

## Tilburg University

### Digital disruption or crisis capitalism?

Lopez Solano, Joan; Martin, Aaron; Ohai, Franklyn; de Souza, Siddharth; Taylor, Linnet

DOI:  
[10.26116/gdj-euaifund](https://doi.org/10.26116/gdj-euaifund)

Publication date:  
2022

Document Version  
Publisher's PDF, also known as Version of record

[Link to publication in Tilburg University Research Portal](#)

*Citation for published version (APA):*  
Lopez Solano, J., Martin, A., Ohai, F., de Souza, S., & Taylor, L. (2022). *Digital disruption or crisis capitalism? Technology, power and the pandemic*. <https://doi.org/10.26116/gdj-euaifund>

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# DIGITAL DISRUPTION OR CRISIS CAPITALISM?

Joan Lopez Solano  
Aaron Martin  
Franklyn Ohai  
Siddharth de Souza  
Linnet Taylor

**TECHNOLOGY, POWER AND THE PANDEMIC**

---

**A report by the Global Data Justice project**

May 2022,  
Tilburg Institute for Law, Technology, and Society



# Table of Contents

<b>Acknowledgements</b>	<b>3</b>
<b>Executive Summary</b>	<b>4</b>
<b>1. Introduction</b>	<b>6</b>
<b>2. Background</b>	<b>10</b>
<u>2.1 What kind of problem does this create?</u>	<b>11</b>
<u>2.2 Whom do we want to inform with this report?</u>	<b>12</b>
<u>2.3 Where did we investigate?</u>	<b>13</b>
<u>2.4 How did we research this?</u>	<b>14</b>
<b>3. Our findings</b>	<b>16</b>
<u>3.1 Health</u>	
<u>3.2 Education</u>	<b>22</b>
<u>3.3 Policing, security and mobility control</u>	<b>23</b>
<u>3.4 Payments</u>	<b>25</b>
<u>3.5 Identification and authentication</u>	<b>26</b>
<b>4. Naming, Blaming and Claiming: strategies for identifying and addressing sector transgressions</b>	<b>28</b>
<u>4.1 Concept map of Sector Transgressions</u>	
<u>4.1 Naming it - how to investigate</u>	<b>29</b>
<u>4.2 Blaming - establishing points of responsibility</u>	<b>30</b>
<u>4.3 Claiming</u>	<b>32</b>
<u>4.3.1 Claiming strategy 1: strategic litigation</u>	
<u>4.3.2 Claiming strategy 2: Documentation</u>	<b>36</b>
<u>4.3.3 Claiming strategy 3: Campaigns</u>	<b>38</b>
<b>5. Conclusions</b>	<b>40</b>
<b>6. Recommendations</b>	<b>42</b>
<b><u>ANNEX: the cases we use for this report</u></b>	<b>44</b>
<u>Health</u>	<b>45</b>
<u>Transport &amp; mobility</u>	<b>48</b>
<u>Employment &amp; events</u>	<b>51</b>
<u>Security</u>	<b>52</b>
<u>Payments</u>	<b>53</b>
<u>Education</u>	

# Digital disruption or crisis capitalism? Technology, power and the pandemic

---

## A report by the Global Data Justice project

Written and researched by:

Joan Lopez Solano, Aaron Martin, Franklyn Ohai,  
Siddharth de Souza, and Linnet Taylor.

## Acknowledgements

This work was conducted thanks to the European AI Fund's Tech and COVID grant programme. It took place within the Global Data Justice project, which is funded by the European Research Council (ERC StG 757247).

We would like to thank Gargi Sharma and Ana Hriscu for their research and input into the start of this project; Elena Casale and Magda Brewczyńska for help with case research; and the group of experts and activists who offered us their observations and insights during the course of the research. This report reflects many people's input, for which we are immensely grateful.

Separately from the Europe-focused project, we also initiated dialogues with civil society actors in Asia, Latin America (specifically Brazil) and East Africa (i.e. Ethiopia, Kenya and Uganda) to explore the extent to which the notion of sector transgressions resonates in other parts of the world. This comparative approach also helped us identify some of the more uniquely European characteristics of the phenomenon.

## Executive Summary

This report – commissioned by the European AI Fund as part of its research programme on Tech and COVID – addresses a critical question: **how have technology firms used the pandemic to expand their reach, change their business strategies and capture new public functions and market positions in Europe?**

While some of the fundamental shifts we identify predate the start of the public health emergency, the crisis context has amplified the encroachment of tech firms across a range of different sectors, and enabled a **rapid expansion of commercial technological power** in areas where public service provision and private-sector business models are not aligned, and in ways that current **regulatory frameworks** are **ill-equipped** to deal with.

So far, public debate in Europe has largely focused on the privacy implications of the onslaught of pandemic tech. Although privacy is a key point of leverage on technological power, it has been used strategically by firms to distract us from broader problems of domination. We argue, using the concept of **'sector transgressions'** - the involvement of commercial actors in spaces where their business models, practices and ethics are misaligned with established actors in those spaces - that we need to understand and contest the far-reaching ramifications of the increased presence and power of tech firms in all areas of public and private life.

We document how tech firms have strategised to move into the **health, education, security, transportation, payments** and **identity sectors during the pandemic**. We identify both a **supply-side** problem of opportunistic moves and a **demand-side** problem where the emergency has made possible new forms of privatisation and the delegation of key public functions.

We chart the resulting increase in **infrastructural power** on the part of firms offering cloud, connectivity and analytics services. These infrastructural changes pose real challenges in terms of preserving the public sector's accountability for the provision of public goods. This is not a privacy problem: it implicates other public goods such as self-determination, political engagement, health, education and knowledge, and ultimately the notion of publicness itself - the capacity and resilience of the public sector in relation to tasks and services that address vulnerabilities and basic needs, and therefore necessitate **democratic accountability**.

Many argue that the pandemic has sparked innovation and that this should be celebrated. A closer look, however, shows **not merely disruption of business as usual** but the **destruction of mechanisms for providing public goods**, and the **risk of genuine destabilisation of that provision**.

The combination of **accelerated privatisation** with **increased ownership of the underlying digital architectures of our societies** puts technology firms not only in control of our public policy, workplaces and homes, but in a position to charge what they wish for that dominance, or to make the functionality we rely on disappear by changing their business models.

In response to these changes, we call for a more holistic perspective on the problems of technological power, and propose ways for civil society organisations and their funders to tackle them. We offer a framework of **naming, blaming** and **claiming** to show how civil society has confronted — and can continue to reckon with — transgressions by tech firms. We offer tools for identifying sector transgressions; analysing and attributing responsibility to those causing them; and finally establishing claims through strategic litigation, documentation and campaigns to raise public awareness and to ensure accountability of tech firms.

We offer **recommendations** for how to combat this technological and infrastructural power and challenge its **legitimacy**:

- ◆ **Think beyond privacy and surveillance:** In order to contest tech firms' strategies and power accumulation, it has become necessary to go beyond arguments based on privacy or surveillance harms alone. A more holistic approach is needed that can address the broader legitimacy of firms' activities in the public sphere.
- ◆ **Use sectoral problems strategically to build public awareness of underlying ones:** The sectoral transgressions described in this report are symptoms rather than self-contained problems. Together, they indicate an underlying penetration of commercial technological power which cannot be addressed effectively by focusing on a single type of transgression or sector-specific injustice.
- ◆ **Join forces with organisations not (yet) focused on digital rights:** A holistic approach at scale requires coordination between domain-based and digital rights organisations. An important resource exists in the form of sectoral organisations (e.g. trade unions or student unions) and in other non-digitally focused rights organisations (e.g. migrants' or children's organisations). This requires resources, strategic capacity and intermediaries to help make connections.
- ◆ **Seek out funding to support collaborative work:** Strategically integrating digital rights groups' work with that of domain and interest-based organisations cannot be done without the support of funders, who play a key role in the choices civil society organisations (can) make about how to orient their work.
- ◆ **Coordinate transnationally to map the challenges:** The map of technological transgressions is multinational and diverse. The only successful strategy for challenging this power grab involves building capacity and alliances amongst civil society, regulators and legal institutions across Europe, including in countries where its manifestations may look different.

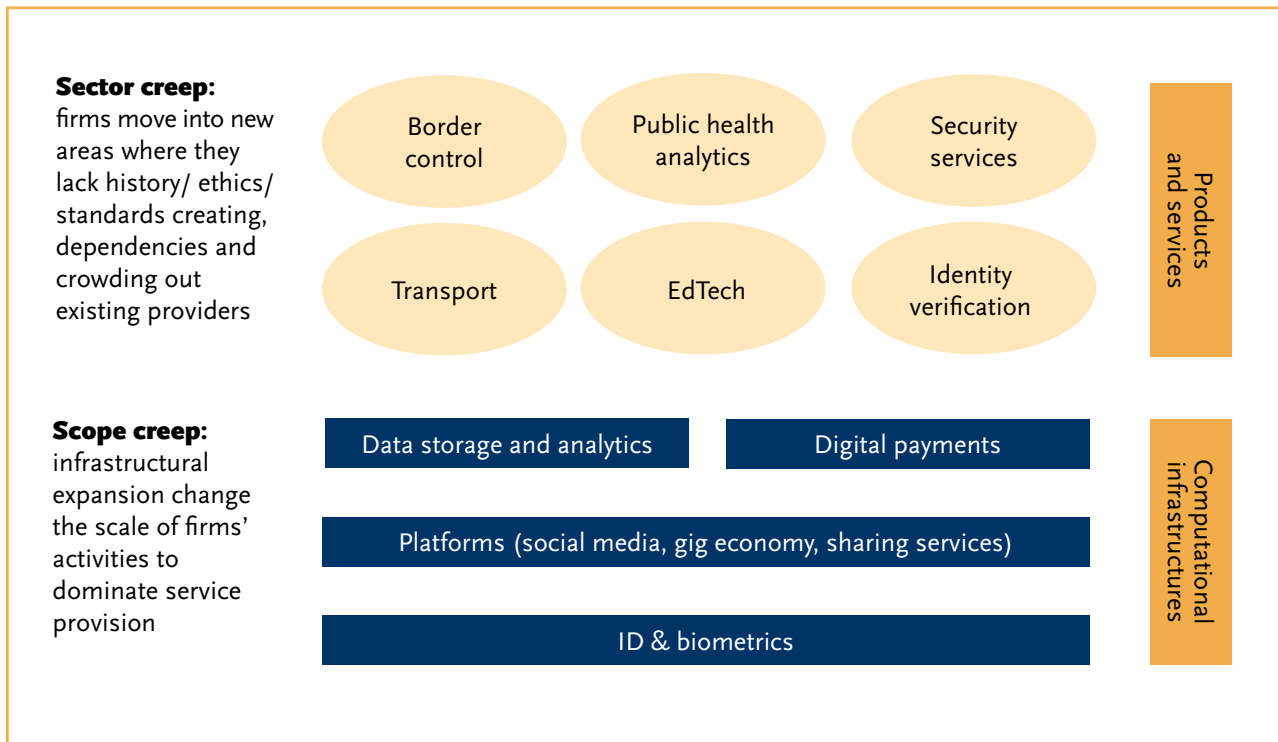
## 1. Introduction

This report examines the ways in which technology firms are using the pandemic to expand their reach, change their business strategies and capture new public functions and market positions in Europe. Not all the changes we chart here are occurring as a direct result of the pandemic—in fact, many were already in progress when it began due to investments in computing infrastructures that have been underway for a decade or more.<sup>1</sup> We aim to relate these long-running and more recent developments to each other, making sense of the changes in both underlying infrastructures and business strategies, in order to understand the implications of this rapid expansion of commercial technological power.

We assert that it matters when firms use computing power to step outside their realm of competence. The scale and reach afforded by big data and algorithms mean that deploying that power as if the nature of the task were immaterial causes harms and dysfunctions that society and politics then have to remedy. When Chris Anderson, editor of *Wired*, wrote in 2008 that ‘Google’s founding philosophy is that we don’t know why this page is better than that one: if the statistics of incoming links say it is, that’s good enough’,<sup>2</sup> we did not yet know that defining ‘good enough’ would become one of the central issues for negotiating digital rights and the power of the technology sector. Infrastructural dominance brings with it forms of ideological dominance, and the pandemic has exposed commercial technology firms’ power to define what is good, what is relevant, and what is effective in almost every area of life.

For this reason we focus on the accelerated growth of the power of technology firms during the pandemic, which in turn has increased those firms’ offering of cloud, connectivity and analytics services. These infrastructural changes pose real challenges in terms of preserving the public sector’s accountability for the provision of public goods. In this report we distinguish between pandemic-driven problems of *sector creep* and *scope creep*. In the former, technology providers extend their activities and business models into new sectors, often with transgressive effects such as ethical inadequacy, the crowding out of public sector providers and new dependencies on private sector infrastructures - hence the language in this report of ‘sector transgressions’.<sup>3</sup> In the latter, tech firms have made massive investments in the under-

- 
- ◆ 1. See, for example, this study of public education institutions’ migration toward cloud services: Fiebig, T., Gürses, S., Gañán, C. H., Kotkamp, E., Kuipers, F., Lindorfer, M., ... & Sari, T. (2021). Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds. *arXiv preprint arXiv:2104.09462*. <https://arxiv.org/abs/2104.09462>
  - ◆ 2. Anderson, Chris (2008). ‘The End of Theory: The Data Deluge Makes the Scientific Method Obsolete.’ *Wired*, June 23, 2008, 16-17. This problem is not new: when the philosopher Berkeley rebuked mathematicians in 1734 for addressing philosophical questions, he claimed ‘you have no right [...] to dictate out of your proper sphere, beyond which your judgement is to pass for no more than that of other men.’ (Berkeley, *The Analyst*, 1734).
  - ◆ 3. We use Tamar Sharon’s terminology: Sharon, T. (2021). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech’s newfound role as global health policy makers. *Ethics and Information Technology*, 23(1), 45-57. <https://link.springer.com/article/10.1007/s10676-020-09547-x>



lying monitoring and surveillance infrastructures that increasingly set the parameters for our public and private lives, and for the ways in which policy can respond to problems.

While the public debate has been focused on privacy, technology firms have done an end run around many other rights. Although privacy is a key point of leverage on technological power, it has been used strategically by technology firms to distract us from the broader problem of market (and other forms of) domination. Whether fighting privacy cases, like Amazon,<sup>4</sup> trumpeting privacy-preserving technologies, like privacy-violating firm Proctorio,<sup>5</sup> or changing data-brokering practices to look less invasive, like Google,<sup>6</sup> firms have used privacy strategically to draw public attention away from the rapid expansion of the presence and power of technology firms in all areas of public and private life.

We have seen over the course of the pandemic how this expansion of power has implications for the way technology is—and can be—governed. We have watched a reduction of the role of government in the delivery of public services, a reduction in the degree to which regulators can scrutinise and set limits for

- ◆ 4. Amazon is challenging a record fine for privacy violations in the EU:  
<https://www.msn.com/en-us/money/other/amazon-challenges-record-865-million-eu-data-protection-fine/ar-AAPypwJ>
- ◆ 5. Proctorio Recognized By 2021 EdTech Awards as Top Data Privacy, Testing, and Assessment Solution  
[https://www.prweb.com/releases/proctorio\\_recognized\\_by\\_2021\\_edtech\\_awards\\_as\\_top\\_data\\_privacy\\_testing\\_and\\_assessment\\_solution/prweb17882109.htm](https://www.prweb.com/releases/proctorio_recognized_by_2021_edtech_awards_as_top_data_privacy_testing_and_assessment_solution/prweb17882109.htm)
- ◆ 6. See Google's move away from tracking cookies and toward on-device analytics of personal data:  
<https://www.theverge.com/2022/1/25/22900567/google-floc-abandon-topics-api-cookies-tracking>



the technologies that affect everyday life, and a profound challenge to the capacity of the civil society organisations (CSOs) who act as the watchdogs and the voice of human rights and social justice when technological overreach occurs. This has been occurring simultaneously with a decrease in controls on both competition and corruption in countries around the world, something which makes it easier for powerful private interests to gain traction on public territory.<sup>7</sup>

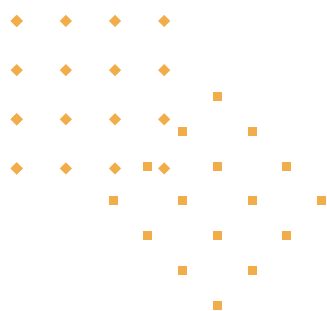
Whether it is Google and Apple reconfiguring mobile phone operating systems to allow other parties than themselves to use devices' location tracking functions, and thus to open those operating systems up to more possibilities,<sup>8</sup> defence and security contractors such as Palantir supplying analytics and cloud functions to public health institutions, or biometrics firms expanding their reach to education and vaccination certification and deploying facial recognition systems for crowd control and temperature sensing, the incursions we can see in our everyday lives are only the tip of the iceberg. Underneath the technologies that move essential (if sometimes mundane) functions online, determine how goods and services become accessible to us, and make us more visible in public space, is a layer of computational infrastructure—analytics platforms and services, as well as functionalities on our everyday devices—that continually expands the ways in which we can be surveilled, monitored, sorted, controlled, manipulated and governed.

These are changes that will not go away. Our challenge is to apply the checks and balances available—civil society pressure and regulatory power—to shape technologies toward the public good, and to control commercial power over these new developments and not to allow them to become normalised—a process that is already well underway.<sup>9</sup> The experts and activists from countries across Europe with whom we spoke for this research all reported a diminished resistance on the part of the public to new modes of monitoring, surveillance and regulating behaviour through technology. Legal regulation has been scaled back across Europe to require less competition and give more power to commercial technology firms, and controls on the length of firms' involvement in what was originally an emergency response are virtually nonexistent.<sup>10</sup> Nor are the problems outlined in this report likely to melt away with the coming of the pandemic's endemic phase. European authorities are welcom-

- 
- ◆ 7. Transparency International: Corruption Perceptions Index 2021: <https://www.transparency.org/en/cpi/2021>; see also V-Dem's Pandemic Backsliding Project (PanDem): <https://www.v-dem.net/pandem.html>
  - ◆ 8. Lanzing, M., Lievrouw, E., & Siffels, L. (2021). It Takes Two to Techno-Tango: An Analysis of a Close Embrace Between Google/Apple and the EU in Fighting the Pandemic Through Contact Tracing Apps, *Science as Culture*. <https://doi.org/10.1080/09505431.2021.1999403>
  - ◆ 9. Burt, C. (2022). Talk turns to leveraging digital identity infrastructure as COVID credentials retire. *Biometric Update*: <https://www.biometricupdate.com/202202/talk-turns-to-leveraging-digital-identity-infrastructure-as-covid-credentials-retire>
  - ◆ 10. Amazon, for instance, has experienced a decrease in antitrust challenges in the EU since the pandemic placed it as central to many countries' survival strategies: <https://www.reuters.com/technology/exclusive-eu-antitrust-regulators-set-clear-amazon-mgm-deal-sources-2022-03-09/>

ing technology firms as partners in the region's economic recovery, centering digital transition in the Next Generation EU<sup>11</sup> recovery plan.

One of the main aims of this report is to argue for a more holistic perspective on the problems of technological power that surfaced during the pandemic, and to offer civil society organisations and funders thinking tools in relation to these problems. We argue that the pandemic shows us it is time to move the analysis of technological interventions beyond a privacy/data protection or algorithmic bias approach that asks whether companies are complying with the law. This is because our established analyses of these problems are no longer adequate for the task of protecting the public from exploitation and our political systems from domination by technology actors. We need to ask additional questions about how we should distinguish legitimate from illegitimate uses of technological power, and how advocacy organisations and regulators can shape their leverage and regulatory power to address the latter. We aim to follow the strategy of 'naming, blaming and claiming'<sup>12</sup>—we define instances where firms have transgressed sectoral or public norms, explore how to frame accountability for the problems we see, and seek to inform civil society, regulators and policymakers about what kinds of new strategies are necessary in response to these transgressions, and how to connect problems to modes of claim and redress.



11. [https://ec.europa.eu/info/strategy/recovery-plan-europe\\_en](https://ec.europa.eu/info/strategy/recovery-plan-europe_en)

12 Felstiner, W. L. F, Abel, R. L., & Sarat, A. (1980). The Emergence and Transformation of Disputes: Naming, Blaming, Claiming . . . *Law & Society Review*, 15(3/4), 631–654. <https://doi.org/10.2307/3053505>

## 2. Background

The COVID-19 pandemic sparked a chain of declarations of states of emergency around the world. In the initial phase of the crisis many new demands were made of states, public sector institutions, organisations in health, education, transport and also of employers and individuals. These were met with a mixture of changes in practices and new technological measures. In many cases technology was a much-needed instrument to make things work in a crisis: materials had to be transported to bolster public health provision, students had to learn remotely, workers had to labour from home (where possible), and so forth. Much of public life had to go online, and at the sharp end of the crisis, in the health domain, new and extreme demands needed to be met.<sup>13</sup>

When we look at the governance of technology, and how it has been affected by the crisis, however, a new picture emerges. The pandemic emergency created new markets, both temporary (such as mass testing and personal protective equipment (PPE) logistics) and longer-term (such as the growth in the gig economy, the integration of public health and identification technologies, and systems supporting remote study and work). These new markets in turn have allowed commercial technology providers to transition between spheres of operation or in some cases significantly deepen their influence in an established sphere. This has enabled firms all over the world to (re) position themselves for new business, either by bidding for contracts in new areas, or by entrepreneurially developing new services. By definition, most have been doing this in domains where they did not already have a history but had an infrastructure or service offerings that could be brought to bear: the most prominent example is Apple and Google, which had no experience with contact tracing, but which had devices in the hands of users around the world pre-equipped with location sensors that could be adapted to channel data through an application programming interface (API) to health authorities, app developers and other platforms.

Similarly, Amazon and Palantir had little experience in the health sphere, but found ways to bring their logistical and analytics apparatus, respectively, to bear on problems of moving PPE and later vaccines from place to place in the case of Amazon, and creating systems for healthcare data aggregation and analysis in the case of Palantir. Amazon's expansion into healthcare is multiple and complex: as well as contracting with governments in Europe and North America to provide logistical services for vaccines and PPE, the company simultaneously moved into pharmaceutical retail, personalised healthcare and health apps and information services.<sup>14</sup> As will be explored in depth later, companies of varying sizes from different parts of the world are also of interest: for example,

---

<sup>13</sup> For a more detailed look at the changes that occurred around the world during the first phase of the pandemic, see: Data Justice and COVID-19: Global Perspectives: <https://meatspacepress.com/go/data-justice-and-covid-19-internet-archive/>

<sup>14</sup> BBC News, January 5 2021: 'Amazon plots a course into the healthcare industry'. <https://www.bbc.com/news/business-55228999>

the Estonian blockchain firm Guardtime, which specialises in data integrity software, is exploring a market niche in vaccination certification in Europe.<sup>15</sup>

Among the key concerns arising from these market-making activities is that political legitimacy is not established in the new spheres in which tech companies are now operating. Moreover, new entrants diminish the space and opportunities for established actors who are qualified both technically and ethically in the domain. The public sector becomes increasingly dependent on corporate actors for the delivery of public goods, particularly digital services, and public policy is increasingly shaped by their interests. Crucially, these concerns have far-reaching implications for the public that go beyond privacy harms.<sup>16</sup>

The pandemic has radically altered contexts for innovation: firms have been incentivised to shift, optimise and reconfigure<sup>17</sup> their activities while governments have been scaling down controls on competition<sup>18</sup> and supervisory scrutiny. In their public communications, regulators from fields such as competition and data protection often suffer from a high degree of opacity, which makes it hard for investigators and advocates to track the regulatory responses to these changes. Freedom of information requests can be a key tool at the disposal of civil society and academic researchers, but do not constitute systematic reporting requirements that may be necessary to fully appreciate the scope and significance of the shifts that are underway. Moreover, important information is often withheld from these requests due to commercial confidentiality concerns.<sup>19</sup> Concretely, these sorts of transparency mechanisms are only effective if the public has some specific sense of what information to request, which in many situations is not the case. Regulators are also likely to become overloaded due to increased corporate activity in new areas, decreased controls and the emergency context creating new regulatory challenges. Thus, the key questions we address are as follows.

## 2.1 What kind of problem does this create?

Our focus in this report is on technology firms' expansive activities during the pandemic. Specifically, we explore technologies and corporate strategies which impact people's ability to participate

---

<sup>15</sup> Murphy, H. (2021). A Look at COVID-19 Vaccine 'Passports,' Passes and Apps Around the Globe. *The New York Times*: <https://www.nytimes.com/2021/04/26/travel/vaccine-passport-cards-apps.html>

<sup>16</sup> For more on this, see Sharon, T. (2020). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, 1-13. <https://link.springer.com/article/10.1007/s10676-020-09547-x>

<sup>17</sup> Cromwell, J., & Kotelly, B. (2021). A Framework for Innovation in the COVID-19 Era and Beyond. *MIT Sloan Management Review*. <https://sloanreview.mit.edu/article/a-framework-for-innovation-in-the-covid-19-era-and-beyond/>

<sup>18</sup> Latham & Watkins LLP (2021). Impact of COVID-19: New Exemptions under Antitrust Law. <https://www.lw.com/thought-leadership/covid-19-impact-new-exemptions-under-antitrust-law>

<sup>19</sup> Foxglove (2020). Why is the UK government hiding its NHS data deals with private companies? <https://www.foxglove.org.uk/2020/05/11/why-is-the-uk-government-hiding-its-nhs-data-deals-with-private-companies/>

in society, from contact tracing to workplace technologies, and from border security to public sector algorithmic technologies. Some technology may be offered as pro bono services, some come in the form of government procurement or public-private partnerships, while other instances involve corporations expanding their infrastructures and capacities in ways that take them into the public sphere and people's everyday lives. The common thread we follow across these different scenarios is technology that affects people's agency, and thereby engenders justice concerns in terms of autonomy, citizenship and rights.

Thus, while our primary interest is in unpacking and assessing these supply-side dynamics, it is also necessary to critically examine the role that government procurement and policy plays in facilitating the expansion of the technology firms' activities and the extent to which government overreach during the pandemic is possibly a contributing factor to the sector's increased power and influence. This is particularly a concern in cases in which we are focusing on public sector bodies purchasing pandemic technology because these, in effect, operate as monopsonies—situations where the power of the buyer is so great that their preferences determine what is worth producing.

Our objective in analysing instances of transgressive sector creep or infrastructural expansion is to understand what kind of constraints are appropriate for companies deploying digital technologies in relation to the public in the particular context of the pandemic, its accompanying climate of emergency action, as well as its eventual aftermath. We do this by analysing what Tamar Sharon<sup>20</sup> has termed 'sphere transgressions'—that is, cases of sector creep in which technology firms establish themselves in one sphere of application, then use the computational infrastructure and insights they gain from it to pivot to other spheres. We also take account of scope creep, where firms use those infrastructures and insights to significantly deepen their influence within a sector—and analyse what differentiates transgressive activities from firms' normal process of innovation and growth, i.e. by posing questions of what constitutes legitimate intervention. We do this in particular in relation to the pandemic and the ways in which it is opening up new market opportunities where firms developing, marketing and deploying digital technologies and related services transition strategically from one sector to another (as with Amazon's move into public health), or build to a radically new scale within a sector (as with educational technologies), which often introduces problems that established regulation and governance mechanisms are not set up to deal with effectively.

## 2.2 Whom do we want to inform with this report?

We aim to inform organisations already working on issues of technology, politics and rights, of

---

20 Sharon, T. (2021). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, 23(1), 45-57.

<https://link.springer.com/article/10.1007/s10676-020-09547-x>

these transgressions and their implications, and to work together to understand what this means for advocacy practices and for our understanding of what regulation should target. This gives us a dual task: we need to define and make recognisable the risks of certain kinds of corporate activity, providing an understanding of how they may become transgressions and for whom; and we also need to integrate our findings with existing understandings and practices amongst civil society and advocacy organisations, in order to inform their work on policy and regulation in relation to the pandemic and after.

We want this report to speak to people and organisations that care about and work on key issues in the different sectors that are being infringed upon, i.e. policy makers, oversight bodies, advocates and pressure groups (as well as their funders) within different sectors, but we also want to explore what the broader character of this phenomenon implies for civil society and regulatory action across multiple sectors. This means connecting specific sectoral concerns and responses, which are the territory of particular actors, with more systemic ones which may (or possibly should) be the focus of digital rights organisations and technology policy makers on a broader level.

### **2.3 Where did we investigate?**

The Global Data Justice project originally approached the research with a country focus, i.e. with the task of identifying and analysing possible cases of sector transgressions across nine European countries with regional, political and cultural diversity (France, Germany, Hungary, Italy, Netherlands, Poland, Romania, Spain, UK). However, it became apparent over the course of the research that a more effective presentation of the phenomenon would be to focus on the particular sectors that are experiencing technology-driven transgressions.<sup>21</sup> This also permits the inclusion of illustrative cases from other European countries where key developments emerged during the research undertaken in 2021. The trans-European nature of this phenomenon makes it easy to miss that it has different national dynamics depending on the economic and technological conditions under which countries entered the pandemic. As one expert has observed, “the COVID-19 pandemic... has revealed just how far behind some major European countries are in digitising their economies and public services. As a result, tech policy debates often unfold on the national level, which can result in distinct discourses and terminology around risks, harms, and opportunities of technology.”<sup>22</sup>

---

◆ 21 Since this research was commenced, others have started documenting sphere transgressions across a range of different sectors. See the Sphere Transgression Watch observatory launched by Radboud University Nijmegen:

<https://www.sphere-transgression-watch.org/>

◆ 22 Kaltheuner, F. (2021). A New Tech ‘Cold War?’ Not for Europe. *AI Now Institute*.

<https://medium.com/@AINowInstitute/a-new-tech-cold-war-not-for-europe-4d4f2f8079b6>

We chose to focus mainly on the following key sectors

which are experiencing transgressions during the pandemic<sup>23</sup>:

- ◆ Health<sup>24</sup> - with a particular focus on public health, and the components of the healthcare sector that intersect with it due to the pandemic (e.g. elderly care<sup>25</sup>)
- ◆ Education<sup>26</sup> - at primary, secondary and tertiary level
- ◆ Policing/security - including law enforcement, border control and private sector security contracting that impacts on public welfare
- ◆ Transportation - from public transport to logistics and supply chains for public health supplies
- ◆ Payments - the public-facing architectures and services that enable consumer goods to be transacted
- ◆ Identification and authentication - controls on entry to buildings and public space; crossing borders

## 2.4 How did we research this?

The approach taken in this project has been to gather case studies from a number of sectors from across different European countries. We have stayed abreast of the relevant research in the academic literature and checked for useful reports from news outlets and CSOs throughout 2021. Sources published in local languages were retrieved and translated into English for analysis. We set up a collectively accessible and centralised repository for relevant information gathered on each of the nine countries in our research proposal. We also maintained a growing list of examples that appear to be potential or actual sector transgressions as we progressed.

In addition, we convened two meetings with civil society in Europe—one in February 2021 and the other in November 2021—to share our understanding of the phenomenon and to test whether others were seeing it manifest in similar or different ways.<sup>27</sup> We organised a panel at the Tilburg Institute for Law, Technology and Society biennial conference in May 2021—aptly themed *Regulating in Times of Crisis*<sup>28</sup>—where we brought together researchers and CSOs who could offer feedback on our research findings and debate the implications of sector transgressions for technology regulation and data governance. In each of these meetings, we were interested in surfacing this new and rapidly developing phe-

---

◆ 23 A detailed account of the different kinds of technology transgressions is available in the annex of the report.

◆ 24 For an introduction to Big Tech's interest in healthcare, see: Nosthoff, A-V. & Maschewski, F. (2021). *Big Tech Won't Make Health Care Any Better*. *Jacobin*.

<https://www.jacobinmag.com/2021/10/big-tech-google-apple-facebook-amazon-health-care-surveillance-capitalism-data>

◆ 25 Lecher, C. (2021). *How Big Tech Is Pitching Digital Elder Care to Families*. *The Markup*.

<https://themarkup.org/privacy/2021/10/28/how-big-tech-is-pitching-digital-elder-care-to-families>

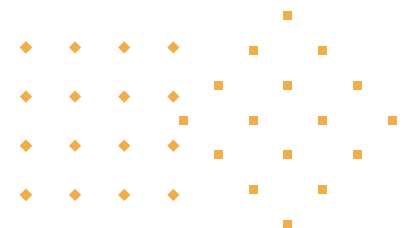
◆ 26 Anand, P. & Bergen, M. (2021). *Big Teacher Is Watching: How AI Spyware Took Over Schools*. *Bloomberg Businessweek*. <https://www.bloomberg.com/news/features/2021-10-28/how-goguardian-ai-spyware-took-over-schools-student-devices-during-covid>

◆ 27 Sphere Transgressions CSO meeting <https://globaldatajustice.org/2021-03-18-sphere-transgressions-meeting/> <https://globaldatajustice.org/2021-11-19-sphere-transgressions-meeting/>

◆ 28 <https://www.tilburguniversity.edu/about/schools/law/departments/tilt/events/tilting-perspectives/2021>

phenomenon as a specific issue of interest for the rights community in Europe and globally, consulting with participants about its manifestations in different places; we wanted to connect it to a range of civil and political rights issues, including but going beyond privacy; and furthermore, wanted to debate possible responses on the part of civil society and rights groups.

As part of our study we also attended industry conferences to validate our emergent findings and to extend our empirical efforts. In June 2020, we attended the three-day CogX 2021 global leadership summit and festival on artificial intelligence (AI) and transformational technology. The CogX festival offered insightful leads that shed light on how big tech is creating new dependencies and potentially crowding out experienced professionals in established sectors. We selected panels on the application of AI and data technology to healthcare, education, finance and defence, noting ethical and normative issues relevant to this project. Similarly, in September 2021 members of the research team attended a digital identity trade conference to assess whether and how the identity technology industry is (re)positioning its offerings in response to the pandemic.<sup>29</sup> Among other discoveries, we came to better appreciate the massive industry growth for ‘identity proofing solutions’ that has been created over the past two years, particularly as in-person identity checks have become much less common due to lockdowns and other restrictions on in-person interactions.



---

29 Martin, A. & Taylor, L. (2021). Give us your poor, your unidentified masses. *Global Data Justice blog*. <https://globaldata-justice.org/2021-09-29-identity-week-2021/>



### 3. Our findings

It would be difficult in 2022 to identify a sphere of social, political or economic activity that has not been digitised in one way or another. These systemic transformations have been underway for years if not decades. The pandemic, however, has provided a unique opportunity for tech firms of varying size and degrees of technological sophistication to move into different spheres of activity in deeper and more profound ways, particularly in the case of a legally declared emergency context, with relaxed oversight and minimal contestation. These interventions are taking place in response to an unprecedented public health crisis, but also find their logic in perceived ‘crises’ in other sectors such as education, transportation and security. Our research shows how these transformations are unfolding through illustrative cases from five different sectors: health, education, policing, security and mobility control, and the cross-cutting theme of identification and authentication, in a number of European countries. While these cases are by no means an exhaustive account of the phenomenon, they do reveal key trends and challenges.

Our findings show several key trends across sectors: a rapid increase in the integration of commercial technology into what were formerly public sector tasks and services; a decrease in public sensitivity to what would previously have been considered privacy-invasive technologies; the political empowerment of both big tech and the smaller firms which use its computational infrastructures to cross over into new functions and sectors; decreased regulatory hurdles and checks and balances in technology procurement by the public sector, and an increase in the presence of security technologies in areas where they were not previously considered relevant.

#### 3.1 Health

**Digital contact tracing:** An obvious departure point for exploring technology firms’ transgressions in the health domain is the case of the Google/Apple partnership, which has been well documented and critiqued by both scholars<sup>30</sup> and activists.<sup>31</sup> In terms of geographical scale, it is one of the more far-reaching cases in Europe and beyond by virtue of the fact that, between them, Google and Apple have near total control over the operating systems running on the world’s smartphones through their ownership of Android and iOS, respectively. During the race to develop and deploy effective contact tracing solutions in the early stages of the pandemic, the companies joined forces to create a privacy-sensitive (i.e. decentralised) technical protocol, known as the Google/Apple Exposure Notification (GAEN) system, following similar efforts by the Decentralised Privacy-Preserving

<sup>30</sup> See, for example: Sharon, T. (2021). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech’s newfound role as global health policy makers. *Ethics and Information Technology*, 23(1), 45-57. <https://link.springer.com/article/10.1007/s10676-020-09547-x>

<sup>31</sup> EFF. (2020). Apple and Google’s COVID-19 Exposure Notification API: Questions and Answers. <https://www.eff.org/deep-links/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answers>

Proximity Tracing (DP-3T) protocol created by the European DP-3T consortium.

The privacy-protective design of the GAEN protocol won it many plaudits among the privacy community – though in some cases the GAEN design specifications have conflicted with the stated needs of public health authorities, while simultaneously raising questions about the implications for digital sovereignty.<sup>32</sup> However, more interesting for our purposes are the consequences of Google and Apple becoming, through their technological and commercial control over the operating systems running on people's smartphones, *de facto governors of global public health infrastructure*. The companies were able to translate their market power and technical superiority in smartphone software to gain leverage and influence in the domain of public health, where they lack both epidemiological expertise and moral authority. And while digital contact tracing apps may not have lived up to their original promise in terms of providing timely and effective notifications of potential contagion and preventing virus transmission<sup>33</sup> (due to a complex set of reasons including low uptake, lingering privacy concerns, technical issues, etc.), it is significant that the underlying infrastructure still exists for potential re-purposing in the future – for public health interventions or potentially other purposes – and that it is controlled by the two technology giants.

- ◆ **Health data analytics:** In the very early moments of the pandemic, governments were overwhelmed with information about infection rates, intensive care unit capacity, mortalities and so forth. Public health authorities were struggling to manage and make sense of pandemic data, and to take informed decisions on, for example, how to allocate limited resources to hospitals. The data analytics firm Palantir, which since the early 2000s has specialised in developing and deploying applications for security, intelligence and law enforcement authorities, saw an opportunity to expand its business and made a concerted effort to pitch its software platforms in Europe. Through our research as well as the tireless work of civil society groups and investigative journalists,<sup>34</sup> we are aware of at least seven European countries where Palantir has either made approaches to health officials or where deals have been signed and executed during the pandemic, i.e. Austria, France, Germany, Greece, Italy, Netherlands and the UK.<sup>35</sup>

---

◆ 32 Veale, M. (2020). Sovereignty, Privacy, and Contact Tracing Protocols in Taylor, L., Sharma, G., Martin, A.K., Jameson, S.M. (eds.), *Data Justice and COVID-19: Global Perspectives*. London: Meatspace Press.

◆ 33 According to one study in the EU, as of November 2021 only 1.82m cases had been notified to contact tracing apps – just 5% of confirmed COVID-19 cases: <https://voxeurop.eu/en/covid-19-track-trace-apps-a-100m-failure/>

◆ 34 See, for example: Howden, D., Fotiadis, A., Stavinoha, L. & Holst, B. (2021). Seeing stones: pandemic reveals Palantir's troubling reach in Europe. *The Guardian*.  
<https://www.theguardian.com/world/2021/apr/02/seeing-stones-pandemic-reveals-palantirs-troubling-reach-in-europe>

◆ 35 Gould, M., Joshi, I. & Tang, M. (2020). The power of data in a pandemic. *Technology in the NHS blog*.  
<https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/>

Despite the folklore surrounding Palantir's data analysis tools, which have been said to turn 'data landfills into gold mines'<sup>36</sup>, the company's involvement in Europe's response to the pandemic exemplifies some of the core issues with sector transgressions. The company has argued that it is 'ideally suited to deal with confidential and sensitive information' during the pandemic because of its previous work in the security and intelligence domains.<sup>37</sup> However, there is a crucial difference between the values, priorities and expertise required for the development and implementation of computational infrastructures for national security or military intelligence applications and those needed in the domain of public health. For one, in public health, objectives are centred around patient care, not national security. Second, transparency ought to play a central role in health policy decision making, including regarding technology investments and data-driven interventions.

But transparency has been desperately lacking. In the UK, Palantir's relationship with the National Health Service began in March 2020, originally on a short-term basis, with the aim of helping the public health system deploy resources during the pandemic. In December of the same year, the short-term contract, valued at £23m, was extended for two years with very little public debate. Advocates sought to understand the specifics of the contract granting Palantir access to public health data but were repeatedly thwarted by limited disclosure of information, forcing them to pursue a lawsuit<sup>38</sup> against the NHS in early 2021.<sup>39</sup> In Greece, the government's data partnership with Palantir was not registered on the country's public procurement system because it was struck as a 'zero-cost agreement', thereby skirting government procurement rules.<sup>40</sup> The deal remained undisclosed for nine months.

Many view the use of data protection impact assessments (DPIAs) as a vital tool in cases such as these to prevent companies like Palantir from gaining inappropriate access to sensitive health information. While in the Greek case, a DPIA was not carried out (much to the dismay of privacy advocates), in the UK the NHS reports to have undertaken a DPIA for their work with Palantir. The use of DPIAs may help against the misuse of personal data, especially sensitive data, but if we focus solely on these fairly nar-

---

36 Waldman P., Chapman L, and Robertson J (2018), Peter Thiel's data-mining company is using War on Terror tools to track American citizens. The scary thing? Palantir is desperate for new customers

<https://www.bloomberg.com/features/2018-palantir-peter-thiel/>

37 Wright, O. (2021). Palantir: the espionage tech firm that's 'ideally suited' for getting Covid jobs into arms. *The Times*.

<https://www.thetimes.co.uk/article/palantir-the-espionage-tech-firm-thats-ideally-suited-for-getting-covid-jobs-into-arms-pb6m-5ywbg> [open-access version available here: <https://www.palantir.com/blog/the-espionage-tech-firm-that-insists-its-ideally-suited-for-getting-jobs/>]

38 Fitzgerald, M. & Crider, C. (2021) Why we're suing over the £23m NHS data deal with Palantir. *openDemocracy*.

<https://www.opendemocracy.net/en/ournhs/why-were-suing-over-the-23m-nhs-data-deal-with-palantir/>

39 BBC News. (2021). Palantir: NHS says future deals 'will be transparent'. <https://www.bbc.com/news/technology-56590249>

40 Howden, D., Fotiadis, A., Stavinoha, L. & Holst, B. (2021). Seeing stones: pandemic reveals Palantir's troubling reach in Europe. *The Guardian*. <https://www.theguardian.com/world/2021/apr/02/seeing-stones-pandemic-reveals-palantirs-troubling-reach-in-europe>

rowly defined assessment tools, we may miss out on more fundamental concerns including the ways in which Palantir (and companies like it) can take insights and lessons learned from the public health domain and use those for commercial benefit in other areas such as security. The involvement of companies like Palantir in Europe's pandemic response clearly demonstrates that civil society critique and regulatory oversight need to focus on more than just privacy and data protection harms—the company has carefully crafted an internal civil liberties programme to help it get ahead of these critiques.

◆ **Quarantine apps:** Quarantine apps were not a common feature in Europe during the pandemic<sup>41</sup>, though at least one country did experiment with their use. A case from Poland highlights the peculiarities of repurposing technology in a public health crisis.

The *kwarantanna domowa* ('home quarantine monitoring') app was developed for Poland's Ministry of Digital Affairs by a company called TakeTask, which specialises in market research. TakeTask repurposed its multifunction marketing project management and consumer behaviour monitoring platform into a quarantine surveillance system to help the police enforce the country's mandatory quarantine. TakeTask's Supervisory Board Chairman explained the company's involvement in the pandemic response as follows:

'TakeTask's participation in creating the Home Quarantine Monitoring application supports the idea of *corporate social responsibility*. In the face of a *humanitarian crisis* such as COVID-19 the company was very quickly able to use its knowledge and technology to support important objectives. We all know how important it is for our life and for our health to stay at home during the quarantine period. Nevertheless, we still hear about those who do not follow the recommendations. That is why TakeTask has provided a solution that significantly contributes to "flattening the curve", i.e. stopping the spread of the virus' (emphasis added).<sup>42</sup>

Introduced in April 2020, the app is mandatory for certain persons, like those crossing the border into Poland.<sup>43</sup> It appears that the procurement of the technology faced minimal scrutiny despite the fact that the Ministry of Digital Affairs spent 3.7m PLN gross (~800,000 EUR) on the app's development and implementation. In accordance with Article 6 of the Act of 2 March 2020 on specific solutions to prevent, counteract and combat COVID-19, other infectious diseases and crisis situations caused by them ("the COVID-19 Act")<sup>44</sup>, the provisions of the Public Procurement

---

◆ 41 They did feature in the pandemic responses in other countries, however, like Australia: <https://www.theguardian.com/australia-news/2021/oct/13/home-quarantine-apps-prompt-privacy-and-racial-bias-concerns-in-australia>

◆ 42 Starzynski, S. (2020). The role of TakeTask in launching the 'Home Quarantine Monitoring' application. *LinkedIn*. <https://www.linkedin.com/pulse/role-taketask-launching-home-quarantine-monitoring-starzynski/?articleId=6653272371543236608>

◆ 43 Visually impaired and persons without telecom access appear to be legally exempted from its use.

◆ 44 *Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych* [2020] Dz. U item 374 <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000374>

Law<sup>45</sup> did not apply to orders for goods or services necessary to counteract COVID-19, in case of a high probability of a rapid and uncontrolled spread of the disease, or if required for the protection of public health.

Besides the technical inadequacies of the system, which are well documented in user reviews,<sup>46</sup> concerns were also raised by the public.<sup>47</sup> The controversy following the launch of the app triggered a response from the Commissioner for Human Rights and the Polish Ombudsman regarding potential privacy violations but with little effect. Formally, the legal obligation to install and use the app still exists and applies to everyone in quarantine, but there seems to be no real enforcement mechanism. Furthermore, due to the flaws in the functioning of the app and poor technical support, even the sanitary inspections and police appear to have given up on executing their obligations. A regional public health inspector in Białystok has been quoted as saying that in practice nobody has ever been fined for not using the app and that it is challenging in a practical sense to verify whether people are actually using it.<sup>48</sup>

In view of the doubtful value and quality of the TakeTask solution, in February and March 2021, MP Paweł Bejda submitted two parliamentary questions<sup>49</sup> seeking answers to several concerns regarding the choice of the app developer and the contract the government made with TakeTask. The answers focus on the urgent need at the time to introduce the solution and the fact that the aforementioned Article 6 of the COVID-19 Act did not require the public procurement process.

While the company's founder and CEO said in April 2020 that they were 'already in talks with other countries interested in our solution', it does not appear that the platform was deployed elsewhere.

◆ **Vaccine certification:** With the reopening of societies after the rollout of vaccines in Europe, there has been a concerted effort to put infrastructures in place to facilitate the verification of people's vaccination status.

In this context, Guardtime—a blockchain firm founded in Estonia and a self-described 'scaleup'—has pivoted from enterprise applications for audit, compliance and cybersecurity to embark on a

---

◆ 45 Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843)

◆ 46 Google Play <https://play.google.com/store/apps/details?id=pl.nask.droid.kwarantannadomowa> and Apple Play <https://apps.apple.com/pl/app/kwarantanna-domowa/id1502997499?>

◆ 47 Fundacji Panoptykon (2020). Odpowiadamy na pytania o aplikację „Kwarantanna domowa”. <https://panoptykon.org/aplikacja-kwarantanna-domowa>

◆ 48 Hukałowicz, I. (2020). Kary za brak aplikacji 'Kwarantanna domowa' są fikcją. Nikt tego nie kontroluje. *Kurier Poranny*. <https://poranny.pl/kary-za-brak-aplikacji-kwarantanna-domowa-sa-fikcja-nikt-tego-nie-kontroluje/ar/c14-15232364>

◆ 49 <https://sejm.gov.pl/sejm9.nsf/InterpelacjaTresc.xsp?key=BYZK7C> and <https://sejm.gov.pl/sejm9.nsf/InterpelacjaTresc.xsp?key=C22HZM>

project to develop digital vaccination certificates for widespread use. In October 2020, the WHO and Estonian government launched a pilot scheme for digitally verifiable international vaccination certificates to support the country's vaccination program. Guardtime is the technical leader of the project, which it is marketing as VaccineGuard.

VaccineGuard is a Keyless Signature Infrastructure (KSI) blockchain-based platform designed to service various aspects of data flow in COVID-19 vaccination programmes. It is marketed as a 'global trust architecture' or 'universal trust framework' for governments, health authorities, citizens and health care providers. VaccineGuard also supports cross-border recognition of electronic health to manage and provide time-stamping and server-supported digital signature services. In January 2021, GuardTime announced that Hungary, Estonia and Iceland are among the pilot countries signing up for the experiment. The technology will be applied to digital verification of vaccination, issuance of COVID-19 test certificates and vaccination passports. The Estonian government went live with VaccineGuard in April 2021.

Like several of the applications that rose to prominence during the pandemic, VaccineGuard has vaunted<sup>50</sup> its security and data protection controls. It allows authorities to track the vaccination status of individuals, employing blockchain to manage the records and certificates, and transmit those records to public health authorities and vaccine manufacturers.<sup>51</sup>

With VaccineGuard, what we are witnessing is a security company using its expertise in providing trust services and data integrity as leverage for driving the COVID-19 vaccine value chain in affected countries. VaccineGuard will deliver automated aggregated reports from vaccination sites, automated monitoring of stock and vaccinations, and facilitate adverse effect reporting. Governments that adopt this technical solution will have to depend on Guardtime's infrastructure and technical expertise to drive their vaccination program. The platform will be accessible to citizens, care providers and immigration authorities who may wish to verify vaccination credentials for travel. This creates dependencies for the states by forcing them to rely on VaccineGuard for the sustainability of the vaccination programme. Wider uptake of this technology might create inequities for citizens that do not have access to mobile phones or the internet. It may also create further dependencies for businesses within the pilot countries who might require onboarding to the platform, e.g. airlines, restaurants, hotels and employers in general.

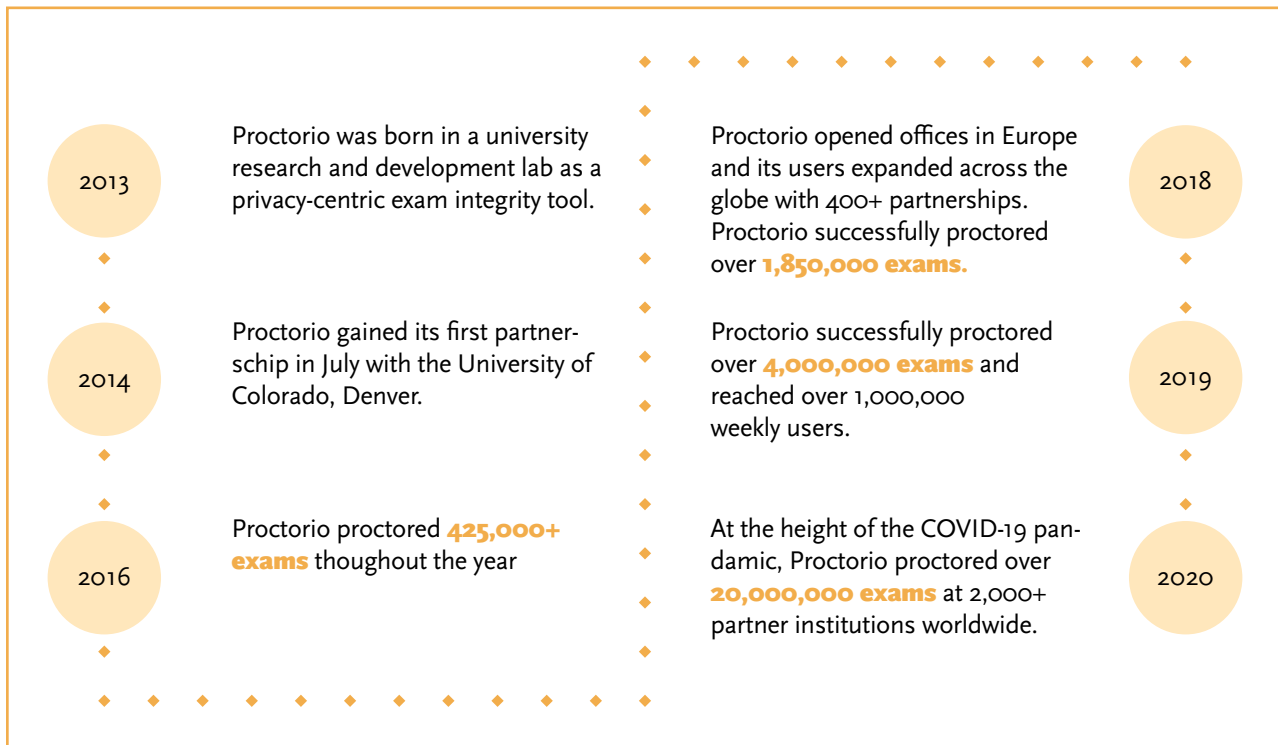
---

◆ 50 VaccineGuard Awarded Top Digital Solution for COVID-19 at the UAE Global Business Summit—Guardtime.

(n.d.). Retrieved 22 June 2021, from

<https://guardtime.com/blog/vaccineguard-awarded-top-digital-solution-for-covid-19-at-the-uae-global-business-summit>

◆ 51 Ain Aaviksoo, Guardtime's Chief Medical Officer. Retrieved 22 June 2021, from <https://guardtime.com/vaccineguard>



Reference and copyrights: <https://proctorio.com/about/history>

### 3.2 Education

◆ **EdTech:** New EdTech has been introduced at every level of the educational system, without schools receiving guidance as to privacy and data protection issues for children and students. Firms are using this technological foothold and the funding streams that facilitate it to expand their involvement from facilitating online learning to student surveillance and the introduction of security-related technologies such as facial recognition into schools.

Take, for example, Proctorio: a multinational educational technology firm headquartered in Arizona and Serbia.<sup>52</sup> It provides automated, AI-enabled exam surveillance services to the education sector. Although the company has been operating since 2013 (see the company's short history – in its own words<sup>53</sup> – in the diagram below), it came to international attention during the pandemic, reporting in May 2021 that 71% of its deployments had taken place since April 2020.<sup>54</sup>

The company's products have been the focus of privacy claims and pushback on the basis of data security and data protection concerns, most notably a court case in the Netherlands where University of Amsterdam students argued that they should have the right to an alternative to online proctoring,

◆ 52 Proctorio: Overview <https://craft.co/proctorio>

◆ 53 Proctorio: Becoming a leader in Automated Proctoring <https://proctorio.com/about/history>

◆ 54 Celebrating Our Eighth Birthday (2021). <https://proctorio.com/about/blog/celebrating-our-eighth-birthday>

and that the software violated their privacy. They lost the case, with the judge ruling<sup>55</sup> that the software was GDPR-compliant because the software did not make recordings or students' other personal data available outside the university's staff, and because the pandemic made it too difficult for the university to provide alternative forms of test-taking. The company has leveraged the publicity from this judgement by creating a branding strategy focused on privacy-by-design and security: in 2021 it was a finalist<sup>56</sup> for the US EdTech awards for 'student data privacy solutions'. It has also been certified as a trustworthy company<sup>57</sup> on standards of security, reliability, legal compliance and privacy. It also publicises its use of encryption<sup>58</sup> to protect the recordings it makes of exams.

Proctorio represents a class of EdTech firms whose business has been transformed by the pandemic. These firms have redefined the criteria for fair and credible examinations, with universities citing the idea that unless students have been subjected to digital surveillance and have given up control over their computers and over the visibility of their workspace to a proctor (or an AI-based proxy designed to flag anomalies to that human proctor), this threatens the standing and credibility of the qualification a university is offering, and in turn the university's own standing and credibility. This has gained enormous traction among universities at a time when they are under pressure to keep degrees running despite the disruptive effect of moving their operations online. Proctorio runs on a mix of Google analytics and Microsoft cloud hosting infrastructure,<sup>59</sup> increasing these companies' already substantial presence in EdTech by adding a testing dimension to their capacity. The analytics it uses, although they are nominally privacy-preserving because they do not send students' identifiable data to Proctorio or to these other firms, nevertheless collect information through facial and behavioural biometrics that can be used by Proctorio but also the companies that form its operational infrastructure to further develop facial recognition and behavioural data-based models and systems. These, in turn, can be used in myriad other contexts, for example in Microsoft's work on security and defence or in Google's adtech.

### 3.3 Policing, security and mobility control

As part of the frontline response to the pandemic, governments were compelled to enforce quarantine measures. Police officers were dispatched to monitor compliance with these measures. Some countries grappled with the shortfall in law enforcement manpower to enforce home quar-

---

55 Amsterdam District Court Decides In Favor of Proctorio and UvA (2020).

[https://www.prweb.com/releases/amsterdam\\_district\\_court\\_decides\\_in\\_favor\\_of\\_proctorio\\_and\\_uva/prweb17185598.htm](https://www.prweb.com/releases/amsterdam_district_court_decides_in_favor_of_proctorio_and_uva/prweb17185598.htm)

56 Proctorio Recognized By 2021 EdTech Awards as Top Data Privacy, Testing, and Assessment Solution (2021).

[https://www.prweb.com/releases/proctorio\\_recognized\\_by\\_2021\\_edtech\\_awards\\_as\\_top\\_data\\_privacy\\_testing\\_and\\_assessment\\_solution/prweb17882109.htm](https://www.prweb.com/releases/proctorio_recognized_by_2021_edtech_awards_as_top_data_privacy_testing_and_assessment_solution/prweb17882109.htm)

57 Proctorio becomes SOC 2 Type 1 compliant proctoring provider (2021).

<https://proctorio.com/about/blog/proctorio-becomes-soc-2-type-1-compliant-proctoring-provider>

58 Celebrating Our Eighth Birthday (2021). <https://proctorio.com/about/blog/celebrating-our-eighth-birthday>

59 <https://craft.co/proctorio>



antine mandates. Actors such as biometrics firms, defence contractors and security companies are therefore becoming increasingly involved in internal and external bordering activities in relation to the pandemic - certifying, identifying and controlling spaces at both national and local levels. As a result, alternative enforcement mechanisms have been deployed in the form of surveillance apps to make up for the shortage.

One interesting example is the HKR app developed by Asura Technologies Ltd. and implemented with the assistance of IdomSoft Zrt. (the same company developing the Hungarian Dragonfly surveillance project<sup>60</sup>). ASURA is a Hungarian company founded in 2017 that started by providing AI video analytics systems and licence plate recognition software for vehicle traffic safety and surveillance in Hungary. During the pandemic, they developed a Home Quarantine System that uses facial recognition and phone location data to monitor home quarantine compliance. The platform is used for monitoring the home quarantine status of patients. The app is also used for manual checks when an automatic check-in process is obstructed, and for contacting the police when manual intervention or further investigation is required. This technology was donated free of charge and commissioned by the government as the official home quarantine system and is operated by the Hungarian Police, but there is no clarity as to the nature and scope of the arrangement between ASURA and the government.

The pandemic has been beneficial to tech companies in the security and biometrics space attempting to use the technological infrastructures at their disposal, such as facial recognition technology, to increase the surveillance of public transportation by linking their provision to activities in identification, security and policing. These are being made under the guise of improving public safety by implementing COVID prevention measures, including social distancing, occupancy control and mask detection in public transportation. An interesting example is the COVID-19 surveillance update to the algorithm offered by Herta Security to identify suspects or criminals even with their masks on.<sup>61</sup> This feature has nothing to do with preventing the spread of the pandemic, yet Herta Security was awarded the COVID-19 Response Seal of Excellence by the European Commission.<sup>62</sup> Before the pandemic, Herta Security used this technology for tracking suspects at the Méndez Álvaro bus terminal in Spain. The pandemic created an impetus for Herta to repurpose a technology with no previously known public health safety application.

---

60 See more about Project Dragonfly here: <https://english.atlatszo.hu/2021/12/09/after-terrorists-crossed-hungary-surveillance-cameras-connected-through-project-dragonfly/>

61 Miralles, N. Campisi, G. & Díaz, C. (2021). High-tech surveillance in times of COVID-19. <https://corpwatchers.eu/IMG/pdf/mass-surveillance-esp-eng.pdf>

62 Herta Awarded the Highly Competitive 'COVID-19 Response Seal of Excellence' from the European Commission (2020). <https://www.prnewswire.com/in/news-releases/herta-awarded-the-highly-competitive-covid-19-response-seal-of-excellence-from-the-european-commission-808052219.html>

Our findings show shifts like this are happening elsewhere in Europe. For instance, France deployed a new AI system developed by Datakalab to help the authorities identify individuals who were not complying with the rules on mask usage in public transportation. The authorities in some parts of France allowed the deployment of this technology without the usual scrutiny that such a public-facing undertaking, fraught with risks, should undergo. However, the question remains on how Datakalab's technology, which was primarily used for analysing consumer emotions and satisfaction, could make its way into the public transportation space. Whether these technologies have indeed helped the authorities in staying ahead of the pandemic or the overall fight against the virus is not yet clear. However, it is evident that current ethical and regulatory controls on such technologies in the public sphere lack the maturity to handle the urgency and severity of a crisis of this magnitude.<sup>63</sup>

### 3.4 Payments

The COVID-19 pandemic has accelerated the digitisation of banking and payment services, especially the push for contactless payments as a safer and more convenient way to transact.<sup>64</sup> This trend has been captured in developments across Europe, especially in places like the Netherlands<sup>65</sup>, France<sup>66</sup>, Poland<sup>67</sup> and Germany<sup>68</sup>. Contactless payment functionality is made possible through near-field communication (NFC) technology, which is available in devices and tokens in which NFC chips have been embedded, such as mobile phones and modern credit cards. The pandemic has made it all-important for businesses to have this payment solution available to their customers.

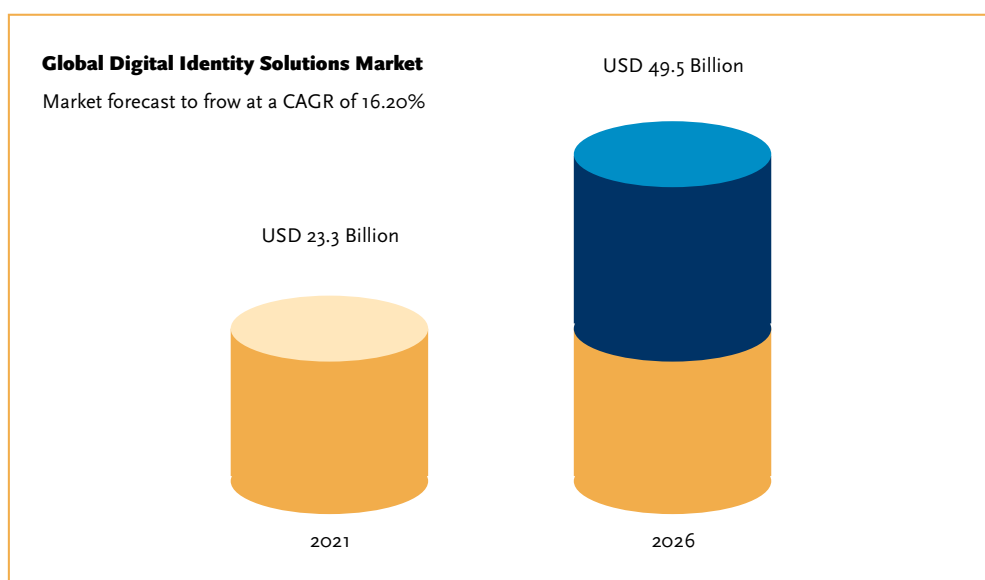
The pandemic has also made it possible for tech companies like Apple to further embed themselves in the payment infrastructure by offering original equipment manufacturer (OEM) pay solutions and restricting access to the NFC chips required for such contactless payments on their mobile devices.<sup>69</sup>

- 
- ◆ 63 Tzachor, A., Whittlestone, J., Sundaram, L. et al. Artificial intelligence in a crisis needs ethics with urgency. *Nat Mach Intell* 2, 365–366 (2020). <https://www.nature.com/articles/s42256-020-0195-0>
  - ◆ 64 BIS. (2021). COVID-19 accelerated the digitalisation of payments. [https://www.bis.org/statistics/payment\\_stats/commentary2112.htm](https://www.bis.org/statistics/payment_stats/commentary2112.htm)
  - ◆ 65 De Nederlandsche Bank (2020). Contactless payments on the rise during the COVID-19 pandemic <https://www.dnb.nl/en/actueel/dnb/dnbulletin-2020/contactless-payments-on-the-rise-during-the-covid-19-pandemic/>
  - ◆ 66 Darné, F. (2021). Contactless 2021: How small business is driving contactless adoption in France. *Ingenico*. <https://blog.ingenico.com/posts/2021/07/contactless-2021-how-small-business-is-driving-contactless-adoption-in-france.html>
  - ◆ 67 Nikolova, M. (2021). Poland is rapidly becoming a cashless society. <https://emerging-europe.com/news/poland-is-rapidly-becoming-a-cashless-society/>
  - ◆ 68 Deutsche Bundesbank. (2021). Making payments in Germany in 2020, the year of COVID-19: card-based and contactless payments trending. <https://www.bundesbank.de/en/press/press-releases/making-payments-in-germany-in-2020-the-year-of-covid-19-card-based-and-contactless-payments-trending--858018>
  - ◆ 69 Levithin, A. (2022). How Apple Locks Out the Competition with Its Digital Key. *ProMarket*. <https://promarket.org/2022/01/12/apple-digital-key-competition-privacy-contactless-payments-antitrust>

Apple is expected to face an antitrust charge in the EU for its anti-competitive practices in the contactless payments domain.<sup>70</sup> Similarly to other cases we have documented so far, Apple cites privacy and safety concerns as the reasons for the lack of interoperability in Apple Pay.

### 3.5 Identification and authentication

**Remote identity verification:** While most of them are not (yet) household names, firms like iProov<sup>71</sup>, Mitek<sup>72</sup> and Veriff<sup>73</sup> (an Estonian ‘unicorn’<sup>74</sup>) have grown massively during the pandemic due to the need for remote identity verification services. Legal and regulatory requirements for ‘customer due diligence’, for example ‘know your customer’ mandates in the financial services sector, have been hard to satisfy in face-to-face environments during extended lockdowns in countries across Europe. Whereas in the past, proving someone’s identity typically consisted of providing physical evidence, for example by



RESEARCH AND MARKETS  
The World's Largest Market Research Store

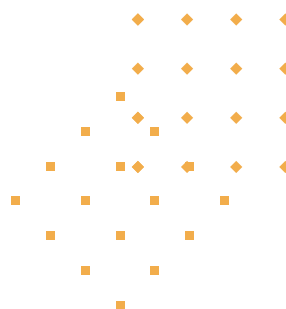
<http://www.researchandmarkets.com/reports/5393866>

- 70 Chee, FY. (2021). EXCLUSIVE Apple to face EU antitrust charge over NFC chip - sources. *Reuters*. <https://www.reuters.com/technology/exclusive-eu-antitrust-regulators-charge-apple-over-its-nfc-chip-tech-sources-2021-10-06/>
- 71 Lunden, I. (2022). iProov snaps up \$70M for its facial verification technology, already in use by Homeland Security, the NHS and others. *TechCrunch*. <https://techcrunch.com/2022/01/06/iproov-snaps-up-70m-for-its-facial-verification-technology-already-in-use-by-homeland-security-the-nhs-and-others/>
- 72 Gupta, S. (2022). Touchless Technology, Digital Banking and Biometrics. <https://vmblog.com/archive/2022/01/31/mitek-2022-predictions-touchless-technology-digital-banking-and-biometrics.aspx>
- 73 Invest in Estonia. (2020). How Estonia's identity verification company Veriff managed to keep growing during the COVID-19 crisis, closing a 15.5M USD financing round. <https://investinestonia.com/how-estonias-identity-verification-company-veriff-managed-to-keep-growing-during-the-covid-19-crisis-closing-a-15-5m-usd-financing-round/>
- 74 Sorainen. (2022). Veriff raises USD 100 million <https://www.sorainen.com/deals/veriff-raises-usd-100-million/>

presenting a government-issued ID credential, assessing its authenticity and verifying that the person presenting the credential is the rightful owner, remote identity proofing methods are a way to verify people's identities without relying on physical presence. They usually do so by having users scan a copy of their ID credentials for validation and, depending on the level of identity assurance required, the submission of biometric data (i.e. face, fingerprint and iris) as well.

The remote identity verification sector has seized this opportunity presented by the pandemic to leverage Europe's relatively well-developed consumer technological infrastructure, i.e. smart devices, webcams, etc. to facilitate these transactions at scale. Smartphones and other devices capable of recording both identity information on ID credentials using optical character recognition and biometrics using increasingly high resolution cameras provide the basic infrastructure for remote identification and authentication.

The use of these services is expanding (and is forecasted to continue to grow – see diagram below) to cover more and more contexts in which identity or age verification is needed – beyond just financial services. For example, iProov, which works with the UK's NHS, Eurostar as well as banks such as ING and Rabobank, serviced more than 1 million face verifications per day in 2021.<sup>75</sup> But this popularity has not come without controversy. For example, the contract with the NHS has been publicly questioned due to the company's links with the ruling Tory party, raising questions about transparency and accountability in the procurement process<sup>76</sup> – the company has received financial backing from a private equity group which counts two Tory party benefactors among its three partners.<sup>77</sup>



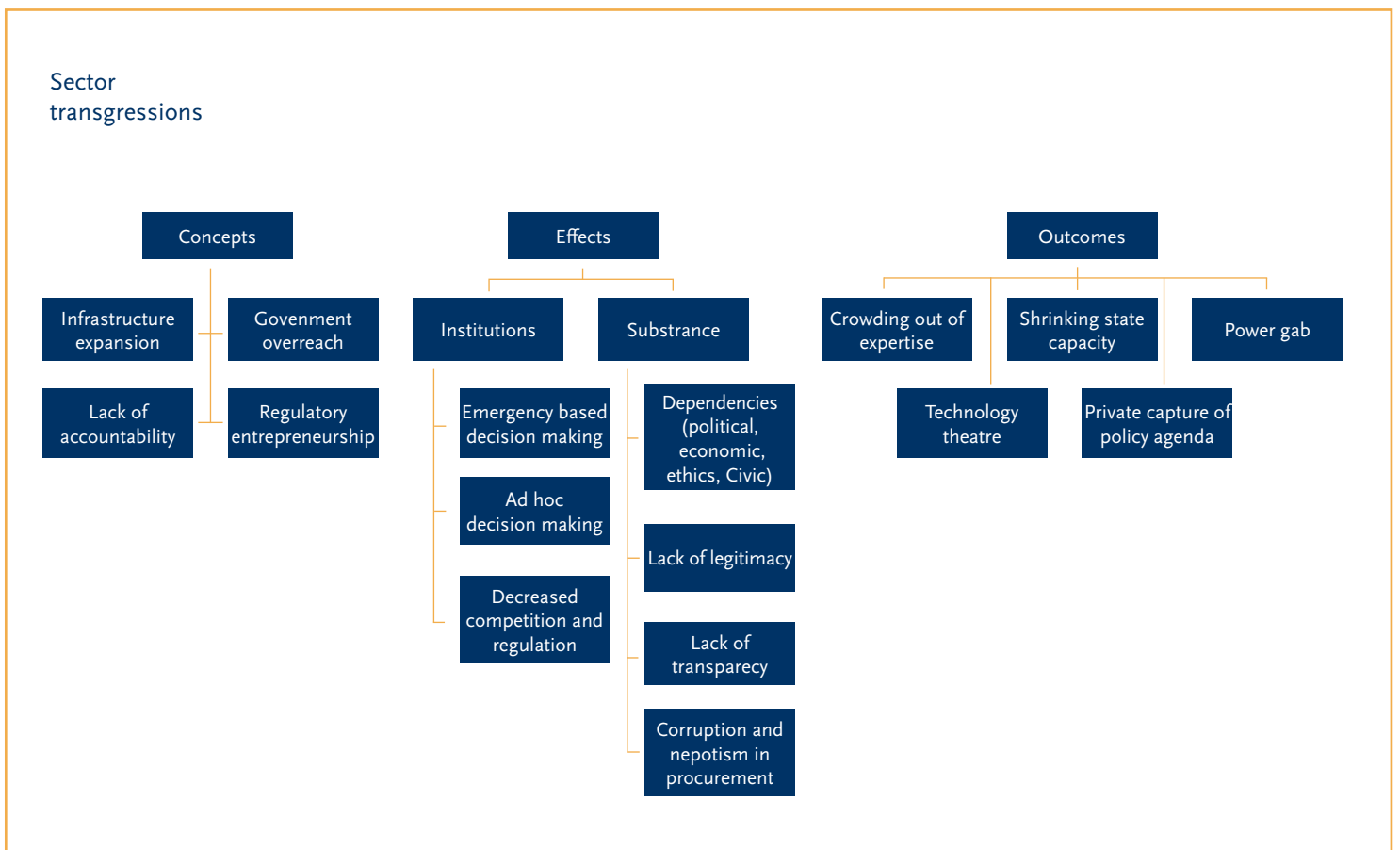
- 75 Lunden, I. (2022). iProov snaps up \$70M for its facial verification technology, already in use by Homeland Security, the NHS and others. *TechCrunch*. <https://techcrunch.com/2022/01/06/iproov-snaps-up-70m-for-its-facial-verification-technology-already-in-use-by-homeland-security-the-nhs-and-others/>
- 76 Davies, R. (2021). NHS app storing facial verification data via contract with firm linked to Tory donors. *The Guardian*. <https://www.theguardian.com/society/2021/sep/15/nhs-app-storing-facial-verification-data-via-contract-with-firm-linked-to-tory-donors>
- 77 Kundaliya, D. (2021). Privacy concerns raised over NHS deal with iProov for facial data collection. *Computing*. <https://www.computing.co.uk/news/4037142/privacy-concerns-raised-nhs-deal-iproov-facial-collection>

## 4. Naming, Blaming and Claiming: strategies for identifying and addressing sector transgressions

### 4.1 Concept map of Sector Transgressions

In this section we examine the role that civil society organisations and oversight bodies have played in addressing sector transgressions through an examination of existing projects and strategies. Rather than imposing a perspective on CSO's work, however, we analyse their responses to imagine ways to characterise and determine targets, as well as resist sector transgressions. We offer a rubric for regulating and resisting that can be adopted from the framework used in dispute resolution: *naming, blaming and claiming*.<sup>78</sup>

In this approach, we argue that a first important step is to be able to articulate and document what sector transgressions mean, and how they emerge and are sustained in different national contexts. We recognise that this phenomenon takes on different forms, and it is critical to be able to 'name' it in its contextual form.



<sup>78</sup> William L.F. Felstiner, Richard L. Abel, and Austin Sarat. 'The Emergence and Transformation of Disputes: Naming, Blaming, Claiming . . .' *Law & Society Review* 15, no. 3/4 (1980): 631–54. <https://doi.org/10.2307/3053505>.

After the ‘naming’ stage of our approach, the second stage involves people and groups not just acknowledging the potential existence of the phenomenon, but also how this phenomenon has material implications for people’s lives. We examine specifically how the phenomenon is linked with its perpetrators, thereby enabling an attribution *blame* according to how the phenomenon infringes on people’s rights and affects them negatively in other ways.

The third stage involves finding methods or campaigns to apply pressure and draw responses from tech firms and governments through litigation, advocacy and storytelling, among other methods ‘claiming’ rights and justification.

#### 4.1 Naming it - how to investigate

As part of the first phase of articulating what constitutes a sector transgression, we have identified a set of criteria. These criteria do not all have to be met in order to constitute a transgression, however, each of them in some way contributes to the creation of new dependencies, the crowding out of expertise, and the shrinking of public sector capacity as discussed earlier.

The cases were determined based on the following criteria:

- ◆ 1. Examine whether technology companies are strategically moving into a new area of business. This may mean:
  - ◆ a. A new product or service.
  - ◆ b. Scaling up an existing offering in ways that create significant change.
  - ◆ c. New ways of interaction with the government through partnerships.
- ◆ 2. When did the process of movement between sectors begin?
- ◆ 3. What is at stake in terms of the protection of public interest? For example:
  - ◆ a. Create political and/or economic dependencies on the part of the state.
  - ◆ b. Use infrastructure or capacity built for one sector or function for a different sector or function.
  - ◆ c. Crowds out existing capacity in the new area where the company is operating.<sup>79</sup>
- ◆ 4. What kind of arrangements or mechanisms are taking place? For instance:
  - ◆ a. A Public Private Partnership (such as Amazon or Palantir’s collaboration with governments on healthcare logistics)
  - ◆ b. Independent action by a firm (e.g. WhatsApp becoming the mode of public health commu-

---

◆ 79 Sharon, T. (2020). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech’s newfound role as global health policy makers. *Ethics and Information Technology*, 1-13.

<https://link.springer.com/article/10.1007/s10676-020-09547-x>

nication by the World Health Organization (WHO)<sup>80</sup> by virtue of its scale and coverage)

- ◆ c. Pro-bono service (such as a firm offering their services without remuneration)
- ◆ d. Public procurement in emergency contexts.
- ◆ e. Ad-hoc legitimising of new applications by government

This template is a guide for identifying a transgression, but it also functions as a guide for considering the local context of emergence, and the given historical and legal environment.

## 4.2 Blaming - establishing points of responsibility

In the second part of the approach we focus on the adverse effects of the phenomenon of sector transgressions on people's lives, in order to attribute blame and establish points of responsibility. We focus on developing a *responsibility assessment framework*, which has three components. The first component establishes what kind of dependency has emerged as a result of the transgression, the second component examines whether the regulatory architecture is the cause or a potential response to the transgression, and the third component is in regard to the rights implications that the transgression has had for people and their lives.

### **Dependency assessment**

In this assessment we ask who is being made dependent and in what ways. The categories of dependencies that we have uncovered include the following:

- ◆ 1. **Economic and infrastructural dependencies:** public authorities become dependent on cloud analytics, adtech-supported services and analytics platforms, leading to data and power concentrating with the biggest players.<sup>81</sup>
- ◆ 2. **Ethical dependencies:** companies are not qualified to work in the new sector or function and either skip ethical deliberation entirely or become dependent on ethics assessments from consultants (who also may not be qualified, as when verification technology provider Vottun and consultants PwC, and RocaSalvatella collaborated to roll out a blockchain based digital health passport in Spain)<sup>82</sup>.
- ◆ 3. **Political dependencies:** the capacities of commercially provided computational infrastructures, and their influence, determine both the parameters within which public authorities make policies for a sector, and the extent of ethical scrutiny of a particular application.
- ◆ 4. **Civic dependencies:** public sector actors become dependent on commercial tools to scale up their provision in response to the pandemic (e.g. WhatsApp being adopted by the WHO for global health messaging).

---

◆ 80 See: WHO Health Alert brings COVID-19 facts to billions via WhatsApp

◆ <https://www.who.int/news-room/feature-stories/detail/who-health-alert-brings-covid-19-facts-to-billions-via-whatsapp>

◆ 81 Relatedly, the uptick in government affairs positions at technology companies is noteworthy and a key concern with respect to dependencies on private sector expertise. See: <https://twitter.com/orientaljanedoe/status/1410227259319984133>

◆ 82 See Redaccion. (2020, April 15) 'Vottun, Con PwC Y RocaSalvatella Crean Los Pasaportes De Inmunidad O Pasaportes

- ◆ 5. **Regulatory dependencies:** relaxation of national regulatory controls in order to ensure continued provision by technology firms.

In each of these dependency domains we ask the following questions:

- ◆ 1. What were the original relations between actors within a market or sector?
- ◆ 2. What has changed?
- ◆ 3. Who has been made dependent on whom?

### **Regulatory assessment**

Many governments received technological solutions without charge during the pandemic's emergency phase, so a lack of regulation meant that tech companies often avoided basic public procurement requirements. Likewise, other governments used the emergency powers to issue ad-hoc regulations to implement technological solutions offered by companies and thereby avoided democratic controls. In other cases, governments used the special powers to downplay the public procurement or the data protection regulations to buy solutions offered by tech companies. In this context, civil society organisations and their funders, as well as oversight organisations, would benefit from understanding the state of regulation vis-a-vis a potential sector transgression.<sup>83</sup>

- ◆ 1. What was the nature of state regulation at the time of the transgression?
  - ◆ Did a regulation exist?
  - ◆ Were regulations relaxed? Was there limited regulatory compliance?
  - ◆ Has an ad-hoc regulation been introduced?
- ◆ 2. Did the private entity offer to regulate? What was the model of regulation proposed and what was the rationale?
- ◆ 3. Did the courts intervene? What was the nature of the complaint?
- ◆ 4. Did the Data Protection Authority intervene? Did the authority have enough power or capabilities to participate in the process?

Options for different regulatory interventions:

- ◆ 1. What was the range of options considered?
- ◆ 2. Who would deliver the options, and what were the implications of the options on existing regulatory instruments?
- ◆ 3. What were the stated policy objectives of each option?

---

Sanitarios - Territorio Blockchain'. <<https://territorioblockchain.com/vottun-con-pwc-y-rocasalvatella-crean-los-pasaportes-de-inmunidad-o-pasaportes-sanitarios/>>

- ◆ <sup>83</sup> See generally the regulatory impact assessment template from the UK Government <https://www.gov.uk/government/publications/impact-assessment-template-for-government-policies>



Decision:

- ◆ 1. Why was a particular option preferred? What were the benefits of its implementation plan?
- ◆ 2. How was this decision communicated to the affected parties? Was it communicated at all?
- ◆ 3. To what extent did the public have access to this information?

### **Rights Assessment**<sup>84</sup>

In this component, we examine the different kinds of questions for fundamental rights that have emerged for people. This includes not just aspects of participation, transparency and accountability but also how grievances are redressed.

- ◆ 1. Was there an assessment of the potential impact of the transgression on people's rights?
- ◆ 2. What kind of data was collected to measure/evaluate the impacts on people?
- ◆ 3. Was there a prioritisation of human rights? If so, on what basis?
- ◆ 4. Was the change in regulatory conditions open and transparent? Did it include meaningful involvement from different interest groups?
- ◆ 5. Were there avenues to challenge the rights assessment?

## **4.3 Claiming**

In the third part of the approach, we focus on approaches that have been taken by civil society organisations in order to resist and respond to cases of sector transgressions and claims redress for the excesses at different levels. We focus on three particular approaches: strategic litigation, documentation and finally, campaigning.

### **4.3.1 Claiming strategy 1: strategic litigation**

Strategic litigation is a method to identify opportunities for legal action that can have social, political and legal impacts. Through such legal action, organisations aim to identify lacunae within the law; they highlight adverse consequences that exist in the absence of robust legislation, as well as ensure that people's legal needs are brought to the attention of adjudicatory forums.<sup>85</sup>

As the pandemic progressed, organisations across Europe began to explore and examine which cases had the potential to effect change. Organisations explored questions of strategic litigation that concerned the questions of surveillance during the pandemic, the lack of transparency in processes adopted by governments across Europe, as well as the impact this was having on people's access to public life.

---

◆ 84 See generally Danish Institute for Human Rights, 'Human rights impact assessment guidance and toolbox', <https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox/introduction-human-rights-impact-assessment>

◆ 85 See for instance the work of ECCHR that uses strategic litigation as a tool to bring about systemic change <https://www.ecchr.eu/en/glossary/strategic-litigation/>. See also the work of systemic justice a new organisation aiming to understand

Organisations employed a mixture of strategies including freedom of information requests to provide the public with information about technologies being implemented by governments; they also used data subject access requests and public campaigning around certain issues. A 2021 report by the Digital Freedom Foundation explains that in the context of technology adoption during the pandemic, some of the key challenges going forward are the need to a) examine the repurposing of COVID-19 tech, b) articulate pandemic-related technology inequalities, and 3) work with judges and courts to better understand the implications of technologies for automated decision making as well as pandemic-related surveillance.<sup>86</sup>

## **Cases of strategic litigation across Europe**

### **Foxglove and OpenDemocracy**

In March 2020, the UK Department of Health and Social Care signed a deal with Palantir to run a COVID-19 database from the National Health Service (NHS). In June 2020, the alliance between the civil society organisations Foxglove and OpenDemocracy forced the UK government to reveal information about the contract. In December 2020, they revealed that the NHS signed without public participation a deal with Palantir to extend the agreement for 23 million pounds<sup>87</sup>. At the beginning of 2021, the alliance of CSOs led a legal action over the government's failure to consult the public before the signature of the agreement. After the judicial review claim, the government put the contract on pause and agreed to consult with the public before signing this expansion and to conduct a new analysis of the data protection compliance of the relationship.<sup>88</sup>

### **Digital Freedom Fund**

The Digital Freedom Fund, an organisation that supports strategic litigation to protect digital rights in Europe, created a COVID-19 litigation fund to collaborate with NGOs challenging digital rights violations in the context of the pandemic. They are funding many organisations using strategic litigation in Europe like Liberties EU, Women on Web, Big Brother Watch, Gesellschaft für Freiheitsrechte, and La Quadrature du Net<sup>89</sup>. Some of these cases are also detailed below.

---

the impacts of community focussed litigation- <https://systemicjustice.ngo/what-we-do/>

- ◆ 86 Digital Freedom Fund. (2021, January). Safeguarding Digital Rights amidst COVID-19 through Strategic Litigation on IA. <https://digitalfreedomfund.org/wp-content/uploads/2021/01/20210104-DFF-AI-COVID-Report-FINAL.pdf>.

87 Adam Bychawski. (2021, November 9). UK Health Department Ends Data Deal with 'Spy Tech' Company Palantir.

- ◆ *OpenDemocracy*. <https://www.opendemocracy.net/en/opendemocracyuk/uk-health-department-ends-data-deal-with-spy-tech-company-palantir/>.

88 Foxglove. (2021, January 4). Success! UK Government Concedes Lawsuit over £23m NHS 'data Deal' with Controversial

- ◆ US Tech Corporation Palantir. *Foxglove*. <https://www.foxglove.org.uk/2021/04/01/success-uk-government-concedes-lawsuit-over-23m-nhs-data-deal-with-controversial-us-tech-corporation-palantir/>.

- ◆ 89 Digital Freedom Fund. (2020). COVID-19 Litigation Fund. *Digital Freedom Fund* (blog). <https://digitalfreedomfund.org/>

### **Gesellschaft für Freiheitsrechte (Society for Civil Rights) and health insurance data**

Gesellschaft für Freiheitsrechte is involved in litigation to ensure that there is greater care and security in the manner in which data around health is shared by health insurance companies for research purposes with other institutions in Germany. The case is designed to also give people the options to control and object regarding the use of their data.<sup>90</sup>

### **Gesellschaft für Freiheitsrechte (Society for Civil Rights) and proctoring software**

In this case, the focus is on litigating in regards to the implications that proctoring software has on students' lives. The case aims to obtain a decision that holds that the processing of data during exams is unlawful.<sup>91</sup>

### **Bulgarian Helsinki Committee and access to information**

The Bulgarian Helsinki Committee (BHC) is a civil society organisation focused on defending the most vulnerable groups in Bulgarian society.<sup>92</sup> The organisation filed a case in the Administrative Court of Sofia City to push the Ministry of Health to provide the Data Protection Impact Assessment (DPIA) about the Bulgarian COVID tracing app ViruSafe. In May 2021, the court obliged the Ministry to provide the DPIA to the BHC.<sup>93</sup>

### **Liberties EU and monitoring of contact tracing apps in the EU**

The Civil Liberties Union for Europe is an NGO that works to safeguard the human rights of everyone in the European Union. The organisation has a network of members in 18 European countries. The organisation is using multiple actions like freedom of information requests, data protection complaints and litigation before courts to stop the use of COVID-19 apps that do not respect fundamental rights. They are also using these litigation mechanisms to expand the transparency about the use and development of these apps. They are working in nine EU countries: Bulgaria, Croatia, Italy, Hungary, Lithuania, Poland, Slovenia, Spain, Sweden, Belgium, Germany, and Ireland.<sup>94</sup>

---

[grants/covid-19-litigation-fund/](#).

◆ 90 Digital Freedom Fund. (2020). Sharing of Health Data by German Public Health Insurance Providers," *Digital Freedom Fund* (blog). <https://digitalfreedomfund.org/sharing-of-health-data-by-german-public-health-insurance-providers/>.

◆ 91 COVID-19 Litigation Fund Case Studies. (2020). *Digital Freedom Fund* (blog). <https://digitalfreedomfund.org/covid-19-litigation-fund-case-studies/>.

◆ 92 Bulgarian Helsinki Committee. (2021). Who We Are | BHC. <https://www.bghelsinki.org/en/who-we-are>.

◆ 93 Civil Liberties Union for Europe. (2021, March 15). Court Decisions. Knowledge Hub: COVID-19 Contact Tracing Apps in the EU. *Liberties.eu*. <https://www.liberties.eu/en/stories/trackerhub4-court-decisions/43531>.

◆ 94 Civil Liberties Union for Europe. (2021). COVID-19 Contact Tracing Apps in the EU. *Liberties.eu*. <https://www.liberties.eu/>

**La Quadrature du Net and drone surveillance:** La Quadrature du Net, a French Civil Society Organisation, went to the French Council of State to ban the use of drone surveillance in the context of the pandemic. On 18 May 2020, the French Council of State ordered the Paris Police to cease carrying out surveillance measures using drones in Paris to monitor compliance with the health security rules during the COVID-19 pandemic. In December 2020, following the first ban, the organisation obtained another victory in the French Council of State banning the Paris Police from using drones in demonstrations.<sup>95</sup>

**La Quadrature du Net and health passes:** The French CSO also used legal actions against the obligation of presenting a health pass that includes information about recent covid tests and vaccination status. In July 2021, the French Council of State rejected their arguments against the legality of the health pass obligation.<sup>96</sup>

**The Human Rights League and the contact tracing app in Belgium:** The Belgian government, using the powers of the state of emergency due to COVID-19, issued Royal Decree No. 44 as a specific regulation to give legal basis to the digital contact tracing app. The government replaced the Decree with a Cooperation Agreement between the federal state and federal entities. The Belgian NGO Human Rights League constructed a complaint against the Decree and the Agreement to the Constitutional Court.<sup>97</sup>

What are the challenges?

Even though strategic litigation is recognised as one of the most effective tools to protect human rights,<sup>98</sup> implementing it could be complicated, considering the kind of problems that the sector transgressions pose. In this section, we draw attention to some limitations that this context could bring to litigation work:

**Funding:** Strategic litigation tends to be expensive and depends on long-term funding that allows civil society organisations (CSOs) to analyse, construct and execute a case.<sup>99</sup> Sector transgres-

---

[en/get-involved/covid-contact-tracing-app-information-hub/68](https://www.laquadrature.net/en/get-involved/covid-contact-tracing-app-information-hub/68).

95 La Quadrature du Net. (2020, December 22). Interdiction des drones : victoire totale contre le gouvernement. *La Quadrature du Net*. <https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/>.

96 La Quadrature du Net. (2021, July 6). Passe sanitaire : le Conseil d'État valide la violation de la loi. *La Quadrature du Net*. <https://www.laquadrature.net/2021/07/06/passe-sanitaire-le-conseil-detat-valide-la-violation-de-la-loi/>.

97 Civil Liberties Union for Europe. (2021, May). COVID-19 Technology in the EU: A BITTERSWEET VICTORY FOR HUMAN RIGHTS. [https://dq4n3btxmr8c9.cloudfront.net/files/c-5f-T/Liberties\\_Research\\_EU\\_Covid19\\_Tracing\\_Apps.pdf](https://dq4n3btxmr8c9.cloudfront.net/files/c-5f-T/Liberties_Research_EU_Covid19_Tracing_Apps.pdf).

98 Dimitrina Petrova. (2018, November 18). Strategic Human Rights Litigation in Tough Times. *OpenGlobalRights*. <https://www.openglobalrights.org/strategic-human-rights-litigation-in-tough-times/>.

99 European Union Agency for fundamental rights. (2017). Challenges Facing Civil Society Organisations Working on Human

sions, on the other hand, tend to be fast and unpredictable, so the organisation needs institutional funding to redirect it towards litigation. In this context, strategic litigation may be too expensive for some organisations that generally depend on short-term and project-focused funding.

- ♦ **Time:** Strategic litigation is not a one-step solution but rather a complicated process that needs to be iterative.<sup>100</sup> Likewise, the timeframe between the design of a litigation strategy and the implementation of a positive judicial outcome could be long, especially in the context of solutions implemented suddenly in the middle of states of emergencies. Furthermore, the team needed for this kind of job that includes litigators, complainants, and members of social movements is difficult to assemble on short notice. For this reason, organisations may depend on other tools like research, advocacy, and public communication that could be used to develop a litigation strategy.
- ♦ **Adverse outcomes:** Human rights litigation could lead to a negative judicial outcome that could impact the organisation on holding accountable the solutions implemented by governments. In the context of the pandemic, the possibilities of governments<sup>101</sup> claiming that the limitation of Human Rights is necessary to protect public health are high. Thus, a negative outcome could end up legitimising the activities of governments that implemented solutions without having legal or administrative grounds.
- ♦ **Interpretation and simple remedies:** The precise interpretation of the ruling is open to interpretation by the government. In this sense, many of the remedies depend on the political will of the government.<sup>102</sup> This situation means that some governments use strategies to diminish the judicial outcomes and interpret the result in a way that does not fundamentally offer a remedy.
- ♦ **Negative discourse and stigmatisation:** The implementation of solutions framed as necessary in a health crisis means that the individuals resisting them could be framed as a danger to public health. The requirement of many litigation contexts of having specific individuals affected by the solution makes them visible to the government. This context could translate into the stigmatisation of the affected community.

#### 4.3.2 Claiming strategy 2: Documentation

Among others, organisations such as Tactical Tech or AlgorithmWatch have also been engaged in documentation and monitoring. In their projects, *Technologies of Hope and Fear* and *Tracing the Tracers*, respectively, an attempt is made to create an open access resource that contributes towards building an understanding of the implications of technologies and tech firms in the everyday lives of

---

Rights in the EU. Luxembourg: Publications Office of the European Union.

- ♦ 100 Open Society Justice Initiative. (2018, October 23). Strategic Litigation Impacts: Insights from Global Experience. <https://www.justiceinitiative.org/uploads/fd7809e2-bd2b-4f5b-964f-522c7c70e747/strategic-litigation-impacts-insights-20181023.pdf>.
- ♦ 101 Tamar Ezer. (2016). *Advancing Public Health through Strategic Litigation: Lessons from Five Countries*. Open Society Institute, and Public Health Program. New York, NY: Open Society Foundations.
- ♦ 102 Open Society Justice Initiative. (2018). Strategic Litigation Impacts: Insights from Global Experience. <https://www.justiceinitiative.org/uploads/fd7809e2-bd2b-4f5b-964f-522c7c70e747/strategic-litigation-impacts-insights-20181023.pdf>.

people. Both projects are designed not just to investigate the design of different technologies, but also question their appropriateness, use and value in terms of securing people's freedoms.

### **Technologies of Hope and Fear (Tactical Tech)**

Over the course of the pandemic, Tactical Tech, a civil society organisation based in Berlin, has been documenting different kinds of technologies that have been introduced to mitigate the impacts of the pandemic. These include quarantine bracelets, contact tracing apps and pandemic drones. Some of the technologies have essential functions but others are designed as distractions, creating further implications for safety, privacy and safety, as they seek to control more and more aspects of how people go about their lives.<sup>103</sup>

### **Tracing the Tracers (AlgorithmWatch)**

AlgorithmWatch, a civil society organisation also based in Berlin, has been documenting and analysing the ways in which automated decision making systems have been employed as a response to the COVID-19 pandemic. The objective of the project is to inform the public about the use, design and implications of technologies like vaccine passports, wearables, contact tracing apps and AI-based diagnostics applications on fundamental freedoms. Doing so is meant to enable people to be able to participate more consciously in terms of the choices they make to use such technologies.<sup>104</sup>

As resources, the role that such documentation plays becomes important from a monitoring perspective, as it provides the basis for demanding accountability and transparency from the government and private sector, and strengthening democratic processes.

### **Sphere Transgression Watch (Radboud University)**

Sphere Transgression Watch, a project by the Digital Goods team at Radboud University in the Netherlands, documents and studies the growing influence of tech companies in the area of health and medicine. The project documents how companies like Amazon, Palantir, Apple and others are using their technology and business advantage in digital infrastructures in other domains. Through documenting these different transgressions, the project aims to offer a 'normative framework for mitigating risks that can account for conflicting societal discourses about justice and the common good.'<sup>105</sup>

### **COVID-19 Infrastructure Playbook (Superr)**

Superr, a civil society organisation in Germany, created a digital playbook which documents the ways in which civil society organisations across Europe have played a role in contributing to building and operating public digital infrastructure during the pandemic. The playbook argues for better coordina-

---

103 Tactical Tech, Technologies of Hope and Fear. <https://techpandemic.theglassroom.org/#normalisation-section>

104 AlgorithmWatch. Tracing the Tracer., <https://algorithmwatch.org/en/tracing-the-tracers/about-the-project/>

105 I-Hub. Radboud University, Sphere Transgression Watch <https://www.sphere-transgression-watch.org/>

tion between government and civil society to deliver on better access to digital services. It argues that civil society in relation to COVID tech plays different roles: from those that built technology, to those that aim to make technology accessible, to those that act as intermediaries ensuring tech is safe, and finally to those that play the role of watchdogs.<sup>106</sup>

### 4.3.3 Claiming strategy 3: Campaigns

Another strategy frequently employed to build public participation has manifested in campaigns and petitions for changes to the law. In these approaches, organisations pressure not just institutions, but also local representatives, to make changes to laws and policies.

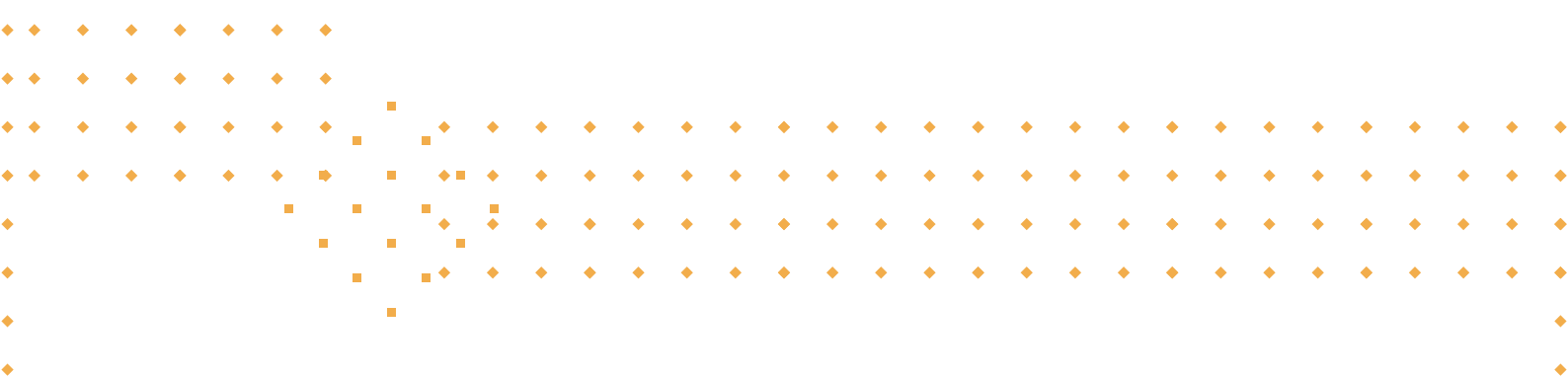
EDRi and the Reclaim your Face campaign: EDRi is a network of European civil society organisations defending and advancing rights and freedoms online. In the case of EDRi's work on Reclaim your Face, they aimed to first garner enough support to mandate the European Commission to meet with them through securing one million signatures in seven EU countries. Consequently, not only is the Commission expected to engage meaningfully with the proposal, but the Parliament is also expected to participate in an open debate.<sup>107</sup>

◆ **Epicenter.works, Liberties EU and the EU Digital COVID Certification:** Epicenter.works is an NGO working on defending and advancing digital rights, which established an advocacy campaign to include their recommendations for the EU Digital COVID Certificate. They were able to include some changes in the original legislation, including more accessible testing, paper-based certificates, sunset clauses, and measures to protect medical data.<sup>108</sup>

### Big Brother Watch and thermal cameras

Big Brother Watch, a civil society organisation in the UK, launched a campaign against the use of thermal cameras that were implemented under the cover of the pandemic. They show that the use of this technology is invasive and inaccurate. To respond to this threat, Big Brother Watch asked over 80 businesses, workplaces, schools, care homes, airports, and hospitality venues to stop using thermal surveillance. They made public the list of the institutions using thermal surveillance and their status. The organisation is planning to take legal action to stop the use of these systems.<sup>109</sup>

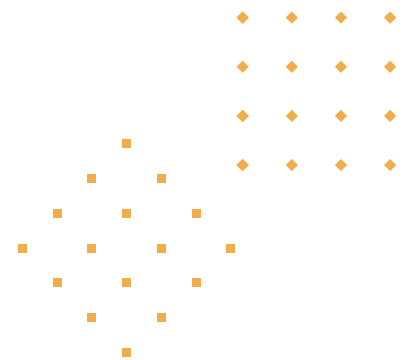
- 
- ◆ 106 Superr. Covid-19 Infrastructure Playbook, [https://superr.net/assets/downloads/COVID-19-Infrastructure-Playbook\\_EN.pdf](https://superr.net/assets/downloads/COVID-19-Infrastructure-Playbook_EN.pdf)
  - ◆ 107 European Digital Rights (EDRi). (2021, May 13). Ban Biometric Mass Surveillance! European Digital Rights (EDRi). <https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>.
  - ◆ 108 Epicentre works (2021). Five reasons to claim victory on the EU Digital Covid Certificate <https://en.epicenter.works/content/five-reasons-to-claim-victory-on-the-eu-digital-covid-certificate>
  - ◆ 109 Big Brother Watch. Stop Thermal Surveillance. (2020). <https://bigbrotherwatch.org.uk/campaigns/thermal-surveillance/>.



The objective of this section was to examine how civil society organisations are responding to the emergence of sector transgressions in Europe. We used the framework of naming, blaming and claiming to characterise the work of the CSOs.

First, we specify the methodology used to characterise phenomena as a sector transgression. The idea of this section was to provide tools and strategies on how to define problems, and characterise sector transgressions. Second, we develop a series of tests to determine the state of the play with respect to regulation and the possible targets for resistance based on the cases explored in the previous sections. Third, we map and describe the CSOs' resistance against sector transgressions. This analysis includes cases of strategic litigation, documentation and campaigns.

This section offers a framework to understand sector transgressions, but at the same time, describes the methodologies that human rights organisations are using to respond. It is meant to be a resource to support the existing work already being carried out by CSOs. In that sense, rather than being a call to action to CSOs, this examination is key for funders, public officials, parliamentarians and academics to support the work of CSOs in understanding the long-lasting impact for public values that the expansion of technology companies into public functions represents.





## 5. Conclusions

Our report has examined how, across Europe, technology firms are making inroads into public sector service provision in the domains of health, education, transport, security and border control, but also less visibly into the analytics, data management, identification and verification tasks that underlie those public functions. Our research suggests that we should no longer think about a ‘tech sector’, but instead about technology firms as possessing the infrastructures and power that underpin some of our most basic public goods, with resulting problems for public control and accountability.

We have explored this phenomenon both in terms of supply-side and demand-side dynamics. In the first, companies have opportunistically moved into new domains in response to the challenges of developing and scaling up new public-sector functions necessitated by the pandemic. In the second, governments have taken advantage of the emergency to open up the possibility of new forms of privatisation and the delegation of key functions.

Both of these dynamics have been accompanied by a weakening of the regulatory scrutiny through which not only technology firms, but also the relations between the state and the private sector are governed. Likewise, this dynamic involves the consumerisation of pandemic technology in certain sectors in which the state’s involvement has been weakened over time, for example in the care sector. The transgressions that have surfaced in this report take place across a wide variety of European countries, manifesting differently in each place depending on the political and economic conditions: in some places nepotism and corruption are the most prevalent mechanisms for allowing transgressions to occur, while in others the existing presence of massive technological market power provides the impetus for sector and scope creep. The effects are concerning, however, in each of the nine very different countries we were able to research.

This expansion of technological power is no longer just another facet of neoliberal privatisation policies, nor a problem that can be tackled by increased attention to privacy rights. We still lack the vocabulary to explain the extent of its implications for policy, regulation and civil society: it threatens to constitute a remaking of the public sector, of our workplaces, schools and households. We have argued in this report that we should address this larger problem, relating the infrastructural level to the public-facing applications and services visible around us, and to offer avenues for civil society and regulation to address it. All the sectoral transgressions by firms described in this report tend to have underlying infrastructure in common, for example Amazon’s web services software, Microsoft’s educational platform, Salesforce’s analytics platform, or Google or Apple’s hardware. These in turn operate based on cloud services, which are run by this group of the world’s wealthiest firms, whose capacity makes possible the sectoral applications we see taking hold on a global scale.

Technology firms are increasingly taking on the functions of states: they are providing essential digital infrastructure to the public sector, and in turn providing the parameters for what policy can achieve in fields such as public health, transport and welfare systems. Meanwhile, states are behaving more like companies: they increasingly prioritise economic efficiency over public welfare, and subcontract key duties and services to private sector firms with inadequate capacities and ethics. In the pandemic this has resulted in a strong current of critique from the business community,<sup>110</sup> holding that governments should weigh the success of pandemic policy mainly in terms of minimising economic disruption.

The increased reach and participation of technology firms in relation to the public sphere in particular poses threats not only to privacy, but to other public goods such as self-determination, political engagement, health, education and knowledge, and ultimately the notion of publicness itself - the capacity and resilience of the public sector in relation to tasks and services that address vulnerabilities and basic needs, and therefore necessitate democratic accountability. Technology firms' infrastructural and strategic reach now often determines the room for policy decisions: the remote education stack now helps functionally determine how many students universities can serve, something which has traditionally been decided by education policy and universities themselves. Digital public health infrastructures such as vaccine certificates, monitoring of location and contacts, and logistics services define the parameters for government decision-making and influence the aims of public policy. Remote payments and identification systems create new forms and degrees of traceability for individuals and our activities, with new and opaque business models attached.

Many have argued that the pandemic has sparked innovation that will in turn promote economic growth at a time when it is sorely needed, and that this should be celebrated. A closer look at the phenomenon of transgressions, however, shows not merely the disruption of business as usual (which could legitimately bring new efficiencies and capabilities to service provision) but the destruction of mechanisms for providing public goods, and the risk of genuine destabilisation. The combination of accelerated privatisation with increased ownership of the digital underpinnings of our societies puts technology firms not only in control of our public policy, workplaces and homes, but in a position to charge what they wish for that dominance, or to make the functionality we rely on disappear overnight by changing their business models. In the final section, we offer recommendations for how to combat this technological and infrastructural power and challenge its legitimacy.

---

<sup>110</sup> <https://www.bloomberg.com/news/features/2021-10-28/how-goguardian-ai-spyware-took-over-schools-student-devices-during-covid>

## 6. Recommendations

We have outlined a dual challenge: first, governing technological power on the sectoral level, where private sector firms are making inroads into formerly public services and functions in ways that create new dependencies and potential harms; and second, controlling the underlying accumulation of infrastructural power that ensures the continuing increase in number and magnitude of these sectoral problems, and that will not be addressed easily by our current regulatory and oversight infrastructures. Civil society organisations are the most effective in challenging, resisting and shaping the changes we have seen either sparked or accelerated by the pandemic. They have the mandate and the power (through ‘naming, blaming and shaming’) to create both public awareness and, through it, potentially political will to regulate both particular technology interventions and infrastructural power more broadly.

Our recommendations, on this basis, are as follows:

- ◆ **Think beyond privacy and surveillance:** in order to contest technology firms’ strategies and power accumulation, it has become necessary to go beyond arguments based on privacy or surveillance harms alone. A more holistic approach is needed; namely, one that can address the broader legitimacy of technology firms’ activities in the public sphere.<sup>111</sup> This in turn requires challenges based on the whole range of civil and political rights, collective as well as individual, that are threatened by this expansion of technological power.
- ◆ **Use sectoral problems strategically to build public awareness of underlying ones:** The sectoral transgressions described in this report are symptoms rather than self-contained problems. Together, they indicate an underlying penetration of commercial technological power which cannot be addressed effectively by focusing on a single type of transgression or sector-specific injustice. Tackling it requires an overarching vision of the work technology should, and should not, do in our societies, what is legitimate and what we collectively wish to declare illegitimate. In this sense, we argue for the value of seeing the sectoral approach as a basis for tackling more systemic problems.
- ◆ **Join forces with organisations not (yet) focused on digital rights:** A holistic approach at scale requires coordination between domain-based and digital rights organisations. An important resource exists in the form of sectoral organisations such as trade unions, patients’ associations and student unions, but also in other non-digitally focused rights organisations such as migrants’ or children’s rights associations, anti-corruption organisations and social justice groups. This requires intermediaries such as funders and academics to help make connections. It also requires

◆ 111 For more on conceptualising this approach, see: Taylor, L. (2021). Public actors without public values: legitimacy, domination and the regulation of the technology sector. *Philosophy & Technology*, 34(4), 897-922. <https://link.springer.com/article/10.1007/s13347-020-00441-4>

resources and strategic capacity - bringing an antiracism group together on a problem with a privacy rights organisation will mean that challenges will take longer to build, but may ultimately be more effective.

- ♦ **Seek out funding to support collaborative work:** Strategically integrating digital rights groups' work with that of domain and interest-based organisations cannot be done without the support of funders. Funders play a key role in the choices civil society organisations make about how to orient their work, as well as their ability to build capacity, knowledge and skills to meet emerging challenges of the kind we have outlined in this report.
- ♦ **Coordinate transnationally to map the challenges:** The map of technological transgressions is multinational and diverse. The only successful strategy for challenging this power grab involves building capacity and alliances across Europe, including in countries where its manifestations may look different. Building the informational links between regulators, legal institutions and CSOs in different countries is important in order for local actors to frame their responses in relation to larger trends.

## ANNEX: the cases we use for this report

This annex contains an overview of all the evidence of sector transgressions and infrastructural scaling-up gathered during this research. It includes a variety of cases that reflect the transgressive nature of tech infrastructure, and as such, illustrates how the application of new and emerging data-driven technologies and the use of existing technologies undermine sectoral perspectives in new ways. This annex contains additional information on the cases of sector transgressions we have identified, and will enable civil society (including policymakers) to analyse and make complete sense of the findings in this report. The cases discussed in this annex are selected primarily from nine European countries (UK, Spain, France, Netherlands, Germany, Poland, Romania, Hungary and Italy), focussing primarily on the key sectors identified elsewhere in this report, including education, payments, policing and security, health, and transport. The cases include:

1. GS4
2. Iproov and Mvine
3. Iproov
4. Hikvision
5. IPLATO
6. SCC Bournemouth
7. Vottun
8. Doctolib
9. RECO<sub>3.26</sub>
10. Bending Spoon S.P.A
11. KC Wearables
12. Vodafone
13. Palantir
14. Central Bureau of Statistics and T-mobile
15. Deutsche Telekom and SAP
16. Luca
17. UiPath
18. Nextsense
19. Onfido and Sidehide
20. Enduring Net
21. Biotip
22. EAS Technologies
23. EYN Limited
24. The Hub Company

- ◆ 25. Logifect
- ◆ 26. Amazon
- ◆ 27. IBM and Cisco
- ◆ 28. Proctorio
- ◆ 29. Zoom

## Health:

- ◆ **1. G4S:** This is a private security company headquartered in the UK. In April 2020, the company began playing a major role in the UK's COVID-19 response, providing overall site management at 15 COVID-19 testing sites in consultation with Deloitte.<sup>112</sup> G4S was also tasked with managing and organising the entire supply chain for Covid testing and handling the booking of tests. The company has no track record in this health sector, but capitalised on its integrated security infrastructure to drive a covid testing programme in the UK. This shows that the company has crossed from offering security services to providing services in the health sector that would ordinarily be handled by professional health workers. Despite its history of defrauding the UK government,<sup>113</sup> the company has cemented its move and has been awarded a £1.1 billion six-month contract to oversee quarantine services in London from September 2021 to March 2022.<sup>114</sup> The reports of inappropriate behaviour by G4S personnel handling quarantine protocols are a clear example of the dangers of allowing companies to function in areas where they lack the professional and ethical competence to operate.<sup>115</sup>
- ◆ **2. iProov and Mvine:** This is a partnership between the two tech companies, iProov and Mvine. iProov is a global leader in biometric technology that works with governments, security agencies and banks,<sup>116</sup> whereas Mvine is a deep tech company well known for its identity management software, which it offers to banks, law enforcement and schools.<sup>117</sup> Mvine and iProov developed a COVID-19 biometric an-

---

◆ 112 'COVID-19 Testing Set up in Days in Response to Pandemic' <<https://www.g4s.com:443/news-and-insights/insights/2020/06/03/g4s-and-covid-19-testing-centres-in-the-uk>> accessed 25 March 2022.

◆ 113 Rob Davies, 'G4S Fined £44m by Serious Fraud Office over Electronic Tagging' *The Guardian* (10 July 2020) <<https://www.theguardian.com/business/2020/jul/10/g4s-fined-44m-by-serious-office-over-electronic-tagging>> accessed 25 March 2022.

◆ 114 '£1.55 Billion Contracts Awarded to Corporate Giants for COVID Quarantine Security' (*Byline Times*, 21 October 2021) <<https://bylinetimes.com/2021/10/21/1-55-billion-contracts-awarded-to-corporate-giants-for-covid-quarantine-security/>> accessed 25 March 2022.

◆ 115 'Covid Quarantine Hotels: Women Say They Were Sexually Harassed by Guards' *BBC News* (26 June 2021) <<https://www.bbc.com/news/stories-57609164>> accessed 25 March 2022.

◆ 116 'Covid-19 Passport from IProov and Mvine Moves Into Trial Phase' (*UKTN | UK Tech News*) <[https://www.uktech.news/technology\\_news/covid-19-passport-from-iproov-and-mvine-moves-into-trial-phase](https://www.uktech.news/technology_news/covid-19-passport-from-iproov-and-mvine-moves-into-trial-phase)> accessed 4 April 2022.

◆ 117 Jane Imrie, 'Biometric Tech Firm Launches Live Testing of UK COVID-19 Passport' (*Bdaily Business News*) <<https://bdaily.co.uk/articles/2021/01/13/biometric-tech-firm-launches-live-testing-of-uk-covid-19-passport>> accessed 4 April 2022.

tibody test results sharing system. The companies were jointly developing a test status digital passport to foster its widespread acceptance and access to COVID-19 test results. The project received funding to the tune of £74,270 from Innovate UK<sup>118</sup> between May 2020 and March 2021.<sup>119</sup> The technology is supposed to link COVID tests to the test subjects by using AI to make an abstract mathematical model of the test subject's face.<sup>120</sup> The technology is also supposed to help persons carrying out covid tests to match and authenticate the tests. The biggest selling point of the technology is that it can easily be integrated with the existing NHS infrastructure that iProov is already part of, cancelling the need to invest in extensive new infrastructure.<sup>121</sup> iProov provides identity management services for the NHS app used to access medical records and book GP appointments.<sup>122</sup> This technology has been rendered obsolete by the development and adoption of COVID-19 vaccination passports.

◆ **3. Hikvision:** the company produces cameras for thermal screening and video solutions for social distancing and crowd control. A nursing home group in the UK issued a press release that it would be installing Hikvision Thermal imaging cameras in 25 of its homes to combat the spread of COVID-19.<sup>123</sup> Spain's airport operator, AENA, which manages around 46 airports in Spain, has worked to implement thermal cameras at various airports, e.g., Alicante-Elche.<sup>124</sup>

---

◆ 118 Innovate UK is the UK's national innovation agency setup to support business-led innovation in all sectors, technologies and UK regions, and to help businesses grow through the development and commercialisation of new products, processes, and services. see, 'Innovate UK' <<https://www.ukri.org/councils/innovate-uk/>> accessed 8 April 2022.

◆ 119 'Covid-19 test status digital passport, with privacy protection for adults and children' <<https://gtr.ukri.org/projects?ref=64901>> accessed 4 April 2022.

◆ 120 *ibid.*

◆ 121 'Covid-19 Passport from IProov and Mvine Moves Into Trial Phase' (UKTN | UK Tech News) <[https://www.uktech.news/technology\\_news/covid-19-passport-from-iproov-and-mvine-moves-into-trial-phase](https://www.uktech.news/technology_news/covid-19-passport-from-iproov-and-mvine-moves-into-trial-phase)> accessed 4 April 2022.

◆ 122 'Face Authentication for NHS Login (Android & IOS) | IProov' (20 May 2020) <<https://www.iproov.com/press/facial-authentication-nhs-login-android-ios>> accessed 4 April 2022.

◆ 123 'Perth Company Balhousie Care Introduces Thermal Imaging Cameras to Reduce Spread of COVID-19' (*Perth Gazette*, 2 June 2020) <<https://perthgazette.co.uk/2020/06/perth-company-balhousie-care-introduces-thermal-imaging-cameras-to-reduce-spread-of-covid-19/>> accessed 3 April 2022; see also, ipvideomarket, 'Dahua and Hikvision Fever Cameras Endanger French and Scottish Nursing Homes' (*IPVM*, 00:55 400AD) <<https://ipvm.com/reports/hikua-nursing>> accessed 1 April 2022.

◆ 124 AleLeo, 'AENA Relies for Its Airports on Hikvision's Thermometric Solutions' (*Digital Security Magazine*, 21 July 2020) <<https://www.digitalsecuritymagazine.com/2020/07/21/aena-confia-aeropuertos-soluciones-termometricas-hikvision/>> accessed 1 April 2022.

- ◆ **4. IPLATO Healthcare:** This company runs the largest independent GP booking and healthcare management app in the UK, called 'myGP'.<sup>125</sup> In response to the pandemic, IPLATO added two new features to the app, video consultation and a COVID-19 vaccination certificate. IPLATO was also among the 11 suppliers selected to provide remote video consultation services to the NHS under a 48-hour accelerated procurement process in March 2020.<sup>126</sup> The vaccination status management feature was added to the app in April 2021 on IPLATO's initiative.<sup>127</sup>
- ◆ **5. Doctolib:** This platform is a cloud-based tool that helps healthcare professionals manage appointments and refer patients to colleagues. The platform is also used by patients to schedule appointments.<sup>128</sup> Doctolib is hosted by Amazon web services. In January 2021, the French Ministry of Health partnered with Doctolib for the management of COVID-19 vaccination appointments. Several health professional associations and unions oppose the arrangement because of Doctolib's use of AWS, but the highest Administrative Court in France (Conseil d'État) rejected their petition for the suspension of the partnership between the Ministry and Doctolib.<sup>129</sup> The reasoning for the Court's decision was that 'the data collected in the context of vaccination appointments do not include health data on medical reasons for eligibility for vaccination and guarantees have been put in place to meet a possible request for access by the American authorities'.<sup>130</sup>
- ◆ **6. Bending Spoon S.P.A:** This company is mainly a consumer app developer, producing apps for fitness, photo editing, password apps and games. In April 2020 the Italian government announced 'Im-muni' as its official COVID-19 contact tracing app.<sup>131</sup> The app was developed by Bending Spoon S.P.A.

- 
- ◆ 125 Lanna Cooper, 'England's First "smartphone Vaccine Status Feature" to Launch in Feb 2021' (*Startups Magazine*) <<http://startupsmagazine.co.uk/article-englands-first-smartphone-vaccine-status-feature-launch-feb-2021>> accessed 1 April 2022.
  - ◆ 126 'Exclusive: 11 Suppliers Chosen to Provide Video Consults during Covid-19' (*Digital Health*, 26 March 2020) <<https://www.digitalhealth.net/2020/03/exclusive-11-suppliers-chosen-to-provide-video-consults-during-covid-19/>> accessed 1 April 2022.
  - ◆ 127 Neil Shaw, 'Vaccine Passport Will Roll out next Month with Trials next Week' (*WalesOnline*, 25 March 2021) <<https://www.walesonline.co.uk/news/uk-news/vaccine-passport-roll-out-next-20250882>> accessed 11 April 2022..
  - ◆ 128 'French Government Partners with Doctolib for Covid-19 Vaccine Appointments - The Local' <<https://www.thelocal.com/20210112/french-government-partners-with-doctolib-to-allow-people-to-book-covid-19-vaccine-appointments-online/>> accessed 3 April 2022.
  - ◆ 129 Mathieu Pollet, 'France under Fire for Use of Amazon-Hosted Doctolib for Job Bookings' (*www.euractiv.com*, 3 March 2021) <<https://www.euractiv.com/section/digital/news/france-under-fire-for-use-of-amazon-hosted-doctolib-for-jab-bookings/>> accessed 3 April 2022.
  - ◆ 130 Conseil d'Etat, Data, Health: No Suspension of the Partnership between the Ministry of Health and Doctolib' (UGGC Avocats, 6 April 2021) <<https://www.uggc.com/en/conseil-detat-data-health-no-suspension-of-the-partnership-between-the-ministry-of-health-and-doctolib/>> accessed 3 April 2022.
  - ◆ 131 'Italy: Extraordinary Commissioner Initiates Development App for Coronavirus Contact Tracing' (*DataGuidance*, 17 April 2020) <<https://www.dataguidance.com/news/italy-extraordinary-commissioner-initiates-development-app-coronavirus-contact-tracing>> accessed 3 April 2022.



for the Special Commissioner for the COVID-19 emergency (Presidency of the Council of Ministers), in collaboration with the Ministry of Health and the Ministry for Technological Innovation and Digitalisation. It was then released under a GNU Affero General Public Licence version 3.<sup>132</sup>

- ◆ **7. Deutsche Telekom and SAP:** This duo developed a contact-tracing app for the German government called 'Corona Warn App', which was launched in June 2020.<sup>133</sup> Corona Warn App was built on the Google/Apple contact tracing API infrastructure, and the developers claim that the app is decentralised. In July 2020, the European Commission entered into a contract for SAP and Deutsche Telekom to develop a platform that would make national coronavirus contact tracing apps interoperable.<sup>134</sup>
- ◆ **8. Nextsense:** This company is a Hungarian ICT solutions provider for the government, as well as for telecom and finance organisations. Nextsense developed and donated the contact-tracing app 'VirusRadar' to the Hungarian government.<sup>135</sup> On 13 May 2020, the Hungarian Ministry of Innovation and Technology (ITM) announced VirusRadar as the official contact-tracing app for the country.<sup>136</sup>

### Transport & mobility:

- ◆ **9. iProov:** in June 2020 iProov announced it would provide contactless facial biometric corridors for Eurostar rail passengers to complete ticket checks and other border exit processes at St. Pancras International station in London.<sup>137</sup> The development, which is being run by Innovate UK and is funded by the Department for Transport, has now gone live as of December 2021.<sup>138</sup>

---

◆ 132 *Immuni's High-Level Description* (Immuni - Commissario straordinario per l'emergenza Covid-19 2022)

<<https://github.com/immuni-app/immuni-documentation>> accessed 3 April 2022.

◆ 133 'Corona Warn App from SAP & Deutsche Telekom' (*SAP News Center*, 17 June 2020) <<https://news.sap.com/2020/06/corona-warn-app-deutsche-telekom-sap/>> accessed 3 April 2022.

◆ 134 Douglas Busvine, 'SAP, Deutsche Telekom to Build Corona App Gateway for European Commission' *Reuters* (31 July 2020) <<https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKCN24W277>> accessed 3 April 2022.

◆ 135 'Hungary Launched VirusRadar Mobile Application, Donated By Nextsense' (*AmCham*) <<https://amcham.mk/news/hungary-launched-virusradar-mobile-contact-tracing-application-donated-by-nextsense/>> accessed 4 April 2022.

◆ 136 'Matteo Mastracci, 'Hungary Introduces VirusRadar, First National Contact Tracing App' (*Balkan Insight*) <<https://balkaninsight.com/techresponses/hungary-introduces-virusradar-first-national-contact-tracing-app/>> accessed 11 April 2022.

◆ 137 'iProov to Provide Contactless Travel Entry for Eurostar as Part of Railway Innovation Initiative' *Financial Post* (17 June 2020) <<https://financialpost.com/pmnp/press-releases-pmn/business-wire-news-releases-pmn/iproov-to-provide-contactless-travel-entry-for-eurostar-as-part-of-railway-innovation-initiative>> accessed 3 April 2022.

◆ 138 'iProov and Eurostar Launch Trial to Provide Contactless Travel at London St Pancras International' (6 December 2021) <<https://www.businesswire.com/news/home/20211205005029/en/iProov-and-Eurostar-Launch-Trial-to-Provide-Contactless-Travel-at-London-St-Pancras-International>> accessed 3 April 2022.

- ◆ **10. SCC Bournemouth:** The adoption of thermal cameras (thermal fever detection technology) by governments, transport authorities and businesses was a huge part of the response to the COVID-19 pandemic.<sup>139</sup> For instance, at Bournemouth Airport in the UK, the IT solutions provider, SCC, installed thermal cameras to identify employees with high temperatures before they could socialise with their colleagues.<sup>140</sup> The company also announced that it would introduce thermal cameras to scan passengers and intercept any passengers showing signs of a high temperature.<sup>141</sup>
- ◆ **11. KuangChi Science Limited (KC Wearables):** This company developed the KC Ng01 Smart helmet for epidemic prevention and control.<sup>142</sup> In May 2020, KC wearables announced partnerships with European Authorities to combat COVID-19. The helmet has been used in both Italy and the Netherlands.<sup>143</sup> The helmet allows the wearer to detect persons with elevated body temperature by using infrared cameras to measure temperature and detect fevers from up to five metres away.
- ◆ **12. Palantir:** the company offers analytics, data mining, security and intelligence tools to governments and organisations.<sup>144</sup> Throughout the pandemic, Palantir has provided its technology to the Netherlands' six safety regions to help them monitor the crisis and measure their response.<sup>145</sup> Palantir's technology is responsible for integrating publicly accessible data, including demographic, economic, traffic and mobility data, and COVID-19 data to help monitor the geographic spread of COVID-19 in real time and analyse the impact of the response measures.<sup>146</sup> In March 2020, Palantir entered a no-cost contract with the Greek government to help the government with data-driven decision making in the context of the COVID-19 pandemic response.<sup>147</sup> The arrangement did not go through the proper public

---

◆ 139 Meredith Van Natta and others, 'The Rise and Regulation of Thermal Facial Recognition Technology during the COVID-19 Pandemic' (2020) 7 *Journal of law and the biosciences* Isaa038.

◆ 140 'SCC to Trial Thermal Fever Detection Technology at Bournemouth Airport' (*Airport Technology*, 30 April 2020) <<https://www.airport-technology.com/news/scc-thermal-fever-detection-technology-bournemouth-airport/>> accessed 1 April 2022.

◆ 141 *ibid.*

◆ 142 'KC Wearable Announces SMART Helmet Is Being Used in 35 Countries' (*AiThORITY*, 19 June 2020) <<https://aithority.com/vision/face-recognition/kc-wearable-announces-smart-helmet-is-being-used-in-35-countries-globally/>> accessed 3 April 2022.

◆ 143 *ibid.*

◆ 144 'Dutch Group Calls for Scrutiny of Palantir Over Opaque Partnerships With EU Law Enforcement Agencies, Possible Privacy Violations' (*Privacy en Online Veiligheid | SOMI*) <<https://somi.nl>> accessed 3 April 2022.

◆ 145 'Powering Pandemic Response in the Netherlands | Palantir Blog' <<https://blog.palantir.com/powering-pandemic-response-in-the-netherlands-9ecc608081c>> accessed 3 April 2022.

◆ 146 *ibid.*

◆ 147 'Non-Transparent Partnership of the Greek Government with Palantir Technologies, a Data Processing Company, to Deal with the COVID-19 Pandemic' <[https://www.europarl.europa.eu/doceo/document/E-9-2020-007026\\_EN.html](https://www.europarl.europa.eu/doceo/document/E-9-2020-007026_EN.html)> accessed 3 April 2022.

procurement procedure: the details of this contract were hidden from the public and the Greek authorities did not conduct a data protection impact assessment.<sup>148</sup>

- ◆ **13. Vodafone:** In March 2020 the telecoms company announced that as part of its response to the COVID-19 pandemic it would be using data assets to produce an anonymous and aggregated heat map for regional authorities in Lombardy, Italy. Vodafone used its analytics platform to give government authorities insight into population movements to contain the spread of the virus. Vodafone has replicated this solution in Spain and are attempting to offer the same insight to authorities in Greece, Portugal and the UK.<sup>150</sup>
- ◆ **14. Dutch Central Bureau of Statistics (CBS) and T-Mobile:** CBS and T-Mobile had an existing arrangement dating back to 2017. The partnership involved the use of software and algorithms to produce socially and economically relevant statistics.<sup>151</sup> In response to the pandemic, CBS was to receive location data from all telecom providers to create statistics of movement for the Dutch National Institute for Public Health and the Environment (RVIM).<sup>152</sup> The Dutch DPA criticised the use of location data in general and its use for tracking population movements in the context of the COVID-19 pandemic and as result, the partnership between CBS and T-Mobile ended on 1 April 2021.<sup>153</sup>
- ◆ **15. Onfido and Sidehide:** Onfido is a global identity verification company partnered with a hotel booking platform (Sidehide) to roll out a COVID-19 immunity passport, which would be integrated into the hotel booking platform.<sup>154</sup> Onfido also approached the UK Government to help develop COVID-19

---

◆ 148 iDaniel Howden and others, 'Seeing Stones: Pandemic Reveals Palantir's Troubling Reach in Europe' *The Guardian* (2 April 2021) <<https://www.theguardian.com/world/2021/apr/02/seeing-stones-pandemic-reveals-palantirs-troubling-reach-in-europe>> accessed 3 April 2022.

◆ 149 'Correct Use of Telco Data Can Help in This Crisis' (*Vodafone.com*) <<https://www.vodafone.com/news/digital-society/correct-use-of-telco-data-can-help-in-this-crisis>> accessed 3 April 2022.

◆ 150 *ibid.*

◆ 151 Peter Olsthoorn, 'Hebben T-Mobile En CBS Mijn Privacy Geschonden? | Tweede Kamer Beschuldigde al, Kabinet Wacht Onderzoek Af | Netkwesties' <<https://www.netkwesties.nl/1497/hebben-t-mobile-en-cbs-mijn-privacy-geschonden.htm>> accessed 11 April 2022.

◆ 152 Wilmer Heck, 'Lang voor de coronaspoedwet volgde het CBS al telefoons van burgers' (*NRC*) <<https://www.nrc.nl/nieuws/2020/06/09/lang-voor-de-coronaspoedwet-volgde-het-cbs-al-telefoons-van-burgers-a4002280>> accessed 11 April 2022.

◆ 153 'Statistics Agency and T-Mobile Broke Privacy Laws over Data: NRC' (*DutchNews.nl*, 11 March 2021) <<https://www.dutchnews.nl/news/2021/03/statistics-agency-and-t-mobile-broke-privacy-laws-over-data-nrc/>> accessed 11 April 2022; see also, Wilmer Heck, 'Hoe het CBS en T-Mobile de privacy schonden' (*NRC*, 10 March 2021) <<https://www.nrc.nl/nieuws/2021/03/10/hoer-het-cbs-de-privacy-schendt-a4035030>> accessed 11 April 2022.

◆ 154 Paul Jarratt, 'Onfido and Sidehide to Bring Immunity Passports to the Travel Industry' <<https://onfido.com/resources/blog/onfido-and-sidehide-to-bring-immunity-passports-to-the-travel-industry>> accessed 4 April 2022.

immunity passports based on the already existing digital identity of individuals.<sup>155</sup>

- ◆ **16. EYN Limited:** EYN is a biometric security company that develops biometric systems for identity verification in airports and government agencies.<sup>156</sup> The pandemic provided the opportunity for EYN to develop its biometric technology into a COVID-19 immunity passport (Novel Immunity Passports for COVID-19). UKRI funded this project to the tune of £46,797 to link facial biometrics to test subjects in order to prove ‘immunity’ status.<sup>157</sup>
- ◆ **17. The Hub Company:** this company offers customer-facing digital platform solutions for passenger travel and transit, finance, events, health, retail and the public sector.<sup>158</sup> Due to the COVID-19 pandemic, the hub company received a grant of £49,448 from the UK government to develop security systems capable of issuing secure digital or physical certificates proving COVID-19 immunity or vaccine results.<sup>159</sup>
- ◆ **18. Logifect:** the company is a digital health solution provider that developed a platform for telehealth, healthcare decision support and chronic disease management.<sup>160</sup> Due to the pandemic Logifect expanded into providing a solution to validate post-vaccination status (Integrated mobile indemnity passport platform).<sup>161</sup> The company received funding (£62,209) from UKRI to develop COVID-19 post-vaccination immunity passports.<sup>162</sup>

### Employment & events:

- ◆ **19. Vottun:** Vottun is a blockchain specialist start-up based in Spain. In April 2020 the company collaborated with PwC and Roca Salvatella consulting firms to roll out a blockchain-based Proof of

---

◆ 155 *ibid.*

◆ 156 ‘EYN - Verify Identities in Seconds, at Scale’ <<https://www.eyn.vision/about-us>> accessed 12 April 2022; see also, ‘Eyn | Venture eRadar’ <<https://www.ventureradar.com/organisation/Eyn/ocd9aee3-b778-4ec2-bff8-c79474c19277>> accessed 12 April 2022.

◆ 157 ‘GtR’ <<https://gtr.ukri.org/projects?ref=54135>> accessed 4 April 2022.

◆ 158 ‘The Hub Platform Solutions – The Hub’ <<https://www.thehub.co.uk/solutions/>> accessed 12 April 2022.

◆ 159 Hannah Boland, ‘Government Funds Eight Vaccine Passport Schemes despite “no Plans” for Rollout’ *The Telegraph* (24 January 2021) <<https://www.telegraph.co.uk/technology/2021/01/24/government-funds-eight-vaccine-passport-schemes-despite-no-plans/>> accessed 4 April 2022.

◆ 160 ‘Cheap GPU Servers for AI Training’ <<https://www.logifect.com/#about-us>> accessed 12 April 2022; see also, ‘Logifect’ (*EU-Startups*) <<https://www.eu-startups.com/directory/logifect/>> accessed 12 April 2022.

◆ 161 UKRI, ‘Integrated Mobile Indemnity Passport Platform’ <<https://gtr.ukri.org/projects?ref=64691>> accessed 12 April 2022.

◆ 162 Ben Riley-Smith and Lucy Fisher, ‘Britons Vaccinated against Covid Could Get QR Codes to Travel’ *The Telegraph* (8 February 2021) <<https://www.telegraph.co.uk/politics/2021/02/08/britons-vaccinated-against-covid-could-get-qr-codes-travel/>> accessed 4 April 2022.

Health Verification Solution in Spain.<sup>163</sup> The technology is essentially a digital health passport to help ascertain the COVID-19 status of employees and enable the resumption of economic activities.

- ◆ **20. EAS Technologies:** This company trading under the name Accredited Solutions received £173,877 from the UK government to develop an accreditation platform (Accredit Go) for COVID-19 credentials such as vaccination certificates and health passports to be used in the 'global sporting and events industry, effectively to allow it to get back to hosting sporting and live events'.<sup>164</sup> Accredited solutions is an accreditation system for event management and venue security for political, sporting and live events.<sup>165</sup> Due to the Covid -19 pandemic, the capabilities of the accreditation system was extended for use in collecting information on COVID-19 credentials and contact tracing.<sup>166</sup>

### Security:

- ◆ **21. RECO3.26:** This company offers a range of solutions in response to the COVID-19 health crisis. These solutions include crowd detection, people counting and DPI check to verify that the subject is wearing personal protective equipment.<sup>167</sup> These solutions have now been offered to the Italian government for use in subways to prevent the formation of gatherings and for implementing measures to inhibit the spread of COVID-19.<sup>168</sup> Before the pandemic, RECO3.26 offered AI and facial recognition technology (S.A.R.I.) to law enforcement for forensic investigation.<sup>169</sup>
- ◆ **22. Luca:** This is a centralised COVID-19 contact tracing app launched in Germany. The app developers claim that Luna is fast and secure.<sup>170</sup> About 13 German federal states used the app for COVID

- 
- ◆ 163 Redaccion, 'Vottun, Con PwC Y RocaSalvatella Crean Los Pasaportes De Inmunidad O Pasaportes Sanitarios - Territorio Blockchain' (15 April 2020) <<https://territorioblockchain.com/vottun-con-pwc-y-rocasalvatella-crean-los-pasaportes-de-inmunidad-o-pasaportes-sanitarios/>> accessed 3 April 2022.
  - ◆ 164 Boland H., 'Government Funds Eight Vaccine Passport Schemes despite "no Plans" for Rollout' *The Telegraph* (24 January 2021) <<https://www.telegraph.co.uk/technology/2021/01/24/government-funds-eight-vaccine-passport-schemes-despite-no-plans/>> accessed 21 March 2022.
  - ◆ 165 'About' (*Accredited Solutions*) <<https://www.accredited-solutions.com/about/>> accessed 11 April 2022.
  - ◆ 166 'Accreditation Health Tools' (*Accredited Solutions*) <<https://www.accredited-solutions.com/our-solutions/covid-tools/>> accessed 11 April 2022.
  - ◆ 167 Super User, 'Reco 3.26 - RECO - COVID-19' (*Reco 3.26*) <<https://www.reco326.com/en/solutions/covid-19>> accessed 6 April 2022.
  - ◆ 168 '[BigDataSur-COVID19] Come La Sorveglianza Biometrica Si Sta Insinuando Nel Trasporto Pubblico – DATACTIVE' <<https://data-activism.net/2021/02/bigdatasur-covid19-come-la-sorveglianza-biometrica-si-sta-insinuando-nel-trasporto-pubblico/>> accessed 3 April 2022.
  - ◆ 169 'RECO 3.26' (*MWC Barcelona 2022*) <<https://www.mwcbarcelona.com/exhibitors/reco-3-26>> accessed 6 April 2022.
  - ◆ 170 'luca App - verschlüsselte Kontaktdatenübermittlung' (*luca*) <<https://www.luca-app.de/>> accessed 3 April 2022.

infection notifications, but at least five governments have discontinued use of the app.<sup>171</sup> The Luna app has been used for contact tracing on school buses, at bars, restaurants and events. Despite the privacy and data protection claims about the app, the German police came under serious criticism in January 2022 after it was discovered that the police misused the Luna app to track down witnesses in a local criminal case.<sup>172</sup>

### Payments:

◆ **23. UiPath:** This is a robotic process automation platform. The company announced it was offering its platform to assist Romanian public sector organisations in combating the spread of COVID-19. UiPath offered hospitals free licences and technical support to use their platform for routine and daily activities like reception of patients in emergency units.<sup>173</sup> In March 2020, the Romanian government provided unemployment benefits to cater to persons whose jobs had been affected by the pandemic. In response, UiPath offered its platform and technical support to the National Agency for Payments and Social Inspection (ANPIS) to manage the applications for their benefit.<sup>174</sup>

### Education:

◆ **24. IBM and Cisco:** These firms provide free access to their platform for teachers and students in Madrid in collaboration with the Ministry of Education and Youth.<sup>175</sup> The platform is Cisco Webex (a cloud computing solution), and IBM offers support to the teaching community for the use of the platform.<sup>176</sup> The platform is accessible to all regions of Spain and possibly to other areas of administration that may benefit from the remote collaboration platform.<sup>177</sup> The free access to the platform allows private companies to participate in the maintenance of a public good/service in light of the COVID-19 pandemic. This creates a dependency on these private companies, who are left to determine the capabilities, features and availability of the free technology.

- 
- ◆ 171 Matthias Monroy, 'Tracking corona infections: German Luca app in a downfall – Matthias Monroy' <<https://digit.site36.net/2022/01/22/tracking-corona-infections-german-luca-app-in-a-downfall/>> accessed 3 April 2022.<sup>172</sup>
  - ◆ 172 Rachel Pannett, 'German Police Used a Tracing App to Scout Crime Witnesses. Some Fear That's Fuel for Covid Conspiracists.' *Washington Post* <<https://www.washingtonpost.com/world/2022/01/13/german-covid-contact-tracing-app-luca/>> accessed 3 April 2022.
  - ◆ 173 'UiPath Launches Measures to Support the Romanian Public Sector in the Fight with the Crisis Caused by Covid-19' <<https://www.amcham.ro/amcham-romania-resource-center-for-covid-19-response/member-initiatives/uipath-launches-measures-to-support-the-romanian-public-sector-in-the-fight-with-the-crisis-caused-by-covid-19>> accessed 4 April 2022.
  - ◆ 174 'Timely Processing of Financial Support Applications during the COVID-19 Pandemic | UiPath' <<https://www.uipath.com/resources/covid-automations/timely-processing-financial-support-applications-covid19>> accessed 4 April 2022.
  - ◆ 175 'IBM and Cisco Facilitate Remote Teaching in Madrid' (*IBM Newsroom*) <<https://newsroom.ibm.com/2020-03-19-IBM-and-Cisco-facilitate-remote-teaching-in-Madrid>> accessed 4 April 2022.
  - ◆ 176 *ibid.*
  - ◆ 177 *ibid.*

- ◆ **25. Proctorio:** As a result of the pandemic, proctoring software started to be used in in some higher education institutions in the Netherland to ensure that students are not cheating during online exams.<sup>178</sup> The use of proctoring has been challenged, with the Amsterdam District Court ruling in favour in June 2020 on the basis that the company did not keep data insecurely, and that it processed students' personal data in compliance with data protection law, although the students' association argued that the use of the tool in a university context was illegitimate because of the potential for hacking and because they were compelled to use it and had no choice.<sup>179</sup> The Dutch DPA (AP) has provided guidance on the use of such software, and 'expects that remote teaching and testing will continue to be part of education, even after the corona measures have been relaxed'.<sup>180</sup>

- 
- ◆ 178 'Dutch Minister of Education Does Not Want to Interfere with Proctoring | DUB' <<https://www.dub.uu.nl/en/news/dutch-minister-education-does-not-want-interfere-proctoring>> accessed 12 April 2022.
  - ◆ 179 'Omstreden software studenten blijkt onveilig: hackers konden meegluren' (*RTL Nieuws*, 14 December 2021) <<https://www.rtlnieuws.nl/nieuws/nederland/artikel/5273869/studenten-nederland-proctorio-hacken-plugin-uva>> accessed 12 April 2022.
  - ◆ 180 'Aanbevelingen voor privacy bij digitaal thuisonderwijs' <<https://autoriteitpersoonsgegevens.nl/nl/nieuws/aanbevelingen-voor-privacy-bij-digitaal-thuisonderwijs>> accessed 12 April 2022.



# Digital disruption or crisis capitalism? Technology, power and the pandemic

A report by the Global Data Justice project



Written and researched by:

- ◆ Joan Lopez Solano
- ◆ Aaron Martin
- ◆ Franklyn Ohai
- ◆ Siddharth de Souza
- ◆ Linnet Taylor

