

COVID-19

INFRARED
STRIKES
TURKEY
PLAY
BOOK

Content

Executive Summary	4
1. Introduction	6
1.1 Situation and motivation	6
1.2 Key Questions	8
1.3 What is the Purpose of this Playbook?	9
1.4 Definition and Terminology	10
2 Civil Society Engagement in the Context of COVID Tech	12
2.1 The (Re-)Creators	14
2.2 The Providers	16
2.3 The Intermediaries	18
2.4 Watchdogs	20
3. Examples of COVID Tech and Civil Society	22
3.1 Technology-Based Contact Tracing	24
3.2 Community Networks	28
3.3 Data Dashboards	30
3.4 Appointment Scheduling Platform: Tests and Vaccinations	32
4. Insights and Recommendations	34
4.1 Understanding Different Perspectives	36
4.2 Establishing Exchange	38
4.3 Finding Suitable Formats for Cooperation	40
5. Conclusion	42
6. References	44

EXECUTIVE SUMMARY

Civil society has contributed immensely to a quick and creative active response to the changed circumstances through the pandemic, especially in the digital sector. Nevertheless, its engagement has not been sufficiently taken into account or integrated into political and administrative processes. As a result, civil society engagement in the digital sector has not been able to reach its full potential.

The COVID-19 Infrastructure Playbook breaks down the different areas where civil society organisations throughout Europe contribute to requesting, designing and operating public digital infrastructure - as providers and (re-)creators of public digital infrastructure, as intermediaries for open data and as watchdogs over the reasonable implementation of technology in society.

This Playbook uses four examples to illustrate the broad range of issues and the impact of civil society engagement on the creation of better digital technologies for the common good in times of crisis and beyond:

- Technology-based contact tracing
- Community networks and the provision of internet access
- Data dashboards
- Appointment scheduling platforms for tests and vaccinations

Politics and public administration must collaborate more effectively with civil society organisations and initiatives in order to better incorporate their urgently needed expertise and to improve access to basic digital services in Europe. To achieve this, they must

- be open to continuous exchange with civil society organisations and to actively integrating their expertise into political decision making processes
- support digital prototypes developed by civil society and, where necessary, take over the provision and maintenance of these
- understand civil society's demand for digital services (such as transparency, open source, usability) and implement those proactively to create trustworthy technologies.

1

INTRODUCTION

1.1 Situation and Motivation

The COVID-19 pandemic has accelerated digital transformation in many areas of society far more quickly than what had previously been anticipated. Work, education, art and social life were shifted to digital spaces at a much faster rate than predicted. This fast pace was the precise challenge for policy makers, for the public administration and for public institutions, employers and the self-employed: Within a very short space of time, they had to find optimal solutions to continue operating smoothly.

In this challenging scenario, civil society organisations offered swift and simple help which was urgently required. They were able to draw upon their local structures, the expertise they had developed through years of engagement and their solution-oriented, unbureaucratic way of operating. The work of civil society organisations went far beyond conventional neighbourhood assistance: Volunteers around the world produced face masks and shields and shared their instructions under a free license, distributing them to hospitals and other institutions that offered indispensable services locally. However, civil society actors did not only themselves use digital tools, but also provided them to others, thereby contributing to the digital transformation all round.

This kind of civil society engagement has long existed quietly, but it became more visible through the pandemic. Civil society organisations and initiatives could draw upon their expertise and their networks, built over years or even decades, to substantially contribute to a fast, active and creative response to the changed environment of the pandemic.

Which role did these projects play in the greater context of society, politics and the economy? The *COVID-19 Infrastructure Playbook* presents tangible examples of the different forms

of civil society engagement, how it can positively promote digital transformation and why civil society is often unable to reach the full potential of its expertise.

1.2 Key Questions

This Playbook tackles the following key questions:

- What role does and did civil society play in developing public digital infrastructure during the COVID-19 pandemic? Which insights and recommendations can we derive from this?
- Can civil society contribute to better preparing Europe for a swift digital transformation and also improve sustainability and fundamental rights in digitalisation?
- The fast pace of digital transformation during the COVID-19 pandemic has led to an increased market concentration. Which alternatives to monopolised solutions are used by civil society and for which reasons?
- Why has civil society taken on the role of an infrastructure provider? What are the resulting advantages and disadvantages and what kind of framework must be created in order for civil society commitment to rise to its full potential?

1.3 What is the Purpose of this Playbook?

The Playbook is a snapshot of digital civil society engagement in Europe during the pandemic. Different communities in Europe already provide and regularly update extensive lists with examples of civil society engagement, knowledge resources and interviews.¹ Additionally, reports containing general analyses of civil society engagement during the pandemic have been published.² Digital transformation is rightly considered a challenge or even a threat to civil society engagement in all of these resources.

However, such general analyses do not consider the important role digitally fit organisations and institutions play in advancing digital transformation. Therefore, in this Playbook we want to focus on describing and evaluating civil society engagement in the digital field based on specific cases. We capture first insights and results on how civil society, public administration and policy makers can improve their collaboration around digital issues and complement one another. The Playbook should serve as a basis for designing, implementing and maintaining public infrastructure together and in accordance with civil society.

The Playbook is divided into different chapters: **Chapter 2** characterises the different roles of civil society actors that can be derived from the aforementioned cases as well as their strengths and weaknesses. **Chapter 3** describes specific cases to reflect the diversity of civil society engagement in this area. Finally, **chapter 4** outlines the insights collected during our interviews and recommendations for how civil society engagement can be better employed to promote digital transformation in times of crisis and beyond.

1.4 Definition and Terminology

Digital Civil Society

The terms civil society as well as digital civil society lack a clear definition.

For the purpose of this Playbook, we have chosen the following definition:

The Digital Civil Society consists of social movements, collectives and organisations which:

- provide free access to digital technologies, to digital available data and knowledge or to the internet for the common good,
- enable participation, e.g. by providing platforms or trainings, ongoing education or courses for young people on digital, media and technical skills,
- develop technologies for the common good,
- reveal the impact of digital technologies on society,
- promote and shape digital policy.³

We focus on representatives of the third sector who work charitably as non-profit volunteers for the common good, acting independently.

Digital Infrastructure – Public Digital Infrastructure

The term digital infrastructure has no clear definition either. It is used to describe communication infrastructure, IT infrastructure or data infrastructure.

We use the term analogously with public digital infrastructure and thereby address its impact on society. Both terms describe the digital tools, building blocks and services a society needs in order to function digitally. We consider digital infrastructure to be larger than mere technical elements: it is a major factor that influences social life, increases or decreases inequalities, builds or breaks down trust.

We understand digital infrastructure to be the sum of technologies that ensure access to the internet and to digital communication, that enable participation in societal discourse and that are used for furthering education. Public digital infrastructure must be transparent, allowing for active participation and for further technological advancement, as well as placing public benefits ahead of economic interests.

2

CIVIL SOCIETY

ENGAGEMENT

IN THE

CONTEXT

OF COVID

TECH

As our case studies show, civil society actors take on different roles in their work on digital infrastructure. The wide range of these different roles reflects the diversity of digital and technological expertise in digital civil society as well as the shortcomings of politics, administration and business in digital transformation from a societal perspective.

The following role profiles should serve to describe the digital civil society engagement and depict the strengths and weaknesses of its actors. The demarcation of these roles is fluid and single organisations or initiatives can take on different aspects of these roles or take on various roles simultaneously, depending on the situation.

2.1 The (Re-)Creators

Their motto

Yes to technology, but please keep it open!

Their motivation

The (re-)creators are technology enthusiasts who want to understand and shape its development. Their aim is to be up-to-date, and they have high expectations regarding openness and transparency: They develop Free and Open Source Software (FOSS) and open hardware.

Their strengths

They are strongly intertwined with open source communities and many of the (re-)creators work as professional software developers, dedicating their free time to FOSS projects. They know the building blocks of open source technology well and prefer building on existing solutions to re-inventing the wheel.

Their contribution during the COVID-19 pandemic

Many digital solutions that were created directly or indirectly in the context of the pandemic were first developed as proprietary or not fully open source solutions. The (re-)creators re-built these solutions as open source products or alternatives. In the best-case scenario, these impulses are integrated into the original projects and improve official digital solutions by allowing for external checks and thus gaining the trust of their users. (Re-)creators across Europe rebuilt booking systems for vaccination appointments, managed by public authorities, that had collapsed due to the high demand for vaccinations and remained unavailable, or were offered in only one language with poor usability.

Their Achilles' heel

The (re-)creators rely on original product owners to take up their work, because this is the only way for them to call out for more openness and transparency with COVID tech. They have little means to actively request a collaboration - this is where they would need support by public authorities.

How can (re-)creators be strengthened?

Proprietary applications make their work much more strenuous. If, however, public administration used well-documented FOSS products, (re-)creators could actively improve the original product. The introduction of community managers of digital projects as single persons of contact for digital communities who work mainly as volunteers, would enable transparent communication and prevent disappointments.

2.2 The Providers

Their motto

We lay the foundations - then you build on them.

Their motivation

The providers want to make digital tools accessible. They have high expectations regarding openness and transparency: They operate services based on FOSS technology and open hardware. Through their work they show how it is possible to create alternatives to tech monopolies.

Their strengths

The providers operate in a de-centralized and self-organised manner and therefore they can take immediate action. They collaborate with other local or digital communities and support them in their digital organisation and engagement. Their high level of technical expertise allows them to provide first-class services that can compete with commercial offers.

Their contribution during the COVID-19 pandemic

The providers further developed offers and raised awareness when the pandemic first started. They connected seniors in retirement facilities and refugees in accommodation centres to the net while they were in quarantine. They provided online applications for video calls and for remote work services, which were used by doctors, therapists and teachers simply because contracting commercial services for schools and in professional organisations took too much time. These services enabled civil society organisations to continue working without needing extra resources to develop their own digital infrastructures.

Their Achilles' heel

Even if the provided services function steadily in the majority of cases, they lack clearly defined contact persons for external users, or support structures when problems arise. Also, these services deliberately stunt their exponential growth, out of concern for sustainability - a conscious decision that cannot always be understood by external persons. Interested parties cannot always clearly recognise how they can collaborate with providers and which tasks cannot be covered by providers. Therefore, public administration favours commercial companies with a clear portfolio and additional services such as customer hotlines.

How can providers be strengthened?

To collaborate successfully with providers, public administration has to understand their particularities and draw upon their strength: the fast and simple installation of networks. Owing to structural arrangements (e. g. the installation of routers in buildings with high ceilings such as schools or city halls), the providers rely on the administration's openness, but (too) often face concerns and rejection.

2.3 The Intermediaries

Their motto

We can do better!

visualisation to third parties and concentrate on ensuring the data's quality.

Their motivation

The intermediaries are convinced that data and information should be available for everyone because this kind of knowledge helps to bring important societal discussions to the fore and filter out the provision of false information - which, now, in times of crisis, is more important than ever.

Their contribution during the COVID-19 pandemic

The debate about the COVID-19 pandemic and the measures taken to contain its spread were based on data from the very beginning: the number of infections, transmission rates, hospital capacity rates or vaccination rates. Numerous projects, sometimes even just very committed individuals, contributed to collecting this data. They called for interfaces which allow third parties to use the data or even created these interfaces themselves.

Their strength

The intermediaries are experts for data and data interfaces. They prepare data and information in a structured manner for others to use. To this end, they collect data, in some cases with a lot of effort, which is published by public administration, research institutions or commercial companies, but which is not made available to other users in a digitalised format. Apart from merely collecting data, some intermediaries also create dashboards to visualise it. Others leave the

Their Achilles' heel

Up to now, data has been published under licences that strongly limit its use and in a very de-centralised manner. Therefore, intermediaries take legal risks when providing and preparing data. In the USA, some individuals face criminal prosecution because their data dashboards showed early alerts when political measures to contain the pandemic were not working effectively.⁴

How can intermediaries be strengthened?

Intermediaries need two things: machine-readable data and documented structures as well as licences that allow them to further process data.

2.4 Watchdogs

Their motto

We need to claim our rights.

know how to present their findings to a larger audience.

Their motivation

Digital solutions developed or used by public authorities must be safe, comply with data protection regulations and protect user privacy. Proprietary solutions do not always allow for tracking whether these requirements are met and for this reason, watchdog organisations and committed individuals fight for transparency with regard to digital solution functionality, to the types of and reasons for data collection and to the kind of security measures that are in place.

Their contribution during the COVID-19 pandemic

The pandemic has triggered the use and even the creation of new digital tools in the public sector, for example contact tracing apps or monitoring apps for exams taken by students from home. On the one hand, the success of technology-based contact tracing depends on the number of people using the programme. On the other hand, a huge number of people can be affected if the application does not fulfil necessary safety requirements or function appropriately. The watchdogs have contributed to a more careful use of technology by initiating public debates about improving digital applications which had too hastily been implemented at the beginning of the pandemic.

Their strength

Watchdog organisations come with a long history and a lot of experience in claiming fundamental rights. They have even developed support structures for cases in which legal action would be necessary, enabling them to finance court costs and legal advice. The organisations are closely linked to the media and

Their Achilles' heel

The watchdogs' strongest tool is media publicity. However, during the pandemic they have had to compete with other COVID-19 issues. Of course, they could try to advocate their causes and present their research results to IT security and data protection departments of public administration, however they have almost no legal lever by which to put forward their agenda. We observed that the media reproduced a shortened version of the watchdogs' criticism about data protection gaps in digital applications and presented data protection and IT security as if they were insurmountable hurdles for digital solutions.

How can watchdogs be strengthened?

Watchdogs would be most satisfied if their work were not at all necessary, and all weak points were eradicated for once and for all. Audits and assessments of IT security and data protection are the first step in the right direction for recognising a tool's weaknesses before it is implemented. These weaknesses, however, can never be fully eliminated and for this reason, clear reporting channels for responsible disclosures are required.

3

EXAMPLES OF COVID TECH AND CIVIL SOCIETY

3.1 Technology-Based Contact Tracing

1 What is it about?

Since the beginning of the pandemic, numerous digital applications such as mobile apps have been developed to complement and simplify manual contact tracing for public health authorities. This kind of technology-based contact tracing stands out as the most prominent and widely discussed example of COVID tech.

Distribution: Contact tracing apps have to be used by as many people as possible in order to be effective.⁶ However, older devices may not support BLE, the usability of these apps is rather poor and the public lacks trust in these applications, especially when it comes to centralised data collection or processing.

2 What is so special about this example?

Data protection: Mobile contact tracing apps track human contact and movement data, and therefore enter into very private domains which are rightfully protected by exceptionally strict data protection regulations.

Civil society: The debate on technology-based contact tracing in civil society was conducted similarly throughout Europe. Yet, the reactions of each country's government were quite different. Comparing these results is therefore particularly interesting.

Technology: The technical implementation is challenging and requires relatively new standards such as Bluetooth Low Energy (BLE). Another novelty is the agreement between Google and Apple (with a market share of almost 100 percent for operational systems in Europe) to use the "Google/Apple Exposure Notification (GAEN) Framework".⁵

3 Approaches in Europe:

Apps were mainly developed by commercial actors and on national level. Therefore, numerous applications with different functionalities were developed within a short period of time.⁷ The majority of EU member states finally opted for the GAEN framework and a de-centralised approach based on an open DP-3T protocol⁸, which

can partly be implemented as open source software.⁹ These solutions are based on the same standard, but they are tailored for use on a national level. Recently, the EU implemented an “interoperability gateway” to make these solutions sufficiently interoperable. At first, commercial concepts envisioned public authorities to collect and process huge amounts of data in a centralised form. Only through the continual debate among researchers and civil society about data protection risks could this initial approach be re-directed. Finally, GAEN put an end to this data-collection method by establishing a decentralised form.

4 Which role does civil society play?

In the case of technology-based contact tracing, civil society has taken the position of a watchdog: Together with researchers, civil society has vehemently been advocating for applications that comply with data protection regulations and function in a de-centralised manner. They called for transparency when policy makers and commercial players were negotiating the design and the commissioning of applications behind closed doors.

The collaboration became especially fruitful when civil society actively participated in such conversations (see the example of the CoronaMelder

app) and had a say in the design of new applications. In some countries, civil society was forced into the role of civil opposition and was even perceived to be disturbing.

Examples

Chaos Computer Club, Germany: 10 requirements for the evaluation of “Contact Tracing” apps

Back in April 2020, the Chaos Computer Club (CCC) already published a list of 10 requirements that contact tracing applications should fulfil in the future.¹⁰ The CCC considers these rather legal and socio-political requirements to be implemented quite easily and it does not see any reason for lowering existing standards in data protection on the grounds of the pandemic. Even if the CCC does not want to actively advocate for specific applications, it directly addresses the ones which do not fulfil the requirements, as was the case in April 2021. At that time, the CCC addressed the considerable ongoing deficiencies of the commercially provided Luca App, which was widely used in Germany, and demanded its immediate halt on a national level.¹¹

CoronaMelder app, Netherlands: An app turned into community project

In the Netherlands, numerous digital communities collaborated to develop a list of requirements¹² similar to those of the CCC in Germany. Commercial companies and app developers could participate in the “Appathon”, a competition for contact tracing products, which was broadcast via live stream after a standard three-day application process. None of the developed concepts and products could comply with security and data protection requirements.¹³ After the Appathon and as a reaction to the published requirement list, the Dutch Ministry of Health decided to develop the app (CoronaMelder) internally and collaborate actively with civil society organisations. This decision is unique in Europe, for several reasons:

→ Individuals of the digital civil society were called upon and in some cases even hired by the Ministry to contribute to the app development.

→ The application was developed “in the open”, which means it was based on a public code repository, to enable continuous exchange with developer teams, the Ministry and digital communities.

→ The project was a precedent: Apps like CoronaCheck and CoronaCheck Scanner, used to read and approve of certificates of testing, vaccination or recovery, were developed in collaboration with digital communities.¹⁴

The Dutch digital community published a report monitoring to which extend their requirements had already been implemented.¹⁵

Corona Contact Tracing Germany: We can do it without Apple or Google

Google’s and Apple’s decision to follow a de-centralised path with their joint “Exposure Notification Framework” led to their services being implemented in many European countries instead of the initial products which use centralised data collection systems. Simultaneously, actors in the private sector decided which technologies could be implemented and which could not. Precisely because digital infrastructure is supposed to lie in public hands, this creates a problematic situation.¹⁶ While the applications as such are open source, the German Corona-Warn-App for Android uses proprietary Google Play services.¹⁷ A group of volunteering developers created a free alternative to the German Corona-Warn-App, which is able to communicate with the so-called “Exposure Notification API” by using free MicroG software instead of Google Play services. Similar to the Corona-Warn-App, the new app, which is called Corona Contact Tracing Germany, is available in European countries and serves as a contact tracing tool as well as a digital vaccination certificate.¹⁸

3.2 Community Networks

1 What is it about?

Connectivity is a basic requirement for digital transformation. The pandemic showed us painfully which areas do not yet fulfil this requirement and where immediate action is needed in order to prevent the intensification of social inequalities.

2 What is so special about this example?

Basic digital services:

The issue of expanding broadband connections and equal internet access is by no means new in Europe. Nevertheless, the pandemic once again pointed out the areas where mobile or cable internet access as yet remains insufficient. Today, the main factors for distribution inequities are no longer gaps between rural areas and urban centres, but mainly demographic and organisational differences.

Seniors in assisted living facilities and refugees in accommodation centres especially were affected by the lockdown and remained deprived of digital communication tools, hence this affected public as well as privately run facilities.

Digital is local: While numerous digital offers exist online only, connectivity depends on physical reality. Internet connection is always provided locally and therefore, civil society commitment to connect more people to the net is organised locally too.

Shortfalls of commercial providers:

The pandemic clearly unveiled a huge gap between the supply and demand for stable broadband internet access and the shortfalls of commercial providers: Broadband internet access is not commercially profitable and for this reason, the network expansion in rural areas is advancing slowly. It takes public institutions a long time to commission commercial companies and, in addition, internet providers cause further delays due to staff shortages and long waiting times for the final connection activation. In addition, private companies have been insecure about the operator's liability or data protection when offering access to the internet.

3 Which role does civil society play?

Numerous community network initiatives secured digital access while

commercial and public players were reacting far too slowly on their own. Community networks are local groups which are connected across regions and offer free internet access, in most cases free Wi-Fi, by providing their own routers locally. They rely on access to suitable buildings (public buildings are suitable because of their location and high ceilings) and a reliable connection of their router network to the internet. Community network initiatives are represented in numerous European countries. It is difficult to measure their engagement because different local groups provide different offers.

Many factors contributed to the fast and simple support those local groups could offer:

→ The initiatives were well connected locally and had contact points in the fields of politics, public administration and non-profit organisations even before the pandemic.

→ As they used open hardware and software, they owned the technology and were not relying upon external support.

→ The initiatives could use their vast experience to clarify issues and provide information about liability.

The community network initiatives no longer limit their work to establishing networks, maintaining router hard-

ware and developing software for the network configuration. Some local groups also offer additional services such as servers for video conferences and tools for online collaboration like Etherpad, using Free and Open Source Software (FOSS).

In some cases, the initiatives connected senior residencies and refugee accommodation centres to the internet, since they were forbidden from receiving visitors and their technical infrastructure was poorly developed. In addition, the initiatives prepared and distributed end devices as well as servers to host video conferences to at least digitally connect affected people to the outside world.

This example of community networks demonstrates how civil society can contribute with quick, simple solutions. However, these networks cannot operate these services in the long run or offer customer services as commercial providers do. When civil society initiatives and public institutions or private providers collaborate, it is necessary to establish clear expectations and define the competences of all stakeholders right at the outset. In the best-case scenario, a concept is established for public institutions to manage networks and services developed by civil society initiatives in the future.

3.3 Data Dashboards

1 What is it about?

Data is the basis for debates in society and politics about measures to counteract the spread of COVID. Across the globe, collected and processed data, provided in different forms, varied greatly in how resilient and up-to-date it was.

2 What is so special about this example?

National solutions: In Europe, there are huge differences regarding the authorities in charge, their proceedings with collecting infection data, the structure of the data and their presentation. Data has mainly been collectively published by centralised authorities of national health care systems. These institutions have medical expertise, but they lack the digital competencies to establish stable reporting systems¹⁹, process data and distribute data on interfaces for it to be used for example by media for their research and visualisations. At the beginning of the pandemic, these discrepancies between national systems caused data about infections to be incomparable between countries, as they were

not updated simultaneously and showed varying information.

Social discourse: This lack in transparency, together with contradictory databases, has nurtured the spread of false information and conspiracy theory narratives since the outbreak of the pandemic. Changes in these databases were not sufficiently explained and lacked transparency. Consequently, this led to mistrust in numbers about infection rates and in measures to counteract rising infection rates.

Digital multiplication: The collection of data about infections is very complex due to the sheer number of different actors (public health authorities, clinics, medical practices and, over time, testing centres) and the challenging situation in the wake of the pandemic. It is for precisely this reason that providing clear databases should be an integral part of the digital toolkit. Such databases are neither overwhelmingly complex, nor are they difficult to operate if they are set up correctly. In Europe, the Open Data Movement has for years actively advocated for structured and machine-readable databases

3 What role does civil society play?

Since the outbreak of the pandemic, around the world and in Europe²⁰, individuals and small teams have worked to provide open data and information about COVID-19. There are numerous data projects among civil society organisations in Europe and it may be hard to get an overview; yet, this clearly shows the interest in working with open data and creating added value for society. Often, data specialists volunteer to bring these projects to life - projects like collecting and cleaning data from different sources²¹, providing data to third parties²², visualising data online²³ and in certain cases even combining all of these steps²⁴. The content of the projects can mainly²⁵ be summarised as the documentation of infection, recovery, death or vaccination rates, hence, the direct impact and figures of the epidemic. Their entire work depends on public data repositories that are made accessible to them. According to an OECD and TheGovLab report analysing Open Government Data Projects worldwide, many of these projects were conducted by public authorities without including potential users of civil society or research. The data provided by public authorities therefore did not correspond with the needs of their target groups.²⁶ The French project *covidtracker.fr* of Guillaume Rozier has processed and visualised publicly available

data from the very beginning of the pandemic and this example illustrates civil society engagement to open data very well. The visualisations of *covidtracker.fr* are now even used by the French Ministry of Health for their outreach activities.²⁷ Rozier received the French Order of Merit for his commitment to projects such as *covidtracker.fr*, *vitemadose.fr* and *vaccinetracker.fr*.

3.4 Appointment Scheduling Platform: Tests and Vaccinations

1 What is it about?

One of the measures against the spread of COVID-19 were testing, and later, vaccination centres. Huge crowds were expected in these centres and therefore, appointments were scheduled via digital platforms. In some cases, these platforms were not very user-friendly (unreliable accessibility, available in one language only) and in other cases, they had enormous security gaps.

2 What is so special about this example?

Diverse group of stakeholders: Different stakeholders were involved in this project - public authorities, private companies (e.g. operators of testing centres or appointment scheduling platforms) as well as private individuals whose data was transmitted and stored on these platforms.

Sensitive data: Personal information such as names, addresses, dates of

birth and in some instances ID numbers were collected on these appointment scheduling platforms, even if some of this data was not directly required to conduct a test. This information is linked with sensitive health data such as infection or vaccination status. In some cases, digital applications shared user data with third parties (e.g. Facebook).²⁸

Indispensability: For private individuals it is almost impossible to choose alternatives to these platforms, especially in countries and regions where public authorities contracted single private companies for the provision of a platform.²⁹

3 Which role does civil society play?

Civil society organisations and volunteers had two different roles in the context of appointment scheduling platforms: The role of a provider and the role of an external examiner.

Civil society organisations took over the role of providers mainly when platforms handled by public authorities were not functioning well or when services were spread out on different platforms and should have been centralised for more convenient usage and easier accessibility. In the case of vaccination appointment scheduling especially, different offers were developed in many European countries.

The French website *Vite ma Dose!* is another project of the *covidtracker.fr* developers. It is now used commercially and displays vaccination appointments from nine different platforms combined into one.³⁰ The code for this website is available under an open licence.³¹ Similar platforms such as the Berlin website *impfstoff.link* for a mainly English-speaking target group came to a halt when official scheduling platforms were no longer overloaded and therefore easier to use. The user interface of these platforms was not very intuitive and they were structured to represent administrative competences, but it did not allow users to see all available vaccination slots in the region first, and then book a suitable appointment. According to press articles, the Berlin based programmer João Guilherme Cheffer Prado³² is the head behind the platform *impfstoff.link*, the website and the associated bot that scrapped the official platform, then developed and ran *impfstoff.link*.³³ Even if some plat-

forms like *Vite ma Dose!* have been recognised by official authorities, most of them were not considered, even though they offered solutions for the massive shortcomings of public and commercial platforms.

Professional platforms have not only been weak in performance, but in some cases, they have even had huge safety leaks.³⁴ In these cases, tens of thousands of personal data records were not sufficiently secured and it has even been verified that certain data was collected and offered for sale. Civil society watchdog initiatives repeatedly pointed out deficiencies and requested immediate repairs. However, public authorities did not have mandatory security checks in place before these platforms were allowed to launch. The watchdogs were backed by data protection officers in charge but received hardly any support by the authorities responsible for the platform or their providers. Security researchers of *Zerforschung* uncovered several massive security vulnerabilities in overall five different systems of testing centre providers in Germany and Austria. In collaboration with Chaos Computer Club (Germany) and Epicenter.works (Austria), they reported these vulnerabilities to supervising authorities. Other local initiatives also revealed the security gaps of testing centre providers locally.³⁵

4

INSIGHTS AND RECOMMENDATIONS

These examples of the COVID-19 pandemic consolidate what we have observed in other working fields of the digitally active civil society: Policy makers and administration come across civil society organisations in numerous contexts, with different objectives and capacities, in different roles and in diverse structures.

The pandemic has shown that public institutions could benefit from civil society engagement and that committed individuals would be willing to contribute even beyond existing possibilities. Still, there is no simple answer to the question of how to collaborate more effectively, due to the sheer variety of issues and areas.

For this reason, the section below lists typical misunderstandings and false expectations that stand in the way of constructive collaboration between civil society organisations and public administrations, offering possible solutions. It is important to note that these solutions are not valid for all cases and could be implemented manifold on a local level.

We want to underline that there is an urgent need to already engage civil society locally during the conception phase for what a possible cooperation in a specific context could look

4.1 Understanding Different Perspectives

Our examples clearly show that **too often economic players are the partners of choice for building digital infrastructure in Europe** and the impact on society, whether this has to do with data protection, usability or the availability of digital services, is given little attention. Often, civil society initiatives can only condemn the vulnerabilities or mistakes of digital offers **in the opposition role** or provide alternative services with little resources. Services could be improved if civil society actors were already involved in the planning phase of digital services and could contribute at the outset, instead of criticising afterwards. Civil society has proven numerous times that their actors have the necessary skills: Even if their alternatives to public digital infrastructure look like prototypes because they lack resources and capacities, they are usually faster ready for use and easier to navigate than commercial offers.

The debate about hastily implemented COVID tech - in the field of infrastructure and beyond - has shown that civil society organisations have the power to **convey trust in digital services** or, if solutions lack security or transparency, rightfully withdraw this trust.

Trust, however, is essential for the technology to reach a greater audience. Public authorities, though, are the decision makers for choosing which digital solutions are adopted and supported. However, the underlying **reasons for their decisions differ** from those of civil society: Administration favours solutions that can be linked to an existing digital ecosystem within the administrative body and represent their structures as well as those service providers which fulfil economic criteria (credit rating, legal form, etc.). In contrast, the civil society sets the focus on transparency of solutions (FOSS), accessibility and intuitive usability on desktop and mobile devices. Civil society's decision to trust a solution is based on technical functions instead of economic factors. Public administrations can learn from civil society and favour solutions that are built for a greater usability.

Recommendations for politics and administration:

- The inclusion of civil society early on during the planning phases for digital infrastructure.
- The provision of transparent and pro-active communication on digital projects in the pipelines.
- The testing of digital infrastructure and its impact on society as well as questioning its added value.
- Developing an understanding for the requirements of civil society for digital services (such as transparency, open code, usability) and testing technology with the help of focus groups from the civil society to create trustworthy solutions.

4.2. Establishing Exchange

Civil society, politics and administration have very different ways of conducting their work and of communicating. In order to understand the standpoint and motivation of the other party, **continual exchange** is required. Time is a limited resource for civil society because it mostly consists of volunteers working on a project basis. Therefore, the exchange format must be well planned, suited to the issue at hand and targeted to meet a specific goal.

The pandemic has demonstrated that in times of crisis, with time constraints and difficult circumstances, good results and the constructive cooperation of all parties could emerge only where contact and cooperation had previously been established. Where contacts had not previously been established, civil society was integrated into the process at a very late stage, pushed into the role of opposition and forced to develop concurring solutions to those offered by the administration and businesses, or to call out for their improvement.

During the pandemic, short-term exchange platforms, such as hackathons with a clear link to COVID-19, evolved. These events generated a great deal of attention, for example in March

2020 as 28,000 volunteers participated in Germany's hackathon *WirVsVirus*³⁶ which has now been thoroughly evaluated.³⁷ In this particular context, the hackathon can rightfully be considered an initiative for open social innovation - a motor for innovation where civil society, administration and business meet. Nevertheless, civil society initiatives have consciously decided to take on a different role in the innovation sector (see 4.3). A hackathon in this form can fulfil a very specific and limited function, but it is not a panacea. The German civic tech community Code for Germany has worked out guidelines³⁸ for how hackathons can make sense, which purposes they could serve and explicitly for which purposes they do not serve. The long-established format of hackathons was called upon in numerous countries within the context of COVID-19 and they were implemented³⁹ by public institutions, companies and tech communities.⁴⁰

Recommendations for politics and administration:

- To maintain a continuous, but informal exchange with local digital communities.
- To define contact persons (community manager) for the communities, actively engaging and staying up to date with developments.
- To choose suitable formats for exchanges and collaborations: Community managers can better evaluate how civil society can be involved in specific cases and balance expectations.
- To integrate short-term formats into existing structures and make sure that the same solutions are not developed twice.

4.3 Finding Suitable Formats for Cooperation

Civil society cannot and usually does not aim to replace business. Instead, their strength lies in developing prototype solutions that can be adopted and offered by public institutions in charge or contracted companies. **Civil society can give new impulses, but it cannot offer services or provide infrastructure.** If the expertise of administration and civil society can be combined, they can develop better digital offers than businesses. That being said, the collaboration of administration and civil society must follow a different approach to that of administration and business.

Successfully tested **digital solutions often fail to be implemented** by administration or public providers because of failures in the collaboration between civil society and administration. The reason for this is mostly the administration's false assumption that concepts developed by civil society would be spun off commercially and continually offered as products. Most initiatives are not interested in such spin-offs. Therefore, it is essential to **align expectations** of the administration with those of civil society and outline beforehand how a successful

project should be consolidated, which role the various stakeholders should take and which partners might have to be integrated in order to provide the solution continuously.

Ultimately, unlike commercial solutions, services that have been created through civil society organisations require feedback, especially in the form of reports on the impact of their work. Instead of only reporting failures to providers, the administration should intensively share positive experiences.

Recommendations for politics and administration:

- To understand the strengths and weaknesses of prototypes developed by civil society, instead of dealing with them as if they were commercial products.
- To outline objectives at the beginning of a cooperation and to define how a project will be consolidated or ended.
- If possible, to refer back to existing solutions such as prototypes and to further develop them together with the respective local communities.



CONCLUSION

Structures for engagement have long done valuable work to overcome crisis.

COVID-19 showed us that this engagement is becoming more important in digital areas. The above mentioned examples illustrate that civil society actors take on different roles and engage actively in different areas.

However, in many cases their engagement cannot be employed to its full potential, because it is not linked to public administration. Decision makers in politics and administration lack awareness for civil society expertise and perspectives and (involuntarily) push civil society into the role of the opposition.

However, civil society fills the gaps when politics, administration and business fail to provide fast and satisfying solutions. Even if civil society does not want to be an infrastructure provider, they are forced into this role. Their offer continues to be a prototypical support only and therefore, in the long run, public administration must step in and take over projects so as to permanently consolidate them.

In order to make the best use of this form of collaboration, administration and politics need to understand civil society's strengths and requirements better and develop new formats of constructive collaboration.

For without the extensive expertise of civil society actors, politics and administration would have too few tools to cope with the next digital crisis.



REFERENCES

- 1** As for example the collective Pirate Care: <https://syllabus.pirate.care/session/coronavirusresources/>
- 2** For the European Union see for example: <https://www.eesc.europa.eu/sites/default/files/files/qe-02-21-011-en-n.pdf>
- 3** Goethe-Institut, SUPERRR Lab: Das Goethe-Institut und die digitale Zivilgesellschaft. Ein Mapping des Status Quo und zukünftiger Potenziale. Munich 2020, p. 8
- 4** A prominent case is the example of Rebekah Jones from Florida, who was eventually recognised as a whistle blower in California: <https://www.npr.org/2020/06/14/876584284/fired-florida-data-scientist-launches-a-coronavirus-dashboard-of-her-own> and <https://cbs12.com/news/local/ousted-covid-dashboard-designer-rebekah-jones-receives-whistle-blower-status>
- 5** In July 2021 their market share was at 99.3 percent: <https://gs.statcounter.com/os-market-share/mobile/europe>
- 6** Cf. <https://www.technology-review.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/>
- 7** Cf. <https://www.liberties.eu/en/stories/trackerhub1-mainpage/43437>
- 8** See <https://github.com/DP-3T>
- 9** GAEN itself, the core of the software, is not open source.
- 10** See <https://www.ccc.de/de/updates/2020/contact-tracing-requirements>
- 11** <https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse>
- 12** <https://www.safeagainstcorona.nl/> (EN)
<https://www.veiligtegen corona.nl/> (NL)
- 13** Cf. <https://euobserver.com/opinion/148265>
- 14** <https://coronacheck.nl/humans.txt>
- 15** Cf. <https://www.veiligtegen corona.nl/analyse.html>
- 16** Cf. Civil Liberties Union Europe: COVID-19 Technology in the EU - A bittersweet victory for human rights?, p. 6-7
- 17** Cf. <https://fsfe.org/news/2020/news-20201208-01-en.html>
- 18** See <https://codeberg.org/corona-contact-tracing-germany/cwa-android#can-i-use-cctg-outside-of-germany-what-if-i-dont-live-there>
- 19** Cf. <https://www.bbc.com/news/technology-54423988> and <https://www.oecd.org/gov/digital-government/open-data-in-action-initiatives-during-the-initial-stage-of-the-covid-19-pandemic.pdf>, p. 6
- 20** This platform of the EU Commission collects open data pools in the context of COVID-19, including various GitHub repositories of private individuals: <https://joinup.ec.europa.eu/collection/digital-response-covid-19/open-data>
- 21** Example for Slovenia: <https://covid-19.sledilnik.org/en/about> and <https://covid19.alpaka.si/>
- 22** Example for Germany: <https://pavelmayer.de/covid/risks/> or <https://www.corona-in-zahlen.de/>
- 23** Example for Italy: <https://enricotedoldi.it/covid-19-data/>
- 24** Example for France: <https://covidtracker.fr/>
- 25** Cf. <https://www.oecd.org/gov/digital-government/open-data-in-action-initiatives-during-the-initial-stage-of-the-covid-19-pandemic.pdf>, p. 11-13
- 26** Cf. <https://www.oecd.org/gov/digital-government/open-data-in-action-initiatives-during-the-initial-stage-of-the-covid-19-pandemic.pdf>, p. 19
- 27** Cf. <https://www.lci.fr/societe/covid-19-coronavirus-guillaume-rozier-createur-de-covidtracker-et-vite-ma-dose-recoit-l-ordre-national-du-merite-2186730.html>
- 28** See <https://mobilsicher.de/ratgeber/verstoerend-doctolib-app-teilte-sensible-informationen-mit-facebook-und-outbrain>
- 29** In France, the government announced an official partnership with the companies Doctolib, Maiia and Keldoc to manage vaccination appointments and centers: <https://www.decision-sante.com/politique-de-sante/sante-publique/vaccination-doctolib-keldoc-et-maiia-vont-generer-les-rdv-grand-public>
- 30** Last updated August 2021, source: <https://vitemadose.covidtracker.fr/apropos>
- 31** See <https://github.com/CovidTrackerFr/vitemadose-front>
- 32** Cf. <https://netzpolitik.org/2021/npp-232-zur-digitalen-vergabe-von-impfterminen-ein-angebot-dass-du-nicht-annehmen-kannst/>
- 33** Cf. <https://www.berliner-zeitung.de/mensch-metropole/wie-komme-ich-frueher-an-einen-impftermin-die-webseite-impstoefflink-hilft-li.156277>
- 34** Examples in the Netherlands: <https://www.computerweekly.com/news/252495983/Data-of-thousands-of-Dutch-citizens-leaked-from-government-Covid-19-systems>, in Germany: <https://www.reuters.com/world/europe/german-pharmacies-stop-issuing-covid-vaccine-passes-after-security-breach-2021-07-22/> and in the USA: <https://techcrunch.com/2021/08/17/a-simple-website-bug-put-thousands-of-covid-19-test-results-at-risk/>
- 35** Cf. https://kraut.space/blog/content/ergebnis_des_corona-schnelltests_datenschutz_negativ
- 36** See <https://wirvsvirus.org/>
- 37** Cf. https://hertieschool-f4e6.kxcdn.com/fileadmin/2_Research/5_Policy_Briefs/OSI_Policy_Brief_2021_EN.pdf
- 38** See <https://github.com/okfde/hackathon-leitfaden/releases/download/v1.0.0/hackathon-leitfaden-v1.0.0.pdf>
- 39** See <https://lists.debian.org/debian-devel-announce/2020/03/msg00010.html>
- 40** An overview can be found here: <https://joinup.ec.europa.eu/collection/digital-response-covid-19/hackathons-and-events#Hackathons>

