The functionality of data protection in a digitizing society – a systemic view of control and trust

Stefan Brink, Clarissa Henning

> *Billions have no idea how a computer works, let alone algorithms. How they can be manipulated, what is manipulated, they stare at pixels and trust, which is actually touching. It makes you so angry, so angry that you get the feeling on the net that everything depends on your own stupid opinion.*
> Marc Bauer: The Blow-Up Regime

Our society now functions digitally, yet we still cling to ideas of system trust and control that date back to analogue times and are increasingly proving to be an illusion. Why do we cling to a trust that has become a relic, in the hope that digitality, controlled by algorithm-based decisions, can be made controllable?

Trust. A value that is a decisive stabilizing factor in a liberal democratic society. People trust that others will adhere to unspoken but culturally anchored norms and thus enable regulated social interaction. We trust that institutions, companies and politicians will abide by the law. If not, then we trust that we can demand it. Trust reduces the complexity of the world, as we do not know everything, cannot (and do not want to) control everything, but trust and can trust that things are as they appear to us, that they function as we expect them to, that they are aligned with the norms we have learned. Trust makes the world controllable and calculable for the individual and creates security. However, the question arises as to whether trust in a society that now functions digitally is not rather the clinging to the illusion of a system that now follows completely different laws that we no longer know or can even comprehend. If we follow Marc Bauer's description of the situation, we have to ask ourselves the question: Are we holding on to a trust that has become a relic, in the hope that digitality, controlled by algorithm-based decisions, can already be made just as controllable?

In order to approach the value of trust in the digitalized society, it should first be noted that the question raised cannot be answered with a clear "yes" or "no". Even at the micro level of the European social system, it is clear that self-determination, privacy and co-determination are still of great importance for the individual sense of freedom of digital citizens. However, as the much-cited and persistent privacy paradox[1] attests, the behaviour of users in the digital society deviates massively from this sense of values. While at the time of the planned census in 1983, the disclosure and permanent storage of personal data such as "information on family and civil partnership, living situation, school and studies, employment, profession and training, childcare"[2] led to storms of protest among the population, citizens today apparently voluntarily disclose a much larger amount of private information to a much larger audience - the world of the Internet. Despite the (more or less existing) knowledge that data is used for countless purposes, most of which remain opaque, and that one paves the way for the manipulation of oneself, trust in the democratic system (macro level of society) seems to contain and silence possible concerns about a society- and culture-dominating process such as digitization. If there was a threat to citizens, the prevailing belief seems to be that political and legislative institutions (meso level) would intervene and regulate digital freedom with a view to the ideal - the macro level - of society. But they would! Freedom is taken, must be taken, in order to maintain freedom. We will return to this supposed contradiction later on.

First, we will look at how trust in the system is responded to within the system, so that the system changes brought about by digitalization do not negatively affect the norms and values at the macro level - or rather: even support them. A new subsystem is created that is to be understood as a reaction to the changes in the environment and is itself an expression of the new challenges or needs that have arisen. According to Niklas Luhmann, "*each* subsystem reconstructs the comprehensive system to which it belongs and which it participates in, through its own (subsystem-specific) *difference between system and environment*. Through system differentiation, the sys-

1 To cite one of the most recent study reports on the topic, see for example Sabine Trepte, Philipp K. Masur, 'Privacy Attitudes, Perceptions, and Behaviors of the German Population.' Research Report (2017) Online: https://www.forum-privatheit.de/wp-content/uploads/Trepte_Masur_2017_Research_Report_Hohenheim.pdf.

2 'Census ruling of 1983 and its significance.' (2023) Online: https://www.juraforum.de/lexikon/volkszaehlungsurteil.

tem multiplies itself in itself, so to speak, through ever new distinctions between systems and environments within the system."[3] What does this mean for the outlined system influence through digitalization? The trust vacuum created by digitalization requires an answer at the meso level. In order to concretize this and build a bridge between the theoretical consideration of system-immanent changes and data protection, it is necessary at this point to trace this systemic change in concrete terms:

It may seem surprising at first that Europe's first law on data protection was passed in the state of Hesse in 1970 - before the development that today bears the name "digitization" was foreseeable. This is because it was only as a result of the aforementioned census that the so-called census ruling of the Federal Constitutional Court in 1983 established in black and white what had long been an inherent systemic need: "Under the modern conditions of data processing, the free development of personality presupposes the protection of individuals against the unlimited collection, storage, use and disclosure of their personal data. This protection is therefore covered by the fundamental right of Art. 2 para. 1 in conjunction with Art. 1 para. 1 GG. In this respect, the fundamental right guarantees the right of the individual to determine the disclosure and use of his or her personal data."[4]

This led to the development of the right to informational self-determination as a good protected by the Basic Law, which in turn led to a series of "causal chains". As Luhmann shows, the differentiation within a subsystem leads to further operations, for example the emergence of another subsystem, which at the same time always has an effect on the overall system and results in new changes or differentiations. A subsystem can never exist independently of the others (for Luhmann, the environment). This also explains why the manifestation of a change or a need always emerges from the system itself and was therefore already present in the system long beforehand. The entry into force of the GDPR in 2016, which has been in force throughout the EU since 25.05.2018, represents a further differentiation, which in turn was only possible in an exceptional historical situation, namely the social and political reality caused by Edward Snowden's revelations.

3 Niklas Luhmann, *Die Gesellschaft der Gesellschaft* (11th edn. Suhrkamp 2021) 598 (italics in orig.).

4 BVerfGE 65, 1; Online: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html.

The GDPR assigned new functions to the state data protection authorities and the Federal Commissioner for Data Protection, which have now become tangible for all other subsystems of society for the first time: Advice - control - sanction. The state data protection authorities and the Federal Commissioner joined forces to form the Data Protection Conference (DSK) in order to exchange information, but the data protection authorities are still organized on a federal level - there is therefore no single opinion on the correct handling of the right to informational self-determination in its many different application contexts, and of course no uniform interpretation of the regulation throughout Europe. As a result, the "data protection" system is in a constant exchange with itself and is becoming increasingly differentiated. As algorithm-driven technologies permeate all areas of society, changing and shaping them and thus posing a direct threat to the individual, data protection in its manifestation through the data protection authorities also influences all areas of society in order to protect the fundamental right to informational self-determination, which is syntagmatically linked to digitalization. Data protection is the system's reaction to the vacuum of trust described above in order to fill this vacuum and thus redeem the individual's trust in the social system.

However, Luhmann also states: "Society has no address. Nor is it an organization with which one could communicate."[5] Rather, society communicates with itself and about itself in the self-referential form of its subsystems - data protection is one of them. Data protection is making its presence felt with its new function of sanction, making it impossible for political and economic forces to ignore it. The possibility of sanctioning responsible data processors with up to four percent of their worldwide annual turnover (cf. Art. 83 GDPR) expresses in figures the importance that the European GDPR attaches to safeguarding informational self-determination in terms of system standards. However, the data protection authorities are not only focusing on data controllers. A new, legally stipulated task is to inform and advise citizens so that they do not just stare at pixels and trust that they will not be exploited and manipulated (if they are aware of this danger at all), but can literally take their informational self-determination into their own hands and thus preserve their autonomy. However, it is also a fact that the causal series described by Luhmann, which an event, a change, triggers, leads to the fact that not only the triggering (sub-)system

5 Niklas Luhmann, *Die Gesellschaft der Gesellschaft* (11th edn. Suhrkamp 2021) 866.

becomes increasingly differentiated, but also the systems interacting with it, which "[...] trigger completely different causal series due to a change in the *environment* of these systems. And this even though it is the *same* event for all systems! This results in an enormous dynamization, an almost explosive reaction pressure, against which the individual subsystems can only protect themselves by building up thresholds of indifference. Differentiation therefore inevitably results in: an increase in dependency and independence at the same time under specification and systemic control of the aspects in which one is dependent or independent."[6]

Data protection is a reaction to a system in which the increasing collection and processing of data by algorithmic applications in turn creates more and more intransparency of the digitized system for the individual and the trust of users is rewarded with control. As a result of the increasing collection and processing of data, which data protection is supposed to protect against, each individual is actually becoming the regrettably powerless user that Marc Bauer is so angry about in the opening quote. Users are becoming more and more transparent, while the system of digitalization and its computing operations is becoming less and less transparent. This also reduces the complexity of the world, but precisely the opposite of what is being sought: Control (of citizens) instead of trust (in digitalization).

Algorithmic calculations and the benefits derived from the calculations influence the overall system at the macro level. The fundamental values to which all system-inherent processes and subsystems are aligned are thus undermined. However, the system also reacts to this by countering control with control. This is the driving force behind the GDPR and its guiding principle. As a consequence, one of the core functions of the data protection authorities is therefore to monitor data controllers. However, this control works differently to the control of digitality. The control of data protection authorities is based on the fundamental values of its environment. And thus on trust.

To illustrate this, let's take a concrete example from everyday official practice: digital contact tracing during the pandemic. A health crisis situation affects the entire system and has a serious impact on its functions. Here too, the subsystems react in very different ways to deal with the crisis. And especially through such a serious event as a pandemic, in the light of the systemic reaction to it, the nature of this system and its laws are reflected and checked for correctness. This was also reflected in the fact

6 Ibid, 599 (italics in orig.).

that digital applications were seen as the saviour for restoring the normal state of the overall system or at least paving the way for it. One building block in this emergency plan should be smartphone applications. This digital approach should enable contacts to be documented and the risk of a possible infection to be tracked by means of a subsequent comparison so that protective and preventive measures can be initiated and spread if necessary. The Corona Warning App (CWA) was an initial digital tool in this regard, giving individuals the responsibility to respond to the new challenges posed by the pandemic situation with the support of a digital solution. The CWA dispenses with the centralized collection and storage of user data, but it is up to the user to compare the data stored locally in the app with infection reports, which must also be made voluntarily and in a self-determined manner via the app, and to derive appropriate actions from them if necessary. When the impression arose in the political arena that this was not providing the hoped-for benefits, criticism of the CWA's data protection friendliness was voiced - which, however, ran counter to securing the systemic "normal state". A step was to be taken away from trust in and responsibility for the individual towards more control by the state and transparency for the individual. Data protection responded to this once again, and the Luca app for contact tracing began its triumphal march. The Luca app is not an anonymized contact tracing service. It allows contact information to be saved in the app so that it can be used to "log in" to events. However, the contact details are stored in encrypted form with the app provider and the health authorities can access the data if an infection is reported. The personal data is encrypted for all other accessing parties (e.g. for the event organizer). The health authorities can only read the data if the organizer provides it and it is decrypted. This small example illustrates how data protection was able to fulfil its system-stabilizing function as well as temporarily changing system requirements without losing sight of the normal state of the system.

Nevertheless, there were opposing calls from the online community asking whether the data protection authority had not checked the source code as part of its control function. And it is precisely at this point that the difference in the concept of control, according to which the various subsystems function, can be illustrated: The criticism demands that the data protection authorities must understand the source code - i.e. the algorithmic instructions for action in machine-readable form - in order to prevent any potential danger to users. This would correspond to the control concept of digitality, which reads citizens' thoughts in order to be able to influence the

social system. The control concept of data protection is different and therefore also the task of the data protection authorities. It is not the algorithms that are being monitored here, but those responsible for the algorithms, because it is not the algorithms that dictate further actions resulting from the calculations, but those responsible for data collection and evaluation. The data processors must account for the legal basis on which they base the data processing, they must submit a data protection impact assessment, demonstrate suitable technical and organizational measures to ensure data security and submit a privacy policy. De facto, this means that it is the statements made by the controller and not the source code itself that are monitored. This may seem problematic, as the user often does not even know what calculations the algorithm used performs. Nevertheless, the GDPR stipulates that the controller must be accountable (see Art. 5 para. 2 GDPR), even if they may not be able to bear the responsibility. This shifts the risk from the manufacturer, provider or programmer of the algorithmic application to the controller as the person who uses the digital application.

The concept of control, which is reflected here, closes the circle to the importance of trust: data protection is based on the citizens' ability to handle digital applications and use them responsibly (in the sense of the GDPR). In addition, the technologies used are not checked directly in the first step, but rather the statements and presentation of the controller are relied upon.

This approach to control and responsibility will not change by law in the near future. With the emergence of the data protection subsystem, the overall system has reacted to the changes brought about by digitalization and developed it from within - with the aim of preserving freedom at the micro level by controlling freedoms at the meso level. Nevertheless, a system managed by algorithms follows completely different system-constituting laws than the original system.

From the considerations outlined here, it follows that the system-immanent dangers that imperceptibly emanate from algorithm-based influences in all system areas must not be thought of at the micro or meso level of society - just like data protection in interaction with this: "The realization of functional differentiation as the primary form of social differentiation profoundly changes the environmental conditions of the systems, both of

the overall system of society and its subsystems."[7] The direction in which this profound change will take is to be expected.

7 Ibid, 789.