mehrwertsteuerrecht (MwStR* **2021**, *12*, 508–512.
20. Seo, Y.; Kim, M.; Jung, Y.; Lee, D. Avatar Face Recognition and Self-Presence. *Comput. Hum. Behav.* **2016**, *69*, 120–127. [CrossRef]
21. Epley, N.; Waytz, A.; Cacioppo, J.T. On Seeing Human: A Three-Factor Theory of Anthropomorphism. *Psychol. Rev.* **2007**, *114*, 864–886. [CrossRef] [PubMed]
22. Waytz, A.; Cacioppo, J.T.; Epley, N. Who Sees Human?: The Stability and Importance of Individual Differences in Anthropomorphism. *Perspect. Psychol. Sci.* **2010**, *5*, 219–232. [CrossRef]
23. FAZ. Roboter Sind nicht die Besseren Anwalte. 2022. Available online: https://www.faz.net/einspruch/einspruch-exklusiv-roboter-sind-nicht-die-besseren-anwaelte-18008817.html (accessed on 14 August 2022).
24. Supplier's Liability for Misleading Online Customer Ratings for Therapeutic Products. *GRUR Int.* **2021**, *70*, 189–193. [CrossRef]
25. Hartzog, W. Unfair and Deceptive Robots. *Md. Law Rev.* **2015**, *74*, 785–829.
26. Storme, M.E. Freedom of Contract: Mandatory and Non-Mandatory Rules in European Contract Law. *Juridica Int.* **2006**, 34–44. [CrossRef]
27. BVerfG, decision of 12. 11. 1958—2 BvL 4, 26, 40/56, 1, 7/57. *Entscheid. Des Bundesverfassungsgerichts (BVerfGE)* **1958**, *8*, 274–331.
28. BVerfG, decision of 16. 5. 1961—2 BvF 1/60. *Entscheid. Des Bundesverfassungsgerichts (BVerfGE)* **1961**, *12*, 341–353.

29. BVerfG, decision of 12.01.1967—1 BvR 335/63. *Entscheid. Des Bundesverfassungsgerichts (BVerfGE)* **1967**, *21*, 87–91.
30. Höfling, W. *Vertragsfreiheit: Eine grundrechtsdogmatische Studi*, 1st ed.; C.F.Müller: Heidelberg, Germany, 1991.
31. Di Fabio, U. GG Art. 2 Abs. 1. In *Grundgesetz-Kommentar, 97. EL*; Dürig, G., Herzog, R., Scholz, R., Eds.; C.H.Beck: München, Germany, 2022.
32. BVerfG, decision of 19.10.1993—1 BvR 567/89 u. a. *Entscheid. Des Bundesverfassungsgerichts (BVerfGE)* **1993**, *89*, 214–236.
33. Canaris, C.-W. Verstöße gegen das verfassungsrechtliche Übermaßverbot im Recht der Geschäftsfähigkeit und im Schadensersatzrecht. *Juristenzeitung (JZ)* **1987**, 993–1004. [CrossRef]
34. BVerfG, decision of 07.02.1990—1 BvR 26/84. *Entscheid. Des Bundesverfassungsgerichts (BVerfGE)* **1990**, *81*, 242–263.
35. Paulus, C.G.; Zenker, W. Grenzen der Privatautonomie. *Juristische Schulung (JuS)* **2001**, *41*, 1–9.
36. European Parliament and the Council. *Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects of Contract Law Relating to the Provision of Digital Content and Digital Services*; European Parliament and the Council: Brussels, Belgium, 2019.
37. European Parliament and the Council. *Directive (EU) 2019/771 of the European Parliament and of the Council of on Certain Aspects of the Sale of Goods Governed by Contract Law, Amending Regulation (EU) 2017/2394 and Directive 2009/22/EC and repealing Directive 1999/44/EC.*; European Parliament and the Council: Brussels, Belgium, 2019.
38. In Welchem Umfang Geben Sie Daten für die Nutzung von Online-Anwendungen frei? 2020. Available online: https://de.statista.com/statistik/daten/studie/1282708/umfrage/preisgabe-von-daten-im-internet-in-deutschland/ (accessed on 11 August 2022).
39. Samuelson, W.; Zeckhauser, R. Status quo bias in decision making. *J. Risk Uncertain.* **1988**, *1*, 7–59. [CrossRef]
40. Dix, A. Daten als Bezahlung—Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht. *Z. Für Eur. Priv. (ZeuP)* **2017**, *25*, 1–5.
41. Barnes, S.B. A privacy paradox: Social networking in the United States. *First Monday* **2006**, *11*. [CrossRef]
42. Norberg, P.A.; Horne, D.R.; Horne, D.A. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126. [CrossRef]
43. Schmitz, B.; Buschuew, E. (Be-)Zahlen mit Daten—Im Spannungsverhältnis zwischen Verbot mit Erlaubnisvorbehalt und Privatautonomie. *Multimedia und Recht (MMR)* **2022**, *25*, 171–176.
44. Kuss, D.J.; Griffiths, M.D. Online social networking and addiction: A review of the psychological literature. *Int. J. Environ. Res. Public Health* **2011**, *8*, 3528–3552. [CrossRef]
45. Widyanto, L.; McMurran, M. The psychometric properties of the internet addiction test. *Cyberpsychology Behav. Soc. Netw.* **2004**, *7*, 443–450. [CrossRef] [PubMed]
46. Meyer, S.; Albrecht, S.; Eibl, M.; Rey, G.D.; Schmied, J.; Tamboli, R.; Taubert, S.; Gesmann-Nuissl, D. Untying the Gordian Knot: Legally Compliant Sound Data Collection and Processing for TTS Systems in China. In Proceedings of the Privacy Symposium 2022, Venice, Italy, 5–7 April 2022.
47. ECJ Judgment of 20.12.2017—C-434/16. *Neue Jurist. Wochenschr. (NJW)* **2018**, *71*, 767–769.
48. OLG Cologne judgment dated 26.7.2019—20 U 75/18. *Z. Für Datenschutz (ZD)* **2019**, *10*, 462–463.
49. Klar, M.; Kühling, J. Art. 4 Nr. 1—personenbezogene Daten (inkl. Betroffene Personen). In *Datenschutz-Grundverordnung, BDSG Kommentar*, 3rd ed.; Kühling, J., Buchner, B., Eds.; C.H.Beck: München, Germany, 2020.
50. Klar, M.; Kühling, J. Art. 4 Nr. 2—Verarbeitung. In *Datenschutz-Grundverordnung, BDSG Kommentar*, 3rd ed.; Kühling, J., Buchner, B., Eds.; C.H.Beck: München, Germany, 2020.
51. Buchner, B.; Petri, T. Art. 6—Rechtmäßigkeit der Verarbeitung. In *Datenschutz-Grundverordnung, BDSG Kommentar*, 3rd ed.; Kühling, J., Buchner, B., Eds.; C.H.Beck: München, Germany, 2020.
52. Buchner, B.; Kühling, J. Art. 7—Bedingungen für die Einwilligung. In *Datenschutz-Grundverordnung, BDSG Kommentar*, 3rd ed.; Kühling, J., Buchner, B., Eds.; C.H.Beck: München, Germany, 2020.
53. Dammann, U. Erfolge und Defizite der EU-Datenschutzgrundverordnung. Erwarteter Fortschritt, Schwächen und überraschende Innovationen. *Zeitschrift für Datenschutz (ZD)* **2016**, *7*, 307–314.
54. Däubler, W. BDSG. In *Bundesdatenschutzgesetz*, 5th ed.; Däubler, W., Klebe, T., Wedde, P., Weichert, T., Eds.; Bund-Verlag: Frankfurt am Main, Germany, 2016.
55. German Bundestag. *Draft of a Law Regulating the Framework Conditions for Information and Communications Services*; BT-Drs. 13/7385, Federal Law Gazette of July 28; German Bundestag: Berlin, Germany, 1997; Volume I, p. 1870.
56. Heckmann, D.; Paschke, A. Art. 7 DSGVO—Bedingungen für die Einwilligung. In *Datenschutz-Grundverordnung, 2nd ed*; Ehmann, E., Selmayr, M., Eds.; C.H.Beck: München, Germany, 2018.
57. Albrecht, J.P. Das neue EU-Datenschutzrecht—von der Richtlinie zur Verordnung. Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog. *Computer und Recht (CR)* **2016**, *2*, 88–98. [CrossRef]
58. Gierschmann, S. Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt. *Zeitschrift für Datenschutz (ZD)* **2016**, *2*, 51–55.
59. Palandt. § 675 f. In *Bürgerliches Gesetzbuch*; C.H.Beck: München, Germany, 2022.
60. Klink-Straub, J. Do ut des data—Bezahlen mit Daten im digitalen Vertragsrecht. *Neue Jurist. Wochenschr. (NJW)* **2021**, *74*, 3217–3222.
61. EDPS Opinion 4/2017. Available online: https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_de.pdf (accessed on 11 August 2022).

62. Arning, M.A.; Rothkegel, T. Art 4. Begriffsbestimmungen. In *DSGVO–BDSG–TTDSG*, 4th ed.; Taeger, J., Gabel, D., Eds.; dtv: Frankfurt am Main, Germany, 2022.
63. European Commission. In *Draft Regulation of the European Parliament and of the Council on Harmonized Rules for Fair Access to and Use of Data*; (Data Act). COM(2022) 68 final, 2022/0047 (COD); European Commission: Brussels, Belgium, 2022.
64. European Parliament. *Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 Final*; European Parliament: Strasbourg, France, 2021.
65. European Parliament. *Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products, COM/2022/495 Final*; European Parliament: Strasbourg, France, 2022.
66. European Parliament. *Regulation (EU) 2017/2394 of the European Parliament and of the Council on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws*; European Parliament: Strasbourg, France, 2017.