SVRV Sachverständigenrat für Verbraucherfragen

Consumer Rights 2.0
Consumers in the Digital World
Potential Solutions

Introduction

These policy recommendations of the Advisory Council for Consumer Affairs, an advisory body for the Federal Ministry of Justice and Consumer Protection, deal with the problems of consumers when seeking and buying digital products and services. The recommendations focus on three fields: firstly on contract law governing the legal relationships between consumers and service providers, services offered on a permanent basis “as is”, pre-installed software, possible payment with consumer data, lack of clarity about the addressee of redress claims; secondly on the massive use of data claimed to be necessary to offering digital goods and services thereby leading to discrepancies between national and EU law with regard to the protection of consumer data and the regulation of algorithms; thirdly on effective legal protection and enforcement of consumer rights as well as the allocation and use of legal and technical competences.

Potential solutions as regards the law of digital services

Any potential solution must above all be geared to maintaining consumers’ autonomy in the digital world – during the contract negotiation phase, when a contract is being concluded, throughout the often long contract term as well as after the contract has been terminated. What is needed is a holistic approach which is not concerned with thinking inside legal boxes, but where sensible solutions are sought to real problems. It is clear that in such an analysis there will be a certain amount of intermixing of private law and public law, of substantive law (data protection law, the law of general terms and conditions, fair trading law and consumer contract law) and procedural law (individual and collective redress at national and international level).

A survey of the current situation reveals a number of serious problems which existing legislation cannot solve. Consumers face completely new forms of distribution. Providers link the sale of a product to the software needed to use it. These package offers (see no. 2 below) impede competition, that is if it is to be possible or desirable for providers to compete for the different parts. Transparency as regards the costs of such package offers is not required. Access is linked to the disclosure of personal data, which can only be processed with consumers’ consent. Consumers generally give their consent, regardless of the content and extent of the legal requirements, which have increased on account of the General Data Protection Regulation. The scope, extent and reach of such consent are not generally obvious and even if they are made transparent, they are hard to grasp in terms of their dimensions (see no. 3 below). Seventy-five years ago, it was believed that a review of incorporation of terms would be enough to get a grip on terms and conditions.[1] Considering the increased requirements being made of consent for data processing, history is now repeating itself.

Once consumers have paid for access to the Internet and digital services (with money or their data), question after question arises regarding the legal relationships they have entered into (see no. 1 below). Is there even a legal relationship? If so, what kind? Is it a contract or a legal relationship sui generis? In the case of online business, who is the contracting party (see no. 4 below)? Where is the contracting party domiciled? What is the subject matter of the contract (see no. 5 below) if it is not the transfer of ownership but only the use of a right?[2] What options are there for getting out of a contract, given that it may have a ten-year term? Is it technically possible to extract the consumer’s data from the data base of those enterprises which are processing these data? What rights does the consumer have vis-à-vis whom (see no. 6 below)? Against the seller/provider, who is often domiciled in another European country? How can those rights be asserted before a German court with the help of

[1] That is the solution Italy chose in 1942 when it undertook a major reform of its *Codice Civile*.
[2] Wendehorst *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, Report commissioned by the Advisory Council for Consumer Affairs at the Federal Ministry of Justice and Consumer Protection, October 2016.

dispute resolution forums? Who is controlling whether everything is above board in this digital world?

The model laid down in German law provides that consumer associations (see no. 7 and no. 8 below) are meant to handle those cases which consumers cannot manage themselves or by means of individual redress mechanisms. Consumer associations are supposed to be in charge of monitoring market practices and terms and conditions across all enterprises (and borders). They not only need the know-how to be able to apply legal provisions, but also to understand and categorise the technical processes which are behind the law of digital services. This policy approach is however not flanked by a class action which the consumer associations or individual consumers or lawyers acting on behalf of consumers could use to file for compensation when things go wrong. The most important and most widespread means of collective redress is a cease and desist order, a stop-order mechanism which is limited to banning illegal practices ex nunc, but which again leaves it, cum grano salis, to each individual consumer to know how and whether they are going to claim damages from an entrepreneur who is acting illegally. The cautious approaches to safeguarding collective consumer interests by administrative means adopted by the Federal Financial Supervisory Authority (BaFin) and the Federal Network Agency and in cross-border matters by official EU and OECD networks may signal that a paradigm shift is underway. Currently, though, no suitable complement to private-law consumer protection is available to consumer authorities with general competencies, especially when it comes to compensating affected consumers.[3]

The Advisory Council for Consumer Affairs (Advisory Council) sees an urgent need to adapt existing rules to the challenges of the digital world. Taking the holistic perspective – from establishing a legal relationship to leaving a digital legal relationship – the Advisory Council proposes the following 11 measures which cover four different types of digital legal relationship.[4] These measures are based on the principle of legal clarity and legal certainty for consumers, a sufficient but also necessary condition for maintaining the autonomy of consumers.[5]

The following list includes only those *key* demands which we feel need to be *urgently* actioned. It also includes policy-advisory considerations regarding implementation of the recommendations (see nos 9 to 11). The reasons as well as further details can be found in the relevant parts of this report, the third-party report commissioned by the Advisory Council and in the working papers to which reference is made.

1. Re information provided before establishing a legal relationship

Before establishing a legal relationship consumers are inundated with a wealth of information. Numerous statutory information and disclosure requirements are supposed to ensure that consumers become aware of the consequences under data protection law, that they become familiar with the subject matter of the contract and all the contractual rights and obligations under the terms and conditions, and that they realise the extent and scope of the end-user agreement. The Advisory Council claims that the rules on information provision

[3] For information on the activities of the CPC and ICPEN networks, see http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm and http://www.bmjv.de/DE/Verbraucherportal/Verbraucherinformation/ICPEN/ICPEN_node.html (both last retrieved 24 Nov. 2016). The networks mainly collate information (e.g. by means of “sweeps”) and attempt to solve problems through direct negotiations with enterprises.

[4] (1) Free digital services; (2) the role and function of online platforms in providing information, advice and mediation; (3) the deterritorialisation of consumption (consumers often do not know where the enterprise is domiciled; if it is domiciled abroad a complicated set of legal building blocks is available which has a great deal to offer legal science but very little to offer consumers); (4) the Internet of Things.

[5] See Rott, *Gutachten zur Erschließung und Bewertung offener Fragen und Herausforderungen der deutschen Verbraucherrechtspolitik im 21. Jahrhundert*, Report commissioned by the Advisory Council for Consumer Affairs at the Federal Ministry of Justice and Consumer Protection, November 2016.

need to be more clearly structured, they need to be reduced in number where possible and compliance ensured by means of sanctioning mechanisms.

Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail products and insurance-based investment products (PRIIPs) can serve as the model. The draft of an Ordinance on Promoting Transparency in the Telecommunications Market (TC Transparency Ordinance)[6] is also on the right track. Both the Regulation and the Ordinance stipulate that enterprises uniformly use the prescribed sample information documents. Administrative sanctions can be imposed against any breaches and the provision of erroneous information can lead to civil-law liability. Information on data protection, terms and conditions, and the end-user agreement should be provided in a standardised form which should be structured together with business and consumer associations. The extent and the linguistic comprehensibility of the information should be geared to readers' cognitive abilities. New designs should be employed.

Special focus must be placed on the market development that digital legal relationships are becoming permanent. This most definitely applies to "as is" services, which cover a broad spectrum of services ranging from Google to social networks. Consumer rights can only be upheld if additional safeguards are incorporated for the duration of the legal relationship and in the event of its termination. In view of the key nature of the information provided in the information documents, consumers must be given the option of withdrawing from the contract if changes are made. Their attention must be drawn to this fact. In cases where the contract is continued over a number of years with the consumer's agreement, that consumer should be given the option of requiring the entrepreneur to provide an update in which all the changes are summarised in an information document and made available to them.

The Advisory Council recommends: (1) Before the contract is concluded the entrepreneur must inform consumers on *one page* (500 words) about the relevant data protection requirements and about the terms and conditions. This obligation also applies when changes are made during the contract term. The entrepreneur must use typographic means to clearly highlight any subsequent changes on the one-page information document. The one-page information document and any updates are to be transmitted to consumers on a durable medium within the meaning of section 126b of the German Civil Code.[7] (2) Each change entitles the consumer to withdraw from the contract, to which reference must be made. (3) Sanctions must be imposed against breaches of the duty to include such a reference.

2. Re package offers (including services) when concluding a contract

Electronic devices which provide access to the Internet are generally offered in conjunction with pre-installed software. Consumers can only access the services available on the Internet after registering. There's no such thing as a free lunch, not even on the Internet. It is decisive for a functioning market economy for consumers to be aware of each individual cost item, such as the price of the electronic device, the price of the software and the "price" of the supposedly free service. The only objective of competition policy is to "unpack" the various services as far as possible. If such unpacking is not possible, consumers should at least be aware of the aforementioned costs for the various services. Where third-parties are paying for advertising, their contribution to the financing is to be clearly indicated.

The Advisory Council recommends introducing the following information requirements: (1) When consumers purchase an electronic device with pre-installed software, they must be (separately) informed about the price of the device and of the

[6] Ordinance for Promoting Transparency in the Telecommunications Market (TC Transparency Ordinance), Bundestag Printed Paper 18/1804 (Ordinance) of 15 June 2016.
[7] To be interpreted in line with CJEU judgment of 25 January 2015, *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG v Verein für Konsumenteninformation,* ECLI:EU:C:2017:38.

software. The case-law of the European Court of Justice, which requires the opposite, must be adjusted by way of an amendment to the EU Directive. (2) Where third parties are financing digital services this must be disclosed to consumers.

3. Re the scope and legal effects of consent

Article 4 no. 11 of the General Data Protection Regulation sets out the substantive requirements made for the consent which consumers must give. That consent does not necessarily have to be given expressly; consent by implication or acceptance of the terms and conditions suffices. In the latter case, the principles of transparency and separation under the provisions of Article 7(2) of the General Data Protection Regulation apply, going further than the existing law on general terms and conditions. The basic idea behind the rule in the General Data Protection Regulation should be transferred to the law on general terms and conditions. It is not apparent why greater requirements are made of consent to data processing than of consent to terms and conditions.

Information regarding the terms and conditions must be provided in a one-page information document; consumers can agree by ticking a box, as has previously been the case.[8]

The Advisory Council recommends: Data protection requirements and requirements as regards terms and conditions for consent are to be put on an equal footing. The principle of separation and transparency under Article 7(2) of the General Data Protection Regulation is to be transferred to the inclusion of terms and conditions. Only those rights and obligations which have been set out in a one-page document (see Recommendation no. 1) are binding.

4. Re determining the contracting partner

When consumers effect legal transactions via a platform, it is often difficult for them to recognise whether they have entered into a contractual relationship with the platform or not and what services the platform provides (free information, free or chargeable referral, or a free or chargeable advisory service). The added problem in the sharing economy is that consumers do not know whether the service providers are themselves a consumer or an entrepreneur. Solutions to these problems must take into account that platforms, in fact, already exercise control over the available information or could at least do so[9] and that proposals as regards the identity of service providers already exist. **The Advisory Council recommends: (1) In accordance with the proposal put forward by France, the platform operator must provide precise information about the service's function and the nature of the legal relationships; if the platform requires consumers to open a user account, this information is to be provided before the account is created. (2) In line with its actual function, the platform operator must take on a monitoring and control function; in the event of violating these obligations it will be liable vis-à-vis the consumer. (3) Following Denmark's example, a rule should be introduced in the sharing economy based on which anyone providing chargeable services via a platform is to be treated like an entrepreneur within the meaning of section 14 of the German Civil Code until the opposite is proven.**

5. Re the subject of the legal relationship

In the case of "as is" digital services, the legislature needs to clarify whether a contractual relationship or a quasi-contractual relationship with mutual rights and obligations has been established. Section 312 (1) of the German Civil Code, which requires nongratuitous

[8] Which they currently hardly ever do, see Domurath/Kosyra Domurath/Kosyra, *Verbraucherdatenschutz im Internet der Dinge*, Advisory Council of Consumer Affairs Working Paper Nr. 3; Schmechel, *Verbraucherdatenschutzrecht in der EU Grundverordnung*, Advisory Council of Consumer Affairs Working Paper Nr. 4.

[9] Adam/Micklitz *Information, Beratung und Vermittlung in der digitalen Welt, Rechtsfragen in Finanzen, Gesundheit und Handel*, Advisory Council for Consumer Affairs Working Paper Nr. 6.

performance in the case of a contract, is not only not compatible with EU law, it also does not reflect reality on the Internet. Consumers de facto pay for the digital service with their data.

The Advisory Council recommends making it clear that "as is" digital services constitute a legal relationship which is linked to rights and obligations. The reference to "nongratitious" in Section 312 (1) of the German civil Code should be deleted.

In the case of "as is" digital services, the provider is responsible for determining and altering the services to be provided. Since a legal relationship has been established, providers of "as is" services are subject to the exact same requirements as the providers of chargeable services. They must provide information in two information documents on the planned processing of data and the subject matter of the contract defined via terms and conditions, as well as about any changes made during the contract term.

The Advisory Council recommends extending the rule on information documents which must be transmitted before a legal relationship is established to include "as is" services.

One of the key challenges in the digital world is the "structural erosion of ownership".[10] Where a consumer purchases an electronic device, the property is without function until the device can be used together with software. The fundamental subject matter of the contract is thus the possibility of using the software installed on the electronic device. Its scope is defined under copyright law and given concrete form in the general terms and conditions. Users have long been formulating their demands under the heading of "fair use".

The Advisory Council recommends adding those clauses which allow the alteration or discontinuation of the provision of the digital service are typically found in digital contexts and, in particular, in end-user agreements to the black and grey list of prohibited clauses.[11]

Those questions which have arisen following the introduction of smart contracts have as yet not been solved. According to Gerald Spindler, a smart contract is a program for self-executing intelligent contracts.[12] A smart contract can be implemented directly using blockchain technology. It enables the conclusion of a contract to be monitored electronically. Factual reasons why, for example, an instalment has not been paid cannot be processed in the system.

The Advisory Council recommends stepping up research into the possible use of blockchain technology and the possible legal consequences of smart contracts.

Three different legal fields come together when the subject matter of the legal relationships is put in concrete form, although their legal effects are compatible only to a very limited degree: data protection law, copyright law, and civil and consumer law. The shifting of a great deal of legislative competence onto the EU has increased the preponderance of overlapping rules. The combination of data protection and copyright law determines the rules applicable in the digital economy and is superimposed on classic civil-law rules laid down in the German Civil Code. This development goes beyond consumer law and also affects B2C contracts. The process is in particular used in the financial sector as such (crypto currencies such as Bitcoin and Ethereum). However, first pilot projects using blockchains are also being run in the United States in other areas, such as the energy sector to sideline energy providers and to be able to effect energy trade more cheaply and directly via producers, for instance prosumers.[13] The problem becomes particularly virulent on account of the use of terms and

[10] The phrase was coined by Wendehorst *(op. cit., fn. 2).*
[11] Here, the Advisory Council follows the suggestions made by Wendehorst *(op. cit., fn. 2).*
[12] From Spindler's report *Regulierung durch Technik*, Report commission by the Advisory Council for Consumer Affairs, November 2016, which makes reference to the Etherum platform: https://www.ethereum.org/ (last retrieved 6 Sept. 2016).
[13] The Consumer Association North Rhine-Palatinate published a short study and a position paper: http://www.verbraucherzentrale.nrw/blockchain (last retrieved 24 Nov. 2016).

conditions which shape the services contract, influence the end-user agreement and indicate that there are points of contact with data protection law.[14]

The Advisory Council recommends systematically analysing the interplay between data protection law, copyright law and private/consumer law, because only a holistic perspective opens up the possibility of finding generalised rules which could provide insights and indicate the way forward for the digital world. From the consumer perspective, what is of the greatest importance in the short term is how terms and conditions can be brought into line with data protection and copyright law.

When merging previously distinct legal fields we have to re-consider whether and how counterperformance "in data" has an impact on the subject matter of the contract. The Advisory Council will take up the issue again in 2017.

Christiane Wendehorst[15] argues that non-compliance with the data protection safeguards under Article 25 of the General Data Protection Regulation on data protection and technology is to be regarded as a material defect within the meaning of section 434 of the German Civil Code. However, on account of its being geared to the functionality of the item purchased, the current definition of "material defect", Wendehorst claims, is not suited to defining *privacy by design* and *privacy by default* as criteria for contractual conformity. According to *Gerald Spindler*,[16] the basic IT security of products represents an essential protective and ancillary contractual obligation.

The Advisory Council recommends making it clear that privacy by design and privacy by default as well as basic IT security measures are part of the definition of the "use intended under the contract" within the meaning of section 434 (1) no. 1 of the German Civil Code.

6. Re the rights resulting from the legal relationship

Following the European Court of Justice's ruling in the *Google*-case, the right to data portability was introduced in Article 20 of the General Data Protection Regulation. The right aims at giving consumers the option of transferring their data to different service providers without technical or legal obstacles, for instance when moving their online profile from one social network to another. However, many questions have not yet been answered and need investigating in more depth: How similar do the networks need to be? How can data portability be effected technically? How are third-party rights to be safeguarded? How can we prevent potential costs being taken into account as a ground for exclusion? Also the question of how the right of data portability is dovetailed with contractual law has not yet been answered. Once again, data protection law and contractual law need to be synchronised. The wording of Article 20 of the General Data Protection Regulation does not clarify whether consumers can only assert the right if they wish to transfer data to another provider or whether they can also request that the data be returned if they do not plan to change providers. It is precisely the right of such transferral to the consumer which needs to be guaranteed.

The Advisory Council recommends making it clear that the right of data portability is also to be understood as a right of termination by means of which consumers can demand that their data be returned free of charge and deleted on a standard, machine-readable and interoperable medium.

The Internet of Things raises specific legal questions, firstly, concerning the digital content of the contract (interoperability, security, functionality, maintenance, updates, patches, privacy by design and by default) and, secondly, because of the discrepancy between the purchase contract and the embedded digital content, outsourced digital content, updates of digital

[14] Wendehorst *(op. cit., fn. 2)*
[15] Wendehorst *(op. cit., fn. 2)* p. 68 et seq.
[16] Spindler, *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären (op. cit., fn. 59),* in particular p. 12 et seqq.

content, digital services and data access, which are generally provided by third parties.[17] Both issues are a matter for intense debate. Account must here be taken of the fact that, from the consumer's perspective, the purchase contract and digital content provided by third parties are a self-contained entity, even though they are legally separate. Neither a unified model, nor an agency model, nor a guarantee model provides satisfactory solutions, because a options hold the dealer/seller liable for third-party services. The solution might be to introduce product warranty liability, which is primarily directed against the producer of a technical device who is liable vis-à-vis the consumer for providing third-party digital services or rather vis-à-vis the importer domiciled in the EU who imports the products into the EU.

The Advisory Council recommends counteracting the discrepancy between the purchase contract and digital content provided by third parties by introducing product warranty liability against the producer or against the importer into the EU who is also liable against the consumer as regards third-party digital services.

7. Re improving individual redress

The German Consumer Dispute Resolution Act implemented the Alternative Dispute Resolution (ADR) Directive and the Regulation on Consumer Online Dispute Resolution (ODR). The Act created a uniform framework for out-of-court dispute resolution both in the national and EU context. In view of the fact that it only entered into force on 1 April 2016, it is still too early for an evaluation.[18] Under section 43 (2) of the Act, the functioning of the arbitration board is to be evaluated by 31 December 2020. The Advisory Council believes it is key that the necessary precautions are taken now in order to be able to evaluate that information which comes together in the arbitration boards. This evaluation should distinguish between the type of legal conflict, the involved enterprises, the affected sectors and the products. Legal practice without law, as it were, is to be avoided, especially when the stored data are located elsewhere in Europe. Section 34 of the Consumer Dispute Resolution Act makes only very vague requirements which lead us to expect there will be a high degree of heterogeneity. In order to ensure legal certainty, , the information (and in particular the evaluation) produced in the arbitration boards needs to be published.Moreover, model contracts could contribute to finding digital contracts by means of arbitration. Business and consumer associations could together make a key contribution to increasing legal certainty.

The Advisory Council suggests that business and consumer associations should be involved in drafting model contracts for digital services which not only safeguard key elements of the content of such contracts but also link in to arbitration mechanisms.

The focus should be on new forms of private action. One such example are passenger rights. These are asserted with the help of commercially active intermediaries who realise consumer rights against payment of a percentage share.[19] They undeniably help many consumers to assert their rights. However, providers of such services only handle clear-cut cases, which leaves many consumers alone to deal with high-risk cases or refers them to publicly-funded consumer associations. Recently, some airlines have also taken to ruling out the option of assigning rights to intermediaries in their terms and conditions (e.g. Ryanair).

The Advisory Board suggests closely monitoring the effects of private, commercial mechanisms on redress backed by associations.

8. Re improving collective redress

At the interface between market practices and general terms and conditions, the German system of legal redress is based solely on a privately organised system of collective redress

[17] Wendehorst *(op. cit., fn. 2)*
[18] For an academic perspective, see the special issue of the magazine *Verbraucher und Recht* on the introduction of the Consumer Dispute Resolution Act, 2016.
[19] See Rott, Claims Management Services: An Alternative to ADR?, (2016), *European Review of Private Law,* p. 143–160.

by consumer associations and by industry associations. When it comes to monitoring terms and conditions, trade associations are de facto not an option. Although they do in fact have legal standing, in the 40 years since the introduction of the right of representative action (*Verbandsklage*), use has been made of this option only under very rare circumstances. For instance, a private action lies with the Federation of German Consumer Associations, which is funded by the Federal Government, and with those consumer associations which the *Länder* (federal sates) have given sufficient means to realise the right of representative action. In the field of fair trading law the trade associations handle around two thirds of cases, some of which at least concern consumer interests. The other third of cases are dealt with by the aforementioned consumer associations. Where there are points of contact with consumer data protection, consumer associations have been entitled, since 2016, to file a cease and desist order against enterprises. However, it is the often under-funded data protection authorities which are primarily responsible, although if the representative actions consumer associations have brought have made a key contribution to clarifying what the requirements for consent are under data protection law.

Despite the considerable legislative effort involved, cross-border representative action is hardly an option in practice. The questions of jurisdiction, applicable law and enforcement of a German judgment abroad or, vice versa, of a foreign decision in Germany are too difficult to answer. Existing EU legislation is not tailored to collective representative action and raises numerous legal questions for the clarification of which – in addition to the procedure under Regulation 2006/2004 on cross-border cooperation in consumer protection – the consumer associations are fairly unwilling to spend their scare resources. That is why consumer organisations in the EU Member States, with the help of the European umbrella association BEUC, identify cross-border practices against which the national associations can take coordinated action. Official cross-border networks cannot fill this gap, including on account of a lack of the necessary powers of intervention beyond a cease and desist order.

Given the current state of the political debate, it appears that one solution could be to expand the Federal Cartel Office. If this expansion were systematic, it would also lead to an expansion of the legal remedies available to the Federal Cartel Office to include the monitoring of advertising and of general terms and conditions. As opposed to the warning procedure and cease and desist claim, the Federal Cartel Office could, under section 32 (2a) of the Act against Restraints of Competition, order reimbursement of the benefits generated. This provision could be extended to include disadvantages which consumers suffer on account of impermissible business terms or unfair advertising. This would be entirely in the spirit of Article 8 of the proposal put forward by the European Commission for the reform of Regulation 2006/2004, which was supposed to serve as the benchmark for those minimum legal remedies which are to be available. These mechanisms for official redress in consumer protection are on no account supposed to replace the work of the consumer organisations, but they can be a sensible complement. However, it would have to be guaranteed that the digital agency exercises its powers to assert consumer rights independently and not based on economic or political considerations.

The Advisory Council agrees with the thrust of this year's Consumer Law Conference at which calls were made to add governmental monitoring (digital agency) to legal redress through associations. Based on the example set by the UK, an additional "super complaint" would be a conceivable option, a procedure in which associations could force the authorities to act by calling on a court if need be.

9. Re the suitable means for implementing the proposals

The proposed solutions touch on a number of statutory provisions. This is due to the different logic applied to the provisions of consumer protection law in the German Civil Code and efforts to synchronise data protection law and the law of general terms and conditions.

The Advisory Council advocates implementing the proposals in a manner which maintains the cohesion between the proposed rules. In view of the political sensitivities which go along with any interference with the German Civil Code,

amendments to the German Civil Code should be limited to what is absolutely essential. More specifically, a presumption rule for commercial activities would have to be incorporated into sections 13 and 14 of the German Civil Code and consent under data protection law brought into line with consent under the law of general terms and conditions.

10. Re the need for an evidence-based consumer policy

The Advisory Council commissioned an exploratory study into which data are available in consumer protection law and which are not.[20] Point VIII of the report enumerates a long list of gaps and makes concrete proposals for how these gaps are to be filled. There are hardly any politically robust data on consumer protection law, beyond needs- and project-based results. Data capture using parameters which are standardised across Europe driven forward by means of market watchdog projects promises to bring about improvements in the field of legal advisory services and legal representation provided by consumer associations in the *Länder*.

The Advisory Council recommends taking the necessary precautions in order to be able to shape an evidence-based consumer *law* policy.

11. Re the problem of competence

The proposed solutions will impact on the European Union's system of competencies. A distinction has to be drawn between directives which merely lay down a minimum level of harmonisation, such as Directive 93/13/EEC on unfair contract terms and Directive 1999/44/EC on the sale of consumer goods, and those directives aiming at full harmonisation. In particular, these include the E-Commerce Directive 2000/31/EC, Directive 2005/29/EC on unfair commercial practices and Directive 2011/83/EU on consumer rights. The definitions of "consumer" and "entrepreneur" are not fully harmonised.

France's attempts to adopt rules on information provision via platforms to the benefit of French consumers met with resistance from the European Commission, including on account of the fact that they touch on the area of application of the E-Commerce Directive and the Directive on unfair commercial practices. In light of this perspective, it is to be expected that the European Commission will also resist the following proposals:

- Packaging of offers (including services),
- Data protection information document,
- Determining the contractual partner,
- Control and monitoring function of platforms,
- Fair use of copyright-protected software programs and, possibly,
- Product warranty liability.

An answer should be found, by way of a legal opinion, to the following question: How precisely should the solution options be defined to avoid conflict with EU law as far as possible and to strengthen national autonomy of action?

The Advisory Council is convinced that Germany is free to take the political lead, possibly together with other Member States, and to call on the European Commission to act.

[20] Schmidt-Kessel, Larch, Erler, Heid, Grimm, *Explorationsstudie zu vorhandenen und fehlenden Daten im Verbraucherschutzrecht,* Report commissioned by the Advisory Council for Consumer Affairs, June 2016.

Potential solutions as regards regulating algorithms and big data

The use of algorithms and the prospects opened up by self-learning algorithms which update the source code raises questions of an altogether different dimension than when one takes the micro perspective of digital services. The issue here is not only one of maintaining the *autonomy* of consumers, which was to be the driver behind potential solutions as regards the law of digital services, but of *human dignity* in the age of artificial intelligence (AI). The political challenge is to answer the question of how to ensure that self-learning algorithms "act" in an ethically responsible manner. Can politics trust in business, in competition, in independent ethical behaviour on the part of those who are responsible for driving forward developments when it comes to AI? And, even more difficult, what will happen when AI takes on a life of its own? How can a self-controlling process be politically, ethically and legally mainstreamed?

The Advisory Council is convinced that political action is needed. The question is no longer whether political action is necessary, but what type of action that could be. A normative component needs to be incorporated into the algorithms. Under the lofty rubric of "human dignity" and the autonomy of human beings, the issue when it comes to consumer law would be compliance with the prohibition of discrimination, fair advertising, consumer data protection law and fair terms and conditions. Once this basic issue has been solved, we will find a serious of obstacles strewn across the path towards implementation of that goal which have their origin in the different rationality behind law and technology.[21]

1. Requirements under the Federal Data Protection Act

The 20th century legislative model requires that the government create a legal framework for technology within the context of which business itself develops its own technical standards. The manufacturers of technical products are obliged by the legislature to comply with the state of technology and the state of scientific knowledge. Standardisation bodies have a key role to play in this, since it is they which flesh out the framework provided by the legislature. In Germany, consumers are involved in the process of standardisation through the DIN Consumer Advisory Board. Once adopted, standards enjoy privileged status. Once the manufacturer has certified that its products meet these standards, either itself or via independent third-party institutions (e.g. TÜV), products can be put on the market without further governmental control. In the event of a claim, it is assumed that the manufacturer has met any legal obligations until the opposite is proven. The EU took over this model cum grano salis in the mid-1980s and applied it to technical regulation in Europe.

The German legislature took a different path in section 28b of the Federal Data Protection Act. In that provision it obliged loan agencies in particular to comply with scientifically-mathematically recognised standards and did not allow them to process especially sensitive data within the meaning of section 3 no. 9 of the Federal Data Protection Act. The provisions read as follows.

Federal Data Protection Act

Section 28b
Scoring

> *For the purpose of deciding on the creation, execution or termination of a contractual relationship with the data subject, a probability value for certain future action by the data subject may be calculated or used if*
>
> *1. the data used to calculate the probability value* ***are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognised mathematical-statistical procedure*** *[emphasis added],*

[21] Boer, *Legal Theory, Sources of Law, and the Semantic Web* (IOS Press, 2009).

2. in case the probability value is calculated by a credit inquiry agency, the conditions for transferring the data used under section 29 and in all other cases the conditions of admissible use of data under section 28 are met,

(...)

Section 3
Further definitions

(...)

"Special categories of personal data" means information on a person's racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life.

(...)

A case is pending before the Federal Constitutional Court against the German credit bureau Schufa concerning the question whether Schufa should have to disclose its scoring algorithms. The Federal Court of Justice negated just that.[22] The Federal Constitutional Court has not yet declared whether it will accept the constitutional complaint for decision. Germany's highest court has therefore not yet clarified which requirements are to be made of *a scientifically recognised mathematical-statistical procedure*. As regards sensitive data, section 28 (8) read in conjunction with subsection (6) of the Federal Data Protection Act at any rate sets limits when it comes to those criteria which may be applied when determining the score value. What has not yet been clarified is the extent to which the boundaries set in section 19 and section 20 of the General Equal Treatment Act have an impact on data capture. The US Equal Access Opportunity Act is clearer in that respect.[23] Monitoring compliance with statutory requirements is the responsibility of the data protection authorities. In view of the relatively low mathematical/technical complexity of scoring and the possibility of assigning responsibilities, competent monitoring ought to be safeguarded.

The Advisory Council notes that the existing rule in section 28b of the Federal Data Protection Act represents a useful starting point when it comes to regulating self-learning algorithms.

2. Requirements under the General Data Protection Regulation

Nevertheless, the provision in section 28b of the Federal Data Protection Act cannot be transferred to self-learning algorithms which *autonomously* update and change programs and network amongst themselves. The US Federal Trade Commission has taken up this problem and is investigating the need to increase and options for increasing transparency. Concrete results are not yet available.

The General Data Protection Regulation only addresses algorithms in the form of an individual entitlement to information and access. This regulatory technique is well-known, as it was used in Directive 2008/48/EC, where the obligation to issue credit responsibly is conceived merely as information.[24]

[22] See Federal Court of Justice, judgment of 28 January 2014, file no. VI ZR 156/13 (Gießen Regional Court, Gießen Local Court). A constitutional complaint has been filed against the Federal Court of Justice's judgment under file no. 1 BvR 756/14.
[23] See Metz, Scoring: New Legislation in Germany, (2012), *35 Journal of Consumer Policy*, p. 297–305
[24] See also Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 60, 28.2.2014, p. 34)

General Data Protection Regulation

Article 13
Information to be provided where personal data are collected from the data subject

(...)

*(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide **the data subject** [emphasis added] with the following further information necessary to ensure fair and transparent processing:*

(...)

*(f) the existence of **automated decision-making** [emphasis added], including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

(...)

Article 15
Right of access by the data subject

*(1) **The data subject** [emphasis added] shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*

(...)

*(h) the existence of **automated decision-making** [emphasis added], including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

(…)

Article 9
Processing of special categories of personal data

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(…)

However, unlike section 28b of the German Federal Data Protection Act, the General Data Protection Regulation does *not* make any legally binding requirements in respect of scoring, apart from in Recital 71, according to which "*the controller should use **appropriate mathematical or statistical** procedures for the profiling*". Unlike section 28b of the Federal Data Protection Act, requirements made of business under the Regulation are subject to a threefold restriction:

- the requirements made under Recital 71 ***should*** be complied with, not "are to be" or "must be" complied with,
- the procedures must be ***appropriate*** and not necessarily "***scientific***",
- the procedure should be ***mathematical or statistical*** and not ***mathematical-statistical***.

Normally, matters on which no political agreement can be reached are moved into the recitals. Ultimately, it is then up to the European Court of Justice to decide to what extent

enterprises must use mathematical-statistical procedures, what that means, what standards are to be applied to the mathematical or statistical procedures or what happens if enterprises do not comply with the requirements set in Recital 71. The concrete impact of this lowering of standards on the distribution of competencies and the scope retained by the German legislature in view of full harmonisation are discussed in the Report of the Advisory Council for Consumer Affairs "Consumer Rights 2.0 – Consumers in the Digital World" on which this summary is based. At least Article 9(1) of the General Data Protection Regulation, like the Federal Data Protection Act, prohibits the processing of sensitive data. The restrictions imposed on this prohibition will not be addressed here.

Opening up Recital 71 of the General Data Protection Regulation by, in a way, generally binding business in the same way as in section 28b of the Federal Data Protection Act cannot hide the fact that the primary addressees of the EU requirements are citizens who want to assert their right to information and access. Under the provision of Recital 63, that right "*should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software*". In light of the Federal Data Protection Act, it is obvious that the General Data Protection Regulation should be interpreted to mean that consumers should at least be informed about the basic assumption of the algorithm logic.[25] Depending on the outcome of the proceedings pending before the Federal Constitutional Court, the question of the relationship between EU law and the Basic Law could also be raised. However, even if it were possible to push through the German legal position across Europe – perhaps after it is underpinned by constitutional law – we are still left with requirements under EU law which do not go very far because they are entirely guided by the power of individuals and their ability to assert their rights.

There are considerable consequences as regards official legal redress. Profiling also has to be measured against the provisions of the General Data Protection Regulation on the admissibility of personal data processing. However, under Article 58(1a) of the Regulation, the data protection authorities are also tasked with monitoring and implementing application of the Directive. This concerns the principles applied to data processing as set out in Chapter II (Articles 5 to 11) of the Directive. It is not entirely clear whether the monitoring obligation also applies to the algorithms used, which are only referred to in regard to the rights of the data subject in Chapter III, and then only in the recitals, which have no legal force. Even if there were such an obligation, there are no uniform standards to which the authorities could gear their activities.

The Advisory Council notes that the rudimentary approaches to regulating algorithms set out in the General Data Protection Regulation are insufficient and fall below even the standard applied in section 28b of the Federal Data Protection Act.

3. Re the three possible options for a regulatory approach

The Advisory Council notes that there are theoretically three possible options for regulating this matter:

- ***proactive* (legality by design): the legislature could oblige enterprises to incorporate binding legal requirements into algorithm development;**
- ***reactive*: the legislature could restrict itself to obliging enterprises to comply with the law when developing algorithms (which actually goes without saying) and then focus on ex-post monitoring;**
- ***the happy medium*: the legislature could set a regulatory framework which combines binding governmental requirements with self-regulation.**

These options will be outlined and analysed in the following.

[25] Schmechel *(op. cit., fn. 8*), who cites Paal, *Beck'sche Kompakt Kommentare Datenschutz-Grundverordnung*, Paal/Pauly (eds), C.H.Beck Verlag 2017, margin no. 31 re Article 13 of the General Data Protection Regulation.

4. Re lack of transferability of technical regulation

If the legislature decides to take the *proactive* approach, in light of a century of experience, it would make sense to oblige industry to comply with the rules of technology. Inspiration can be sought in the field of product safety, where the following triad has become established both legislatively and constitutionally[26]: the generally recognised rules of technology; the state of the art; and the current state of science and technology.[27] It is obvious even at first glance that the German legislature has set the bar high in section 28b of the Federal Data Protection Act. Credit institutions must apply scientifically validated methods, that is not only those which are generally recognised and generally applied but those which stand up to being measured against scientifically validated standards. One of these three standards has taken root, namely the generally recognised rules of technology in the field of consumer goods and the current state of science and technology for medicinal products. Where products are subject to pre-market control exercised, government authorities are obliged to examine compatibility with binding government requirements when licensing products. Where no such pre-market controls are conducted, which – for good reason – is the case for all technical consumer goods, either the manufacturers themselves or authorised certification agencies establish whether the product meets the generally recognised rules of technology. The point of reference when conducting this assessment is generally the technical standards drawn up by German standardisation bodies or by EU standardisation institutions. Within the EU, self-certification or third-party certification guarantees manufacturers (or importers) access to the Single Market. However, manufacturers are not obliged to abide by technical standards. They can also apply other methods to ensure they are complying with the statutory safety requirements. Corrective measures are taken under labiality law. Where products give rise to damage despite standards being complied with, the courts can hold manufacturers liable in so far as this proves justified.

Transferring this approach to digitalisation, the legislature could set binding standards as regards the development of algorithms. One conceivable option would be, for example, to reformulate Article 9 of the General Data Protection Regulation (the prohibition of processing sensitive data and its exceptions) by reference to standards. As simple and convincing as such a rule may appear, it would at best solve questions concerning *automatic* programming by software agents, but not programming by *autonomous* software agents. Compliance with legal requirements can, therefore, only be guaranteed if they are not only incorporated into the source code but if they are also automatically taken into account whenever an autonomous change is made. To be able to do that, legal rules would have to be made compatible with the logic of the “code”, which only understands “yes” and “no” and cannot cope with vaguely formulated general legal clauses (e.g. “good faith” or “good morals”).

Across the world research teams are working on the options opened up by *legality by design*, albeit opinions differ as to their feasibility. Full compatibility of law and technology would mean reducing the law down to a “yes” or a “no” and incorporating legal reality into this “yes/no” logic. Legality by design would have to be shaped in such a way that all possible cases could be broken down into “yes/no”. It would also be worth thinking about incorporating an option into an algorithm in which a competent human being would have to be called in where uncertainty arises as to how to handle reality. This rationale is already incorporated in Article 22 (1) of the General Data Protection Regulation, which stipulates the rights of individuals to not be subject to an automated decision that has legal or other significant effect on the individual. It is clear that a great deal more research needs to be done here. It is currently still unclear whether such compatibility can actually be created by technical means.

---

[26] Federal Constitutional Court, order of 8 August 1978, file no. 2 BvL 8/77

[27] Marburger, *Die Regeln der Technik im Recht*, (Heymanns Verlag, 1982); Joerges/Falke/Micklitz/Brüggemeier, Die Sicherheit von Konsumgütern und die Entwicklung der Europäischen Gemeinschaft, (1988), *Schriftenreihe des Zentrums für Europäische Rechtspolitik,* Vol. 2, p. 523.

One special problem is the observable trend towards standard setting through general clauses. It is not least the adoption of the idea of social protection (the protection of the weakest under law) which has meant that the number of legal rules which bind the contracting parties to the principles of good faith, good morals and, less spectacularly, compliance with sensible and adequate rules has increased exponentially. The politically desired greater level of protection in private-law relationships contrasts with a loss of legal certainty. At any rate, the functional logic of algorithms could have positive consequences if the legislature were forced to differentiate more strictly than before between prohibitions which are absolute and those which are linked to sensible benchmarks. The development of black lists in fair trading law and the law of general terms and conditions, as well as the prohibitions of discrimination, which are absolute, bear witness to the possible developments which modern consumer legislation might undergo.[28] Even if it were possible to shift the focus of consumer law, we would still be left with many rules where the standards themselves leave considerable scope for interpretation on account of being formulated in the style of general clauses. As well as considerable doubts as to how complex legal realities can be processed, the criticism raised against the feasibility of implementing the law in algorithms is above all directed against the fact that it is hardly conceivable how general clauses are to be translated into a mathematical programming language.

The Advisory Council notes that it will not be possible to regulate algorithms using the means and technologies available for regulating industrial products.

5. Re the deficits and consequences of a reactive approach

In reality, control is currently being exercised purely *reactively*. Enterprises in the digital economy use the freedom afforded by liberal market economies to define algorithms independently. To what extent existing algorithms comply with the requirements of applicable consumer law and of anti-discrimination law, for example, is currently largely not subject to any ex post factum control of whatever shape or form. The reason is simple: Potential illegal results can only be identified by the respective addressee, and that only theoretically.

If one nevertheless wanted to advocate purely ex post controls, then there would be two prerequisites: (1) a digital agency which has the requisite technical and legal resources to be able to check whether the technology is compatible with the law and (2) an obligation to disclose the algorithm with all its autonomous modifications to a closed circle of government controllers.

The need for a digital agency entirely independently of the existence of a law of algorithms is addressed below. Letting things continue as they are and trusting in the self-responsibility of business and the self-regulatory power of competition without an obligation to register and without the obligation to disclose algorithms is at any rate not a serious option. In view of the current pace of social change, not only in the world of business, and its potential impacts on human beings, a purely reactive political approach is not an option.

The Advisory Council is convinced that sticking to "business as usual" is, politically speaking, not a serious option. The political realm is called to drop the option of ex post controls, the de facto approach, and to look for a regulation which does justice to the specific features of algorithms.

6. Re the limited possibilities of co-regulation

Attempts to link governmental and private regulation can be found along the spectrum between the two extremes of pre-market and post-market controls. All these considerations are, tacitly, based on the idea that it will be possible to get a handle on algorithms in the same was as it was possible to get a grip on the health and safety risks of consumer goods on the one hand and the machines and technology used in the production of goods on the other.

[28] The report commissioned by the Advisory Council and submitted by Rott *(op. cit., fn. 5)* adopts the same approach.

Gerald Spindler and Christian Thorun put forward a carefully elaborated proposal for co-regulation in a report they submitted to the *Selbstregulierung Informationswirtschaft e.V.*[29] The basic idea is that the (German) legislature should adopt framework legislation which sets out the minimum requirements as regards standard-setting (clear targets, participatory approach, decision-making, transparency, financing, standardisation organisation gets no copyright) as well as regarding enforcing those standards (binding commitment, monitoring, complaints mechanism, sanctions).[30] *Spindler/Thorun* do not themselves address co-regulation so as to pick up on the risks of automated and self-learning algorithms by software agents. They test their proposal in four areas: data protection; unfair competition; IT security; liability law and telemedia law with civil law and ancillary areas (in particular consumer protection law). Without calling the potential of co-regulation in regard to the four areas into question from the outset, scepticism as to how the model proposed by *Spindler/Thorun* could be transferred to the regulation of algorithms nevertheless predominates.

Even the EU's attempts to take advantage of the tried and tested system of governmental framework-setting and private standard-setting for services by and large miss the mark. One could raise the objection that there is as yet no European legislation available for standardising services;[31] in addition, when it comes to the digital world, it is hard to see why the digital economy should agree to set voluntary standards which could go beyond general guidelines or even codes of practice. The digital economy is dynamic; new business models are constantly evolving which generally involve algorithms. However, standard-setting is a rather more static process. Private standard-setting tends to codify the past, at any rate in so far as standards describe products. If one takes the example of health apps,[32] the question arises why companies providing these services should cooperate with each other, given that their main business purpose is to set themselves apart from potential competitors. The world of industrial products, by comparison, is reliant on standard-setting, because products would otherwise not be compatible with each other. This applies all the more since translating the law into the language of codes goes hand in hand with a very considerable level of investment in which there is above all a public interest.

The Advisory Council notes that the widely touted co-regulation in the form of government procedural framework-setting to regulate algorithms needs to be modified.

7. Re the need for an Algorithm Act

The Advisory Council sees an urgent need for political action in order to maintain consumers' autonomy and dignity in a digital world. The use of algorithms and the foreseeable developments as regards self-learning algorithms in a world which is networking more and more all affect deep-seated ethical principles of our communal life. It is up to politics in Germany to face up to this challenge. Leaving things up to business as in the past is not a serious option, considering that the most innovative sectors of the economy are not based in Germany. In an ideal world, the forum in which an adequate solution would be sought would be the European Union or, perhaps better still, the OECD and the United Nations. But action needs to be taken now.

The Advisory Council recommends

[29] See https://sriw.de/images/pdf/Spindler_Thorun-Eckpunkte_digitale_Ordnungspolitik_final.pdf (last retrieved 28 Nov. 2016), since published as Spindler/Thorun, Die Rolle der Ko-Regulierung in der Informationsgesellschaft: Handlungsempfehlung für eine digitale Ordnungspolitik, (2016), *MultiMedia und Recht Beilage*, Vol. 6, p.1–28.
[30] Busch's editorial in Towards a 'New Approach' in European Consumer Law: Standardisation and Co-Regulation in the Digital Single Market, (2016), *Journal of European Consumer and Market Law*, Vol. 5, p. 197–232, p. 197 takes the same approach.
[31] Van Leeuwen, *European Standardisation of Services and its Impact on Private Law Paradoxes of Convergence*, (Bloomsbury 2017)
[32] Adam/Micklitz *(op. cit., fn. 9)*

(1) putting in place the legal requirements to ensure that algorithms take account of the requirements of consumer law, data protection law, anti-discrimination law and digital security. In the case of algorithms which enter into direct contact with consumers, the underlying parameters need to be made transparent. Legal responsibility also needs to be assignable in the case of self-learning algorithms and applicable consumer protection regulations need to be complied with;

(2) ensuring that, based on standardised disclosure requirements, algorithms are disclosed to a circle of experts in the digital agency who carry out spot checks to see whether they are legally sound. Standardised software engineering procedures need to be developed to that end;

(3) that enterprises should also be called on to draw up a code of conduct on the use of personal data, AI systems and big data analysis.

8. Re the problem of competence

One conflict with the EU which is likely foreseeable is inherent in the General Data Protection Regulation with its objective of full harmonisation. The above-cited rights to information and access under Articles 9, 13 and 15 of the Directive do not justify a line of argument which the European Commission may put forward, namely that the Directive leaves no room for enacting national legislation on algorithms. Article 40 of the Directive and the concomitant Recital 72 go much further*:*

General Data Protection Regulation

Article 40
Codes of Conduct

(1) The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

(2) Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(…)

(5) Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

(…)

(9) The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

(…)

> *Recital 72: Profiling is subject to the rules of this Regulation governing the processing of personal data, such as* ***the legal grounds for processing or data protection principles*** *[emphasis added]****.*** *The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.*

In view of the general wording of Article 40 of the Directive and of Recital 72, combined with the fact that the Directive also covers mathematical and statistical profiling procedures, it does not seem so far-fetched that the Member States might have handed over competence for regulating legal matters relating to algorithms to the EU. That is, at any rate, true as regards the field of data protection. An Algorithm Act would, however, go way beyond formulating mere data protection principles. At its core, it has to address the economic and social order in a digital world, for which the EU does not have a mandate. The EU cannot interfere so far into the future of the Member States' economic and social order via the "backdoor" of data protection regulations and claim such wide-ranging competencies for itself.

Subject to more in-depth investigation, the Advisory Council believes that competence for drawing up an Algorithm Act has remained with the Member States, despite the objective of full harmonisation set out in the General Data Protection Regulation.

Potential solutions as regards the need for a digital agency

The law of digital services contains a *problem as regards legal redress*. In the world of software agents, of regulation through the code and big data, the primary problem is that competence is not concentrated in governmental agencies. The problems as regards legal redress when it comes to digital services can be countered by improving individual redress and restructuring the Federal Cartel Office into a consumer protection authority so as to strengthen collective redress. The Advisory Council has made proposals in this regard. In order to be able to tackle the really big challenges posed by the digital world, AI, autonomous algorithms, regulation through the code, big data and profiling, a further, decisive political step needs to be taken, namely the establishment of a digital agency which is sufficiently equipped so that it can be expanded into a digital competence centre where discourses are channelled, bundled and actioned.

The Federal Ministry of Justice and Consumer Protection and the Federal Ministry for Economic Affairs and Energy have adopted a clear position:[33]

> *Digital agency: Pooling consumer protection, competition and market rules. Economic and consumer policy need to keep pace both with digitalisation and with the dynamics of change. One important step is strong monitoring competence. The current fragmentation of competencies within supervisory authorities and above all the lack of competencies is of no help to any of the market players. When it comes to competition, market and consumer issues which concern digitalisation, we not only need a digital agenda but also a "digital agency". At least, though, the remits of existing authorities need to more precisely defined.*

The focus must be on expanding technical competence. Only such competence makes regulation and monitoring possible. Germany does not yet have such a competence centre. Technical and regulatory competence is spread across several different ministries. The following questions thus arise as regards the establishment of a digital agency:

- Should the digital agency be institutionally independent or part of an existing institution? Should the tasks arising in the digital world be assigned to the Federal Cartel Office or should an independent authority be created into which data protection would be integrated? Is bundling competencies in a single ministry an option (based on the example of the European Commission, which has a separate ministry dedicated to the digital world and largely independent of business and consumers)?
- What competencies should the digital agency have? Investigative and advisory or also regulatory? In the latter case, should it also be given the competence to issue bans, impose sanctions, set standards (like in the US) and claim collective damages (like in the UK)?
- What should cooperation with consumer organisations look like when it comes to legal redress? Should the digital agency pass the results of its own investigations on to consumer associations upon their request if the agency does not itself plan to take any further steps? Should there be any cooperation with the market watchdog for the digital world and if so what form should it take?
- How can it be guaranteed that the digital agency exercises its powers independently, possibly based on the example of the Federal Commissioner for Data Protection and Freedom of Information?

---

33 https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/Ma%C3%9Fnahmenprogramm_BMJV_BMWi.pdf?__blob=publicationFile&v=2 (last retrieved 24 Nov. 2016).

1. Re the need for immediate political action

The Netherlands, the United Kingdom and the United States have already acted. They have incorporated digital competence centres into their available governmental competition and consumer protection monitoring agencies. A series of reports on dealing with current or long-term problems published after consulting with business and consumer representatives bear witness to the growing political commitment of these bodies. Depending on how they are structured, these authorities propose governmental measures, recommend relevant measures to the government and parliament, or adopt measures themselves. Germany is lagging behind in this regard.

It is obvious that political action is necessary. The decision to establish a digital agency, in whatever form, cannot be postponed. No ministry, no authority likes to relinquish competence. But that is exactly what needs to happen so as to first be able to join all forces and then find out what deficits in terms of competence exist. Some fundamental re-thinking is needed and a new administrative legal culture needs to be developed in which it is understood that the current fragmentation of competencies across the ministries and the lack of legal instruments for effective regulation is a matter which urgently needs remedying.

The Advisory Council recommends establishing a digital agency in which previous competencies linked to digital services are pooled and expanded.

2. Re institutional embedding of the digital agency

From the point of view of consumer protection, there are three options as far as the institutional embedding or integration of a digital agency is concerned: the Federal Cartel Office, the Federal Commissioner for Data Protection and Freedom of Information, or a separate, new authority.

In the course of liberalising its markets, the EU has massively promoted the establishment of authorities – to control and monitor telecommunications, energy and finances and to control consumer law only when it comes to cross-border redress. Germany created the Federal Network Agency and the Federal Financial Supervisory Authority, two authorities which, under pressure from the EU, incorporated the law to protect collective consumer interests into their remit. Germany only acted to the extent that the EU imposed requirements. That is why the Federal Office for Motor Vehicles is under no obligation to protect consumer interests. Not even the scandal engulfing VW was sufficient to politically confirm a change to its remit. Should the German Government's plan, namely to assign the Federal Cartel Office competence for consumer protection, come to fruition, this would provide the option, for the first time, of firmly establishing official control of consumer protection law horizontally and not sectorally.

From the point of view of consumer protection, it is desirable that the entire complex of issues surrounding the digital economy should be assigned to the Federal Cartel Office. That would make it possible to tap into considerable synergies between the individual fields, competition law, commercial practices and consumer law. In that case it would have to be ensured that the Federal Cartel Office would be able to monitor unfair advertising and general terms and conditions as well as to pursue infringements of the General Equal Treatment Act.

The other options appear more problematical by comparison. Establishing a separate authority may be easier to achieve, because that way all the ministries have to relinquish competencies in equal measure and these are then bundled in the new agency. However, this option could prove dysfunctional, because there would be no links to anti-trust law, consumer law, and anti-discrimination law. The other option, blending data protection and digital tasks, appears even more difficult to implement politically, because the *Länder* are also involved in monitoring data protection. One option worth considering would be

upgrading the Federal Network Agency, though in view of its broad-based competence for electricity, gas, telecommunications, post and railways this appears problematical.

The Advisory Council is in favour of assigning the Federal Cartel Office those tasks which are being considered as part of the digital agency's remit. This will ensure that those legal issues which the digital economy raises and which go together are not pulled apart on extraneous grounds.

3. Re the tasks and competencies of the digital agency

Assigning these tasks to the Federal Cartel Office would ensure that the available monitoring and control mechanisms could also be available to the digital economy. In the first instance that would mean redress mechanisms, to which the list of proposals for the reformed Regulation 2006/2004 would need to be added.

Competence for those tasks which are upstream of legal redress has not yet been assigned. The digital agency must be given the possibility of investigating relevant sub-issues itself, of financing third-party research, drawing up proposals, discussing these with the involved sectors of the economy and consumers, drawing up codes of conduct and introducing concrete measures into the legislative process.

The Advisory Council recommends assigning all the necessary tasks to the digital agency and guaranteeing it the necessary resources so that it is in a position to proactively investigate technical and legal issues raised in the digital economy, to draw up proposals, discuss these in the public domain, develop codes of conduct with business and consumers, and to develop recommendations and proposal for the legislature.

4. Re the problem of competence

The Member States are *in principle* free to organise and shape legal redress as they see fit. That goes both for the question of whether enforcement of consumer law is to be placed in the hands of associations and the extent and reach of the competencies. But the scope for action is not unlimited. Legal redress must be based on the principle of effectiveness and equivalence developed by the European Court of Justice. The diverse EU Directives and EU Regulations set institutional and procedural requirements which the Member States must comply with in their implementation.

More specifically, amalgamating the government agencies involved in regulating sectoral markets raises a problem which has now reached the European Court of Justice: EU law obliges the Member States to establish independent agencies to control regulated markets (telecommunications, energy, finance and cross-border consumer protection). The precise meaning of the term "independent" - as well as the extent to which the independence required under the EU Regulations and EU Directives could be endangered as a consequence of authorities being amalgamated or tasks being merged – is unclear and will be based entirely on how that agency is institutionally embedded.

The Advisory Council recommends commissioning a legal expert opinion which addresses the question of the merging of German authorities to the extent that these are also required to implement tasks for which EU law sets legally binding institutional and procedural requirements.

Berlin, December 2016

SVRV Sachverständigenrat für Verbraucherfragen