When Ethics demands the already Present – How Ethics undermines effective data protection in the case of the Corona-Warn-App in Germany

Rainer Rehak

Introduction and Background

Since spring 2020 the discussion on how to contain the global SARS-CoV-2 pandemic has revolved around many medical and non-medical interventions. One of the epidemiological key characteristics of the current Corona virus is the fact that an infected person usually becomes infectious some time, even days, before the onset of recognizable symptoms. Therefore, apart from information campaigns, mask mandates or physical distancing rules to prevent direct infection, the use of technical tools to interrupt subsequent infections had been widely discussed in 2020 and also practically put in place later in many countries from Singapore to Germany. In previous decades contact tracing had been carried out manually by health authority employees, for example by interviewing infected persons for past contact events and then subsequently warning or quarantining the involved contacts, e.g. via telephone. This tedious work, so it was envisioned recently, could be greatly accelerated through the use of new digital technologies. Especially in Germany the so-called "Corona-Warn-App" (CWA) for pseudonymous digital contact tracing became a political centerpiece for combating corona.[1] Digital contact tracing apps are supposed

1 "The federal government wants to use the [corona warn app] to better identify corona virus infection chains and ensure that the spread of coronavirus does not surge again after relaxing corona restrictions" (Beer 2020) or "A key element in the fight against any pandemic is to interrupt the chains of infection. The Corona-Warn-App can make an important contribution to this and thereby support the health authorities in tracing contacts" (RKI 2021).

to automatically record all contact events of their users and thus make it possible to quickly and retrospectively warn them immediately after one of the contacts has been tested positive for Corona. Users at risk can then self-quarantine.

In some countries, such as China or South Korea, contact tracing is done using many other sources of information and data categories such as mobile phone location data, credit card data or travel information, but this article only deals with direct contact tracing by mobile apps.

Even with the basic functionality of app-based contact tracing in mind, there are several degrees of freedom concerning the concrete purpose (e.g. only interrupting infection chains or also collecting contact data for later research, handling group events or enabling vaccine passports) or technical design details (e.g. centralized as in PEPP-PT 2020 or decentralized approaches as in DP3T 2020).[2] Therefore, meaningful analyses of ethical, individual and societal implications should also always take into account and refer to concrete technical implementations. Interestingly in April 2020, at the summit of discussions in Germany and Europe, the biggest makers of mobile operating systems, Google and Apple, announced to introduce a decentralized contact tracing function much like DP3T into their operating systems (Google/Apple 2020) and therefore practically forcing official design decisions in this direction.

Since then, digital contract tracing was widely and continuously debated in science, media and politics in terms of IT security, data protection (law), privacy and ethics. This paper intends to analyze the specific relationship between the ethical tech discourse and the data protection discourse to develop a critical view of ethics in this concrete aspect without criticizing ethical perspectives in general.

Research question and approach

In this article I deal with the relationship between ethical analysis and data protection analysis in the discourse concerning digital contact tracing. Concretely, I compare and contrast specific ethical conclusions with respective data protection conclusions. I do this referring to data protection theory in

2 Compare functionality of the CWA pre-v2.0 and v2.0+ see RKI 2021.

general as well as taking into account the existing legal framework of the GDPR including its concrete tool "data protection impact assessment". In the closing discussion the findings are put in a wider context of discussing the digital constellation (Berg et al. 2020) and from there I outline suggestions, how ethics could make better use of its perspective to help discussing the responsible societal use of technology given already existing data protection thought.

Since there is not one single approach or opinion in ethics regarding analyzing digital tools, the basis for this article is Luciano Floridi's prominent academic ethical contribution "Mind the App" (Floridi 2020) which played an important role in the international debate about app-based digital contact tracing, e.g. publicly discussing the German Corona-Warn-App (CWA). Floridi is a professor of Philosophy and Ethics of Information, and director of the Digital Ethics Lab at the Oxford Internet Institute, University of Oxford. Each core demand from his contribution is contextualized with the relevant parts within data protection theory and the existing legal framework of the GDPR to see, how those demands either open new views or also match with already existing regulation. A similar undertaking could be done with other ethical contributions making comparable demands, e.g. the less theoretical but similarly influential "10 requirements for the evaluation of 'Contact Tracing' apps" (Neumann 2020) from the Chaos Computer Club, one of the world's largest and most influential hacker associations.

A comparison of ethical and data protection conclusions will help us to assess the widely stated proposition "that we are entering some uncharted areas of digital ethics. The way forward may lie in designing the right policies" (Floridi 2020).

Key terms

Since the topic of this article takes place at the intersection of ethics and data protection, the key terms should first be outlined in brutal brevity.

Ethics is the philosophical discipline dealing with the preconditions and evaluation of human action. It is the methodical reflection on morality and values, especially concerning their reflection and justifiability. It involves systematizing, defending, and recommending concepts of right and wrong behavior (Fieser 2009). The work referenced above can be located in the field of applied ethics, dealing less with abstract (meta-)ethical questions, but with

specific situations or a particular domain of action. In this case we deal with the basic values of freedom and privacy while looking at a concrete technology: mobile corona apps.

Concerning the concept of data protection, I first make a necessary and important distinction between data protection (theory), IT security and data protection law. This is to create a basis for an informed discussion about the relation of ethics and data protection.

Data protection or data protection theory is a field in the social sciences dealing with unintended social and societal consequences of data processing (Steinmüller 1972). The data protection discourse emerged in the 1960s and started in the U.S. (Pohle 2018). Data protection intends to protect individuals as well as societal functions, hence the name is clearly a misnomer. It can be said that data protection maintains the functional differentiation of modern societies and thus safeguarding many basic societal functions by making structural power asymmetries a central topic (Rost 2018). In addition to the structural nature of data processing, societies with division of labor can in principle not let the overstrained individual deal with all details of information processing, if they want to be fair (Hull 2015; Kröger et al. 2021). The focus of data protection therefore does not lie on the "privacy" and "privacy decisions" of the individual data subject, but on the overall structural societal effects of data processing (Bock/Engeler 2016). If at all, the scientifically blurry concept of "individual privacy" can be seen as one of the many secondary effects of good data protection (Rubinstein 2012; Pohle 2018). It is noteworthy, that in terms of data protection the primary source of risk is always the processing organization. Then platforms, service providers, other users and external third parties such as hackers come in scope insofar they threaten the data subjects. In short, data protection protects people and society from the effects of data processing by the processor. Data protection therefore enforces the protection of the interests of the affected people against the interests of the organization, especially if the former contradict the latter. Data protection measures can be applied on the technical level, on the organizational level and on the legal level.

In contrast, the field of IT security is part of the computer science discipline and deals with protecting the processing organization, its processes and data from external influences including hackers but also regular users or rogue employees who work against the organization (Anderson 2018). It therefore centers the interests of the organization itself, which already outlines possible clashes between data protection and IT security. IT security can also

be practiced on the technical level, on the organizational level and on the legal level. IT security is that part of information security which deals with information processed by computer systems (i.e., not on paper). Data protection also uses IT security methods, but as stated above with a completely different (maybe even contradictory) goal in mind (Steinmüller 1972). Oftentimes the topics of data protection and IT security are mixed up in digital discourse, but from the description above it should be apparent, that for digital contact tracing the topic of IT security is relevant, but of minor interest for this paper and will therefore be ignored for the sake of brevity.

Finally, data protection law is the legal form of data protection. It is the result of academic discourse, societal debate, political negotiation and oftentimes serendipity (or bad luck, depending on the perspective) within the concrete political lawmaking process. Data protection continuously and critically evaluates its legal implementation in data protection law (Karg 2012). This difference can create peculiar situations, where certain measures are legally required although they have no proper data protection effect (Solove 2013; Crain 2016; Bergemann 2018; Kröger et al. 2021) while at the same time some really useful data protection measures are not legally required (cf. SDM 2021).

The globally first formal data protection law came into being in Germany in 1970 in the federal state of Hesse. Data protection law in Europe in its current form is based on the Charter of Fundamental Rights of the European Union (CFR 2012) Article 8 – Protection of personal data, and it is written out in the General Data Protection Regulation (GDPR 2016). Protected by it are "natural persons with regard to the processing of personal data" (Article 1 (1) GDPR) and concretely protected are all "fundamental rights and freedoms of natural persons" (Article 1 (2) GDPR). In other words, all fundamental rights and freedoms are protected by data protection law insofar data processing is concerned (see Articles 6 (1) f, 24 (1), 25 (1), 32 (1), 35 (1), 35 (7) lit c & d GDPR). This relates not only to individual rights from the right to health to the right to free movement, but also to collective rights like the freedom to assemble or even the "fairness" of the whole processing context (Article 5 (1) lit a GDPR). For achieving the protection of all fundamental rights and freedoms (protection goal) the law uses the concept of "personal data" as anchor point (protection object). Whether using the concept of personal data is actually a good and useful approach for facilitating the protection of all fundamental rights and freedoms and how it could be meaningfully interpreted has long been discussed in many ways within the data protection community (Art29 2007; Karg 2012).

Finally, it has to be noted, that even though the topic is broadly framed merely as a discussion about "apps", in reality we are discussing a complex data processing procedure implemented by a complex digital system with millions of mobile clients, many servers in data centers and complex technical interactions with the underlying digital infrastructures and mobile operating systems of Google and Apple. So, whenever the seemingly light term "app" appears, it should be interpreted accordingly.

With this foundation of key terms, we can now start to discuss digital contact tracing by concretely looking at the German implementation called the Corona-Warn-App. First, I briefly describe its functionality and technical design, then it will be analyzed.

The German Corona-Warn-App (CWA)

The Corona-Warn-App is a digital tool designed to help combating the COVID-19 pandemic. The CWA is a project that was initiated in spring 2020 by the German Federal Ministry of Health and which was then carried out by the subordinate Robert Koch-Institute (RKI), a research institute responsible for disease control and prevention. The CWA is being developed and maintained by SAP and T-Systems, which is a subsidiary of Deutsche Telekom, and was initially released in June 2020. Initially, the CWA only worked for and between German users, but in October 2020 the CWA was connected to the EU InteroperabilityGateway and started to exchange data with many other national corona apps from other European countries.

The main purpose of the CWA is to break infection chains by warning users after close contact with people, who later turned out to have very likely been infectious at the time of meeting. The warned users can then decide to quarantine to not pass on the (possible) infection (Bock et al. 2020).

Technically, the CWA is a client-server system using the digital contact tracing framework provided by Google and Apple (Google/Apple 2020). In order to achieve the described functionality, all contact events are stored locally on the users' smartphones utilizing proximity tracing via Bluetooth Low Energy (BTLE) technology which works within maximum distances of several meters. Concretely each app regularly emits a changing pseudonymous BTLE identifier and at the same time records all foreign identifiers it locally receives from other apps. Using this approach, each app locally manages two lists:

one list of identifiers sent out and one list of identifiers received from others (RKI 2021b).

If at some point a CWA user tests positive for Corona, the app uploads all identifiers from the "sent" list to the CWA server. The server storage therefore contains many pseudonymous identifiers of infected people. At the same time each app periodically downloads the complete set of identifiers and compares it to all identifiers in its own "received" list. If a match is found, this means the app has been in close vicinity to another app of a user, who has been infectious at the time of contact. Then a local risk calculation is done on the smart phone based on, among other things, the state of infection at that time as well as the length and the closeness of the contact event in question. If a certain risk threshold is met, the user is immediately warned of the detected high risk by the app and asked to self-quarantine. Since the matching and warning are done locally on the smart phone and not centrally on the server, this concrete approach is called decentralized. Centralized solutions were initially discussed but eventually dropped, when Google/Apple presented their decentralized framework in spring 2020 (Bock et al. 2020).

Floridi's ethical demands and the data protection analysis

Based on the described basic functionality of digital contact tracing and concretely the CWA, we can now take a closer look at Floridi's ethical reflections (Floridi 2020) and put them in relation with existing data protection discourse and even data protection law.

First, we need to briefly contextualize Floridi's text. On the one hand, it is an article in the academic journal "Philosophy & Technology" and he writes "that we are entering some uncharted areas of digital ethics" implying a contribution to "digital ethics". On the other hand, within the text he also explicates a somehow political motivation by saying "the way forward may lie in designing the right policies" (Floridi 2020). I therefore see his work as a prelegal reflection in the form of academic ethical considerations.

In his contribution, Floridi suggests a two-step ethical analysis for digital contact tracing: validation and verification. The first step "validation of a system" offers requirements to answer the question, whether "we are we building the right system" given the societal context. Technically speaking he asks if, in general, the functionality of the system can appropriately approach or even solve the given problem. The second step "verification of a system" intends to

answer the question whether we are "building the system in the right way?" and concerns problems of its proper implementation and implications of its actual society-wide use (Floridi 2020).

First step: Validation

According to the Floridi paper, the first step, validation, fails, if the app is a) illegal, b) unnecessary, c) a disproportionate solution to the problem, d) goes beyond the purpose for which it was designed and e) continues to be used even after the end of the emergency.

From an academic ethical perspective, it is interesting that he does not explicate which ethical school or framework he follows or which ethical goals he assumes to then infer his concrete requirements from. Furthermore, none of his demands are properly motivated or explained and especially the demand a) for legality is surprisingly ill-founded given the historically long philosophical and political debate about the relation of ethics and law, legitimacy and legality. I am not implying to personally reject demand a), but an explanation is certainly missing here. His very general remarks regarding the validation step and his implicit ethical base on common sense lead me to read his contribution with a slight political focus to improve the policy debate about public technology use, rather than with an academic focus to improve the ethical debate regarding technology assessment.

According to Floridi in a), legality is necessary, but not sufficient for an "ethical app". I outlined above, why the demand for legality is not self-evident and should be well-founded for an ethical analysis or an ethical argument. However, from a data protection perspective, the legality question is also only remotely relevant, since legality in itself does not prevent unwanted consequences of data processing (Solove 2013; Kröger et al. 2021). The primary goal of data protection is the protection of people and society, not the protection of legal principles. However, from a data protection law perspective, the fulfillment of the legality requirement is indeed self-evident.

According to Floridi in b), the app has to be necessary given all kinds of solutions, i.e., there should not be better solutions. This very general remark seems useful, even obvious. However, from a data protection perspective, this requirement cannot be stated in such generality, since such question can only be asked according to a clearly specified purpose. If the purpose is as broad as "fighting the pandemic", there might be many other much more effective

means than digital contact tracing (Wibbens et al. 2020, Haug et al. 2020) and it would have to be discussed, which role an app can play in this context (cf. Bock/Engeler 2016). However, if the defined purpose is as narrow as "warning users of possible infectiousness", then the question of necessity would have to evolve around comparing concrete processing procedures, different app designs and implementations. Data protection even critically assesses the described purpose hierarchies from broad to specific to conduct a detailed necessity analysis. An ethical analysis also should get as detailed to be actually useful.

From a data protection law perspective, according to the GDPR necessity is central, concretely necessity to fulfill a given specified, explicit and legitimate purpose (Article 5 (1) lit. b GDPR). Article 5 (1) lit. c GDPR requires that the personal data processed has to be adequate, relevant and limited to what is necessary in relation to this purpose. Further clarification can be found in Recital 39 – Principles of Data Processing GDPR, where it is stated, that "personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means". In addition, Article 25 GDPR requires data protection by design regarding the design of the processing procedures and the concrete technical implementation.

According to Floridi in c), an app has to be a proportionate solution to the problem, for example, if there are many corona cases in the country to be prevented. However, the question of proportionality can only be meaningfully answered, if the risks can be clearly stated and weighed against the benefits. Floridi does not really mention which risks he is referring to and since the ethical framework is also not explicated, a plain demand for proportionality hangs in thin air. However, from a data protection perspective risks would be all kinds of unintended consequences for individuals and society, which arise from organizations doing data processing. Practically useful reflections on proportionality concerning the effects of data processing can already be found in Steinmüller 1973. From a data protection law perspective those risks would be infringements on all fundamental rights and freedoms, which then would have to be compared to the benefits of a Corona app system (Rost 2018). Furthermore, "proportionality is a general principle of EU law. It restricts authorities in the exercise of their powers by requiring them to strike a balance between the means used and the intended aim. In the context of fundamental rights, such as the right to the protection of personal data, proportionality is key for any limitation on these rights" (EDPS 2021). But even apart from EU law, ethics and data protection, according to modern political and legal theo-

ry, any action by a constitutional state has to be proportionate, i.e. legitimate, suitable, necessary and appropriate. So the stated demands for proportionality and necessity are actually a commonplace requirement independent from corona or apps and are a cornerstone of modern states. Only the concrete answer here is one comprising the details of digital technology, epidemiology, fundamental rights and data protection.

According to Floridi in d), the app must not go beyond the purpose for which it was designed. From the perspectives of data protection and data protection law, purpose limitation is a long-established cornerstone. This means, that the purpose(s) itself should be specified beforehand, explicit and very limited, and that the processing system only fulfills the purpose(s), nothing more. Article 5 (1) lit. b GDPR explicitly demands, that data must be "not further processed" as the "legitimate purpose" defines.

According to Floridi in e), the app must not be used after the end of the emergency. From the perspectives of data protection and data protection law, this is already part of proportionality, necessity and purpose limitation, since data processing in itself is already considered a risk. Therefore, the remarks above apply here as well. In addition, storage limitation is another long-established cornerstone. This principle concretely means, that the data must not be kept for "longer than is necessary for the purposes" (Article 5 (1) lit. e GDPR) or in other words "the period for which the personal data are stored is limited to a strict minimum" (Recital 39 – Principles of Data Processing, GDPR).

Second step: Verification

Subsequently, Floridis second step "verification of a system" intends to answer the question whether "are we building the system in the right way?". In this step, he wants to evaluate, if the actual technical implementation and the use within the concrete social reality do meet the requirements and expectations. In this seconds step, he raises questions of "privacy (or personal data protection to be more precise)", questions of effectiveness of the app depending on the number of users, questions of the problem of truly voluntary use of the app, questions of transparency and accountability, and finally questions of inclusion/exclusion and the digital divide. However, he is much less structured, only raises these issues and offers no way to actually answer or even systematically approach them. However, those questions and especially

structured ways to answer them are not unknown to data protection theory and data protection law, as we will now see.

Data Protection Impact Assessment – an existing practical tool

The very important questions Floridi raises in his two steps of validation and verification have a long and well documented history in data protection theory (Bock 2012; Pohle 2018). Since 2016 they also have an EU-wide legal manifestation, e.g. generally in Article 5 GDPR "Principles relating to processing of personal data" and more detailed in the form of a structured Data Protection Impact Assessment (DPIA) according to Article 35 GDPR.

The principles in article 5 GDPR are applicable to all data processing covered by the GDPR. They demand lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability for any data processing affecting natural persons (Art29 2007). However, for digital contact tracing as discussed in this article, a detailed Data Protection Impact Assessment according to Article 35 GDPR comes into play: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. […] This assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned." It should be mentioned, that data protection authorities can prohibit any data processing based on the findings in a DPIA, if they see too many unmet risks for fundamental rights and freedoms.

For a DPIA different methodological approaches are possible. The European Data Protection Supervisor (EDPS) and the German Conference of

Federal and State Data Protection Commissioners recommend the "Standard Data Protection Model" (SDM). This model first requires a threshold analysis to clarify the extent to which a DPIA for a given data processing system is not only ethically desirable but also required by data protection law. Since contact tracing apps are both a novel technology and they process personal data on a large scale (in the case of infection even health data) a DPIA is legally required. To deepen the understanding what can be achieved by a DPIA, I will now briefly outline a widely perceived one, that has been created for the CWA in April 2020 by a group of data protection researchers and practitioners including myself (Bock et al. 2020).

Analysing the Corona-Warn-App using the tool

To illustrate the power and detail of utilizing a DPIA, I will just sum up the method based on the SDM, fleshed out in DSKKP5 2018 and Friedewald 2017, and then contour three main findings.

The first methodological step is to define the purpose of the entire data processing operation, in this case it is exclusively the detection and interruption of infection chains. After that, it is important to work out the context of the processing. This includes not only the general social and political situation as well as technical circumstances, but also explicitly the different actors involved and their interests. Only on this basis can a well-founded analysis of risks and attack scenarios be created later.

Assumptions and use cases for the processing must then be explicated in order to subsequently describe the processing activity in detail. It should be noted that the procedure must be broken down into sub-steps, not all of which have to be technology-supported. In this case, the procedure includes not only the app, but also the associated server systems, specialized applications and infrastructure components such as operating systems, used frameworks or technical communication relationships. On this basis, legal relationships and responsibilities for the processing activity are discussed and legal implications developed.

Combining this preliminary work, all vulnerabilities, hazards and risks of the processing are worked out. This means risks related to all fundamental rights and freedoms of the data subjects and everyone affected, in this case the whole society including the ones not using the app (Bock et al. 2020). Based on this risk analysis, concrete protective measures for the rights of

the data subjects are then determined and finally recommendations for the data controller are gathered. The recommendations also include particularly problematic aspects, such as risks for which no protective measures exist in the current design.

Findings of the DPIA

In the following, I will contour three important findings of a DPIA. All of them are still relevant today and cover some of Floridi's questions. More insights can be found in the full DPIA (Bock et al. 2020).

1. Real voluntary use of the app requires many complex preconditions in a society. It can quickly turn out to be an illusion in practice. Presenting the app should never serve as a condition of access to public or private buildings, spaces, or events. Such use could be enacted by third-party actors (e.g., employers or private event organizers), but would not be covered by the purpose of the system and must therefore be prevented, because such scenario would mean an implicit coercion to use the app and would lead to a significant unequal treatment of non-users; the already existing "digital divide" between smartphone owners and non-owners would hereby expand to further areas of life. In addition, the purpose and efficiency of the system could be undermined if users fear negative effects of having a warning in the app and would then deliberately not carry their smartphones with them or alternate between different devices. This risk can only be mitigated by accompanying legislation that effectively prevents all misappropriations outside the purpose.
2. All variants of Corona apps discussed so far including the CWA do process personal data and are therefore subject to the GDPR. Some data is pseudonymous and some is anonymous in some steps of the process, but that still means the process as whole processes personal data, because all data on a smartphone is personal, namely related to the user of the device. This applies regardless of whether anyone can trace the Bluetooth identifiers back to a person or whether a device is well secured against access by third parties. And because only positively tested people transmit data to the server, this uploaded data is health data. This uploaded data can only be anonymized through an interplay of organizational, legal and

technical measures and must be continuously verifiable by the responsible supervisory authorities by putting in place a data protection management system.

3. The role of the largest mobile operating system providers, namely Apple (iOS) and Google (Android), must be critically discussed and accompanied throughout the entire processing procedure, because current Bluetooth-based corona tracing apps heavily rely on them. In spring 2020, those platform providers have used their position of power to practically force a decentralized and thus more data protection friendly architecture against numerous governments. This was desirable in the outcome, but at the same time it is highly problematic from a democratic point of view. In the public discussion this move has largely overwritten the data protection risks posed by the providers themselves. Google and Apple can easily obtain the Bluetooth identifiers and derive information about infection cases and exposure risks from it. Moreover, the source code of the relevant parts of their exposure notification framework in iOS and Android is still secret, even for the data protection supervisory authorities (Google/Apple 2020). Critical monitoring of the role of Apple and Google therefore requires comprehensive awareness of this problem, the legal obligation of the companies to behave in a data protection friendly manner and effective oversight.

Those three points are the main findings suitable for this article, but of course there are many more insights and details to be found in the DPIA. Now we will return to the ethical perspective.

Conclusion and discussion

After this short excursion to data protection theory, the GDPR and the CWA data protection impact assessment two important observations can be made. First, practically all of Floridi's points in the first step (validation) are not only ethical commonplace requirements applicable to any technology employed by governments in any emergency situation, but they are also existing constitutional practice for evaluating any measure applied by a constitutional state and in this concrete case, they are even already existing data protection law in the EU. Especially the last part sharpens Floridi's requirements to a point

where they can already be legally enforced. Especially the complex question of overall necessity of a corona app is already covered by the proportionality requirement of a constitutional state as well as it is a central and detailed discussion in data protection theory. This means from an academic ethical point of view, that in the case of corona apps interestingly ethics can be enforced by law. And from a political point of view it means, that the right policies have already been designed and just have to be applied properly. Both should at least have been mentioned.

Second, the issues Floridi rightfully but only lightly mentions in the second step (verification) are indeed already a core part of any DPIA legally required by the GDPR. There is no need to stay superficial. Furthermore, the DPIA presented above found many more issues to be discussed regarding individual, societal and even ethics related risks while following an already established, theoretically founded and methodologically sound data protection method. However, the instrument DPIA is not without flaws: Such assessments are not always of good quality as the one initially published by the Robert Koch-Institute (RKI) as the responsible body for the CWA shows. It did not address the relevant data protection and ethical problems due to significant methodological, technical and legal deficits (Rehak et al. 2022). But if all ethical questions raised by Floridi 2020 have already been dealt with, even in great detail and most are also legally covered already, what then is the role of ethics concerning digital contact tracing and digital technologies in general?

A new task for ethics?

First, I have to mention, that of course there is not one kind of digital ethics and Floridi is also just one voice among many. Hence my conclusions apply only to this and similar kinds of analysis. Ethical debates in academia and society are important for knowledge creation, societal self-realization and reflection of common values. Especially with new technologies, they can also help to fathom perspectives on new artifacts or help to continuously evaluate existing legislation. However, a productive mode of philosophical inquiry should include relevant and related developments and research in other fields, such as the philosophy of mind should take into account the insights of neuroscience, even if "rejecting" them. Stating that "it is clear that we are entering some uncharted areas of digital ethics" (Floridi 2020) implies untouched territory, when in fact many digital aspects of our complex modern society,

which started to evolve in the 1960ies, have been extensively analyzed by social sciences, debated broadly in society and have even partly been negotiated by political bodies.

Contrary to common belief many information technological areas such as (ethical and social) theory of computer science (Coy 1992; Capurro 1995), data processing in general (Steinmüller 1973; Pohle 2018), artificial intelligence (Coy/Bonsiepen 1989; Rost 2018b; Rehak 2021), blockchain technology (Rehak 2019), self-determination, consent and transparency (Solove 2013; Bergemann 2018; Crain 2016; Kröger et al. 2021), and also precisely digital contact tracing applications (Bock et al. 2020) have already been the topic of technically informed academic research producing many results and insights highly relevant for ethical analyses of the digital world. And if "the way forward may lie in designing the right policies" (Floridi 2020), we should all take into account the already existing legislation, its background and its genesis.

This realization does not constitute any superfluency of philosophical and concretely ethical discourse in those areas, quite the contrary, but it constitutes the need for such discourses to continuously connect with technical, societal, political and legal developments in order to meaningfully contribute. Digital ethics discourses have recently even been under fire for watering down, setting back or even replacing already solid legal approaches to tech regulation (Wagner 2018; Sloane M 2019), willingly or not, but of course this can and must be actively prevented and is already being discussed within the ethics community (Bietti 2020).

This paper intendeds to contribute to this discourse by showing, how misleading, and maybe unethical, it can be to ethically demand precisely what has been developed legally already. Only focusing on the former without mentioning the latter is something to be prevented in future ethical discussions about technology. And as seen above, data protection theory already asks so many much more detailed questions, that ethics can profit greatly from taking that rich perspective into account.

There are so many important topics of digital ethics which have not yet been covered systematically and which are only partly in scope of data protection, such as how society changes when people get used to permanent surveillance of their contacts or how (mis)trust in the government having been build up over time now pays off in times of emergency or what the ethical specificities of an app are, which only really works if used voluntarily or even how a DPIA could be methodologically extended to get an ethics impact assessment.

If ethically founded positions don't manage to catch up with developing realities, societal discourse will stay stuck in a time loop of perceived simplicity and lawlessness. But if ethics can acknowledge the already present, and many ethics scholars already do, it can stay at the forefront of thinking about values of societal and technical futures – a place it has had for millennia.

Literature

Anderson R (2008) Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley India

Art29 – Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Beer K (2020) Spahn: Corona-Warn-App wird nächste Woche vorgestellt, Heise.de 08.06.2020, https://www.heise.de/news/Spahn-Corona-Warn-App-wird-naechste-Woche-vorgestellt-4776582.html (last visited 9/9/2021)

Berg S, Rakowski N, Thiel T (2020) The Digital Constellation, (Weizenbaum Series, 14), Berlin: Weizenbaum Institute for the Networked Society – The German Internet Institute. https://doi.org/10.34669/wi.ws/14

Bergemann B (2018) The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection. Hansen M, Kosta E, Nai-Fovino I et al. (Eds) Privacy and Identity Management. The Smart Revolution, ISBN 978-3-319-92925-5, Springer International Publishing, Cham, 111-131, http://dx.doi.org/10.1007/978-3-319-92925-5_8

Bietti E (2020) From ethics washing to ethics bashing: a view on tech ethics from within moral philosophy. In: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20). Association for Computing Machinery, New York, NY, USA, 210–219. DOI: https://dl.acm.org/doi/abs/10.1145/3351095.3372860

Bock K (2012) Impact Assessment im Lichte des Standard-Datenschutzmodells. DuD – Datenschutz und Datensicherheit 10/2012, 743-747

Bock K, Engeler M (2016) Die verfassungsrechtliche Wesensgehaltsgarantie als absolute Schranke im Datenschutzrecht. DVBl – Deutsches Verwaltungsblatt 10/2016, 593

Capurro R (1995) Informationsethik. Schriften zur Informationswissenschaft; 18. UVK Universitätsverlag, Konstanz, ISBN 3-87940-507-7

CFR – Charter of Fundamental Rights of the European Union (2012) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:12012P/TXT

Coy W (1992) Für eine Theorie der Informatik! Sichtweisen der Informatik. Theorie der Informatik. Wiesbaden: Vieweg+Teubner. 17-32

Coy W, Bonsiepen L (1989) Erfahrung und Berechnung: Kritik der Expertensystemtechnik, Springer

Crain M (2016) The limits of transparency: Data brokers and commodification. New Media & Society, 20(1), 88-104. https://doi.org/10.1177/1461444816657096

DP3T – Decentralized Privacy-Preserving Proximity Tracing (2020) EPFL and ETH Zurich advance digital contact tracing project. https://actu.epfl.ch/news/epfl-and-eth-zurich-advance-digital-contact-tracin/ (last visited 9/9/2021)

DSKKP5 – Independent Data Protection Supervisory Authorities of the Federation and the Länder (2018) Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. Kurzpapier Nr. 5, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (last visited 9/9/2021)

EDPS – European Data Protection Supervisor (2021) Necessity & Proportionality, https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en (last visited 9/9/2021)

Fieser J (2009) Ethics. The Internet Encyclopedia of Philosophy (IEP), ISSN 2161-0002), https://iep.utm.edu/ethics/ (last visited 9/9/2021)

Floridi L (2020) Mind the App—Considerations on the Ethical Risks of COVID-19 Apps. Philosophy & Technology 33, 167-172. https://doi.org/10.1007/s13347-020-00408-5

Friedewald M, Bieker F, Obersteller H et al. (2017) Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. White Paper. Version 3. Forum Privatheit, https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_DSFA-3.pdf (last visited 9/9/2021)

GDPR – General Data Protection Regulation (2016) Regulation (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj

Google/Apple (2020) Exposure Notification Framework – ENF / Googe-Apple-Exposure-Notification – GAEN, https://developer.apple.com/documentation/exposurenotification and https://www.google.com/covid19/exposurenotifications/ (last visited 9/9/2021)

Haug N, Geyrhofer L, Londei A et al. (2020) Ranking the effectiveness of worldwide COVID-19 government interventions. Nat Hum Behav 4, 1303-1312 (2020). https://doi.org/10.1038/s41562-020-01009-0

Hull G (2015) Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data. Ethics and Information Technology 17, 2, 89-101

Karg M (2012) Die Rechtsfigur des personenbezogenen Datums. Ein Anachronismus des Datenschutzes? Zeitschrift für Datenschutz 6/2012, 255-261

Kröger JL, Lutz OHM, Ullrich S (2021) The Myth of Individual Control: Mapping the Limitations of Privacy Self-management, http://dx.doi.org/10.2139/ssrn.3881776

Neumann L (2020) 10 requirements for the evaluation of "Contact Tracing" apps. Chaos Computer Club. https://www.ccc.de/en/updates/2020/contact-tracing-requirements (last visited 9/9/2021)

PEPP-PT – Pan-European Privacy-Preserving Proximity Tracing (2020) High-Level Overview, https://github.com/pepp-pt/pepp-pt-documentation/blob/master/PEPP-PT-high-level-overview.pdf (last visited 9/9/2021)

Pohle J (2018) Datenschutz und Technikgestaltung – Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, Dissertation, Humboldt-Universität zu Berlin, https://edoc.hu-berlin.de/handle/18452/19886

Rehak R (2019) A trustless society? – A political look at the blockchain vision. Beiträge zur Hochschulforschung, 41. Issue, 3/2019, 60-65, https://www.bzh.bayern.de/fileadmin/user_upload/Publikationen/Beitraege_zur_Hochschulforschung/2019/3_2019_Gesamt.pdf

Rehak R (2021) The Language Labyrinth: Constructive Critique on the Terminology Used in the AI Discourse. Verdegem P (ed) AI for Everyone: Critical Perspectives. 87–102. London: University of Westminster Press. https://doi.org/10.16997/book55.f.

Rehak R, Kühne CR, Bock K (2022) Analysis and constructive criticism of the official data protection impact assessment of the German Corona-Warn-App, Conference proceedings of the Annual Privacy Forum (APF) 2022, Springer LNCS

RKI – Robert Koch-Institut (2021) Interrupt chains of infection digitally with the Corona-Warn-App, https://www.rki.de/EN/Content/infections/epidemiology/outbreaks/COVID-19/CWA/CWA.html (last visited 9/9/2021)

RKI – Robert Koch-Institut (2021b) Corona-Warn-App: Documentation, https://github.com/corona-warn-app/cwa-documentation (last visited 9/9/2021)

Rost M (2018) Risks in the context of data protection/Risiken im Datenschutz. vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik, 57(1/2), 79-92. English version: https://www.maroki.de/pub/privacy/Rost_Martin_2019-02_Risk:_8types_v1.pdf

Rost M (2018b) Künstliche Intelligenz: Normative und operative Anforderungen des Datenschutzes. DuD - Datenschutz und Datensicherheit. 42, 558-565. 10.1007/s11623-018-0999-9. https://www.maroki.de/pub/privacy/2018-09_DuD-KI.pdf

Rubinstein I (2012) Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 12-56

SDM – UAG "Standard Data Protection Model" of the AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder (2020) The Standard Data Protection Model – A method for Data Protection advising and controlling on the basis of uniform protection goals, AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf (last visited 9/9/2021)

Sloane M (2019) Inequality Is the Name of the Game: Thoughts on the Emerging Field of Technology, Ethics and Social Justice. Proceedings of the Weizenbaum Conference 2019 "Challenges of Digital Inequality – Digital Education, Digital Work, Digital Life", 1-9. Berlin https://doi.org/10.34669/wi.cp/2.9

Solove DJ (2013) Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review 1880

Steinmüller W (1972) Grundfragen des Datenschutzes, Gutachten, BT-Drucksache 6/3826, German Bundestag

Wagner B (2018) Ethics as an escape from regulation. BEING PROFILED: COGITAS ERGO SUM: 10 Years of Profiling the European Citizen, Amsterdam University Press, https://doi.org/10.2307/j.ctvhrd092

Wibbens PD, Koo WWY, McGahan AM (2020) Which COVID policies are most effective? A Bayesian analysis of COVID-19 by jurisdiction. PLOS ONE 15(12) e0244177. https://doi.org/10.1371/journal.pone.0244177