Sociologica. V.14 N.3 (2020)
ISSN 1971-8853

A Pandemic of Prediction: On the Circulation of Contagion Models between Public Health and Public Safety

Maximilian Heimstädt[*] Simon Egbert[†] Elena Esposito[‡]

Submitted: August 19, 2020 – Revised version: November 18, 2020
Accepted: December 14, 2020 – Published: January 29, 2021

Abstract

Digital prediction tools increasingly complement or replace other practices of coping with an uncertain future. The current COVID-19 pandemic, it seems, is further accelerating the spread of prediction. The prediction of the pandemic yields a pandemic of prediction. In this paper, we explore this dynamic, focusing on contagion models and their transmission back and forth between two domains of society: public health and public safety. We connect this movement with a fundamental duality in the prevention of contagion risk concerning the two sides of being-at-risk and being-a-risk. Both in the spread of a disease and in the spread of criminal behavior, a person at risk can be a risk to others and vice versa. Based on key examples, from this perspective we observe and interpret a circular movement in three phases. In the past, contagion models have moved from public health to public safety, as in the case of the Strategic Subject List used in the policing activity of the Chicago Police Department. In the present COVID-19 pandemic, the analytic tools of policing wander to the domain of public health — exemplary of this movement is the cooperation between the data infrastructure firm Palantir and the UK government's public health system NHS. The expectation that in the future the predictive capacities of digital contact tracing apps might spill over from public health to policing is currently shaping the development and use of tools such as the Corona-Warn-App in Germany. In all these cases, the challenge of pandemic governance lies in managing the connections and the exchanges between the two areas of public health and public safety while at the same time keeping the autonomy of each.

Keywords: pandemic; COVID-19; prediction; risk; contagion; health care; safety; predictive policing; contact tracing.

* Weizenbaum Institute (Germany); https://orcid.org/0000-0003-2786-8187

† Department of Sociology, Technische Universität Berlin (Germany); https://orcid.org/0000-0002-3729-0393

‡ Department of Political and Social Sciences, University of Bologna (Italy); Faculty of Sociology, Bielefeld University (Germany); elena.esposito@uni-bielefeld.de

Copyright © 2021 Maximilian Heimstädt, Simon Egbert, Elena Esposito
The text in this work is licensed under the Creative Commons BY License.
https://creativecommons.org/licenses/by/4.0/

Acknowledgements

This work was supported by the European Research Council (ERC) under Advanced Research Project PREDICT no. 833749. Simon Egbert's work on predictive policing was supported by Fritz Thyssen Stiftung (grant number 10.16.2.005SO) and by Deutsche Forschungsgemeinschaft (project number 163866004). For their helpful comments, criticisms, and suggestions we are grateful to David Stark as well as the two anonymous reviewers of *Sociologica*.

1 Introduction: Predicting Contagion in Pandemic Times

The explosion of forecasting techniques triggered by the COVID-19 outbreak is happening at a time when a profound transformation of the techniques and the meaning of forecasting is already underway in various areas of society (Esposito, 2020). The need to manage the pandemic-related emergency has led to a tremendous acceleration in the development of corresponding predictive practices, including intense experimentation that could not have been achieved in less dramatic circumstances.[1] Against this backdrop, the pandemic can be observed as a gigantic experiment in social prediction.

This essay analyzes this situation from a specific point of view: the role and transformations of contagion models as forecasting schemes for the spread of a phenomenon. More specifically, we focus on the interaction and exchange between the study of biological infections in public health and the field of public safety, where predictive techniques are used to identify the diffusion of criminal activity and intervene before it materializes (Ferguson, 2017; Egbert & Krasmann, 2019; Kaufmann et al., 2019).[2] We connect the relationship between public health and public safety with a fundamental duality in the prevention of contagion risk, concerning the two sides of *being-at-risk* and *being-a-risk*. A person at risk can be a risk to others — and vice versa.

In our opinion, this duality as illustrated in section 2, underlines the back and forth movement of analytic tools between the two fields of public health and public safety, both concerned with contagion risk. The movement is presented and discussed in sections 3 to 5. Our argument is articulated in three steps, corresponding to three distinct phases in the transfer of contagion models. In the *past* (section 3), contagion models have moved from public health to policing. One exemplary case is the Strategic Subject List (SSL) initiated by the Chicago Police Department in 2013. Through the SSL, the health-based concept of infection-by-association was translated into the concept of guilt-by-association. In the *present* of the current COVID-19 pandemic (section 4), data infrastructure providers such as the Silicon Valley-firm Palantir are offering their technological tools (e.g. systems for integrating heterogeneous and unstructured databases) to governments and public health agencies around the world to help predict the spread of the infection. The expectation that in the *future* (section 5) the technologies developed in digital contact tracing apps might spill over from public health to policing is currently

1. The special theme "Viral Data" in *Big Data & Society* (Leszczynski & Zook, 2020) explores the evolution of big data practices as a consequence of the COVID-19 pandemic. See also Chiusi (2020).

2. On the "dialogue" between health care and predictive policing triggered by the use of big data, see also Cohen and Graver (2017).

shaping the development and reception (or refusal) of tools such as the Corona-Warn-App in Germany.

What can we learn from observing this circular movement from public health to police to public health — and then presumably back to policing systems? How is the meaning of forecasting changing, together with its social acceptance, the techniques used and their diffusion, the image of companies, and the convergence between different areas? What threats and opportunities can be identified? Following up on these questions, in the final section of the paper we discuss some open issues.

2 Being-a-Risk and Being-at-Risk in Contagion Models

Contagion models, in a broad and rather generic sense, have been applied to quite different phenomena: from infectious diseases to marketing (Rayport, 1996), from gun violence to the "viral" diffusion of memes and news on the web (Rushkoff, 1994) — including the cases we address in our analysis: medical epidemics and the spread of criminal behavior. According to these models, the "rules of contagion" (Kucharski, 2020) apply when contact with an "infected" person passes a condition on to other people — be it physical contact in presence, virtual proximity on the web, or other forms of influence.[3] Contagion occurs when the state of an individual depends on what happens to others.

The effects of contagion can be undesirable (as in the case of viruses, criminal behavior or financial panic), but also intended (in phenomena like innovation, advertising or fashion). In both cases, the spread can take different forms. The curve of the epidemic, Kucharski (2020) argues, can be shaped like the letter S, when the infection grows and eventually levels off on a plateau, or like an inverted V, when the line has a peak, after which the numbers tend to decrease. The diffusion of information through the mass media, for example, can be described as S-shaped contagion, with an initial knowledge gap that is overcome when the information is shared by the entire public (Thunberg et al., 1982). An epidemic, on the other hand, ought to be shaped like an inverted V, because infected people recover and no longer present the disease. Prevention and control measures must take all these variables into account.

The COVID-19 pandemic has brought to the forefront the model of contagion, which is adopted to describe and possibly control the evolution of the disease (Stark, 2020). In the current emergency, we are dealing with an undesired contagion, i.e. a condition of *risk* referring to the possibility of becoming ill and/or transmitting the virus. The spread should be avoided, and measures are being taken to prevent and stop the infection.[4] We argue that under these conditions, a fundamental duality of the risk of contagion emerges, concerning the two sides of *being-at-risk* and *being-a-risk*. This duality links the medical management of the epidemic to activities carried out in the field of public safety.

What do we mean by the distinction *being-at-risk / being-a-risk*? Although under pandemic conditions everyone can be affected by the disease, the level of exposure is unevenly distributed

3. The Italian term "influenza" means both influence and flu.

4. The sociology of risk distinguishes a condition of danger (when possible future damage is attributed to external factors) from a condition of risk (when the damage is seen as a consequence of present decisions and behavior): see Luhmann (1991, ch.1). Even if the pandemic is perceived as a danger, when it comes to prevention — i.e. social management of the consequences of contagion — one inevitably shifts to the side of risk: what can and must be done today to avoid future damage. This is also the case when a person's reckless behavior, taking a risk, becomes a danger to other people involved: their danger is a risk from the viewpoint of prevention agencies.

and some people, such as health workers or teachers, are particularly vulnerable to a health-threatening condition. These are persons *at risk*, who must be primarily targeted by public prevention. At the same time, however, their illness is a threat to other people with whom they have been and will be in contact, who may also become infected in turn: the sick people become *a risk* to others. The two manifestations, risk for an individual and risk to others, are two sides of the same coin and are inevitably coexistent[5] — as New York Governor Andrew Cuomo vehemently argued in his conference on the coronavirus response on July 4: "If I can't convince you to show discipline for yourself, then show discipline for other people. [...] You do not have the right to burden other people with your irresponsibility."[6] In this, as in all cases of contagious, negatively evaluated conditions, a person at risk becomes a risk to others — and vice versa. A person who is a risk to others can be at risk herself.

In our society, two areas are primarily concerned with contagion risk and its duality: public health and public safety. They are engaged in managing and limiting the possible damages to citizens due to illness and criminal behavior respectively. In both cases, to protect health as well as to protect public safety, it is necessary to combine an activity of care with an activity of prevention (and prediction). To end up treating the sick is a failure of the public health system, just as to end up punishing the guilty is a failure of the public safety system (Scheffer et al., 2017). In both cases, in order to protect people, it is necessary to manage the contagion risk by monitoring people at risk who may be a risk to others.

Faced with contagious diseases, therefore, the service of public health cannot merely treat those who are sick, but must also supervise those who are not sick in order to manage the risk of people becoming infected and infecting others. The public safety service in Western societies, on the other hand, not only has the task of controlling criminals, but also of preventing crimes from spreading by targeting people who are not criminals (yet) but are at risk of becoming involved in illegal activities.[7] Public health is not only health care and public safety is not only repression — they also strive to prevent damage from occurring through advance intervention in the conditions that generate it.

It is not surprising, then, that there is an exchange of tools and techniques between the two areas.[8] Both public health and public safety must avoid contagion, for example by predicting it and intervening before it occurs. We explore this interchange in the next sections of the paper, where we describe the evolution of the mutual relations between public health and public safety in the past (section 3) and in the present of contagion management (section 4). The interchange becomes more intense in the case of pandemics, when the emergency requires the

5. Although this may be at different levels. Not all persons at risk are an equal risk to others: potentially, a grocery clerk or a bar attendee can spread the disease more than a person working from home. Prediction models must take all these dimensions into account.

6. "New York Gov. Cuomo holds news conference on coronavirus response", Video by *The Washington Post* from April 6, 2020 (at approximately 33:00 minutes) https://www.youtube.com/watch?v=_mziwN4fjGo

7. Since the first half of the Nineteenth century, referring to the theories of Cesare Beccaria and Jeremy Bentham.

8. Sometimes, there is also exchange of information. From the perspective of policing, being at risk of mental illness might easily turn into being a risk to others. For example, the system RADAR-iTE ("rule-based analysis of potentially destructive offenders to assess the acute risk of Islamist terrorism") for person-based predictive policing, used in Germany since summer 2017 (BKA, 2017; Sonka et al., 2020), operationalizes, among others, the criteria "aspects of a problematic personality" and "diagnosed psychological abnormalities" to determine the risk of individuals — so called "endangerers" — engaging in future terrorist attacks (Deutscher Bundestag, 2017). Likewise, one of the thematic complexes of the German tool for predicting Islamist radicalization processes, "Screener Islamism", refers to the dimension of "personal crisis", consisting of "despondency" and "suicidality" (Böckler et al., 2017, p. 500).

activation of all available resources. This intensification can become a problem if it leads to a blurring of the border between the areas of public health and public safety, which have different purposes, methods and priorities (French & Monahan, 2020; Kitchin, 2020; Gentithes & Krent, 2020).[9] Medical intervention should not operate as a policing activity nor be perceived as such, while policing should not intervene in health care or give the impression of doing so. The challenge of pandemic governance lies in managing the connections and the exchanges between the two areas, while at the same time maintaining their respective autonomy. We deal with this issue in section 5.

We explore our argument through three case studies, namely the development of the Strategic Subject List by the Chicago Police Department, the cooperation between Palantir and the UK government during the COVID-19 pandemic, and the development and use of the Corona-Warn-App in Germany. We selected these cases due to their revelatory nature with regards to our research interest (the role of contagion models as a link between public health and public safety). In each of the cases, a movement between these two domains becomes visible and hence available for analysis. At the same time, we suggest that what we can learn through these revelatory cases is a more general dynamic inherent to the fields of public health and public safety, which may apply to other contexts and countries as well.

3 Past: From Epidemiology to Predictive Policing

Although the relationship between public safety and public health is growing tighter due to modern approaches of big data policing and predictive policing, the connection of policing with health-related practices is not new. From Foucault (1977) onwards, observation of the medical field has provided useful clues with which to analyze the spread and acceptance of disciplinary practices and surveillance models — particularly when the matter is not repressing phenomena already underway but preventing them before they occur or spread (Ewald, 1991). In fact, the merging of epidemiological and criminological insights — now known as "epidemiological criminology" (Akers & Lanier, 2009; Akers et al., 2013; Reingle Gonzalez, 2015) — began explicitly several decades ago (Cressey, 1960) and can also be found implicitly in earlier criminological approaches. The Chicago School of Criminology, for example, active in the first third of the 20th century, analyzed crime mainly at the community level (Bryant, 2014) and with reference to the social environment of offenders, thereby sharing some basic assumptions with epidemiology (Akers & Lanier, 2009, p. 398).

Predictive policing, one of the most heavily discussed police innovations in recent years, carries this connection of epidemiology and criminology forward. For the purpose of fighting crime more "efficiently" and "objectively" (Ferguson, 2017, pp. 20–33), predictive policing uses algorithmic (big) data analysis to discover crime patterns in data from the past. These patterns are then extrapolated into the future, enabling a proactive approach instead of merely reacting when a wrong has been done (Kaufmann et al., 2019). The production of "operable predictions" should enable short-term preventive interventions based on crime-related foreknowledge about risky places or persons (Egbert & Leese, 2021).[10]

9. In terms of sociological systems theory, they refer to different, functionally differentiated subsystems of modern society: see Luhmann (1997, pp. 743 ff.).

10. Place-based predictive policing approaches are still more common, but significant developments can already be observed in person-based predictive policing systems, also known as "predictive profiling" (Lammerant & de Hert, 2016) or "person-based predictive targeting" (Ferguson, 2017, p. 34).

One of the forerunners in the field of person-based predictive policing is the Chicago Police Department, which implemented its Strategic Subject List (SSL) in 2013, decommissioning it again in October 2019 (Johnson, 2015; Lipari, 2020; O'Malley, 2020). The SSL, renamed CVRM (Crime and Victimization Risk Model) in January 2019 (Johnson, 2019), is one of the most prominent examples of person-based predictive targeting. It is especially interesting for our research interest because its prediction style is clearly inspired by epidemiology and public health. In what has been described as a "public health approach to crime prevention" (The Police Foundation, 2019), crime is treated "like an infectious disease" (Brown, 2019). This implies thinking of violence as being contagious, with violence-related risk-factors conveyed by persons and/or groups interacting with others, like relatives, friends, or neighbors. In short, the underlying assumption of this approach to public safety is that "violence spreads like a virus" (Ferguson, 2017, p. 35). In the SSL/CVRM, the epidemiologically based approach to crime prediction is combined with social network analysis, predominantly focusing on gang-related violent crime (Green et al., 2017). Violence, so goes the argument, is transmitted through social networks following an epidemic-like logic — a process termed "social contagion" (Papachristos et al., 2015, p. 140).

In concrete terms, the SSL/CVRM — also referred to as the "heat list" — aims at reducing gun violence by targeting the individuals with the greatest risk of becoming victims or perpetrators of gun-related acts of violence. The corresponding scale ranges from zero (extremely low risk) to 500 (extremely high risk). Every individual arrested in the previous four years was subjected to this assessment (Lipari, 2020, p. 2). The underlying idea in terms of crime prevention was to issue "custom notifications" (by letter or visit) to high-risk persons in order to inform them about their risky situation, to warn them that the police had an eye on them, and to convince them that it was in their best interest to behave properly (McCarthy, 2015). These activities were launched when people had a risk score of 400 or higher, and were accomplished with the help of community members and service organizations (Hollywood, 2016).

The background to the development and implementation of the SSL/CVRM was the high level of (suspected) gang crime in Chicago and, in connection with this, a high number of deaths from gun violence. In a project sponsored by the National Institute of Justice (NIJ, 2011), a team from the Medical Imaging Research Center of the Illinois Institute of Technology (IIT) combined their expertise on the algorithmic detection of prostate cancer (IIT, 2019, p. 4; Artan et al., 2010)[11] with results from crime-related social network analysis in order to develop a person-based predictive policing approach (Kump et al., 2016). These results most notably build upon studies conducted by Papachristos and colleagues, discussing the social networks and dynamics of gun-related crime victims and offenders (e.g., Papachristos et al., 2012; Papachristos et al., 2015; Green et al., 2017). Roughly speaking, these studies argue that persons whose circle of acquaintances and/or relatives includes victims or perpetrators of gun-related acts of violence have a higher risk of being involved in such acts as well in the future. As IIT professor and project leader Miles Wernick puts it: "It's not just shooting somebody, or being shot. It has to do with the person's relationships to other violent people." (quoted in Stroud, 2014)

These insights are converted into an algorithm that performs "link analyses" to identify likely perpetrators and victims of gun violence, and eventually assesses high crime risks for certain individuals. All in all, six variables are incorporated into the crime assessment: number of

11. The connection between these quite disparate research subjects is based on the common technical background of automatically detecting statistical correlations between elements in large amounts of data — be it pixels in MRI images or persons in social networks (Faye, 2016, p. 14; IIT, 2019, p. 4).

times being the victim of a shooting incident; age at the most recent arrest; number of times being the victim of aggravated battery or assault; number of prior arrests for violent offenses; trend in recent criminal activity; number of prior arrests for unlawful use of a weapon (Johnson, 2019; Lipari, 2020, p. 2).[12] In the calculation, the criteria are also weighted according to recency — more recent events have a higher value than older ones (Johnson, 2019).

Before this backdrop, the SSL/CVRM can be characterized as an epidemiological approach to crime prevention on at least three dimensions. First, it follows the public health related approach to crime fighting of preferring (primary) prevention to reaction (Butchart & Emmett, 2000, pp. 5–6). Second, it focuses on (environmental) risk factors for crime-related behavior (Moore, 1995, pp. 244–245). Third, it treats violence like a contagious disease (Reingle Gonzalez, 2015, p. 1). As information about an individual's associates plays a central role in the prediction algorithm of the SSL/CVRM, its utilization has the potential to materialize the principle of "guilt by association" (Lum & Isaac, 2016; Završnik, 2017, p. 140), meaning that a person is suspected of having committed a crime because she interacts with individuals who have committed crimes before. This reasoning implies a logic of (social) contagion, treating an individual as a risk because she habitually interacts with (past) offenders and/or known high-risk persons. These interactions, the argument goes, have put that person at risk of being "infected" with a proneness to crime.

To be able to retrace these contagion-like risk dynamics, police departments not only need access to many different data sources, they must also be able to relate them to each other. Therefore, one of the technological prerequisites for such a policing approach is a database architecture that allows for quick searches across several police databases as well as external data sources, such as media reports and social media traces. As we will show in the next section, this maxim of interconnectedness between databases ("desilosation") originating in the field of public safety has moved towards the field of public health in the time of the COVID-19 pandemic.

4 Present: From Surveillance to Public Health Protection

In the current global COVID-19 pandemic, the move of contagion models is reversed: in a transfer of tools from public safety back to public health, organizations are striving to connect previously unconnected data points across databases. Following what Fourcade and Healy have called an "institutional data imperative" (Fourcade & Healy, 2017, p. 8), in most cases organizations do not integrate different databases with a clear current question but make up the reasons for such connections and the issues they can be helpful for retrospectively (see Brayne, 2017, p. 994).

The movement of this logic of data integration from public safety to public health can be examined by looking at the technology firms that provide such databases and analytic tools. The most prominent firm is the "data analytics company" Palantir Technologies (Thiel & Masters, 2014, p. 132). The Silicon Valley firm Palantir was founded in 2004, and since then it has served customers from the public as well as the private sector (Hardy, 2014; Waldman et al., 2018; Steinberger, 2020). Palantir offers a range of software products, which allow its customers to link databases and perform searches and analyses across previously disconnected sources (Knight & Gekker, 2020, pp. 345–346). In its corporate communication, the firm

12. In the original version of the SSL, the variables "gang affiliation" and "number of previous arrests due to narcotics offences" were also included, but they were later erased because apparently, they contributed little to the quality of the forecast (Saunders et al., 2016; IIT, 2019, p. 2).

describes itself as being in the business of "data integration", linking previously unconnected "silos" of data through a "layer of Palantir on top" (Palantir, 2012; see also Brayne, 2017, p. 994). Palantir argues that what distinguishes its services from those of other data management firms is that Palantir is able to link extremely heterogeneous and unstructured types of data, thereby allowing users to discover patterns — including patterns of contagion and risk — in their streams of information (Egbert, 2019).

Palantir began developing data mining services for police departments in the early 2010s. In 2012 Palantir approached the Mayor of New Orleans and developed the first test case for their policing software (Ferguson, 2017, pp. 40–42; Winston, 2018). Competing with other providers of predictive policing software, Palantir did not await the results of this test case but forged additional cooperations with other police departments, including the Los Angeles Police Department (LAPD) (Brayne, 2017). There is only little empirical evidence of how Palantir's software works in practice, and which types of data are being associated (Winston, 2018), but the existing sources — e.g. Brayne (2017) and Egbert (forthcoming) — converge with Palantir's corporate communication. In a promotional video that portrays the use of Palantir software at the LAPD, an officer describes how he and his colleagues were able to make an arrest by combining databases such as "crime and arrest report information", "field interview cards" or "automated license plate reader information" (Palantir, 2013).

At the time of writing, Palantir sells its services to government organizations and private sector firms around the world. In addition to these directly commercial activities, Palantir has repeatedly made its services temporarily available to governments and non-profit organizations for free during humanitarian crises, framing these initiatives as acts of corporate philanthropism. For example, in one of its corporate videos Palantir states that the firm "is proud to donate its software and the expertise of its Philanthropic Engineering team to Team Rubicon [a disaster response non-profit organization] to support both Hurricane Sandy relief efforts and future missions" (Palantir, 2014). On the one hand, such philanthropic engagements help the firm develop their positioning as a guardian of US citizens. On the other hand, Palantir has used philanthropic engagement strategically in the past to introduce their technologies into public organizations without having to go through the official public procurement process. This strategy has been well-documented for Palantir's predictive policing engagement in New Orleans (Winston, 2018).

In the wake of the global COVID-19 pandemic, Palantir offered a version of the company's software "Foundry" to several governments free of cost, including to Austria, Canada, Greece, Spain and the US (Chapman, 2020). Again, Palantir emphatically stated the philanthropic aspect of its engagement in fighting the pandemic and repeatedly underlined its commitment to ensuring privacy protection, data security, and data governance.[13] In March 2020, the UK government announced that it would develop a new platform to integrate and analyze data from the UK's publicly-funded healthcare system (NHS) and other organizations (Gould et al., 2020). To develop this platform, the government began to cooperate with several technology firms including Microsoft, Amazon, Google, the predictive analytics startup Faculty, and Palantir. The UK government justified the need for this new platform by describing new and interdependent questions that had surfaced during the public health crisis related to the COVID-19 pandemic:

13. As Robert Fink, one of the investors of Palantir's "Foundry" platform, states: "I'm sure I speak on behalf of every Palantirian when I say how grateful we are for the opportunity to assist our partners in government and industry as we all fight the pandemic and its effects." (Fink, 2020)

> To understand and anticipate demand on health and care services, we need a robust operating picture of the virus, how it's spreading, where it might spread next and how that will affect the NHS and social care services. On the supply side, we need to know where the system is likely to face strain first, be that on ventilators, beds or staff sickness. (Gould et al., 2020)

In addition to this Palantir-led NHS-platform development, at the time of writing the UK government is in negotiation with Palantir concerning the utilization of their "Foundry" software for an effective contact-tracing tool (Warrell & Neville, 2020).

It is not surprising that in situations of pressing health threats governments will try to centralize and connect information streams to increase their control (or at least to signal the ability to control the situation). More remarkable, however, is that the tools to cope with the challenge of the pandemic are sought in systems aimed at maintaining social order and preventing actions that threaten it — as in policing.[14] But in both cases — in public safety efforts to contain the spread of criminal behavior and in public health measures to control the diffusion of the pandemic — the goal is to prevent the contagion acting on people at risk that can become a risk to others. Similar problems faced by these domains, it seems, are leading to a steady convergence of their tools.

What is interesting analytically about the events in the UK and in other countries is the way in which the duality of risk and our two domains of interest figure in the public presentation of Palantir's database tools. On the one hand, Palantir makes every effort to describe itself as a neutral and trustworthy intermediary — offering broad and nonpartisan protection against the medical risk of virus contagion. For example, it deliberately describes its software product as a "layer on top" rather than a modification of existing databases. On the other hand, Palantir also maintains its image as an organization devoted to the needs and interests of governments, and especially those parts engaged in protection — aiming to ensure public safety against criminal behavior.[15] The question that will concern researchers, policy-makers and citizens in the following months is if, and in what way the adoption of technologies of data integration and analysis provided by Palantir and other firms in the prevention of the epidemic's spread maintains the separation between the areas of public health and public safety. In other words, does the transmission of technological infrastructures between policing and public health also infect the latter with the assumptions, values and procedures of the former?

5 Future: The Ambiguity of Digital Contact Tracing

The issue of the reciprocal links between the field of public health and the field of public safety is even more acute when one considers the future of the relationship between care and prevention, together with the corresponding forms of forecasting. The predictive tools in this case have been developed primarily in the area of health care, yet criticism mainly revolves around their possible shift into the area of public safety and policing.

14. In the UK, the decision to involve Palantir and other technology firms has triggered a public controversy regarding the firm's access to personal data and the question of when and how the firm will need to disentangle itself from the UK government's databases (Lewis at al., 2020).

15. Shortly before the global spread of COVID-19, Palantir released two promotional video clips. Both clips deal with the use of data for military purposes, and both end with the slogan "Protecting the protectors since 2004".

In most countries, the spread of COVID-19 has been countered primarily through isolation of people and testing, both of which are very costly in economic and social terms. In several countries tracing policies have also been developed, i.e. the reconstruction of contacts between infected people and other people in order to map the possible spread of the virus, warn those at risk, isolate them, and test them (e.g., Stark, 2020; Sandvik, 2020). Since the epidemic, like all contagions, circulates primarily through proximity between people, tracing is a promising action to prevent the spread of the disease, and less costly in social terms than isolation and testing (e.g., Braun & Spahn, 2020).

However, manual tracing, for example by local health officials, is slow and imprecise because it is very difficult to reconstruct the contacts of risky individuals for the entire duration of the 14-days incubation period of COVID-19 (Ferretti et al., 2020): people do not remember their past encounters, contacts occur inadvertently, or those concerned cannot be traced. Therefore, several countries have switched to digital contact tracing (DCT), which uses digital tools (usually mobile phones) to detect and record the proximity between individuals, evaluating infection risks once a person has tested positive (Nature, 2020; Vaughan, 2020; Canca, 2020; Sandvik, 2020; Jahnel et al., 2020). Through such digital tools, tracing should become faster, cheaper and more accurate. Through DCT it is much easier to identify infection suspects and to contact them if it becomes necessary (Ferretti et al., 2020).

Given these advantages, at first glance it seems incomprehensible that contact tracing apps, once available, have turned out — from a public health perspective[16] — to be basically a flop (Abboud & Miller, 2020; Rosenbach & Schmergal, 2020; Müller-Török & Prosser, 2020).[17] At the time of writing, about 50 national governments have released contact tracing apps, yet the adoption rates around the world are very low, well below the threshold necessary for effective tracking (Rivero, 2020; Yee, 2020). Worldwide, presently about 20% of the population has downloaded the app, which therefore serves very little purpose (Gardner, 2020; Guerrera, 2020).

Sometimes the apps were released too late, but the main reason for this reluctance can be traced back to the ambiguity between the medical and policing usage of contact tracing apps. As the heated debate about digital tracing systems shows, controversies and resistance are not so much about the medical aspect (although it is far from unproblematic) but mainly about the aspect — or suspicion — of police surveillance (Singer, 2020; Fährmann & Arzt, 2020). DCT apps, developed to manage the medical emergency and avoid overburdening hospitals, are observed and criticized mainly in view of their possible (future) use for the control of people in contexts of policing (e.g. Bock et al., 2020; Parker et al., 2020; Jahnel et al., 2020). While in previous exchanges of forecasting tools between public health and public safety the possible intermingling between the two areas had gone fundamentally unnoticed, in DCT the proximity between the fields becomes much more evident, focusing attention on possible policing activity and overshadowing the medical relevance of the tool.

We argue that the broad rejection of the app is linked particularly to this shift of focus, which also explains the different reaction of the public towards other tracking practices: in fact, the same citizens who refuse to download the DCT app that can be valuable to protect

16. From a data security perspective, for example, the German contract tracing app is conceived as success (e.g. Dix, 2020).

17. In France, according to Oliver Blazy, a computer science professor at the University of Limoges, "adoption has been derisory and the results are ridiculous. There were more people involved in the creation of the app than people who have benefited from it." https://www.ft.com/content/255567d5-b7ec-4fbe-b8a9-833b3a23f665.

everyone's health often have many other tracing tools on their mobile phone, from Fitbit to Pokémon GO — in addition to various location-based services and the trackers installed all over the Internet (Crocker et al., 2020; Morrison 2020a). As long as the data are collected by private companies, however, the impression that they can flow into a surveillance network impinging on citizens' privacy is less strong — even if countless studies have been warning about this for some time (most recently Zuboff, 2019). On the other hand, worries arise immediately if the tracking is attributed to a public body — i.e. if a possible mix between data collection for medical purposes and policing activity is perceived (Sloane & Fox Cahn, 2020; Morrison, 2020b; Jahnel et al., 2020). To illustrate our claim, in the following pages we present and analyze the history of the development and spread of the Corona-Warn-App in Germany, which enables us to observe the social dynamics at stake in more detail.

At the beginning of the pandemic, the main political mantra in Germany to inhibit the spread of COVID-19 was minimizing physical interaction with others, that is, staying home as much as possible, reducing physical encounters with others to a minimum: "The aim is to slow down the virus on its way through Germany. And in doing so, we have to rely on one thing, which is existential: to shut down public life as much as possible" (Merkel, 2020). Over time, however, a growing desire to fine-tune this regulation emerged, completely restricting social interaction only for those people who are a risk to others or who are particularly at risk (e.g. Kekulé, 2020; Otto, 2020). To achieve this balance between isolation and social interaction, the German government commissioned the development of a contact tracing app. By tracing the movements of smartphone users and integrating infection-related information, the aim of the tool was to make it possible to identify individuals who had been in direct contact with infected persons, in order to test, treat and/or quarantine them in a timely manner (e.g. Braun & Spahn, 2020; Jahnel et al., 2020).

The German government initially supported a software architecture in which individual contact data and data about COVID-19 infections were matched on a central server. This commitment was strongly criticized by technologists and civil society groups (for example in an open letter: FIfF, 2020), who favored a decentralized solution. These groups identified several types of risks associated with different types of "attackers", such as suppliers, programmers, private firms, political decision makers, or state authorities (Bock et al., 2020).

In mid-April 2020, the German government announced its support to the multi-stakeholder initiative PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing),[18] which started to develop a technological infrastructure to be used for different European contact tracing apps (Bundesregierung, 2020). Shortly afterwards, the German government revised its initial option for a centralized architecture and commissioned the technology firms SAP and Deutsche Telekom for the development of a German contact tracing app based on a decentralized concept. Most influential for this decision was apparently the announcements of Google and Apple that the technical specifications of the operating systems on their smartphones would only allow decentralized contact tracing (e.g. Buermeyer, 2020; Nicas & Wakabayashi, 2020; Dix, 2020). At a similar point in time, a privacy-preserving (PP) design was opted for by many other European nations as well, such as Austria, Latvia, Estonia, Finland and Ireland (Criddle & Kelion, 2020).

The controversy around the Corona-Warn-App in Germany discloses, first of all, a significant aspect of the general debate about DCT apps: it was rarely debated whether these tools would make accurate predictions to combat the spread of the virus. This is surprising, as

18. See https://www.pepp-pt.org/

the question of medical effectiveness remains open (Jahnel et al., 2020; Gardner, 2020). The adopted protocol uses Bluetooth Low Energy to track and log encounters among people without enabling governments to know who has infected whom and where the individuals have been. However, it is not certain that Bluetooth signals can detect proximity with the necessary accuracy (6-feet) (Laaff, 2020).

The app needs to avoid both false positives, which would produce an unjustified alarm, and false negatives, which would question the reliability of the technology and make the whole effort ineffective (Jahnel et al., 2020). But Bluetooth signals can travel through physical boundaries and send a (false positive) notification to people who were separated by walls or were sitting in nearby cars stopped in traffic jams — or were wearing protective equipment (e.g. Howell O'Neill, 2020; Laaff, 2020). At the same time, the system does not send signals when a person further than six feet away coughs or sneezes, or when the carrier stays in a closed environment for a long time — the result: false negatives yielding a misdirected sense of safety (e.g. Fussell & Knight, 2020).

The biggest risk for the effectiveness of the app, however, is statistical: if the device is not adopted by a sufficient number of individuals[19] or if the phone or the Bluetooth is turned off, the protection does not work (e.g., Müller-Török & Prosser, 2020). This is what is currently happening — due to considerations that are not based on any lack of confidence in the medical effectiveness of contagion prevention, but instead on doubts about the future use of the apps for police surveillance (Jahnel et al., 2020). For the app to work effectively, it is also necessary for individuals tested positive to give their permission to be entered into the system, activating the process that leads to reporting the risk of infection to people who have been in contact with them. In many cases, users refuse permission, presumably due to data privacy concerns (Boeri & Perotti, 2020).[20] Above all, moreover, a massive health support system is needed to coordinate post-reporting activities: contact with doctors, booking tests, organization of isolation, and many other issues that require major investment and political decisions (Luna, 2020).

It is far from obvious, therefore, that DCT is effective in protecting from the virus. Critics of the Corona-Warn-App, however, do not fear primarily that the tool might not work well, but rather that it could work *too well*, according to the interests of domains other than public health (e.g. Bock et al., 2020; FIfF, 2020). Recent news reported that Bavarian police officers, in at least two cases, confiscated COVID-19-related guest lists from restaurants for their investigations (Fuchs, 2020)[21] — with the responsible minister of the interior seeing no problem with this: "Our citizens rightly expect the police to do everything legally possible to protect and solve crimes. In this respect, I do not understand the criticism." (Herrmann as cited in Osel, 2020). Police forces in Hamburg (Meyer, 2020), Bremen (Randt, 2020), Rhineland-Palatinate (Zahn & Ludwig, 2020) and Hesse (Bebenburg, 2020) are also confronted with accusations of having illegally used guest lists from local restaurants for investigation purposes (see also Fährmann & Arzt, 2020).

19. Medical indications are controversial and range from 60% to 15% — in any case, percentages higher than the current numbers regarding app adoption.

20. In Germany, 57% of the users gave the authorization (RKI, 2020b), compared to a much smaller number in Italy (Boeri & Perotti, 2020) — one of the differences on which the lower effectiveness of tracing in Italy seems to depend.

21. According to the Corona Protection Ordinance, restaurants are required to keep guest lists — including contact details — in order to enable effective contact tracing (e.g. Suliak, 2020). The utilization of pandemic-related data by the police has also been discussed in other international examples: see, for example, Morrison (2020b) on the alarm raised by the Minnesota Department of Public Safety declaring that law enforcement was using contact tracing on arrested protesters.

In Germany as elsewhere, the protection of privacy has been the focus of attention and debate from the outset. The possibility of location tracing via GPS was immediately discarded in favor of proximity tracing systems adopting decentralized protocols, in which the central reporting server never has access to contact logs and is not responsible for processing information (Beerheide & Krüger-Brand, 2020). Again, to protect privacy, data are stored in the user's device, encrypted with anonymized keys changing every 15 minutes, and encounters are recorded in anonymized format (RKI, 2020a). But above all, the entire program is voluntary. The option to make the download of the DCT app mandatory has always been fiercely rejected by all governments, to the point where the voluntary nature of the tool can be observed as a real dogma in public debate (Dachwitz, 2020; Müller, 2020; Neuerer, 2020; Dix, 2020). As Canca (2020) argues, however, population-wide mandatory use of privacy-preserving DCT apps could be considerably more efficient than the current solutions — but apparently cannot be taken into account seriously (see also Parker et al., 2020).

The proximity to and possible intermingling with the field of public safety has deeply affected the observation and development of tools to deal with the pandemic in the medical field, even discarding some structural differences between the two sectors. The most evident is the form of the contagion. As we have seen above, contagion curves can be S-shaped, with a plateau and the permanence of the "viral" condition, or be shaped as an inverted V, when people heal and the infection is reduced and eventually disappears. Epidemics have the second form: the disease transmitted by a virus like COVID-19 should progressively disappear from the population. Public safety surveillance, on the other hand, deals with infections with an S form, since there is no reason to think that the spread of criminal behavior, once set in motion, will tend to recede.

One of the most widespread concerns regarding the adoption of DCT apps is the fear that tracking, once adopted, will be maintained even after the end of the medical emergency, confirming a trend of policing measures in many cases (Bock et al., 2020; Morrison, 2020a; Parker et al., 2020).[22] By promising an expiration date for their apps, Apple and Google have addressed a chief concern for privacy advocates. But the permanence of surveillance would only make sense for crime prevention in the field of public safety, not for the protection against the virus in the medical field. The debate around DTC, apparently centered on medical care, revolves around the risks of an S-shaped contagion, referring to policing issues instead.

These issues — among others — have shaped the adoption and use of the Corona-Warn-App in Germany. At the time of writing, around 22% of the German population have downloaded the app, with no information available on its actual use (RKI, 2020b; Jahnel et al., 2020). The proximity to and possible future intermingling with public safety has deeply affected the development and observation of prediction tools to deal with the pandemic in the field of public health. Worries about police surveillance supersede the debate about the possible advantages of medical surveillance.

6 Conclusions

The pandemic of prediction has remarkable features. Rather than an epicenter from which contagion predictions spread through society, we observe a circular movement of predictive tools between two domains of society: public health and public safety (see Table 1). This ex-

22. For example, measures such as those included in the USA PATRIOT Act in the aftermath of 9/11, which has been continuously renewed several times in the last years (Sloane & Fox Cahn, 2020).

change dynamic leads to a number of consequences for the areas involved, as well as for the evolution of prediction practices in the digital society.

Phase	Element of Prediction	Direction of Movement	Exemplary Case
Past	Epidemic models	From public health to public safety	Strategic Subject List
Present	Analytic infrastructures	From public safety to public health	Palantir and NHS
Future	Digital contact tracing	From public health to public safety?	Corona-Warn-App

Table 1: Three waves in the movement of prediction tools

In general, the pandemic has led to a huge spread of digital tools and related skills, due to the lockdown and the transfer of many practices to online channels. This digital traffic produces a huge amount of data and metadata, which can also be collected and used for purposes that have nothing to do with the medical emergency. In this context, the urgency of risk prevention has generated previously unthinkable forecasting possibilities, aimed primarily at the medical field. Given the intrinsic connection between being-at-risk and being-a-risk, however, medical forecasting indirectly produces unprecedented possibilities of criminal forecasting, while law enforcement surveillance tools can help to control the spread of contagion. The circuit of exchange of predictive tools between the spheres of public health and public safety is evidence of their affinity and of possible intermingling.

Beyond the technical issues, the circulation of the tools that we have illustrated in the previous pages highlights complex dynamics of legitimation and delegitimation. On the one hand, controversial companies such as Palantir take advantage of the urgency of the emergency to try to frame their activities as being in the public interest — a legitimation that could persist even outside the field of health care. On the other hand, however, the widespread distrust of police control tends to extend to all digital surveillance practices — also to Decentralized Privacy-Preserving Proximity Tracing tools in the field of heath care, which cryptographers and security experts do not consider more dangerous than many other devices used every day (Greenberg, 2020). The suspicion of police surveillance is so widespread that it hinders app downloads, jeopardizing the effectiveness of medical surveillance. Both effects have obvious disadvantages. A clear separation between areas, accesses and expertise, enabling a more balanced and transparent risk assessment,[23] should be one of the priorities of post-emergency regulation — with special reference to predictive technologies.

23. For a recent discussion between the complicated relationships between transparency and accountability, see Heimstädt & Dobusch (2020).

References

Abboud, L., & Miller, J. (2020). French Give Cool Reception to Covid-19 Contact-Tracing App. *Financial Times*, June 23. https://www.ft.com/content/255567d5-b7ec-4fbe-b8a9-833b3a23f665

Akers, T.A. & Lanier, M.M. (2009). "Epidemiological Criminology": Coming Full Circle. *American Journal of Public Health*, *99*(3), 397–402. https://doi.org/10.2105/AJPH.2008.139808

Akers, T.A., Potter, R.H. & Hill, C.V. (2013). *Epidemiological Criminology. A Public Health Approach to Crime and Violence*. San Francisco: Jossey-Bass.

Artan, Y., Haider, M.A., Langer, D.L., van der Kwast, T.H., Evans, A.J., Yang, Y., Wernick, M.N., Trachtenberg, J., & Yetik, I.S. (2010). Prostate Cancer Localization with Multispectral MRI Using Cost-Sensitive Support Vector Machines and Conditional Random Fields. *IEEE Transactions on Image Processing*, *19*(9), 2444–2455. https://doi.org/10.1109/TIP.2010.2048612

Bebenburg, P. (2020). Datenschützer in Sorge: Polizei in Hessen greift auf Corona-Listen aus Restaurants zu. *Frankfurter Rundschau*, July 25. https://www.fr.de/rhein-main/corona-hessen-polizei-gaestelisten-restaurant-bar-straftaten-datenschutz-13843569.html

Beerheide, R., & Krüger-Brand, H.E. (2020). Corona-Warn-App: Neustart mit dezentraler Lösung. *Deutsches Ärzteblatt*, *117*(19), A979–A981. https://www.aerzteblatt.de/archiv/213861/Corona-Warn-App-Neustart-mit-dezentraler-Loesung

BKA (2017). Presseinformation: Neues Instrument zur Risikobewertung von potentiellen Gewaltstraftätern. *Online Document*, February 2. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/170202_Radar.html

Bock, K., Kühne, C.R., Mühlhoff, R., Ost, M.R., Pohle, J., & Rehak, R. (2020). Data Protection Impact Assessment for the Corona App. *Preprint*. https://dx.doi.org/10.2139/ssrn.3588172

Böckler, N., Allwinn, M., Hoffmann, J., Zick, A. (2017). Früherkennung von islamistisch motivierter Radikalität. *Kriminalistik*, *71*(8–9), 497–503.

Boeri, T., & Perotti, R. (2020). È nato con tre errori. Il nuovo call center non salverà Immuni. *La Repubblica*, November 1. https://rep.repubblica.it/pwa/generale/2020/10/31/news/e_nato_con_tre_errori_il_nuovo_call_center_non_salvera_immuni-272578269/

Braun, H., & Spahn, J. (2020). Erklärung von Kanzleramtsminister Helge Braun und Bundesgesundheitsminister Jens Spahn zur Tracing-App. *Online Document*, April 26. https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/2020/2-quartal/tracing-app.html

Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, *82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Brown, J. (2019). How is the Government Implementing a "Public Health Approach" to Serious Violence? *House of Commons Library*, July 22. https://commonslibrary.parliament.

uk/home-affairs/crime/how-is-the-government-implementing-a-public-health-approach-to-serious-violence/

Bryant, K.M. (2014). Chicago School of Criminology. In J. Mitchell Miller (ed.), *The Encyclopedia of Theoretical Criminology*. Chichester: Wiley-Blackwell. https://doi.org/10.1002/9781118517390.wbetc186

Buermeyer, U. (2020). Google und Apple haben Bundesregierung Weg gewiesen. Interview by Jörg Münchenberg for *Deutschlandfunk*, April 27. https://www.deutschlandfunk.de/datenschutzexperte-zur-corona-app-google-und-apple-haben.694.de.html

Bundesregierung (2020). Kontaktketten digital identifizieren. *Online Document*, April 6. https://www.bundesregierung.de/breg-de/themen/coronavirus/corona-app-1738516.

Butchart, A., & Emmett, T. (2000). Crime, Violence and Public Health. In T. Emmett & A. Butchart (Eds.), *Behind the Mask. Getting to Grips with Crime and Violence in South Africa* (pp. 3–28). Pretoria: HSRC Press.

Canca, C. (2020). Why "Mandatory Privacy-Preserving Digital Contact Tracing" is the Ethical Measure against COVID-19. *Medium*, April 10. https://medium.com/@cansucanca/why-mandatory-privacy-preserving-digital-contact-tracing-is-the-ethical-measure-against-covid-19-a0d143b7c3b6

Chapman, L. (2020). Palantir's New "Driving Thrust": Predicting Coronavirus Outbreaks. *Bloomberg News*, April 2. https://www.bloomberg.com/news/articles/2020-04-02/coronavirus-news-palantir-gives-away-data-mining-tools

Chiusi, F. (2020). Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective. *Algorithm Watch. Automating Society Report 2020*. https://algorithmwatch.org/en/project/automating-society-2020-covid19/

Cohen, G., & Graver H.S. (2017). Cops, Docs, and Code: A Dialogue Between Big Data in Health Care and Predictive Policing. *UCDL Rev*, *51*, 437–474. https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Cohen_Graver.pdf

Cressey, D.R. (1960). Epidemiology and Individual Conduct: A Case from Criminology. *The Pacific Sociological Review*, *3*(2), 47–58. https://doi.org/10.2307/1388200

Criddle, C., & Kelion, L. (2020). Coronavirus Contact-Tracing: World Split Between Two Types of App. *BBC News*, May 7. https://www.bbc.com/news/technology-52355028

Crocker, A., Opsahl, K., & Cyphers, B. (2020). The Challenge of Proximity Apps For COVID-19 Contact Tracing. *Electronic Frontier Foundation*, April 10. https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

Dachwitz, I. (2020). Grüne legen Gesetzentwurf für Corona-Warn-App vor. *Netzpolitik.org*, June 17. https://netzpolitik.org/2020/gruene-legen-gesetzentwurf-fuer-corona-warn-app-vor/

Deutscher Bundestag (2017). Instrument des Bundeskriminalamtes zur Risikobewertung potentieller islamistischer Gewalttäter. *Drucksache 18/13422*, July 28. https://dip21.bundestag.de/dip21/btd/18/134/1813422.pdf

Dix, A. (2020). Die deutsche Corona Warn-App — ein gelungenes Beispiel für Privacy by Design? *Datenschutz und Datensicherheit*, *44*(12), 779–785. https://doi.org/10.1007/s11623-020-1366-1

Egbert, S. (2019). Predictive Policing and the Platformization of Police Work. *Surveillance & Society*, *17*(1/2), 83–88. https://doi.org/10.24908/ss.v17i1/2.12920

Egbert, S., & Krasmann, S. (2019). Predictive Policing: Not Yet, but Soon Preemptive? *Policing and Society*, *0*(0), 1–15. https://doi.org/10.1080/10439463.2019.1611821

Egbert, S., & Leese, M. (2021). *Criminal Futures: Predictive Policing and Everyday Police Work*. Abingdon: Routledge.

Esposito, E. (2020). Unpredictability. In N.B. Thylstrup, D. Agostinho, A. Ring, C. D'Ignazio & K. Veel (Eds.), *Uncertain Archives* (pp. 533–540). Cambridge: MIT Press.

Ewald, F. (1991). Insurance and Risk. In G. Burchell, C. Gordon & P. Miller (Eds.), *The Foucault Effect* (pp. 197–210). Chicago: University of Chicago Press.

Faye, M. (2016). Cogent Calculations. *IIT Magazine*, Fall 2016, 13–15. https://magazine.iit.edu/fall-2016/cogent-calculations

Fährmann, J., & Arzt, C. (2020). Polizeilicher Umgang mit personenbezogenen Daten in der Corona-Pandemie. *Datenschutz und Datensicherheit*, *44*(12), 801–805. https://doi.org/10.1007/s11623-020-1370-5

Ferguson, A.G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., & Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, *368*(6491), eabb6936. https://doi.org/10.1126/science.abb6936

Fink, R. (2020). In Crisis Response, Answer the Simple Questions First. *Palantir Blog*, March 30. https://medium.com/palantir/in-crisis-response-answer-the-simple-questions-first-a7f04da9e786

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) (2020). Offener Brief: Geplante Corona-App ist höchst problematisch. *Online Document*, April 24. https://www.fiff.de/presse/coronaappproblematisch

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. New York: Random House.

Fourcade, M., & Healy, K. (2017). Seeing like a Market. *Socio-Economic Review*, *15*(1), 9–29. https://doi.org/10.1093/ser/mww033

French, M., & Monahan, T. (2020). Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19? *Surveillance & Society*, *18*(1), 1–11. https://doi.org/10.24908/ss.v18i1.13985

Fuchs, F. (2020). Polizei nutzt Corona-Gästelisten für Ermittlungen. *Süddeutsche Zeitung*, July 15. https://www.sueddeutsche.de/bayern/bayern-polizei-gaestelisten-corona-1.4966622

Fussell, S., & Knight, W. (2020). The Apple-Google Contact Tracing Plan Won't Stop Covid Alone. *Wired*, April 14. https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone/

Gardner, A. (2020). Contact-tracing apps: there's no evidence they're helping stop COVID-19. *The Conversation*, October 21. https://theconversation.com/contact-tracing-apps-theres-no-evidence-theyre-helping-stop-covid-19-148397

Gentithes, M., & Krent, H.J. (2020). Pandemic Surveillance. The New Predictive Policing. *Constitutional Law*, *12*(1), 57–74. https://ssrn.com/abstract=3681962

Gould, M., Joshi, I., & Tang, M. (2020). The Power of Data in a Pandemic. *Technology in the NHS Blog*, March 28. https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/

Green, B., Horel, T., & Papachristos, A.V. (2017). Modeling Contagion Through Social Networks to Explain and Predict Gunshot Violence in Chicago, 2006 to 2014. *JAMA Internal Medicine*, *177*(3), 326–333. https://doi.org/10.1001/jamainternmed.2016.8245

Greenberg, A. (2020). Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered, *Wired*, April 17. https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/

Guerrera, A. (2020). Difetti Tecnici e Dubbi Sulla Privacy. Le App Contro il Covid Sono un Flop. *La Repubblica*, June 25. https://rep.repubblica.it/pwa/generale/2020/06/24/news/dal_giappone_alla_francia_difetti_tecnici_e_dubbi_sulla_privacy_le_app_contro_il_virus_sono_un_flop-260103367/

Hardy, Q. (2014). Unlocking Secrets, if Not Its Own Value. *The New York Times*, June 1. https://www.nytimes.com/2014/06/01/business/unlocking-secrets-if-not-its-own-value.html

Heimstädt, M., & Dobusch, L. (2020). Transparency and Accountability: Causal, Critical and Constructive Perspectives. *Organization Theory*, *1*(4). https://doi.org/10.1177/2631787720964216

Hollywood, J.S. (2016). CPD's "Heat List" and the Dilemma of Predictive Policing. *Crain's Chicago Business*, September 19. https://www.rand.org/blog/2016/09/cpds-heat-list-and-the-dilemma-of-predictive-policing.html

Howell O'Neill, P. (2020). Bluetooth Contact Tracing Needs Bigger, Better Data. *MIT Technology Review*, April 22. https://www.technologyreview.com/2020/04/22/1000353/bluetooth-contact-tracing-needs-bigger-better-data/

IIT (Illinois Institute of Technology) (2019). Crime and Victimization Model. *Online Document*, n.d.. https://home.chicagopolice.org/wp-content/uploads/2019/01/FACT-SHEET-Crime-and-Victimization-Risk-Model-1.pdf

Jahnel, T., Gerhardus, A., & Wienert, J. (2020). Digitales Contact Tracing: Dilemma zwischen Datenschutz und Public Health Nutzenbewertung. *Datenschutz und Datensicherheit*, *44*(12), 786–790. https://doi.org/10.1007/s11623-020-1367-0

Johnson, G.F. (2015). Special Order S10-05: Customs Notifications in Chicago. *Online Document*, October 6. http://directives.chicagopolice.org/directives/data/a7a57bf0-1456faf9-bfa14-570a-a2deebf33c56ae59.html

Johnson, G.F. (2019). Special Order S09-11: Subject Assessment and Information Dashboard (SAID), Strategic Subject List (SSL) Dashboard. *Online Document*, July 9. http://directives.chicagopolice.org/directives/data/a7a57b85-155e9f4b-50c15-5e9f-7742e3ac8b0ab2d3.html

Kaufmann, M., Egbert, S., & Leese, M. (2019). Predictive Policing and the Politics of Patterns. *British Journal of Criminology*, *59*(3), 674–692. https://doi.org/10.1093/bjc/azy060

Kekulé, A. (2020). Wege aus dem Lockdown. *Zeit Online*, March 26. https://www.zeit.de/wissen/gesundheit/2020-03/coronavirus-quarantaene-lockdown-ausgangssperre-alternative-pandemie-alexander-kekule

Kitchin, R. (2020). Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19. *Space and Polity*. https://doi.org/10.1080/13562576.2020.1770587

Knight, E., & Gekker, A. (2020). Mapping Interfacial Regimes of Control: A Qualitative Analysis of America's Post-9/11 Security Technology Infrastructure. *Surveillance & Society*, *18*(2), 231–243. https://doi.org/10.24908/ss.v18i2.13268

Kucharski, A. (2020). *The Rules of Contagion. Why Things Spread — and Why They Stop*. London: Profile Books.

Kump, P., Alonso, D.H., Yang, Y., Candella, J., Lewin, J., & Wernick M.N. (2016). Measurement of Repeat Effects in Chicago's Social Network. *Applied Computing and Informatics*, *12*(2), 154–160. https://doi.org/10.1016/j.aci.2016.01.002

Laaff, M. (2020). Moment, wie viel Infizierte soll ich getroffen haben? *Zeit Online*, October 8. https://www.zeit.de/digital/mobil/2020-10/corona-warn-app-infektion-kontakte-warnungen-smartphone

Lammerant, H., & de Hert, P. (2016). Predictive Profiling and its Legal Limits: Effectiveness Gone Forever. In B. van der Sloot, D. Broeders, & E. Schrijvers (Eds.), *Exploring the Boundaries of Big Data* (pp. 145–173). Amsterdam: Amsterdam University Press.

Leszczynski, A., & Zook, M. (2020). Viral Data. *Big Data & Society*, *7*(2), 1–5. https://doi.org/10.1177/2053951720971009

Lewis, P., Conn, D., & Pegg, D. (2020). UK Government Using Confidential Patient Data in Coronavirus Response. *The Guardian*, April 12. https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response

Lipari, J.L. (2020). Advisory Concerning the Chicago Police Department's Predictive Risk Models. *Report of the Public Safety Section of The Office of Inspector General*, January 23.

https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf

Luhmann, N. (1991). *Soziologie des Risikos*. Berlin-New York: de Gruyter.

Luhmann, N. (1997). *Die Gesellschaft der Gesellschaft*. Frankfurt a.M.: Suhrkamp.

Lum, K., & Isaac, W. (2016). To Predict and Serve? *Significance*, *13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Luna, R. (2020). Vespignani "Immuni non va. Deve diventare un'app utile e aiutarci a fare subito il test." *La Repubblica*, October 20. https://www.repubblica.it/cronaca/2020/10/20/news/vespignani_immuni_non_va_deve_diventare_un_app_utile_e_aiutarci_a_fare_subito_il_test_-271175941/

McCarthy, G.F. (2015). Custom Notifications in Chicago. Special Order S10-05. *Chicago Police Department*, October 6. http://directives.chicagopolice.org/directives/data/a7a57bfo-1456faf9-bfa14-570a-a2deebf33c56ae59.html

Merkel, A. (2020). *Fernsehansprache von Bundeskanzlerin Angela Merkel*. Online Document, March 18. https://www.bundesregierung.de/resource/blob/975232/1732182/d4af29ba76f62f61f1320c32d39a7383/fernsehansprache-von-bundeskanzlerin-angela-merkel-data.pdf

Meyer, P.U. (2020). Vorwurf: Hamburger Polizei missbraucht Corona-Gästelisten. *Hamburger Abendblatt*, August 2. https://www.abendblatt.de/hamburg/kommunales/article229986006/Restaurants-Gaestelisten-Polizei-Hamburg-Allgemeinverordnung-Corona-Virus-Datenschutz-Missbrauch-Datenklau.html

Moore, M.H. (1995). Public Health and Criminal Justice Approaches to Prevention. *Crime and Justice*, *19*, 237–262. https://doi.org/10.1086/449232

Morrison, S. (2020a). Apple and Google Look Like Problematic Heroes in the Pandemic. *Vox*, April 16. https://www.vox.com/recode/2020/4/16/21221458/apple-google-contact-tracing-app-coronavirus-covid-privacy

Morrison, S. (2020b). Minnesota Law Enforcement Isn't "Contact Tracing" Protesters, Despite an Official's Comment. *Vox*, June 1. https://www.vox.com/recode/2020/6/1/21277393/minnesota-protesters-contact-tracing-covid-19

Müller, K. (2020). Corona-Warn-App: "Aus Freiwilligkeit darf kein Zwang werden". *Verbraucherzentrale Bundesverband*, June 15. https://www.vzbv.de/pressemitteilung/corona-warn-app-aus-freiwilligkeit-darf-kein-zwang-werden

Müller-Török, R., & Prosser, A. (2020). It's the Statistics, Stupid! *Behörden Spiegel*, *36*(9), 30. https://www.hs-ludwigsburg.de/fileadmin/user_upload/200902_BehoerdenSpiegel_Corona-Warn-App.pdf

Nature (2020). Editorial: Show Evidence that Apps for COVID-19 Contact-Tracing are Secure and Effective. *Nature*, *580*, 563. https://doi.org/10.1038/d41586-020-01264-1

Neuerer, D. (2020). Verbraucherschützer zweifeln an der Freiwilligkeit der Corona-App. *Handelsblatt*, June 16. https://www.handelsblatt.com/politik/international/warn-app-verbraucherschuetzer-zweifeln-an-der-freiwilligkeit-der-corona-app/25918552.html

Nicas, J., & Wakabayashi, D. (*2020).* Apple and Google Team Up to "Contact Trace" the Coronavirus. *The New York Times*, April 10. https://www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html

NIJ (National Institute of Justice) (2011). Chicago Police Predictive Policing Demonstration and Evaluation Project: Phase 2. Funding & Awards. *NIJ Website*, September 11. https://nij.ojp.gov/funding/awards/2011-ij-cx-k014

O'Malley, D. (2020). *CPD's Response to OIG Advisory Concerning Predictive Risk Models*. Online Document, January 7. https://igchicago.org/wp-content/uploads/2020/01/CPD-Response-to-OIG-Advisory-on-Predictive-Risk-Models.pdf

Osel, J. (2020). Innenminister Herrmann verteidigt Corona-Gästelisten. *Süddeutsche Zeitung*, July 19. https://www.sueddeutsche.de/bayern/corona-bayern-gaestelisten-polizei-herrmann-1.4971971

Otto, F. (2020). Aus dem Lockdown gedrängt. *Zeit Online*, May 6. https://www.zeit.de/politik/deutschland/2020-05/coronakrise-lockerungen-beschluesse-bund-laender-gipfel-angela-merkel

Palantir (2012). Palantir 101. *Palantir's Youtube Channel*, August 31. https://youtu.be/e6OebModQ8g

Palantir (2013). Palantir at the Los Angeles Police Department. *Palantir's Youtube Channel*, January 25. https://youtu.be/aJ-u7yDwC6g

Palantir (2014). Bringing Order to Chaos with Team Rubicon in the Wake of Hurricane Sandy [Part II]. *Palantir's Youtube Channel*, April 14. https://youtu.be/V38JzJ10Mms

Parker, M.J., Fraser, C., Abeler-Dörner, L., & Bonsall, D. (2020). Ethics of Instantaneous Contact Tracing Using Mobile Phone Apps in the Control of the COVID-19 Pandemic. *Journal of Medical Ethics*, *46*(7), 427–431. https://doi.org/10.1136/medethics-2020-106314

Papachristos, A.V., Wildeman, C., & Roberto, E. (2015). Tragic, but not Random: The Social Contagion of Nonfatal Gunshot Injuries. *Social Science & Medicine*, *125*, 139–150. https://doi.org/10.1016/j.socscimed.2014.01.056

Papachristos, A.V., Braga, A., & Hureau, D. (2012). Social Networks and the Risk of Gunshot Injury. *Journal of Urban Health*, *89*(6), 992–1003. https://doi.org/10.1007/s11524-012-9703-9

Randt, J. (2020). Bremer Polizei nutzt Gastronomie-Gästelisten. *Weser Kurier*, August 1. https://www.weser-kurier.de/bremen/bremen-stadt_artikel,-bremer-polizei-nutzt-gastronomiegaestelisten-_arid,1926295.html

Rayport, J. (1996). The Virus of Marketing. *Fast Company*, December 31. https://www.fastcompany.com/27701/virus-marketing

Reingle Gonzalez, J.M. (2015). Epidemiological Criminology. In W.G. Jennings (Ed.), *The Encyclopedia of Crime and Punishment*. Chichester: Wiley-Blackwell.

Rivero, N. (2020). Global Contact Tracing App Downloads Lag Behind Effective Levels. *Quartz*, July 15. https://qz.com/1880457/global-contact-tracing-app-downloads-lag-behind-effective-levels/

RKI (Robert-Koch-Institut) (2020a). *So funktioniert die Corona-Warn-App im Detail*. Online Document, July 21. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Funktion_Detail.pdf

RKI (Robert-Koch-Institut) (2020b). *Kennzahlen zur Corona-Warn-App*. Online Document, November 12. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_13112020.pdf?__blob=publicationFile

Rosenbach, M., & Schmergal, C. (2020). Viel Aufwand, wenig Nutzen. *Spiegel Online*, September 18. https://www.spiegel.de/politik/deutschland/corona-warn-app-viel-aufwand-wenig-nutzen-a-00000000-0002-0001-0000-000173100112

Rushkoff, D. (1994). *Media Virus! Hidden Agendas in Popular Culture*. New York: Ballantine Books.

Sandvik, K.B. (2020). "Smittestopp": If you want your freedom back, download now. *Big Data & Society*, *7*(2), 1–11. https://doi.org/10.1177/2053951720939985

Saunders, J., Hunt, P., & Hollywood, J.S. (2016). Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot. *Journal of Experimental Criminology*, *12*(3), 347–371. https://doi.org/10.1007/s11292-016-9272-0

Scheffer, T., Howe C., Kiefer E., Negnal D., & Porsché, Y. (2017). *Polizeilicher Kommunitarisms. Eine Praxisforschung urbaner Kriminalprävention*. Frankfurt: Campus.

Singer, N. (2020). Virus-Tracing Apps Are Rife with Problems. Governments Are Rushing to Fix Them. *The New York Times*, July 8. https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html

Sloane, M., & Fox Cahn A. (2020). Today's COVID-19 Data Will Be Tomorrow's Tools of Oppression. *The Daily Beast*, April 1. https://www.thedailybeast.com/todays-covid-19-data-will-be-tomorrows-tools-of-oppression

Sonka, C., Meier, H., Rossegger, A., Endrass, J., Profes, V., Witt, R., Sadowski, F. (2020). RADAR-iTE 2.0: Ein Instrument des polizeilichen Staatsschutzes. *Kriminalistik*, *74*(6), 386–392.

Stark, D. (2020). Testing and Being Tested in Pandemic Times. *Sociologica*, *14*(1): 67–94. https://doi.org/10.6092/issn.1971-8853/10931

Steinberger, M. (2020). Does Palantir See Too Much? *The New York Times*, October 21. https://www.nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html

Stroud, M. (2014). The Minority Report: Chicago's New Police Computer Predicts Crimes, but is it Racist? *The Verge*, February 19. https://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist

Suliak, H. (2020). Datenschutzrechtlich völlig unklar. *Legal Tribune Online*, May 11. https://www.lto.de/recht/nachrichten/n/restaurants-gaststaetten-oeffnung-kontaktdaten-namensliste-corona-unsicherheit-nrw-niedersachsen-baden-wuerttemberg/

The Police Foundation (2019). *Public Health Approaches to Crime Prevention and the Role of the Police*. Online Document, January. http://www.police-foundation.org.uk/2017/wp-

content/uploads/2019/08/Public-health-approaches-to-crime-prevention-and-the-role-of-the-police-FINAL-PUBLISHED.pdf

Thiel, P., & Masters, B. (2014). *Zero to One: Notes on Startups, or How to Build the Future*. New York: Random House.

Thunberg, A.M., Nowak, K., & Rosengren K.E. (1982). *Communication and Equality*. Stockholm: Almquist and Wicksell.

Vaughan, A. (2020). We Still Don't Know How Effective the NHS Contact-Tracing App Will Be. *New Scientist*, May 4. https://www.newscientist.com/article/2242609-we-still-dont-know-how-effective-the-nhs-contact-tracing-app-will-be/

Yee, W.Y. (2020). Coronavirus: More Need to Use Contact Tracing App for It to Be Effective. *The Strait Times*, May 1. https://www.straitstimes.com/singapore/more-need-to-use-contact-tracing-app-for-it-to-be-effective

Waldman, P., Chapman, L., & Robertson, L. (2018). Palantir Knows Everything About You. *Bloomberg Businessweek*, April 19. https://www.bloomberg.com/features/2018-palantir-peter-thiel/

Warrell, H., & Neville, S. (2020). UK in Talks with Palantir over Test-and-Trace Programme. *Financial Times*, November 3. https://www.ft.com/content/6f6575a8-799f-42a4-b1cc-3f7452b2166f

Winston, A. (2018). Palantir has Secretly Been Using New Orleans to Test its Predictive Policing Technology. *The Verge*, February 27. https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

Zahn, M., & Ludwig, G. (2020). Polizei nutzte Corona-Kontaktdaten in Einzelfällen. *SWR Aktuell*, July 22. https://www.swr.de/swraktuell/rheinland-pfalz/polizei-darf-corona-daten-fuer-strafrechtliche-ermittlungen-nutzen-100.html

Završnik, A. (2017). Algorithmic Crime Control. In A. Završnik (Ed.), *Big Data, Crime and Social Control* (pp. 131–153). Abingdon: Routledge.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Maximilian Heimstädt: Weizenbaum Institute (Germany)
https://orcid.org/0000-0003-2786-8187
https://heimstaedt.org
Maximilian Heimstädt is head of the research group "Reorganizing Knowledge Practices" at the Berlin-based Weizenbaum Institute and an affiliated senior researcher ("Habilitand") at Witten/Herdecke University. Drawing on analytic resources from organization theory and STS, he studies new forms of organizing in digitally networked environments.

Simon Egbert: Department of Sociology, Technische Universität Berlin (Germany)
https://orcid.org/0000-0002-3729-0393
https://www.innovation.tu-berlin.de/v_menue/postdoc_undwissenschaftlicher_mitarbeiter/dr_simon_egbert
Simon Egbert is a postdoc researcher at Technische Universität Berlin, studying the social implications of (algorithmic) predictions. He completed his PhD in 2018 at Universität Hamburg, with a dissertation about the status of materiality in discourse theory, focusing empirically on drug testing devices. He is the co-author of *Criminal Futures. Predictive Policing in Everyday Police Work* (Routledge, 2021) (with Matthias Leese). His work appears in journals including *Futures, Policing and Society* and *British Journal of Criminology*.

Elena Esposito: Department of Political and Social Sciences, University of Bologna (Italy); Faculty of Sociology, Bielefeld University (Germany)
elena.esposito@uni-bielefeld.de; https://www.elena-esposito.com
Elena Esposito is Professor of Sociology at the University Bielefeld and the University of Bologna in Italy. Working in a systems theory framework, she studies problems of time in social systems, including memory and forgetting, probability, fashion and transience, fiction, and the use of time in finance. Her current research on algorithmic prediction is supported by a five-year Advanced Grant from the European Research Council.