PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

# The Citizens' Info Pack and Guide for Vulnerable People



*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.. It reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.*

**Project information**

| | |
|---|---|
| Project title | Participatory Approaches to a New Ethical and Legal Framework for ICT |
| Project acronym | PANELFIT |
| Grant agreement number | 788039 |
| Project coordinator | UPV/EHU |

**Document information**

| | |
|---|---|
| Deliverable number | D5.5 |
| Document title | Citizens' Info Pack |
| Document version | 3.0 |
| Document date | 22 April 2022 |
| Work package | WP5 |
| Task | Task 5.7 |
| Document lead | OBCT / ECSA |
| Copyright licence | Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. |
| Dissemination level | PU = Unrestricted PUBLIC Access – EU project |
| Contractual due date | 2021-08-31 (Month 34) |

**Project partners involved in the document**

| No. | Organization name | Acronym |
|---|---|---|
| 1 | Universidad del País Vasco / Euskal Herriko Unibertsitatea | UPV/EHU |
| 7 | European Citizen Science Association | ECSA |
| 8 | European Network of Research Ethics Committees | EUREC |
| 9 | Institut de Ciències del Mar (Consejo Superior de Investigaciones Científic | ICM-CSIC |
| 10 | OBC Transeuropa | OBCT |

**Document history**

| Status | Version | Date | Author(s) | Reviewed by |
|---|---|---|---|---|
| Draft | V1.0 | 21.7.2021 | Tim Woods (ECSA) | |
| Edit | V1.1 | 22.7.2021 | | Iñigo de Miguel Beriain (UPV/EHU) |
| Edit | V1.2 | 18.8.2021 | | Federico Caruso (OBCT) |
| Final | V2.0 | 19.8.2021 | | |
| Final | V3.1 | 31.8.2021 | | Roberta Monachello (EU) |
| Final | V4.0 | 08.04.2022 | | Carolina Doran (ECSA), Federico Caruso (OBCT), Johann Cas (ÖAW) and Alessandro Ortalda (VUB) |

# Table of contents

**ICTs, data and vulnerable people: a guide for citizens** ..... 4
**About this guide** ..... 5
**Glossary of key terms** ..... 6
**What are the ethical and legal issues around ICTs?** ..... 8
**Who is vulnerable?** ..... 10
**How do the ethical and legal issues around ICTs affect vulnerable people?** ..... 14
**What can you do?** ..... 24
**Acknowledgements** ..... 32
**Thematic dossiers** ..... 34
1. Data commercialisation: mobile operators and personal data ..... 34
2. Focus on the European cybersecurity strategy ..... 41
3. Power imbalances and freedom of consent: Digital fortress Europe ..... 54

# ICTs, data and vulnerable people: a guide for citizens

## Disclaimer

This project received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

## Citation

PANELFIT consortium (2021) *ICTs, data and vulnerable people: a guide for citizens*. UPV-EHU, Bilbao.

# About this guide

ICTs, personal data, digital rights, the GDPR, data privacy, online security; these terms, and the concepts behind them, are increasingly common in our lives. Some of us may be familiar with them, but others are less aware of the growing role of ICTs and data in our lives - and the potential risks this creates.

Throughout this guide we use the term citizen to refer to all those individuals who are European residents regardless of their nationality or whose rights fall under the European jurisdiction, even if only temporarily.

These risks are even more pronounced for vulnerable groups in society. People can be vulnerable in different, often overlapping, ways, which place them at a disadvantage to the majority of citizens (Table 3 presents some of the many forms and causes of vulnerability). As a result, vulnerable people need greater support to navigate the digital world, and to ensure that they are able to exercise their rights. This guide explains where such support can be found, and also answers the following questions:

- What are the main ethical and legal issues around ICTs for vulnerable citizens?
- Who is vulnerable in Europe?
- How do issues around ICTs affect vulnerable people in particular?

This guide is a resource for members of vulnerable groups, people who work with vulnerable groups, and citizens more broadly. It is also useful for 'data controllers'[5] who collect data about vulnerable citizens. While focused on citizens in Europe, it may be of interest to people in other parts of the world.

It forms part of the citizens' information pack produced by the PANELFIT project, and is available in English, French, German, Italian and Spanish. You are welcome to translate this guide into other languages. Please send us a link to online versions in other languages, so that we can add them to the project website.

# Glossary of key terms

Table 1 explains some of the key terms used in this guide. These are not the 'final word' on these terms, but provide a useful definition for those new to the terminology around ICTs, data and vulnerable groups.

**Table 1. Key terms for understanding ICTs, data and vulnerable groups**

| | |
|---|---|
| Cybersecurity | This refers to how well protected private online data and information are; for example, how safe they are from being hacked, stolen, or made public without permission. |
| Data commercialisation | This means processing data about individuals or groups in order to make money; for example, through targeted online advertising or by selling it on to others. |
| Data controller | A data controller is anyone who obtains data, including personal data, to use for a specific purpose. It can be a company, an organisation, a government or local authority, a public body (e.g., a school or hospital) or a research institute, among others. |
| Data management | Data management covers the whole life cycle of data processing: collection, use, storage, sharing and deletion. It also refers to the fact that whoever collects your data (the data controller) must control what the data is used for, and who can use it. |
| Data protection | Nothing should happen to your personal data unless you have given your permission for this. Data controllers are required, under EU law, to put in place measures to ensure it is stored securely and privately. Your data should not be shared, or made publicly available, unless you have agreed to this. |
| Data subject | The person whose personal data is being collected and used by the data controller. |
| Data use and reuse | When asking for your data, data controllers should explain the purposes for which it will be used (e.g., a census, a research project). If they, or a third party, want to use your data for a further purpose - known as data reuse - they should ask again for your consent to do so. They cannot assume you are happy for your data to be reused. |

| | |
|---|---|
| Digital divide | This describes the gap between people who are able to benefit from technology (e.g. ICTs, the internet) and those who cannot. This phenomena is becoming increasingly important as more and more aspects of our lives move partly or fully online (e.g. education, healthcare, banking, shopping). Those with limited or no access to digital services risk being 'left behind'. |
| Digital literacy | Sometimes referred to as 'ICT literacy', this refers to a person's ability to find, evaluate and communicate information on digital platforms and devices. |
| Digital rights | This refers to the laws and procedures (e.g., the GDPR) that are in place to protect our rights in the digital world. These rights include, among others, the right to privacy and the right to withdraw consent for data use. |
| Discrimination | Discrimination means making unjustified distinctions between people, based on perceptions about that group, or the category (or categories) they belong to; for example, their race, gender, age, religion or sexual orientation, among others. |
| GDPR | The General Data Protection Regulation regulates how European citizens' personal data is managed. In effect, it sets out the laws through which your personal data is protected and kept private. |
| ICTs | Information and communication technologies include all forms of technology used for communication, such as the internet, mobile phones and smartphones, computers, social media networks, video-conferencing tools, and many others. |
| Informed consent | With respect to data and ICTs, this refers to informing and asking the data subject for permission to use their personal data in a specific way - which must be done before collecting or using their data. |
| Personal data | Personal data is anything that relates to you as an individual: your name, age or address, for example. In the digital world, it can also include your interests, habits and preferences; for example, pages you 'like' on social media, websites you visit to buy items, YouTube videos you have watched, and many others. |
| Privacy | In relation to ICTs and data, privacy refers to how confidential your information is (data protection) and how widely you want it to be shared (e.g., publicly, or only by the data controller). |
| Stigmatisation | Stigmatisation, or social stigma, means disapproving of, or discriminating against, a person or group of people based on perceptions about the person or the group(s) they belong to. |

| | |
|---|---|
| Vulnerable people | Vulnerable people are those who, for any number of reasons, find themselves at higher risk of harm when compared to the majority of people in society. You can find examples of vulnerable groups later in this guide (Table 3). People in certain social groups are sometimes referred to as ‘disadvantaged’ or ‘socially excluded’. |

# What are the ethical and legal issues around ICTs?

ICTs have brought many benefits to our lives. They have made it possible to speak quickly and cheaply to people across the world; they have given us instant access to more information than we ever knew we needed; they have brought huge advances in healthcare; they have helped us to combat poverty and bring education to more and more people globally.

Yet these advancements have not been without costs. Many ICTs require data to function and, as a result, companies, organisations, researchers and governments are increasingly asking for - or simply taking - our data. Data and information are powerful, and those who control them are increasingly able to find out about every aspect of our lives, both professional and private - and benefit from this information, whether financially, politically or in other ways.

For many people, debates around these ethical and legal issues are difficult to understand, or dismissed as boring or irrelevant to their everyday lives. Furthermore, the ethical debates around ICTs evolve very quickly, and it can be hard for people to keep up with them. As a result, we are often quick to give up our rights in return for the many benefits that ICTs bring.

But as ICTs continue to spread into every aspect of our lives, growing demands for our personal data make these issues increasingly important. Who is getting hold of our data? Who else are they sharing it with? What are they all doing with it - and what can I do to control this?

ICTs are a rapidly developing field, and as such, the ethical and legal issues around them are also constantly changing. Table 2 highlights some of the main current ethical and legal issues for citizens around ICTs.

### Table 2. Ethical and legal issues related to ICTs

| | |
|---|---|
| **Many citizens have a limited understanding of, and/or interest in, issues around ICTs** | Issues around ICTs are often difficult for non-experts to understand. This is true for both legal issues (e.g., the details of online terms and conditions) and ethical issues, such as surveillance and the future role of Artificial Intelligence. For many, this is combined with a lack of interest in what can be complex subjects or documents full of legal terminology such as the GDPR. In other instances, citizens may want to know more, but do not know where to find help with understanding these issues.<br><br>This has knock-on effects, such as people clicking "I agree" without having read, or having not understood, a website's terms and conditions or privacy policy. Furthermore, people may not know about the laws in place to protect their rights in the digital world - which makes it harder for them to exercise these rights. |
| **There are a number of barriers that limit citizens' understanding** | For many people, there are major barriers that deny them access to further information about ICTs and digital rights. Language is one: much of this information is in English and other major European languages, but not everyone in Europe is fluent in these languages.<br><br>Furthermore, much of this information is only available online. For offline communities - those with limited or no access to the internet - it remains out of reach. This lack of access to information accessed via ICTs is an example of the 'digital divide'. |
| **There is a perceived imbalance of power between citizens and technology companies** | The "tech giants" - large global technology companies, such as Facebook and Google - can seem very powerful. For some people, this can also be true for smaller technology companies. As a result, it can be difficult to say "no" or "I don't agree" when these companies ask for our data. People think they may miss out on using their services, or worry that these companies will simply have access to their data anyway. This sense of powerlessness is, of course, increased when people cannot or do not read the information about their digital rights. |
| **The diversity among citizens means people have different concerns around ICTs** | Different groups in society use ICTs in very different ways - and therefore have varying concerns, problems and challenges with using ICTs.<br><br>Providing the information each group or individual needs, and in the format and language they want, is challenging. As a result, a lot of the information about ICTs and digital rights is generic - which makes it harder for people to find what they need. |

| | |
|---|---|
| **The ICT landscape is constantly changing** | ICTs and digital rights are complex. Adding to this complexity is the fact that technology is always developing, and our data is forever being used in new and increasingly complicated ways. This brings its own challenges, not least the fact that there are always new laws, procedures and developments for us to try to understand.<br><br>This complexity is increased due to the different interpretations of these rights, and the protections put in place to ensure them (e.g., the GDPR) in different countries. |

*Source: Adapted from the report of the COST Action/PANELFIT workshop held in March 2020; supplemented by the other resources listed at the end of this guide.*

# Who is vulnerable?

The ethical and legal challenges around ICTs affect everyone, in Europe and beyond. For vulnerable groups in society, however, these risks are often even more acute - and in many cases, their ability to adapt to these risks is lower. Furthermore, there is a possibility that some vulnerable people will miss out on the opportunities and benefits that ICTs can bring if they are unaware of them, or if their fear of these risks outweighs their desire for the benefits.

But who counts as vulnerable? This is not a simple question to answer because, for a number of reasons, vulnerability is complex. Box 1 provides a summary of this complexity, and the factors that contribute to this complexity are then explained in more detail.

**Box 1. How to 'unpack' vulnerability**

The points outlined here do not cover all the elements of vulnerability, but highlight that it is a complicated and many-sided concept. The overall message is that vulnerability is a fluid, dynamic concept, and most people do not fit into neat, binary categories of vulnerability.

Instead, we suggest seeing vulnerability as a spectrum: individuals or groups can have high or low levels of vulnerability, which can be fixed (static) or changing (dynamic). Vulnerability is likely to change over a person's lifetime: with age, through changing personal circumstances, and due to factors beyond their control.

It is also worth noting that *everyone* is potentially vulnerable, and that their level of resilience - their ability to cope with vulnerability - is determined by their access to resources (e.g., public services available in a country) and cultural factors (e.g., their support networks).

Above all, it is important to remember that all of the groups and individuals mentioned in this guide are *people* first and foremost, and any other definition - as a data subject, a vulnerable person, even as a citizen - is secondary to this.

**The causes of vulnerability vary greatly**

People can be vulnerable in many different ways. For example, vulnerability can be caused by financial problems (e.g., unemployment, unmanageable debts) or health- and capacity-related barriers, such as illness, old age or disability. Other causes of vulnerability can be location-based, such as living in remote rural areas with few facilities (e.g., hospitals, schools). The causes of vulnerability can be societal, such as prejudice against refugees, foreigners or Travellers. They can also be due to discrimination based on (among others) race, ethnicity, nationality, class, caste, religion, belief, sex, gender, language, sexual orientation, gender identity and sex characteristics.

**People or groups may experience more than one form of vulnerability**

The form that a person's vulnerability takes can be complicated. At an individual level, a person may be affected by poor health and low financial capacity. These vulnerabilities have different impacts, but are often interconnected; indeed, one cause of vulnerability can often exacerbate others, creating a 'vicious cycle'. Building on the example given, a lack of money can lead to ill health (e.g., due to a limited diet or unsanitary living conditions) and the resulting ill health can make it harder to find a job - which in turn increases or maintains the person's financial vulnerability.

**Vulnerability can vary within a group in society**

Individuals within a vulnerable group may experience different impacts, and levels of impact, from a shared situation. For example, some refugees in Europe may be more vulnerable than others due to a range of factors such as: the country they are from (e.g., why they left and whether this caused trauma or psychological issues); the country in which they are currently living (e.g., its facilities for refugees, public attitudes towards refugees); and their education, training and competencies (e.g., language skills, professional qualifications). These all influence their ability to settle, find work and access the facilities available to them. So while it is true to say 'refugees are vulnerable', the severity of that vulnerability, and people's experience of it, will vary greatly within that broad group. Indeed, describing a certain type of vulnerability with one broad term may overlook individuals' specific challenges, which makes it harder to address them.

**Vulnerability can be dynamic**

While some vulnerabilities do not change significantly during a person's lifetime (e.g., incurable disabilities), others can worsen or improve over time. For example, many people experience changing personal circumstances, such as in their financial status or health. External factors that affect their vulnerability may also change; this could be the political climate in their country, which may bring in a government less supportive of marginalised groups. In other cases, the cause of a vulnerability may become redundant over time, such as a health issue improving, or unemployed people finding work, which removes or reduces their financial vulnerability.

Some of these changes are predictable, such as increasing vulnerability with age. In some instances, though, the cause of vulnerability can be rapid and unexpected: people may be hit by phenomena beyond their control, such as extreme climate events. These 'shocks' can create a vulnerability for which people have not prepared.

**Vulnerability can be assumed**

When considering vulnerability within society, there is often a temptation to assume characteristics for certain groups - but they may not apply to all members of that group. For example, refugees may be well educated and speak the native language to their host country well. However, they are still likely to share other vulnerable traits with other refugees, such as more limited access to resources and employment opportunities (compared with non-refugees), or abuse, neglect, exploitation, prejudice and antagonism from others in society.

Certain groups that are often seen as vulnerable need careful definition, and at times even sub-categorisation. For example, children and young people (those aged 16-25) are often identified as vulnerable, but the nature of vulnerability will vary widely, depending on whether they are:

- school students, who are not legally able to make all decisions for themselves
- in higher education, which may lead to stress or other mental health issues
- in employment, which is often low-paid or insecure among this age group
- outside of education and employment, which can lead to a number of vulnerabilities (e.g., financial, living conditions, mental health issues).

Vulnerability can also be subjective and invisible. One person may feel vulnerable, or class themselves as such, whereas someone else in a similar (or perhaps even worse) situation may not. At the same time, any citizen might consider themself to be vulnerable, for reasons that are not immediately evident to others.

**Vulnerability can affect the person - but also their culture**

In some instances, it is not (just) the individuals within a group who are vulnerable. Certain groups may find their cultural heritage is under threat, or their access to it is. This could be due to external threats, such as climate change: in polar regions, indigenous peoples' entire way of life is under threat. People's cultural resources can also be vulnerable, such as their language, their family and social structures and networks, and their natural heritage and environment.

# Vulnerable groups in Europe

While keeping this complexity in mind, there is often still a need to identify vulnerable groups and individuals. So who can, or should, be seen as 'vulnerable' in Europe? There is no single definition for vulnerability but a helpful definition to set the stage is the one used by the EU[6] for migrants:

> *"Minors, unaccompanied minors, disabled people, elderly people, pregnant women, single parents with minor children, victims of trafficking in human beings, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence, such as victims of female genital mutilation."*

Building on this definition, Table 3 identifies several vulnerable groups within Europe,[7] as well as people experiencing certain types of vulnerability.[8] This should not be seen as a complete list of vulnerable groups in Europe; given the changing nature of vulnerability, this would be impossible to achieve. However, it offers a useful starting point for thinking about who is vulnerable.

Table 3 also provides an example of how their vulnerability may affect them in terms of ICTs (see the next section for more discussion on this subject). The examples given are to illustrate possible types of ICT-related vulnerability for each group; many other types are likely to exist, depending on the degree of vulnerability and circumstances.

We have not attempted to sort these groups under broader headings or themes. To do so would contradict one of our key recommendations: that vulnerability should be seen as dynamic and complex, not a 'label' to apply to certain groups or individuals. Labelling large groups in society as vulnerable can, in fact, increase the discrimination and stigmatisation they face.

# How do the ethical and legal issues around ICTs affect vulnerable people?

The ethical and legal issues around ICTs - such as those related to data privacy, data commercialisation, and the growing use of new technologies such as facial recognition - affect everyone in society. But, as mentioned, vulnerable people and groups in society are often at a greater risk of harm than others - and at risk in different ways; Box 2 presents some of these.

**Box 2. How do ICTs affect vulnerable people in particular?**

- Such people and groups are not just vulnerable in themselves; they are also more vulnerable to having their data used in ways that puts them at risk (e.g., greater surveillance). While this is a risk for all citizens, vulnerable people often face a higher risk. For example, they may be incapable of granting consent, or may not be fluent in the national language(s) of the country they live in.
- Power imbalances between data subjects and data controllers may be exacerbated with vulnerable data subjects. For example, in cases where personal data is open to misuse by data controllers, vulnerable people may find themselves less able to control or prevent this, because they have less power, knowledge or awareness of the issue.
- There is a risk of (greater) stigmatisation, as people are put into groups for the purposes of research and analysis.

These risks do not just relate to the nature of a person's vulnerability, but also the kind of data about them that is being collected and used. Certain types of data - such as information about a person's religion, medical history or sexual orientation - may bring a greater risk, depending on the place and context in which they are used.

Furthermore, as mentioned, vulnerability can change over time - and this raises issues in terms of the personal data. Individuals or groups who are not vulnerable when they share their data may become so later on. As a result, the conditions under which they gave their consent for their data to be used may

no longer apply. Research teams that are under-resourced may lack the time, money and, in some cases, information they need to implement measures to ensure the data and privacy rights of their subjects are enforced.

As before, the message is this: vulnerability is complex! Table 3 highlights some of the ways that vulnerable groups in society may be particularly affected in relation to the ethical and legal issues around ICTs and data. We are not saying these apply to everyone in these groups; they are simply examples to highlight the ways in which vulnerability, and vulnerability related to ICTs and data, can happen.

## Table 3. Examples of vulnerable groups in Europe, and the nature of their vulnerabilities

| Vulnerable group | Possible vulnerability | Possible vulnerability with respect to ICTs and data |
|---|---|---|
| **Women** | Pregnant or breastfeeding women may be, or may feel, more vulnerable than other women; for example, due to changes in their health. Women in fertile age are at higher risk of discrimination in hiring processes. | Women who have undergone gender reassignment surgery may have data stored about them that no longer reflects their status. |
| **Single parents or guardians / parents or guardians of vulnerable children or dependants** | Additional care duties may leave them with less time and resources to take care of themselves, increasing their vulnerability. | They may have less time to read about and understand ICT-related issues. |
| **Homeless people** | People in this situation often experience greater health risks, and an increased risk of violence, unemployment and poverty. | They are likely to have lower access to information about these issues than others in society. Also, data about them may be collected without their informed consent (e.g., when they use homeless services provided by charities). |
| **People with addiction(s), such as drug addiction and/or alcoholism** | People living with addictions face many forms of vulnerability, such as health risks, an increased risk of violence, unemployment and poverty. | They may have a reduced capacity to understand information about their ICT and data rights. |

| | | |
|---|---|---|
| **People suffering from, or at risk of, domestic violence, and psychological and/or sexual abuse** | People facing violence and abuse are likely to experience a range of vulnerabilities, such as physical and mental health issues. | In some situations, victims' access to information may be restricted as part of the abuse they suffer; for example, they may live with a partner who restricts what they can do or where they can go. |
| **People who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence, such as victims of female genital mutilation** | Among many other forms of vulnerability, people who have experienced these are likely to face long-term trauma or other psychological damage, in addition to the impacts on their physical health. | A reluctance to share their personal information - for example, if they are a migrant or lack legal status in a country - may mean that victims are less willing to seek medical help or inform the police of their situation. |
| **Victims of human trafficking** | A lack of legal status in a country may mean these people do not access the support available; for example, they may fear being deported. | These people may be unable to access online services or information, depending on the conditions they find themselves in (e.g., illegal confinement, modern-day slavery). At the same time, by not being 'in the system', they may be overlooked by service providers who could help them. |
| **Religious minorities** | It can be difficult to erase societal bias away from these groups. | Some people may consider their religion to be a private matter, but certain unavoidable data-collection processes still require people to state their religion (e.g., tax regulations in Germany). |
| **LGBTQIA+ people[9] and sexual minorities** | Individuals in this group still face widespread discrimination across Europe. | New technology that violates privacy (e.g., facial profiling) may be more likely to target such groups. |
| **Transgender populations** | Individuals in this group still face widespread discrimination across Europe. For example, Hungary recently passed a law ending the legal recognition of trans status.[10] | Male/female tick boxes, which are commonly found on many data-collection forms, discriminate against them, while the 'traditional' language used in many online situations (e.g., he/she, his/her) does likewise. |

| | | |
|---|---|---|
| **Prisoners** | Prisoners are cut off from their support networks, and often face additional threats, such as a greater risk of violence in prison. | Being in prison may reduce their access to information about their data and digital rights. |
| **People leaving prison** | Newly released prisoners may lack support networks, and find it hard to gain employment or secure housing. | Their vulnerable state may reduce access to information about their data and digital rights. Depending on how long they were in prison, they may be unaware of developments in terms of data protection and privacy. |
| **People who are under-educated or poorly educated** | Their vulnerability is exacerbated by not being aware of, or unable to understand, support systems to reduce their vulnerabilities. They tend to have lower incomes, increasing their financial vulnerability. | Information about ICTs and data rights tends to be complex and hard to understand; low education will increase this barrier. |
| **People who are outside of training and/or education** | This situation can exacerbate many types of vulnerability, including financial, health (especially mental health) and support networks. | Information about ICTs and digital rights is often passed through formal settings, such as schools or colleges. Being outside of these reduces people's access to such information. |
| **People who are misinformed, including those who may not be able to understand the information provided** | Information is power; those who cannot access or understand the information designed to help them are, as a consequence, more vulnerable than those who can. | This is true of digital information as well as non-digital forms of information. |
| **People with learning difficulties, such as dyslexia, dysorthography, dysgraphia and dyscalculia** | Learning difficulties can make people vulnerable in multiple ways. For example, people who cannot understand information designed to help them are, as a consequence, more vulnerable than those who can. | These and other learning difficulties make it harder to find out about and/or understand information related to data rights, data privacy, ICTs, etc. |

| | | |
|---|---|---|
| **Indigenous groups** | Such groups under threat or experiencing declining numbers may require protection of their heritage, for example in museums. | Provenience data - on the origin, ownership and custody of objects - is not always captured by ICTs; in other cases, indigenous people's knowledge may be stored without their knowledge or approval. |
| **The Sámi**[11] | As a minority group living in one of Europe's harshest regions, the Sámi experience many forms of vulnerability. A report by the United Nations Special Rapporteur on the rights of Indigenous Peoples concluded that Sweden, Norway and Finland do not fulfil their stated objectives of guaranteeing the human rights of the Sámi people.[12] | The Sámi have always been targeted for different types of research. This includes register- and biobank-based research. These projects have sometimes bypassed ethical considerations, for example by failing to communicate fully that a project is targeting the Sámi people. |
| **Ethnic minorities** | Ethnic minorities in a country often face discrimination and may exhibit a higher prevalance of several types of vulnerability (e.g., low income, low education, health issues, language barriers). | They may have lower access to information about their data rights (e.g., if it is not available in their first language). |
| **Refugees** | Refugees often face discrimination and may exhibit a higher prevalance of several types of vulnerability (e.g., low income, low education, health issues, language barriers). | They may be reluctant to provide personal data due to concerns about its misuse. This may exclude them from the potential benefits that ICTs can offer. |
| **Asylum seekers** | Asylum seekers may experience mental health issues or trauma, for example if they have fled a warzone or catastrophe. | They may be reluctant to provide personal data due to concerns about misuse. This may exclude them from the potential benefits that ICTs can offer. |

| | | |
|---|---|---|
| **Migrants** | The nature of migrants' vulnerabilities varies widely. Poorer migrants may experience many of the vulnerabilities that refugees and asylum seekers face, while high-income migrants may experience very different vulnerabilities (e.g., stress, resentment among the local population). | Language barriers may increase the risk of their personal data being misused. Also, data and ICT regulations in their new country may differ to those they are used to. |
| **Members of Traveller communities** | Traveller communities often face discrimination and may find themselves outside of formal support systems (e.g., schools, healthcare). | They may be reluctant to provide personal data due to concerns about misuse. This may exclude them from the potential benefits that ICTs can offer. |
| **Members of the Roma community** | The Roma have been historically persecuted across Europe, which leaves many Romani more vulnerable than other populations, in terms of low income, employment, threats to their welfare, and many other forms of vulnerability. | They may be reluctant to provide personal data due to concerns about misuse. This may exclude them from the potential benefits that ICTs can offer. |
| **Sick or injured people, including hospital patients and long-term patients** | Health issues make people immediately vulnerable, and can exacerbate other types of vulnerability (e.g., loss of income). | They may not be able to give consent to how their data is used, for example if they are sedated, confused or unconscious. Or, they may give consent too easily, for example if they want the medical research to make them better (temporary vulnerability). |
| **People with chronic and/or long-term conditions, or multiple chronic conditions** | Vulnerabilities are determined by the nature and severity of the condition. For example, many such conditions will reduce people's ability to work and earn an income. | These people are often excluded from online information, depending on whether inclusive ICT tools are implemented and available. For example, people with epilepsy may be vulnerable to exclusion from certain online non-inclusive resources due to flashes/light from screens (photosensitive epilepsy).[13] |

| | | |
|---|---|---|
| **People living in residential care** | People living in residential care (also known as assisted living) have many day-to-day decisions taken away from them. This lack of control over their lives can increase their vulnerability in many ways (e.g., their diet, their health care, their finances). | For many people in residential care, data about them may be controlled by others, such as family members of staff at their residential home. This reduces their ability to control, or even influence, how their personal data is used. |
| **People with disabilities and disorders, either physical or mental (or both), and both temporary and permanent** | Vulnerabilities are determined by the nature and severity of the disabilities and disorders. As an example, people with limited mobility may be dependent on others, increasing their vulnerability to exploitation or neglect. | Some disabilities may mean people need assistance to access or share data, or to understand privacy statements / give consent. This reduces their control over their own data privacy. |
| **People with limited communications capacity, such as speech impediments** | Limited communications capacity prevents people requesting, or contributing to, information in a range of scenarios. This may mean their needs, views or expectations are not fully considered (e.g., in public debates). | Some limitations in communications capacity may mean people need assistance to access or share data, or to understand privacy statements / give consent. This reduces their control over their own data privacy. |
| **Visually impaired or blind people** | While many provisions exist for visually impaired and blind people, these may not be available or affordable for all people, increasing their vulnerability. | They are likely to use software that reads the screen / platform to them, which reduces the privacy of that information. Furthermore, they might find their access to information restricted, for example if the websites to which they need access don't allow the software to read everything (e.g., options in tick boxes). |
| **People excluded by language, or facing language barriers** | People who do not speak the language of their country of residence (e.g., some migrants and refugees, or minorities such as Creole speakers in Portugal) have reduced access to information about support measures, which increases their vulnerability. | Non-native speakers within a country, or minority language speakers, often lack information in their own language about their digital rights. |

| | | |
|---|---|---|
| **People who are not fluent in English** | As English is the predominant language across Europe, certain information may only be available, or more prominently available, in this language. Those who cannot speak or understand English may find themselves at a disadvantage compared with those who can. | Much of the information on data rights and privacy is in English, putting these groups at a disadvantage. They are also likely to find they have lower access to share their views on how ICTs develop and progress, if surveys and debates are held in English. |
| **Children / dependants / minors** | Younger people are inherently vulnerable, lacking many of the attributes that reduce vulnerability (e.g., size, strength, completed education, independence, income). | Young people cannot legally consent to the use of their data. They may not know how to complain about misuse of their data, or be aware that they can. |
| **Emerging adults (aged 18-25)** | In many countries, this age group struggles to access the advantages that older generations did, such as secure and well-paid jobs, or affordable housing. | A lack of employment and/or housing may make it harder to access information about digital rights and ICTs (e.g., due to the lack of internet access at home). |
| **Early adults (20-40)** | In many European countries (e.g., Portugal, the Netherlands), people in this age group have a higher tendency to be self-employed or freelancers. As such, especially during moments of crisis (such as the Covid-19 pandemic), they are vulnerable to dramatic changes in their income. They may also have young families, and hence have an increased level of vulnerability (e.g., financial). | Conversely, they may potentially have higher levels of technical skills and education than other age groups. This means they are less likely to be vulnerable to legal and ethical issues around data privacy, ICTs and their digital rights. |
| **Older, frail or incapacitated people** | Old age is an inherently vulnerable stage of life, as people may become weaker and more dependent on others. | While old age is not always linked to digital illiteracy, there may be lower awareness of legal and ethical issues around ICTs, data and privacy among older people, compared with the 'digital generation' who have grown up with this technology. |

| | | |
|---|---|---|
| **People who are unemployed or underemployed, both in the short term and the long term** | Unemployment exacerbates other forms of vulnerability, especially financial vulnerability and housing. It may also lead to health and mental health issues. | Unemployed people may miss out on ICT training and information provided through workplaces. They may have no online access at home (for financial reasons), meaning they are unaware of information about ICTs, which is increasingly shared online. |
| **People who have low economic status** | Similar to unemployment, low economic status exacerbates other forms of vulnerability, especially financial vulnerability and housing. It may also lead to health and mental health issues. | People in this group may have no online access at home (for financial reasons), meaning they are unaware of information about ICTs, which is increasingly shared online. |
| **Social care clients and beneficiaries** | People in social care may experience many other forms of vulnerability (e.g., poor health, low income, insecure housing). | People in this group may lack access to ICT training and information provided through workplaces, and/or may have no online access at home (for financial reasons), meaning they are unaware of information about ICTs, which is increasingly shared online. |
| **People who are illiterate** | Much of the information that governs our lives and aims to support us is provided primarily in written forms. Illiteracy is a major barrier to accessing this, leaving these people vulnerable. Illiteracy may also be a factor in people having lower economic status. | A lot of information about legal and ethical issues around ICTs is shared in written form, especially online. Illiteracy means people will be less aware of, and less able to understand, this information. |
| **People who are digitally illiterate, or who have limited technological expertise** | Much of the information that governs our lives and aims to support us is increasingly provided online; for example doctor's appointments that are only bookable online, or information that is only shared through social media. | These people are at risk of being left behind as information and services move increasingly online. |

| | | |
|---|---|---|
| **Offline communities** | This is not the same vulnerability as digital illiteracy: it is an access/infrastructure issue, rather than a skills/capacity issue. However, offline communities will face many of the same vulnerabilities as those who are digitally illiterate. | These people are at risk of being left behind as information and services move increasingly online. |
| **Those with limited access to public infrastructure** | As an example, people in rural areas in some countries lack good access to infrastructures such as hospitals, libraries, strong broadband, childcare, and other support systems. This makes them relatively vulnerable, especially during crises such as the Covid-19 pandemic. | Lack of infrastructure may extend to limited internet access (e.g., weak or expensive broadband) and other ICT services. This can reduce people's access to information about their rights related to ICTs, data and privacy. |
| **Communities who remain outside of research processes** | Science and research underpin many elements of society, such as healthcare, governance and education. By being outside of these processes, either as researchers or data subjects, these communities find their lives influenced by research processes in which they have no stake or voice. As a result, policies informed by research may not address their particular needs or reduce their specific vulnerabilities. | This is also true for ICT-based research: communities with no stake or voice in the process, or no access to the findings, may find that the impacts of such research (e.g., policy, funding decisions) do not address their needs or support them. For example, online surveys or questionnaires are an increasingly common research method - but almost totally exclude offline communities. |
| **People hit by phenomena beyond their control** | Extreme events or phenomena can cause unexpected vulnerability. While this may take the form of natural disasters (e.g., volcanoes, global pandemics) and extreme climate events (e.g., droughts, floods), it can also be in the form of life events (e.g., unexpected illness, accidents, loss of employment, a death in the family). The unexpected nature of such events makes it difficult to prepare for them, leaving people less resilient. | In the aftermath of a crisis, people may be tired, stressed or confused, and therefore share their personal data more easily (i.e., with less attention) or do so to access certain services (e.g., post-disaster support, emergency healthcare). A recent example is the Covid-19 pandemic, in which personal freedoms and privacy issues were often put aside to combat the spread of the virus. |

| | |
|---|---|
| **Any citizen who, for any reason, considers themselves to be vulnerable** | The nature and severity of this vulnerability, whether ICT related or otherwise, depends on the perception of the subject. However, it is important to recognise that vulnerability is not a simple, measurable issue, but can be subjective, hidden and personal. |

*Source: Adapted from the report of the COST Action/PANELFIT workshop held in March 2020; supplemented by the other resources listed at the end of this guide.*

# What can you do?

It is clear that vulnerable people should receive more attention in relation to ethical and legal discussions around ICTs, and there should be greater efforts to include them in development and deployment of ICTs and new other technologies that will affect them (e.g., Artificial Intelligence). Ideally, there should be specific safeguards to protect vulnerable people in terms of their data privacy and how data about them is used.

However, as noted, it is difficult - maybe even impossible - to create a definitive list of all vulnerable groups in society. It is not even desirable, due to the dynamic nature of vulnerability and the risk of oversimplifying the complexity of people's situations, or increasing the risk of stigmatisation. As such, specific safeguards for vulnerable people's digital rights may take a while to come into effect - if they ever do.

In the meantime, there are actions that all citizens can take to ensure that vulnerable people's digital rights are met. Figure 1 outlines a series of actions.

There are also specific actions that data controllers can take to protect vulnerable data subjects. Figure 2 illustrates some of these.

| FIGURE 1 | FIGURE 2 |
|---|---|
| **Data subjects** | **Data controllers** |

| **Who?**<br><br>*All citizens, including vulnerable citizens and those who have responsibility for vulnerable citizens* | **Who?**<br><br>*Researchers, employees, companies, authorities, project organisers, etc.* |
|---|---|
| When someone requests your data, check the following: Who are they? What will they use it for? How long will they keep it? Who will they share it with? | At the very start of the process, ask: Who are the vulnerable data subjects in my project, process or task? How are they vulnerable? |
| If they provide you with general information (e.g., terms and conditions, consent forms), check: Do you understand them?<br><br>If not, ask for a version that is easier to understand (e.g., in your first language). | Consider the risks that the members of each vulnerable group will face when you use their data - and think about how these can be reduced or overcome. |
| If you are still unsure or unhappy about how your data will be used, find out more. This could be through a citizen's advice office, or your national data protection authority. | When asking vulnerable citizens for personal data, check: Have they understood what their data will be used for? How can I make it simpler for them to understand? Have they really given their consent to its use freely? |
| In most cases, you have the right to withdraw consent to your data being used. Before sharing your data, check: How do I withdraw consent later on? Who do I need to contact? | Don't look for concrete solutions, or see addressing vulnerability as a 'box to be ticked' in your project. Instead, see it as an ongoing process that should be reviewed regularly. |
| If your data rights have been violated immediately, contact the corresponding data protection office. If you do not feel comfortable in doing so, there is a list of organisations that might be able to help you on table 4 | Think about data protection for vulnerable groups at every stage of the project: Does this activity pose a risk to vulnerable groups? How can I address this? |

# Useful resources

There are several organisations, websites and projects dedicated to helping people understand their rights in our increasingly digital world, and which support vulnerable groups in different ways. We have included in table 4 a list of NGOs that you can contact and seek information/help in case of data privacy misconduct. If you are keen to find out more about these subjects, we recommend the following.

**Table 4. Examples of organisations offering support to vulnerable groups in Europe.**

| Vulnerable group | NGO | NGO contact info (just in case) |
|---|---|---|
| **Women** | European Women's Lobby: https://womenlobby.org/?lang=en | ewl@womenlobby.org |
| **Single parents or guardians / parents or guardians of vulnerable children or dependants** | COFACE Families Europe: https://coface-eu.org/about-us/ | secretariat@coface-eu.org |
| **Homeless people** | FEANTSA: https://www.feantsa.org/en/about-us/what-is-feantsa | information@feantsa.org |
| | Homeless in Europe International: https://www.homelessineurope.eu/ | homelessineuropehope@gmail.com |
| **People with addiction(s), such as drug addiction and/or alcoholism** | Dianova International: https://www.dianova.org/ | switzerland@dianova.org |
| **People suffering from, or at risk of, domestic violence, and psychological and/or sexual abuse** | Women Against Violence Europe: https://wave-network.org/ | office@wave-network.org |
| | Rape Crisis Network Europe --> They also have a long list of organisations (some are NGOs): https://www.rcne.com/contact/countries/ | Each organisation has its own email |
| **People who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence, such as victims of female genital mutilation** | International Rehabilitation Council for Torture Victims: https://www.irct.org/ | irct@irct.org |
| | End FGM European Network: https://www.endfgm.eu/who-we-are/vision-and-mission/ | https://www.endfgm.eu/resources/resource-items/contact/ |
| **Victims of human trafficking** | La Strada International: https://www.lastradainternational.org/ | info@lastradainternational.org |
| **Religious minorities** | Minority Rights Group International: https://minorityrights.org/about-us/ | minority.rights@minorityrights.org |
| **LGBTQIA+ people[1] and sexual minorities** | Here you have a long list with NGOs of different countries: https://www.ilga- | |

| | | |
|---|---|---|
| | europe.org/who-we-are/members | |
| **Transgender populations** | Transgender Europe: https://tgeu.org/ | tgeu@tgeu.org |
| **Prisoners** | European Prison Education Association: https://www.epea.org/epea/ | secretary@epea.org |
| | European Prison Observatory: http://www.prisonobservatory.org/ | info@prisonobservatory.org |
| **People leaving prison** | European Prison Observatory: http://www.prisonobservatory.org/ | info@prisonobservatory.org |
| **People who are under-educated or poorly educated** | Waag - https://waag.org/en | https://waag.org/en/contact |
| **People who are outside of training and/or education** | Waag - https://waag.org/en | https://waag.org/en/contact |
| **People who are misinformed, including those who may not be able to understand the information provided** | European Association for Viewers Interests (EAVI): https://eavi.eu/about-us/ | eavi@eavi.eu |
| **People with learning difficulties, such as dyslexia, dysorthography, dysgraphia and dyscalculia** | European Dislexia Association: https://eda-info.eu/about-the-eda/ | eda-info@eda-info.eu |
| **Indigenous groups** | Minority Rights Group International: https://minorityrights.org/about-us/ | minority.rights@minorityrights.org |
| | European Network of Indigenous peoples: https://www.enip.eu/ | enip@enip.eu |
| **The Sámi[2]** | Saami Coucil: https://www.saamicouncil.net/en/the-saami-council | saamicouncil@saamicouncil.net |
| **Ethnic minorities** | Minority Rights Group International: https://minorityrights.org/about-us/ | minority.rights@minorityrights.org |
| | European Network Against Racism: enar-eu.org/About-us | info@enar-eu.org |
| **Refugees** | European Council on Refugees and Exiles: https://ecre.org/ | vzahle@ecre.org |

| | | |
|---|---|---|
| | RedCross Europe: https://redcross.eu/about | infoboard@redcross.eu |
| **Asylum seekers** | European Council on Refugees and Exiles: https://ecre.org/ | vzahle@ecre.org |
| | RedCross Europe: https://redcross.eu/about | infoboard@redcross.eu |
| **Migrants** | European NGO Platform Asylum and Migration: http://www.ngo-platform-asylum-migration.eu/ | comms@migpolgroup.com |
| | RedCross Europe: https://redcross.eu/about | infoboard@redcross.eu |
| **Members of Traveller communities** | Waag - https://waag.org/en | https://waag.org/en/contact |
| **Members of the Roma community** | European Roma Rights Centre: http://www.errc.org/ | office@errc.org |
| **Sick or injured people, including hospital patients and long-term patients** | Brain injured people and families: https://bif-ec.com/about-2/ | https://bif-ec.com/contact/ |
| **People with chronic and/or long-term conditions, or multiple chronic conditions** | EUROFEA: https://www.euforea.eu/ngo | contact@euforea.eu |
| **People living in residential care** | AGE: https://www.age-platform.eu/about-age | info@age-platform.eu |
| **People with disabilities and disorders, either physical or mental (or both), and both temporary and permanent** | Inclusion Europe: https://www.inclusion-europe.eu/what-we-do/ | secretariat@inclusion-europe.org |
| **People with limited communications capacity, such as speech impediments** | Inclusion Europe: https://www.inclusion-europe.eu/what-we-do/ | secretariat@inclusion-europe.org |
| **Visually impaired or blind people** | European Blind Union: https://www.euroblind.org/ | ebu@euroblind.org |
| **People excluded by language, or facing language barriers** | European Council on Refugees and Exiles: https://ecre.org/ | vzahle@ecre.org |
| **People who are not fluent in English** | European Council on Refugees and Exiles: https://ecre.org/ | vzahle@ecre.org |
| **Children / dependants / minors** | Eurochild: https://www.eurochild.org/ | info@eurochild.org |
| **Emerging adults (aged 18-25)** | ERYICA - European Youth Information and Counselling Agency: https://www.eryica.org/eryica | secretariat@eryica.org |

| | | |
|---|---|---|
| **Early adults (20-40)** | ERYICA - European Youth Information and Counselling Agency: https://www.eryica.org/eryica | secretariat@eryica.org |
| **Older, frail or incapacitated people** | AGE: https://www.age-platform.eu/about-age | info@age-platform.eu |
| **People who are unemployed or underemployed, both in the short term and the long term** | The European Anti-Poverty Network (EAPN): https://www.eapn.eu/who-we-are/what-is-eapn/ | https://www.eapn.eu/who-we-are/contact-us/ |
| **People who have low economic status** | The European Anti-Poverty Network (EAPN): https://www.eapn.eu/who-we-are/what-is-eapn/ | https://www.eapn.eu/who-we-are/contact-us/ |
| **Social care clients and beneficiaries** | Social Services Europe: https://www.socialserviceseurope.eu/why-we-do-it | info@socialserviceseurope.eu |
| **People who are illiterate** | World Literacy Foundation (This NGO is global, not European but they have an office in the UK): https://worldliteracyfoundation.org/about-us/ | Contact form at the end of the page: https://worldliteracyfoundation.org/about-us/ |
| **People who are digitally illiterate, or who have limited technological expertise** | All digital: https://all-digital.org/about-us/ | contact@all-digital.org |
| | European Digital Learning Network: http://dlearn.eu/ | http://dlearn.eu/contact/ |
| **Offline communities** | RED CROSS EU office | +32 (0) 2 230 54 64 |
| **Those with limited access to public infrastructure** | PREPARE - Partnership for Rural Europe: http://www.preparenetwork.org/partnership/partners#ecovast | Kim.Smedslund@suomenkylat.fi |
| | European Council for the Village and Small Town: http://www.ecovast.org/english/about_e.html | valeriecarter@ecovast.org |
| **Communities who remain outside of research processes** | European Centre for Minority Issues: https://www.ecmi.de/ | info@ecmi.de |
| **People hit by phenomena beyond their control** | Climate Action Network (CAN) Europe: https://caneurope.org/about-us/ | info@caneurope.org |
| **Any citizen who, for any reason, considers themselves to be vulnerable** | Waag - https://waag.org/en | https://waag.org/en/contact |

## Vulnerable people and groups

**Statewatch** encourages the publication of investigative journalism and critical research in Europe in the fields of the state, justice and home affairs, civil liberties, accountability and openness. Available in English. www.statewatch.org/about/

The **Social Protection and Human Rights** website contains a guide to disadvantaged and vulnerable groups in society. Available in English.

https://socialprotection-humanrights.org/key-issues/disadvantaged-and-vulnerable-groups/

**These videos from the Web Accessibility Initiative** explore the impacts of greater web accessibility, and the benefits for everyone, with examples from a variety of situations. Available in English.

www.w3.org/WAI/perspective-videos/

## Legal and ethical issues around ICTs, data and privacy

The **Global Data Justice** project focuses on the diverse debates and processes occurring around data governance in different regions, drawing out the overarching principles and needs that can push data technology governance in the direction of social justice. Available in English.
https://globaldatajustice.org/

The **Data Justice Lab** examines the relationship between 'datafication' and social justice, such as the politics and impacts of data-driven processes and Big Data. Their website contains lots of helpful publications, and news of upcoming events. Available in English. https://datajusticelab.org/

**Access Now's digital security helpline** works with individuals and organisations around the world to keep them safe online. If you're at risk, they can help you improve your digital security practices. If you're already under attack, they provide rapid-response emergency assistance. Available in Arabic, English, French, German, Italian, Portuguese, Russian, Spanish, Tagalog. www.accessnow.org/help/

**Tactical Tech's Data Detox Kit** provides everyday steps you can take to control your digital privacy, security and wellbeing in ways that feel right to you. Available in 35 languages.
https://datadetoxkit.org/en/home

The **Future of Privacy Forum** and the **FPF Education and Innovation Foundation** are catalysts for privacy leadership and scholarship, and advance principled data practices in support of emerging technologies. Available in English. https://fpf.org/resources/

The **European Digital Rights** (EDRi) network defends fundamental rights in the digital age, advocates for appropriate laws and policies, and raises awareness of the key issues impacting digital rights. Available in English. https://edri.org/

**Privacy International**'s Data Protection Guide contains a wealth of useful information on issues around data protection. Available in English.

https://privacyinternational.org/report/2255/data-protection-guide-complete

## Further reading

If you would like to read more about some of the issues raised in this guide, then the contributors to this guide suggest the following articles as a good starting point.

This article from **Privacy International** examines how data-driven immigration policies routinely lead to discriminatory treatment of migrants, with a focus on the UK.
https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees

This article on the **Data-Pop Alliance** website is the abstract of a book chapter, titled 'Group privacy in the age of Big Data'. It discusses how Big Data is blurring the lines between individual data and group data, and what can be done about it.

https://datapopalliance.org/item/group-privacy-in-the-age-of-big-data/

This article from the **European Data Journalism Network**, on 'The uncountable: How Covid-19 affected migrants and refugees' health' provides an example of how vulnerabilities often exacerbate one another. Available in English, French, German and Italian.

www.europeandatajournalism.eu/eng/News/Data-news/The-uncountable-How-Covid-19-affected-migrants-and-refugees-health

## Further watching and listening

The PANELFIT Monthly Chats covered a broad range of subjects around data, ICTs, privacy and rights. The whole series can be watched again - or, if you prefer, listened to - via the PANELFIT website. Available in English.

www.panelfit.eu/2020/03/23/monthly-chats/

# Acknowledgements

## Sources of information used for this guide

The PANELFIT project collated the information in this guide from the following sources (specific sources are noted in the text).

**Talks and workshops**

- A PANELFIT workshop on 'Creating a citizens' information pack on ethical and legal issues around ICTs: what should be included?', 9-10 March 2020 in Berlin, Germany.
- A talk on vulnerable populations by Dr Jedrzej Niklas, Department of Media and Communications, LSE, UK (formerly University of Leeds), at a PANELFIT workshop, 5 June 2019, in Bilbao, Spain.
- Personal communication with Professor Anna Lydia Svalastog, Department of Health and Social Studies, Østfold University College, Norway.
- Personal communication with Professor Iñigo de Miguel Beriain, Department of Public Law University of the Basque Country, Spain.
- Reviewing the final version and providing constructive feedback: Professor Gianclaudio Malgieri, EDHEC Business school; Aurelie Pols, Center for Privacy & Cybersecurity board member; Dr. Anna Berti Suman, The European Comission JRC and Marko Šijan, AZOP.

**Documents**

- Berti Suman, A and Pierce, R (2018) 'Challenges for citizen science and the EU Open Science Agenda under the GDPR', *European Data Protection Law Review* 4(3): 284-95, https://doi.org/10.21552/edpl/2018/3/7 (open access)
- Malgieri, G and Niklas, J (2020) 'Vulnerable data subjects', *Computer Law & Security Review* 37: 105415, https://doi.org/10.1016/j.clsr.2020.105415 (open access)
- Milan, S and Treré, T (2017) 'Big Data from the South: The beginning of a conversation we must have', DataActive, 16 October, https://data-activism.net/2017/10/bigdatasur/ (open access)
- Peroni, L and Timmer, A (2013) 'Vulnerable groups: The promise of an emerging concept in European Human Rights Convention law', *International Journal of Constitutional Law* 11(4): 1056-85, https://doi.org/10.1093/icon/mot042 (open access)

- PANELFIT consortium (2020) 'D5.2 Critical Analysis of the ICT Data Protection Regulatory Framework (Consolidated Version)', Bilbao, Spain

**Videos and podcasts**

- PANELFIT podcast with Gianclaudio Malgieri, 'Vulnerable data subjects and EU Law', 27 February 2020. Available at: www.youtube.com/watch?v=fqLfvF-cS70&feature=emb_title

## Photos

Page 1: © pixabay.com; geralt-9301 / stocksnap-894430 / geralt-9301 / geralt-9301/ josemdelaa-2004715/ vipragen-13256880/

## Contributors

We would like to thank the following people for their help in writing this guide:

Alexandra Castañeda, Andreas Matheus, Andrzej Klimczuk, Anna Berti Suman, Annelies Duerinckx, Carolina Doran, Christoforos Pavlakis, Corelia Baibarac-Duignan, Elisabetta Broglio, Federico Caruso, Gefion Thuermer, Helen Feord, Janice Asine, Jaume Peira, Karen Soacha, Katerina Zourou, Katherin Wagenknecht, Katrin Vohland, Linda Freyburg, Marcel Leppée, Marta Camara Oliveira, Mieke Sterken, Tim Woods

## Disclaimer

This project received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

The workshop held in Berlin, March 2020, was organised through a collaboration between: the European Citizen Science Association (ECSA), COST Action 15212, the Institute of Marine Sciences (ICM-CSIC), and the PANELFIT and EU-Citizen.Science projects. Financial support was provided by PANELFIT (EU grant agreement 788039) and COST Action 15212 (supported by European Cooperation in Science and Technology).

# Thematic dossiers

## 1. Data commercialisation: mobile operators and personal data

### How phone companies use our personal data

**Abstract:** In the past, some telephone companies have become known for their unscrupulous use of customers' personal data. While things have improved in Europe, it is important to know what we are agreeing to when we sign a new contract.

**Link:** https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/How-phone-companies-use-our-personal-data

**Author:** Gianluca De Feo, Federico Caruso (OBCT(CCI)

**Text:**

With a few exceptions, the one device that we all have a relatively close and lasting relationship with is the smartphone. This device can collect a large quantity and variety of data about us, which can then be used to generate further value in various ways.

The collected data can reveal a vast range of personal information: location data, internet browsing data, biometric data, behavioural data, etc. From this data some of the most sensitive information can be inferred, such as sexual orientation, political persuasion, membership of a vulnerable minority, or health status. This information can then be used to reach the user with targeted messages. The most frequently cited example is Cambridge Analytica, the British agency that received the personal data of more than 50 million users from Facebook in 2016 and attempted to influence the US presidential election from which Donald Trump emerged victorious.

In recent years, there has been some progress in data protection, thanks to innovations introduced by the European Union (above all, the introduction of the GDPR in 2018) as well as initiatives taken by large tech companies. In 2019, for example, Apple decided to make it more difficult to geolocate users through the apps in its App Store. While this does indeed protect user privacy, it has also been seen as a strategy to cause trouble for companies that provide similar services.

### Why companies collect our data

Just like when phones weren't so "smart", phone owners need to subscribe to an operator to use their device. Each country has a range of providers to choose from, each with their own corporate affiliations of varying size, and their own policy for handling personal data.

The latter is a particularly sensitive subject for phone companies; they can use private data for profiling purposes, in order to create 'tailor-made' services or targeted advertising, or they can give or sell such data to other companies. The latter can then use this data to generate further value, for instance by providing names to call centres which will then contact the phone user with often undesired commercial proposals.

## Legal, illegal and problematic practices

This market's importance for phone companies (and others too) is clear enough from all the scandals involving unscrupulous policies that have emerged over the years. One example is Telefónica, a Spanish company that developed an app for the German market encouraging users to share their personal data.

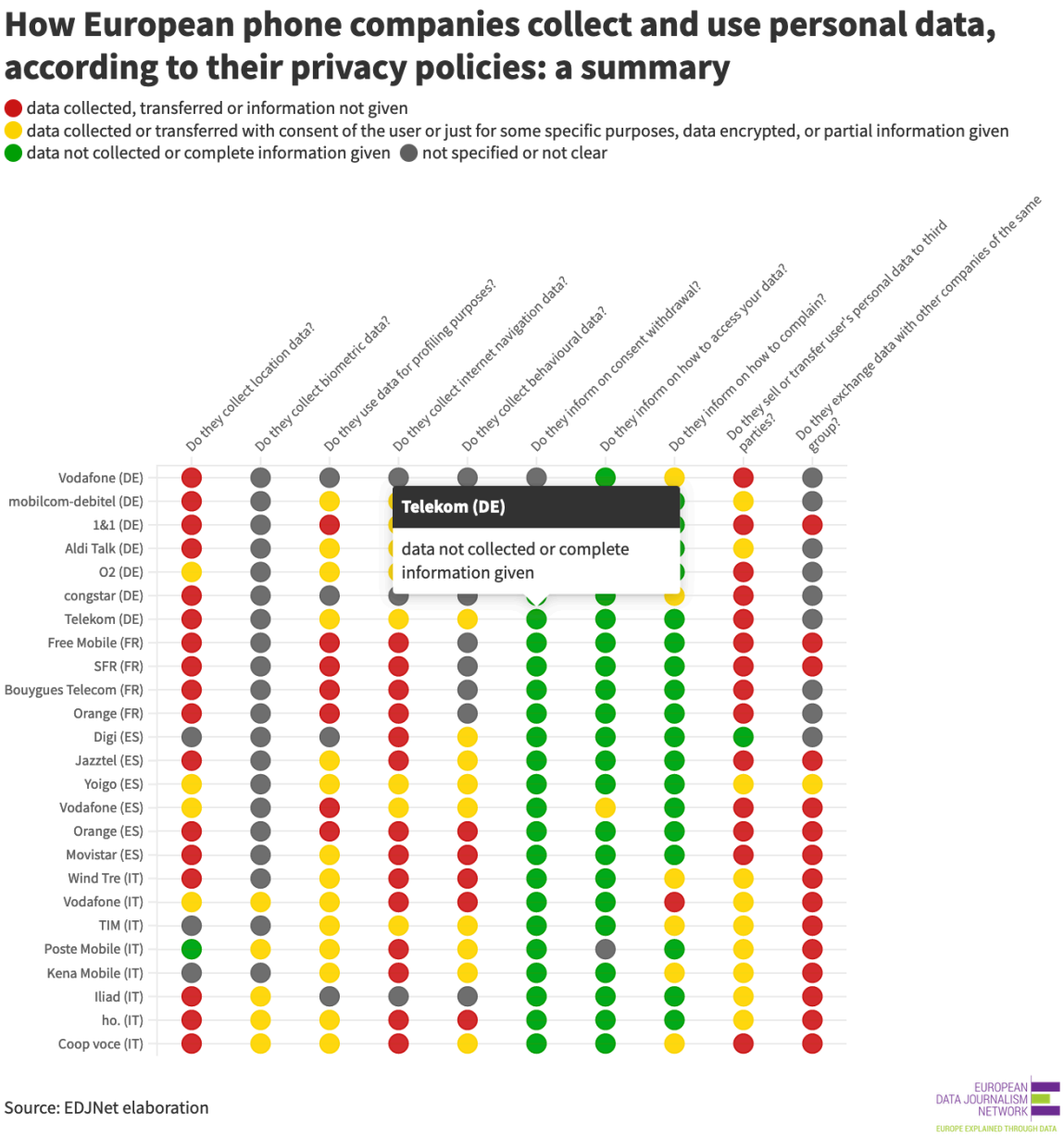
The EU's introduction of the General Data Protection Regulation (GDPR) has made such practices riskier, making companies liable to fines from national privacy authorities. Despite this, problematic cases periodically still emerge in every sector. Sticking with phone companies, a Netzpolitik investigation in 2021 revealed that in Germany the company O2 tended to present customers with a series of pre-checked options allowing all possible uses of their personal data.

In another sense, the importance of personal data emerged during the pandemic when phone companies shared aggregated location data with the authorities, without really explaining how this data would be used and for how long. This was obviously anonymised data, but several recent studies seem to confirm experts' concerns about the possibility of re-identifying people even within these large datasets. While this does not mean data is actually being de-anonymised, the mere possibility presents a clear threat, especially at a time when cyber-attacks are increasingly common.

## What privacy policies can tell us

How many of us actually read and understand all the authorisations and clauses we consent to when we buy a sim card or switch to a new operator? With this question in mind, we decided to analyse the privacy policies of telecommunications companies that concern the services and apps that nearly all operators encourage you to install to manage your profile, assessing the amount and type of data collected, and the completeness of information.

Problems arise when during the subscription process users tick a box authorising, for instance, the processing of their data for commercial purposes. In such cases, telephone companies may use personal data, as well as navigation and location data, to identify buying habits or preferences and show targeted advertisements. The data may also be transferred to third parties (often difficult to identify or described in a generic way) who in turn may use the data for commercial purposes. In some cases, data is used for these purposes even several years after the contract has been terminated.




Phone companies often invite users to download smartphone apps to monitor their remaining credit, the status of active deals and much more. These apps have their own privacy policies, sometimes specific, sometimes similar or identical to the service policy. However, they also often contain a tool that allows them to track activities by the users: trackers. Trackers are softwares that collect information about the person using the app, and there are various types of them. The most controversial ones in terms of data protection collect information for the purpose of identifying the user and create a profile for targeted advertising, and locate the mobile device. A tool developed by exodus allows us anyone to analyse the apps concerned and discover which and how many trackers they contain.

## Penalties for unlawful practices

To date, several large fines have been issued against telephone companies by national authorities for GDPR violations. In 2020, the Italian Data Protection Authority fined TIM just under 28 million euro after repeated complaints from users about receiving unwanted commercial phone calls as a result of

violations in the management of user data. In 2021, a fine of 4.5 million euro was imposed on Fastweb for similar reasons. In 2020, the Polish authority imposed a fine of 443,000 euro on Virgin Mobile for failing to ensure the security of subscribers' personal data. In 2021 the French national authority punished Free Mobile with a 300,000 euro fine for failing to guarantee the right to view and opt out of data processing. Finally, the most recent case concerns the affiliated Greek companies Cosmote and Ote, fined 6 million euro and 3.25 million euro respectively for a series of irregularities that emerged following a cyber attack causing the loss of 30 gigabytes of personal data.

### Methodology

We consulted the privacy policies of the major French, Italian, German and Spanish mobile companies' services on each operator's website. The objective was to answer ten previously formulated questions (which can be found in the infographics above) relating to the type of data collected, the way in which this data is used, and the completeness of certain information. The information obtained was collected in a datasets, which was then processed to create the infographics above.

## Mobile operators and personal data in Europe

**Abstract:** This article explores in more detail our research into how phone companies use customers' personal data, with notes on the legal issues relating to European law.

**Link:** https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Mobile-operators-and-personal-data-in-Europe

**Author:** Federico Caruso, Gianluca De Feo (OBCT/CCI)

**Text:**

### Readability

As stipulated numerous times in the GDPR (recitals 39, 42, 58; Articles 7 and 12), information on any potential personal data processing must be provided in an easily accessible and understandable way. With this in mind, there is not much noticeable effort on the part of the companies under consideration to go beyond the so-called "wall of text" with, for example, layouts, language or graphical aids aimed at improving readability. Of course, this problem is hardly exclusive to telecommunications companies, as large-scale research and everyday user experience shows. Academic research has long hypothesised that icon-based graphical systems an optimal method for presenting information intuitively. None of the companies analysed adopt such methods. Nevertheless, approaches vary between those who simply publish a legal document in pdf format, without any particular attention to layout and readability, and those who go a step further in communicating their policies, for example with Q&A sections or pages that are almost like mini-websites . More can certainly be done, and perhaps greater homogeneity in the structure of policies across different companies would make comparison easier, to the benefit of transparency.

### Completeness

Information about how to access, rectify, cancel, restrict, refuse or revoke personal data use, as well as the right to lodge a complaint, should be clearly stated in the privacy policy. As noyb points out in its report on videoconferencing software , citing the Article 29 Working Party guidelines , it is not

enough to simply inform users about the existence of these rights: the operator should also include “a summary of what each right involves and how the data subject can take steps to exercise it and any limitations on the right”. There are different approaches on this point. Often the information is presented in a partial way, with a very brief description of the user's rights, and sometimes lacking contact information for requests. A notable example is the Vodafone Germany app, where no information is provided in the privacy policy. Meanwhile several Italian companies adopt rather vague formulas such as “you have the right to lodge a complaint with the Representative for the protection of personal data“ (TIM and the affiliated Kena Mobile), without including any information on how this might be done, or the legal basis for doing so.

### Categories of collected data and data processing

When it comes to the types of data considered in this study, the picture is fairly homogeneous from country to country. The overall trend is to collect location, navigation and behavioural data. Generally, the legal basis for collection is the user's consent, while some collect data regardless of consent, by invoking the legitimate interest clause. The situation with biometric data is more varied. In many cases, it is not specified whether biometric data is collected or not, but this could be due to the fact that they are merged into the other categories mentioned. Indeed, things like typing or scrolling styles can be defined as both biometric and behavioural data. However, biometric data also includes things like fingerprints or facial recognition, which are possible to record with any smartphone produced in recent years. For this reason, such data would be better specified separately.

As for profiling activities, i.e. analysing user data in order to improve the service, but also to create “tailor-made” commercial offers, asking for explicit consent seems to be the general approach. However, in some cases (e.g. Orange and Vodafone in Spain) it is said that profiling will take place anyway. The situation for Vodafone and Congstar GmbH customers in Germany (and to some extent Digi and the Yoigo app in Spain) is unclear, since, as far as we could verify, none of these companies explicitly mention the categories of data collected, nor whether or not they are used for profiling activities.

### Transfer and deletion of data

All companies state that they will, under certain conditions, transfer personal data to third parties. In most cases this is for activities related to contract execution or assessment of customer solvency. In some cases explicit reference is made to commercial partners (sometimes affiliated with the operator) to whom, with the user's consent, data may be transferred for a wide range of purposes, including commercial proposals for goods or services completely unrelated to phones. The formulas used are sometimes very general, especially in the case of French (Orange, Bouygues Telecom) and German (Vodafone, O2, Congstar GmbH) companies. The same goes for the apps of these companies, as well as those of the Spanish Yoigo and the German Telekom, Aldi Talk and 1&1 Telecom GmbH.

For data retention, several companies adopt concise formulas to explain in a few lines that data will be retained “for a period of time not exceeding the achievement of the purposes for which they were collected or subsequently processed” (TIM Italia) and indicating a maximum time limit after which they will be deleted. Others take a more transparent approach and publish a table detailing retention periods for the various categories of data (Coop Voce, Ho., Vodafone and Wind Tre in Italy; Bouygues Telecom in France). In Germany, data is generally deleted within 12-14 months.

## GDPR

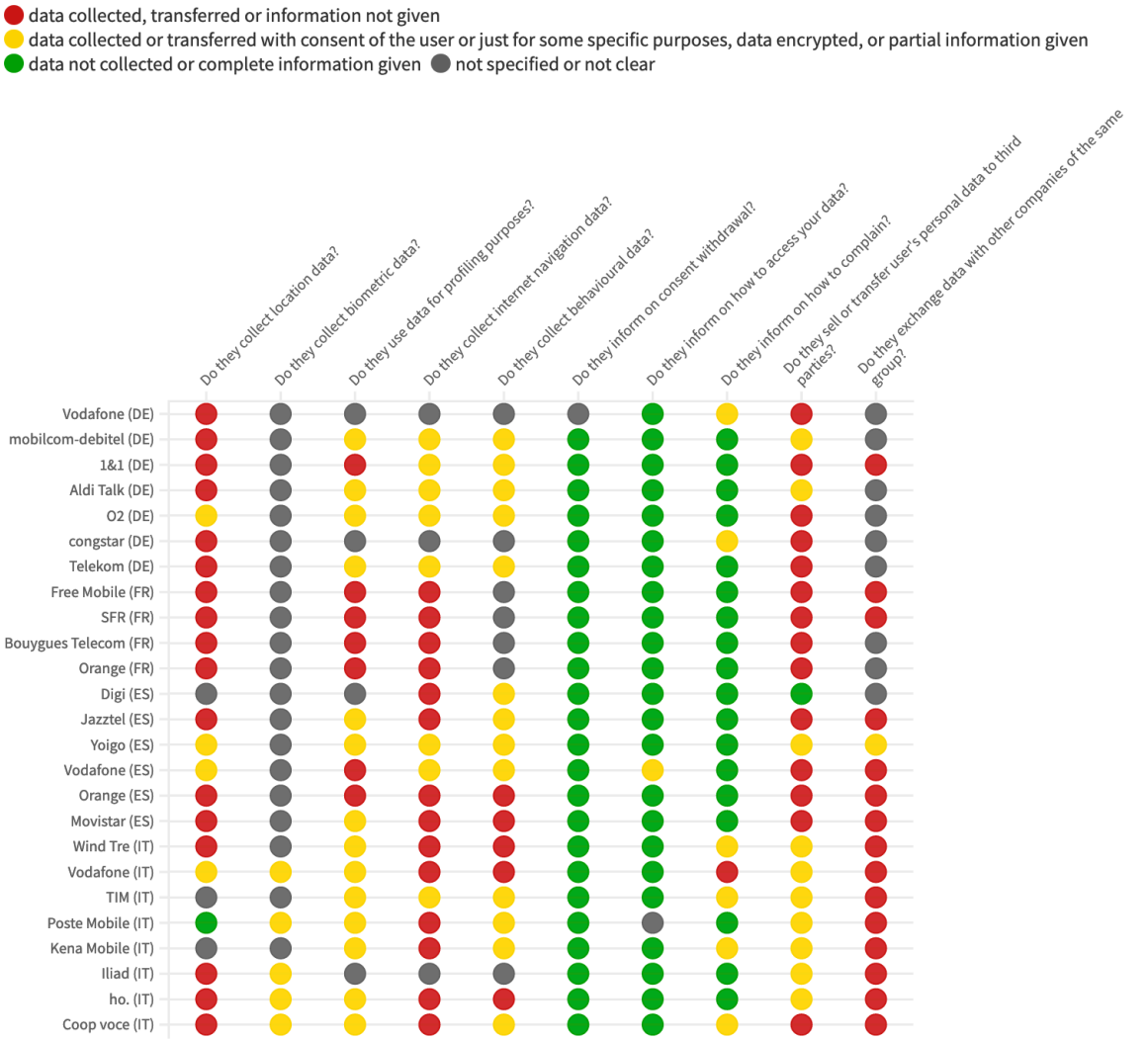
The two most relevant GDPR articles in the present context are 13 and 15 . As Stefano Rossetti, a lawyer with the noyb.eu team, explained to us, these articles regulate the two "moments" when personal data processing becomes an issue in the relationship between user and company.

Article 13 lists the information that the company must provide in the first of these two moments, i.e. when the user subscribes to a service. This information, as explained in the aforementioned noyb report, is usually listed in a document known as a "privacy policy", the main subject of our analysis. Three elements must always be present in the description of privacy policies: the categories of data collected, the purpose for which the data is requested, and the legal basis on which the data is processed. The information that the company is required to provide also includes the identity of the data controller, possible recipients of the personal data collected (public authorities, other companies, etc.), the storage period, and information on the possibility of requesting access to the data or its deletion, as well as the possibility of filing a complaint in case of misconduct.

As for the completeness of information provided, the new guidelines on the right to access data currently being drafted by the EDPB (European Data Protection Board) seem to leave a certain margin of "generality" to the data processor: "information [about the processing and on data subjects' rights] can be based on what is already compiled in the controller's record of processing activities (Art. 30) and the privacy notice (Art. 13 and 14). However, this general information may have to be updated to the time of the request or tailored to reflect the processing operations that are carried out in relation to the specific person making the request".

This brings us to the second "moment", namely Article 15, which states that "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data". Thus, while Article 13 specifies that the company is obliged to inform the user (and how it must do so), Article 15 specifies the former's duty to respond to any request for access so that it is possible to verify that the data collected and its processing comply with what is stated in the privacy policy, as well as with the law. For the purposes of this study, we limited our analysis to the first part.

## How European phone companies collect and use personal data, according to their privacy policies: a summary




Source: EDJNet elaboration

EUROPEAN DATA JOURNALISM NETWORK
EUROPE EXPLAINED THROUGH DATA

# 2. Focus on the European cybersecurity strategy

## Brussel's plan to protect the EU from cyberattacks

**Abstract:** The Covid-19 crisis has turned us into a digital society. Large parts of our day-to-day lives now take place in the digital sphere and this has made Member States much more vulnerable to cyberattacks. To neutralise them, the European Commission launched its new Cybersecurity Strategy in December 2020.

**Author:** Álvaro Merino (El Orden Mundial)

**Link:** https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Brussel-s-plan-to-protect-the-EU-from-cyberattacks

**Text:**

"Who are you? You're in our meeting. General, what do you suggest we do? General, you are right: we need to invest in privacy". This is how Josep Borrell, High Representative of the European Union for Foreign Affairs, reacted when a secret videoconference of EU defence ministers was crashed last year . In a careless oversight, the Dutch defence minister had shared a picture on Twitter where the access code for the meeting was visible. A compatriot journalist noticed the error and joined the videocall, leaving the institution red-faced

The scene, despite being pretty wild, highlights the EU's ongoing difficulties with cybersecurity: in a club of twenty-seven countries, with meetings and conversations that would ideally take place in person but that, owing to logistical difficulties, have moved online, it is difficult to ensure that every door remains closed. This, in a world as connected as ours, is the enormous risk that has forced the EU to arm itself against digital attacks, whenever they take place, wherever they come from and whatever shape they take.

The threat is silent yet not invisible. Not unsuccessfully, the European Union Agency for Cybersecurity (ENISA) identified three-hundred-and-four significant malicious attacks against "critical sectors" in 2020 , more than double 2019's tally. Many of them targeted hospitals and health networks, institutions which, during the pandemic, held very valuable information on the evolution of Covid and subsequent vaccination projects.

Their aims can be varied, from stealing data to paralysing key infrastructure, with the disastrous consequences that that represents for the targeted country. The biggest example in recent times is the attack on the Colonial pipeline , the largest in the United States, in May 2021. The attack, perpetrated by an apolitical group of professional hackers called Darkside, forced operators to halt the flow of oil, leading to a gasoline shortage across the East coast, and to pay the group 75 bitcoins, equivalent to €3.8m.

Fortunately for European citizens, the EU has a plan that means that the crashing of a secret defence meeting remains merely an amusing anecdote, rather than a cyberattack that compromises the entire security of the European community. In December 2020, the European Commission presented a new Cybersecurity Strategy and a proposal to reinforce the directive regarding measures for heightened levels of community cybersecurity in the EU (Directive NIS2 ).

## A new arms race

The European Union has been preparing itself since 2013 to respond to digital attacks and, in recent years, it has launched various initiatives to advance the creation of a common defence and security strategy.

Among them stands out a common cyberdiplomacy toolbox and a joint EU cyberdefence framework , both approved in 2018 and designed to improve coordination between Member States; the Cybersecurity Act (2019), which renewed the European Network and Information Security Agency's (ENISA) mandate, renaming it the European Union Agency for Cybersecurity; and the EU toolbox for 5G security , also in 2019.

Yet in a hyperconnected world like this, where hybrid threats are more and more sophisticated and powers compete to develop different technologies that allow them to secure their systems, the risk of being left behind in the cyber race becomes greater and greater. In this sense, the cybersecurity race is reminiscent of the arms race of the Cold War, when the United States, the Soviet Union and their respective allies became engaged in a secretive war of nuclear arms development. As is the case now, each advance was guarded jealously and developments forced each side to move faster and faster.

This is what is causing the European Union to continually modernise its Cybersecurity Strategy; it is trying to stay one step ahead of cybercriminals. That is why, although the document was first published in 2013, the strategy was revised in 2017 and again in December 2020.

Nevertheless, the most recent version represents a change in paradigm: now that the European institutions and Member States count on unified and coordinated security measures, the EU wants to work on the creation of tools that allow it to respond immediately and effectively or, better still, to prevent cyberattacks.

## An ambitious plan

In this respect, the new Cybersecurity Strategy brings three key areas into play: first of all, it intends to improve common resilience against cyberattacks through both the creation of a network of security operations centres across the EU that work with artificial intelligence technology and a reform to security laws regarding information networks and systems, incorporated into Directive NIS2.

The NIS Directive, passed in 2016, provoked a change in the institutional focus on cybersecurity in Member States- it obliged them, among other things, to create a national cybersecurity strategy and to establish emergency cyber response teams-, though it has started to show limitations.

"The digital transformation of society, intensified by the Covid crisis, has increased the threat level and is creating new challenges that require innovative and adapted responses. Now, any interruption can have wide-ranging effects on the entire internal market". These were the words of the European Commission in the presentation of its new strategy.

In short, Directive NIS2, which received the green light from the European Parliament in October , expands the definition of critical sectors and strengthens the requirements for the 160,000 businesses that the definition covers. The objective is to bridge the gap between European and US companies, who invest 41% more, on average, in cybersecurity than their European counterparts.

Secondly, with its new Cybersecurity Strategy, the Commission also wants to build up its operational capacity to prevent, deter and respond to cyberattacks, which has led to a proposed Joint Cyber Unit . This team will work to guarantee a coordinated EU response to cyberincidents and cybercrisis on a large scale and to offer assistance in recovery from these attacks. "These threats are a common

enemy, which is why it is necessary to coordinate, to share intelligence and to raise the alert early", argues the Commission.

Finally, Brussels wants to promote a global and open cyberspace, bringing exterior countries to the table to replicate its laws worldwide and to contribute to international security. The strategy, in other words, aims to prevent a cybersecurity landscape reminiscent of the Cold War, instead bringing nations together in the spirit of cooperation to shield the world against these types of threats.

## ENISA: The cornerstone of the EU's cybersecurity strategy

**Abstract:** The Cybersecurity Agency has been tasked with building a common defence, without any faults, against cyberattacks in the EU. While it seemed like an uphill struggle at first, restructure after restructure has built it into an organisation at the forefront of fighting Brussels' war on cybercriminals.

**Author:** Álvaro Merino (El Orden Mundial)

**Link:** https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/ENISA-The-cornerstone-of-the-EU-s-cybersecurity-strategy

**Text:**

When the European Union Agency for Cybersecurity (ENISA) was founded back in 2004, Facebook had just been set up and the word 'cyber' was more commonly heard in science fiction. Its initial mandate was only for five years, a term limit which the European Commission kicked into the long grass until 2019, when it finally made it a permanent agency. On top of these early difficulties, its headquarters were based in the Greek cities of Heraklion and Athens, the antipodes of Europe.

Despite all this, ENISA has become a cohesive element in a common cybersecurity strategy. In fact, although it has maintained its old acronym from its days as the European Network and Information Security Agency, its last restructuring changed its name to the European Union Agency for Cybersecurity with the new purpose of "achieving a higher level of common cybersecurity in the whole Union, particularly through the active support of Member States, institutions and organisms of the Union".

It is, in other words, the point of reference, the crux of the European plan for network and information security. Without a common defence strategy, without Union-wide protection, the EU would be an easy target for cybercriminals, and this is why the Commission proposed the creation of ENISA: to count on an agency whose first commitment is to secure the continent, to tie up loose ends and ensure that there are no unimplemented directives that leave countries vulnerable to attack. Furthermore, the agency works closely with Europol and the European Cybercrime Centre.

In 2004, the organisation represented a slightly premature project, a step ahead of the internet's explosion into the daily life of its citizens, but as information and communications technology (ICT) grew, the risks associated with it grew exponentially as well. Protection against cybercrime was not a visionary precaution but a necessity, and now the work of ENISA has proved to be crucial.

Without their work, cyberattacks like the one that hit the University Hospital of Brno (Czechia) in March 2020 which caused it, in the midst of the pandemic, to postpone urgent operations and relocate severely ill patients, would be seen much more frequently. The pandemic has complicated things: in accelerating the digital transformation of society and the economy, the threats have multiplied. From

water supply to control over our homes, each becoming more and more connected, the scope of cybercriminals has no limits.

## A progressive rise

ENISA was conceived as a small agency with a specific task: help institutions and organisations within the EU and Member States to protect their connectivity. One year before it surpassed its initial mandate, in 2008, the European Parliament and European Council decided, as proposed by the Commission, to renew its term until 2012 as the evaluation and improvement of protection for European networks had hardly even begun.

In 2011, the mandate was extended once again, this time to 2013 and then again , once this date was reached, to 2020. In contrast to previous extensions, the last one came accompanied by an enlargement of its brief. Coinciding with the publication of the EU's first Cybersecurity Strategy, the European institutions also modernised the agency, which required assistance in certain areas of its new brief. Among them, the most important was a future network of teams to handle cyber emergencies (EU CERT), spread across all European capitals.

Yet it was in 2019, with the passing of the Cybersecurity Act, when ENISA received its definitive brief. As well as increasing its resources, the new legislation made its 2004 mandate permanent, changed its name to the European Union Agency for Cybersecurity, expanded its advisory role and gave it clear operative instructions for the first time .

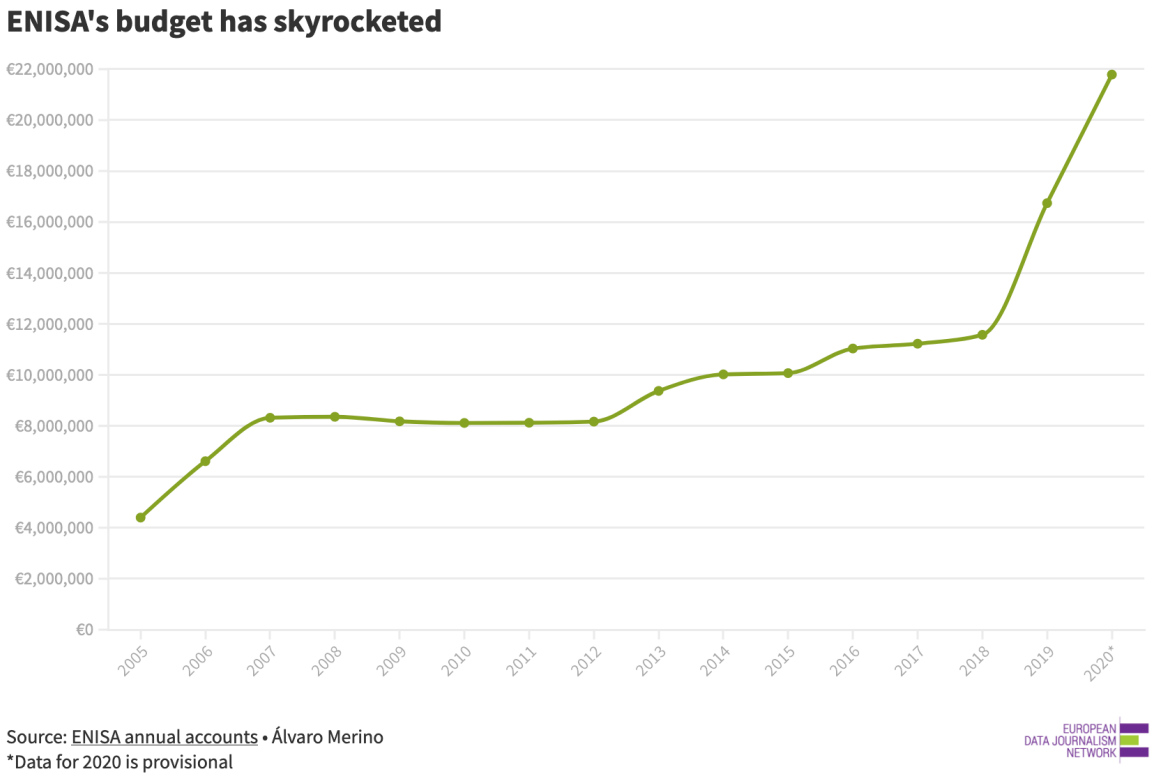
Therefore, among other things, the agency also began to help Member States to establish priorities in research and development funding and, most importantly, worked to create a system of security certification for ICT products and services in the EU.

In order for businesses and consumers to trust that their online information is safe, they need to use secure devices, but the lack of a unified certification system in the EU undermines this confidence and limits cross-border trade. To this end, ENISA must establish common criteria and unify the national mechanisms to award cybersecurity certification, a hallmark that is needed from smart cards - credit cards, bus passes, SIM cards - to cloud services.

As far as financing is concerned, ENISA has had its budget increased year on year up to nearly €22m in 2020 , five times more than its initial budget. The vast majority of money comes from the European Commission, while EEA countries- Iceland, Liechtenstein, Norway and Switzerland- and the Greek government- which rents its premises- also contribute a small portion. In 2019, ENISA had seventy-five employees.

The growing role of ENISA in the EU's cybersecurity strategy has made the European Commission aware of the need to have the organisation closer to its centre of power. To this end, rather than changing its headquarters, last June they authorised the opening of a third office in Brussels with the intention of maintaining "regular and systematic cooperation" between the agency and the European institutions.

Incarnation to incarnation, the European Network and Information Security Agency has remained a pillar of European cybersecurity since its foundation in 2004. The culmination of this process was realised with its new office in Brussels the consolidation of its operational functions, a change that marks the EU's intent to tackle cyberattacks head-on and become




the number one enemy of cybercriminals across the world.

## Cybersecurity: between European coordination and national agencies

**Abstract:** European agencies play a supporting and coordinating role in European cybersecurity. However, with reference to specific EU regulations, every member state can establish its own organ to safeguard both private and national interests.

**Author:** Openpolis

**Link:** https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Cybersecurity-between-European-coordination-and-national-agencies

**Text:**

In recent years, The European Agency for Cybersecurity (ENISA) has become an increasingly important asset in addressing the growing challenges in this sector. The European Union's cybersecurity remit derives from Article 5 of the Treaty on European Union (TEU), which provides for shared competence in areas where there is no exclusive competence.

The EU (and by extension ENISA) should thus limit itself to issues that cannot be resolved by individual member states. For this reason, along with this European agency, each member state has adopted its own institutional framework and bodies for dealing with cybersecurity. The remit of ENISA is therefore to assist member states and the Commission, and to facilitate cooperation and exchange of information.

### European coordination

While the main regulatory reference point for European cybersecurity is currently the NIS directive , an updated text is under discussion and is expected to lead to the approval of NIS 2 .

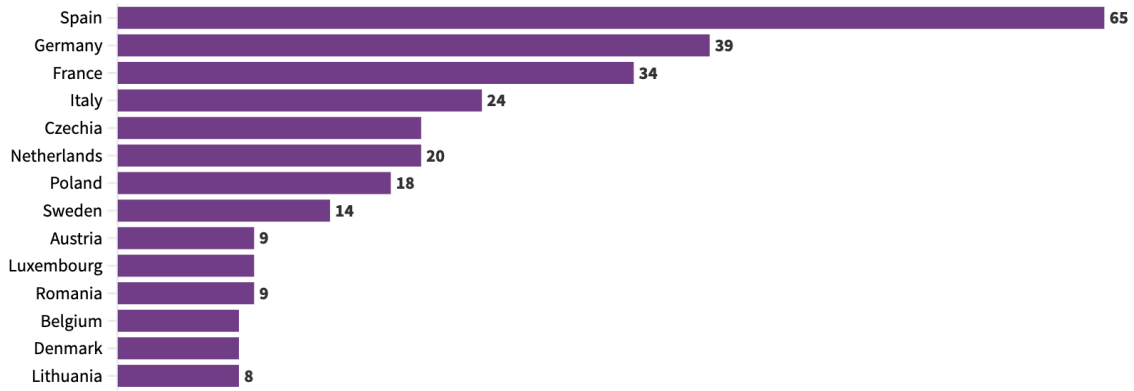
Given the nature of European directives (Article 288 of the Treaty on the Functioning of the European Union, TFEU ), the text limits itself to indicating to member states the desired results, leaving them with ample autonomy to structure their own cybersecurity agencies.

Among the obligations set out for member states is the identification of specific agencies that can coordinate adopted policies to maintain a high level of cybersecurity. These are the competent national authorities, the single points of contact and the CSIRTs (Computer Security Incident Response Team).

Already established in 1990, CSIRTs are organisations in charge of collecting and managing reports of incidents and potential software vulnerabilities. Each country has a different number of CSIRTs that can be accredited by various international consortia such as Trusted Introducer, First (Forum of Incident Response and Security Teams) and The European CSIRT Network.

**The top 15 EU countries by number of CSIRTs**

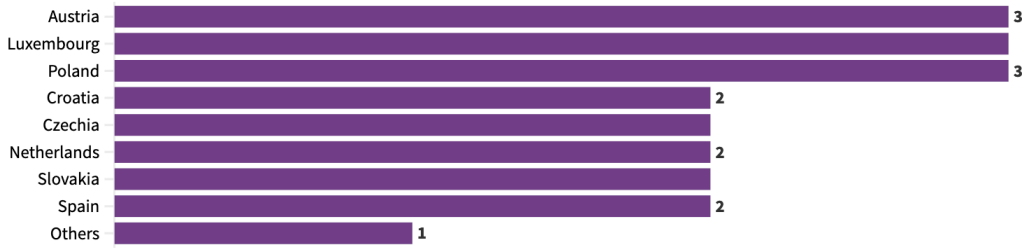
The European countries with the most Computer security incident response teams (CSIRT) accredited by the three main international consortia




The NIS Directive obliges each member state to designate one or more CSIRT to join the European CSIRT Network. In most cases member states have designated a single CSIRT, but not all; in fact, some countries have designated two or three.

**National CSIRTs designated by member countries**

The number of national CSIRTs designated by each member country of the European Union as part of the Csirts Network




While CSIRTs deal with IT incidents and potential vulnerabilities, the competent NIS authorities operate at the regulatory and management level. These are the national bodies responsible for the security of networks and information systems in the sectors indicated in the directive. In this case too, each state can identify one or more competent bodies. 13 countries nominated a single competent NIS authority.

If only one authority is identified, it automatically becomes the single point of contact. Otherwise the state must indicate which body will play the role of liaison to ensure cooperation with authorities of other member states as well as ENISA and the CSIRT Network.

## NIS competent authorities: a look at Germany, France and Italy

As we have seen, each country has the right to structure its own relevant bodies as it sees fit, as long as it respects the obligations of the European directive. Taking the three most populous EU countries as examples, the first fact that emerges is that all three, to date, have identified a single NIS authority.

In Italy's case, the sole NIS authority is the new Cybersecurity Agency . Before this agency was established in May 2021, there were five nominated authorities, namely the ministries of economic development, infrastructure, economy, health and environment, now defined as "sector authorities" (Article 7 of Legislative Decree 65/2018 ). The Cybersecurity Agency thus represents the single point of contact, while also containing the Italian CSIRT , which was previously included in the department of information for the security of the republic (thus coming under the rubric of intelligence).

The Cybersecurity Agency is in many regards autonomous. However, it is placed under the supervision of the Presidency of the Council, which oversees the management of the sector as well as the appointment of the director (Roberto Baldoni) and vice-director (Nunzia Ciardi). Internally, the agency is structured as eight general services, subdivided in turn into divisions. Currently, the maximum staff envisaged is around 300 people, while the budget for 2022 amounts to 41 million euros. However, for the coming years, a strong increase in resources is expected. 122 million euro is the planned budget for the Italian cybersecurity agency starting in 2026.

In France, the competent authority is the Agence nationale de la sécurité des systèmes d'information (ANSSI). As in Italy, the agency is part of the Council Presidency. Specifically, the French agency is part of the General Secretariat of Defence, a specific body assisting the Prime Minister in the exercise of his responsibilities in matters of defence and national security. Established by law in 2009, ANSSI immediately set itself ambitious goals , including becoming a world leader in cybersecurity. This wording is no longer present in the most recent version of the French cybersecurity strategy.

At the top of ANSSI is a Directorate General , which includes the Director General, Guillaume Poupard, along with the Deputy Director General and the Chief of Staff. Below , there are four sub-directorates, which in turn contain divisions. Excluding salaries, in 2020 ANSSI's budget amounted to about 21 million euros (excluding personnel costs), while the staff numbered over 500 officers and 100 recruits.

Germany also has a single competent authority, the Federal Cyber Security Authority (BSI). Contrary to France and Italy, this authority is not under the authority of the Prime Minister (Chancellor in this case) but instead part of the Directorate General of Cyber and Information Security in the Ministry of the Interior . The office was already established in 1991, but today its functions are mainly regulated by a law from 2009 . Subsequent measures have then been adopted, one in 2015 , anticipating many elements of the European directive issued the following year, and another only a few months ago. With the latest legislation , the German government intends to further strengthen BSI, especially when it comes to consumer protection, business security, and cell phone networks.

At the top of BSI is the president, Arne Schönbohm, and the vice president. The agency is divided internally into eight divisions, which in turn are divided into 18 branches and several sections. Its budget for 2021 amounted to almost 200 million euro, and its staff numbered 1550 people.

Information on budgets and staffing at these facilities, while interesting, is difficult to compare. This is not only because of the different sources from which the data was collected and the different methodologies used therein, but also because cybersecurity is not in any country the exclusive responsibility of a single organisation. Different structures such as ministries, defence, and intelligence have important roles in this area, and it is therefore very difficult to assess each country's cybersecurity efforts in these terms.

### The relationship between the defence sector and intelligence

As mentioned above, before the birth of the Italian Cybersecurity Agency, the sector fell within the competence of the Department of Information for the Security of the Republic (DIS). The new law , however, has placed the agency outside of the intelligence sector, even though there remain many links between the two sectors. Meanwhile, the government undersecretary in charge of intelligence has now been given the same remit in cybersecurity by law. In addition, coordination with the intelligence sector is ensured by the presence of representatives of intelligence agencies in the cybersecurity core, in which representatives of various ministries also participate. The presence of a representative of the Ministry of Defence is also foreseen, which probably guarantees the link between the Agency and the Network Operations Command (COR), the cybersecurity body under the command of the Chief of The Defence Staff. In the rules published so far, however, there is no explicit link between the agency and the COR.

The German Federal Cyber Security Authority also emerged from the intelligence sector , starting in the early 1990s as an office that dealt with the technological protection of state secrets. Over the years, however, the BSI has become a completely autonomous body. Relations with the intelligence community are maintained through the National Centre for Cyber Defence , an interinstitutional body that includes various federal structures interested in cybersecurity. This body also maintains relations with the military, which is of considerable importance in this sector in Germany. Cyber defence is in fact constitutionally assigned to the armed forces. In 2017 the Kommando Cyber -und Informationsraum (CIR) was established, a body considered on a par with the other commands of the German armed forces , responsible for the security of cyber defence infrastructure and weapon systems. Given the close relationship between defence and cyber security, the CIR provides support to

the BSI in case of need. However, given the strict constitutional limits placed on the German military, it can only provide '"administrative" assistance. In fact, in the event of the need to deploy military personnel in response to a nationwide cyber attack, prior authorisation by parliament is constitutionally required.

As we have seen, in France ANSSI is established within the General Secretariat of Defence . This structure guarantees coordination with the military and intelligence sectors. In fact, the General Secretariat of Defence has various competences in both defence and intelligence, carrying out for the President of the Council of Ministers the direction, proposal, coordination and regulation of general defence and national security matters. In addition, as we have seen, the General Secretariat of Defence is answerable to the President of the Council of Ministers, who is also responsible for the activities of the domestic and foreign intelligence services, even though these come under the Ministries of the Interior and Defence respectively.

*Harald Zwingelberg from Unabhängige Landeszentrum für Datenschutz and Álvaro Merino from El Orden Mundial contributed to this investigation.*

## Russia wants your data: cyber attacks are growing in the European Union

**Abstract:** The shadow of Russia has always loomed over the internet, but the pandemic, which moved citizen's lives into the digital sphere, saw a rise in security breaches within European businesses and institutions. Cyber attacks against key European sectors doubled in 2020. Although Brussels is working to plug the gaps, the invasion of Ukraine threatens to intensify the cyber war.

**Author:** Álvaro Merino (El Orden Mundial)

**Link:** https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Russia-wants-your-data-cyber-attacks-are-growing-in-the-European-Union

**Text:**

On 14th May 2021, Donna-Marie Cullen was waiting for her radiotherapy appointment as part of her battle against an aggressive brain tumour, when she received an unexpected call : a cyber attack had brought down the IT network of the Irish health service and her treatment had to be temporarily suspended.

After an intense year of pressure as a result of the pandemic, the Irish Health Service Executive (HSE) had succumbed, not to the virus nor to the chaos that ensued with lockdowns, but as a result of an invisible aggression being carried out hundreds of kilometres away.

Subsequent investigations concluded that the cause had been a ransomware attack perpetrated by Wizard Spider , a cybercriminal group based in Saint Petersburg who were demanding 14 million pounds – around 17 million euros – in return for calling off the attack. The Irish authorities chose to fight back, a decision which resulted in the suspension of thousands of appointments, a return to pen and paper records for months, the leaking of confidential medical records of 520 patients, and a financial loss of approximately 100 million euros .

Far from being an isolated case, the aggression suffered by HSE stands out among the avalanche of cyberattacks that had as its goal key institutions and businesses in the European Union. The shadow of

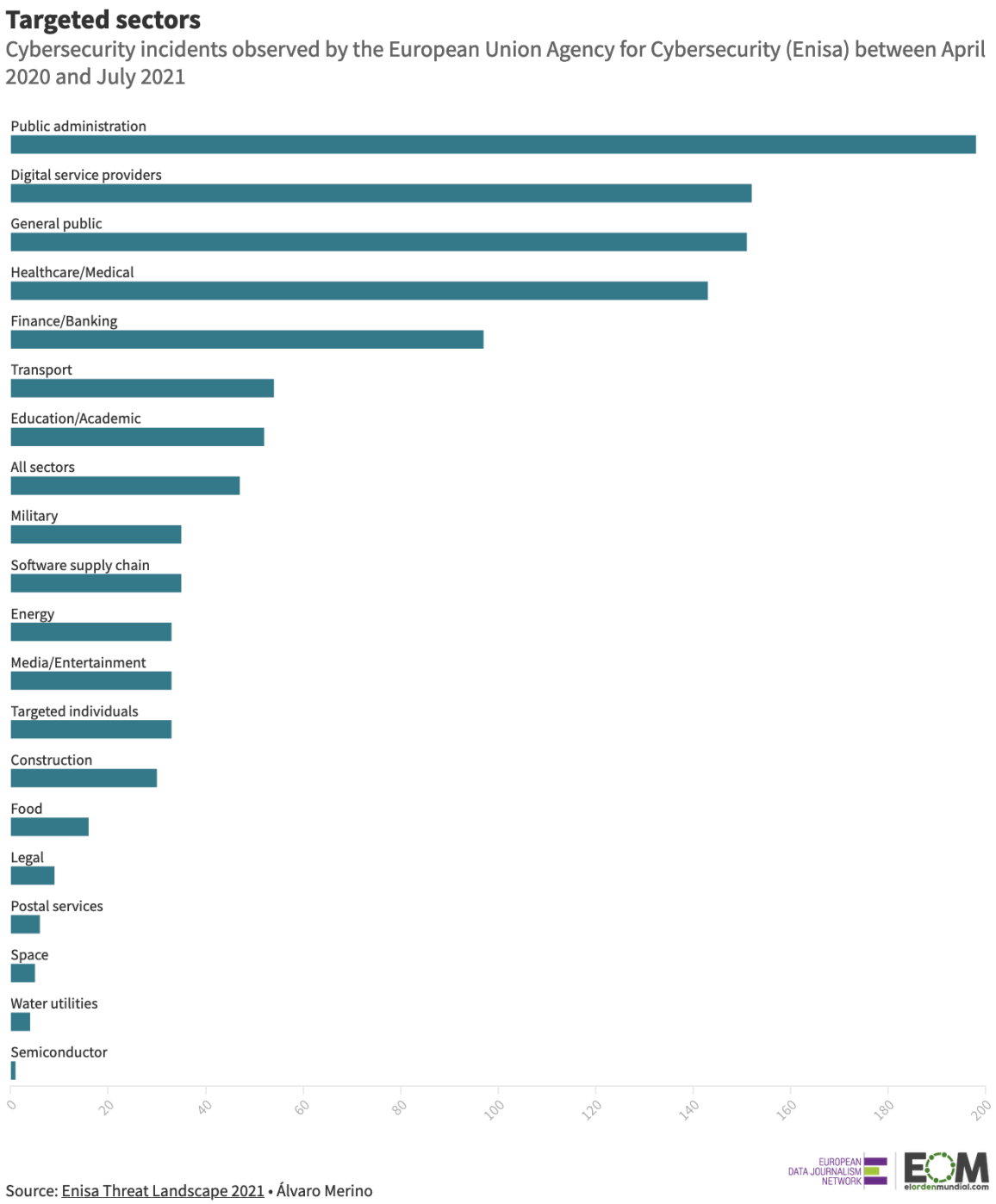
Russia has always loomed over Europe's digital world, but the pandemic has increased the frequency and virulency of attacks.

Unsurprisingly, in 2020, significant malicious attacks against key sectors doubled in Europe – up to 304 incidents compared to 146 in 2019 – according to the European Union's Cybersecurity Agency (Enisa). Cyber attacks on hospitals and healthcare networks rose by 47%.

## The new normal provides rich pickings for cyber criminals

Day by day, as cases rose and the pandemic ravaged Europe, the lives of its citizens gradually moved online. Suddenly, remote working, internet shopping and socialising through a screen became the norm. Although digital solutions meant that the world did not completely collapse, thanks to years of innovation, it also presented a pot of gold to cyber criminals.

On top of Covid-19, the transition from traditional infrastructure to the web, growing interconnectivity and the appearance of new technologies such as artificial intelligence has provoked a growth in cyber attacks "with regard to sophistication, complexity and impact", according to Enisa. In its 2021 report , Enisa warned that "this trend [of accelerated digital transformation] has raised the risk of attacks and, as a result, the number of cyber attacks directed at businesses and other organisations has increased".




Furthermore, public bodies, supply chains (which can wreak havoc as a consequence), and health networks became priority targets for cybercriminal groups at the beginning of the pandemic. Another target in the healthcare sector that suffered a paralysing cyber attack was the University Hospital of Brno , Czechia, which in March 2020 was forced to shut its IT networks, causing a delay in urgent operations and relocations of severely ill patients. Even the European Union's own institutions suffered a cyber attack in March of 2021 , though apparently without a security breach.

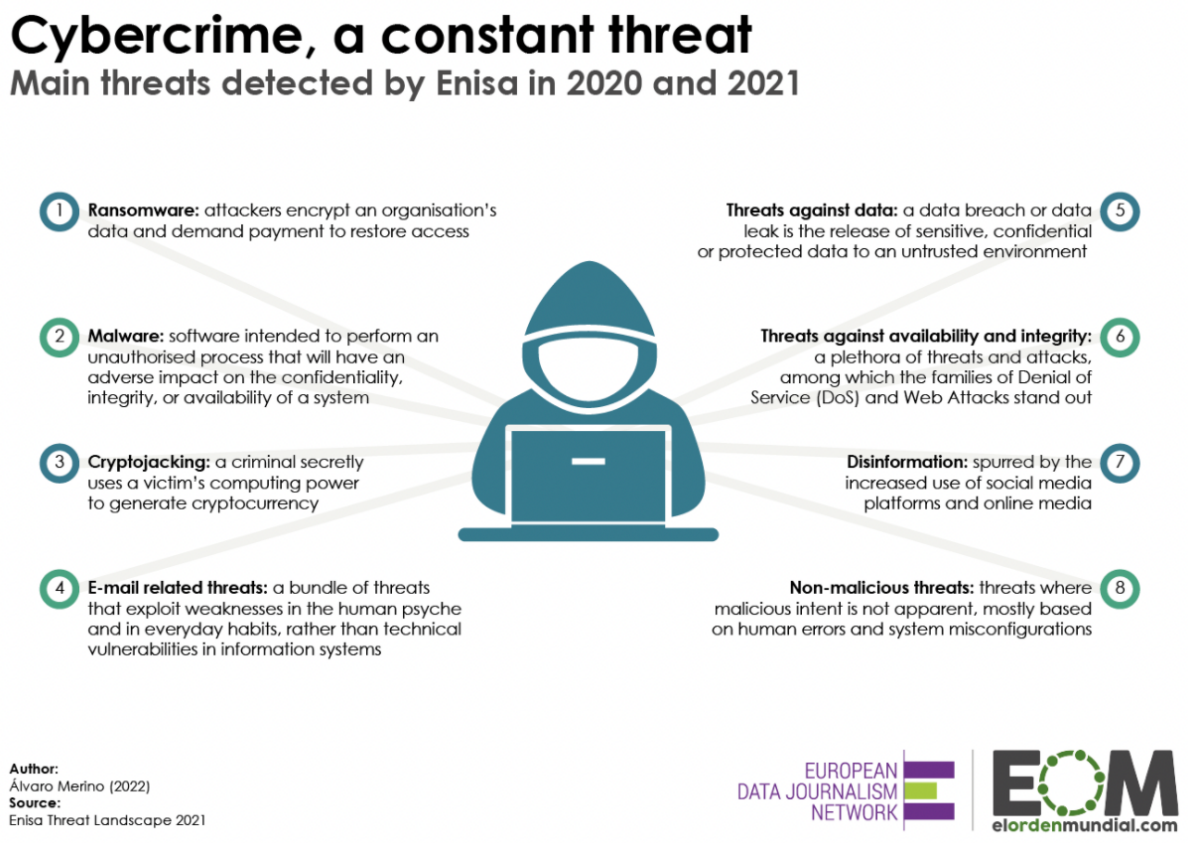
## Russia, the constant threat

The anonymous nature of these aggressions often makes it difficult to identify the enemy and respond proportionally. It is even harder in the case of supposedly non-state actors who are shielded by those who condemn them in public.

Although this makes it hard to establish the precise cyber capacity of each country, it is clear that Russia is one of the most prolific actors in the international sphere. Moscow uses the cyberspace to act on its geopolitical aspirations: reinforcing its role as a global power, consolidating control of its 'sphere of influence', and disrupting organisations that it deems to be an enemy, such as the EU or NATO.

There are dozens of examples: Germany, Italy, the Netherlands and Denmark have identified themselves in recent years as being victims of Russian cyber espionage; France announced at the beginning of 2021 that several of its key businesses, including Airbus and Orange, had been compromised by hacker attacks linked to Russia; last September, Josep Borrell, the High Representative of the European Union for Foreign Affairs and Security Policy, accused Moscow of attempting to hack into the computers of several European politicians and journalists, as well as leading figures in the energy sector and other citizens with a certain social relevance.

Apart from accessing sensitive information, Russian cyber criminals look to extract the personal data of European citizens in order to blackmail them or thwart European data protection systems, highlighting the vulnerability of the European digital society. The problem for investigators lies in the fact that it is hard to trace these attacks back to the Kremlin, because, in the majority of cases, the accusations are based on indicators, rather than on evidence strong enough to demand an explanation from Russia.



## The reaction in Brussels

The European Commission and Member States are perfectly aware that they are now central targets for cyber attacks, and that if Moscow keeps operating unimpeded in European networks there will be more security breaches.

To protect its networks, the European Commission updated its Cybersecurity Strategy in December 2020 and introduced a new directive concerning a tighter common level of cybersecurity in the Union (Directive NIS2). Both measures aim to strengthen its capacity to repel cyber attacks and extend network protection to new sectors, as well as support greater investments in cybersecurity for European organisations, which are currently 41% less than in the United States .

On top of that, the Russian invasion of Ukraine has further alerted the European Union: the European Central Bank has asked its national central banks to prepare to counter Russian cyber attacks, and the French Presidency of the European Council has promoted training drills to prepare for large scale attacks on supply chains in Member States.

All of this proves one thing: cyber wars are no longer science fiction stuff, they are already in full swing. Although they might not spill blood, they can have a crippling effect on the daily lives of citizens. With raised swords – or, rather, computers – and Russia that together with digital transformation pose enormous threats, the European Union is ready for battle, bringing the world with it to make cyberspace a safer environment for all.

# 3. Power imbalances and freedom of consent: Digital fortress Europe

## The ecosystem of European biometric monitoring and surveillance data

**Abstract:** A description of the main systems in use in Europe to manage the mobility of people through the European borders and across its countries, with a focus on the aspects that can be improved of the current mechanisms.

**Author:** Mediterranean Institute for Investigative Reporting (MIIR)

**Link:** Available starting from 26 April 2022

**Text:**

The digitisation and online transition of ever more aspects of our lives is a long-term trend accelerated by the COVID-19 pandemic. However, what goes largely unnoticed is the same trend involving the data collection and surveillance superpowers of EU states.

Member states' national authorities, such as police, internal security services, border guards, immigration authorities and European bodies such as Europol and Frontex, operate large-scale data collection and storage infrastructures. Under the guise of 'national security', a space is being created for potential violations of fundamental human rights, at a time when 'militarised' border security has already led to violence against refugees, push-backs with the risk of people returning to unsafe countries and inhumane conditions, and an alarming increase in avoidable deaths.

Countries are closing migration routes – with the discriminatory recent exception of Ukrainian refugees – thereby forcing migrants and refugees to seek other, often more dangerous, alternatives and pushing them into the arms of criminal smuggling networks.

But it is not only physical walls that are being erected; as the independent Transnational Institute TNI (Border War Series reports) reports, a key part of so-called 'Fortress Europe' consists of 'virtual walls' that seek to restrict migrants from entering the Schengen area or to monitor their movements within it. These 'virtual walls' come in many shapes and forms: from advanced surveillance systems that monitor migration flows and track people's movements at (and sometimes before) the external borders to 'smart', interoperable AI databases that aim to identify, record and profile migrants at and within the borders.

The common denominator of physical and virtual walls is the very social construction of the 'man on the move' as a potential threat to the EU and its member states. People trying to reach and enter the

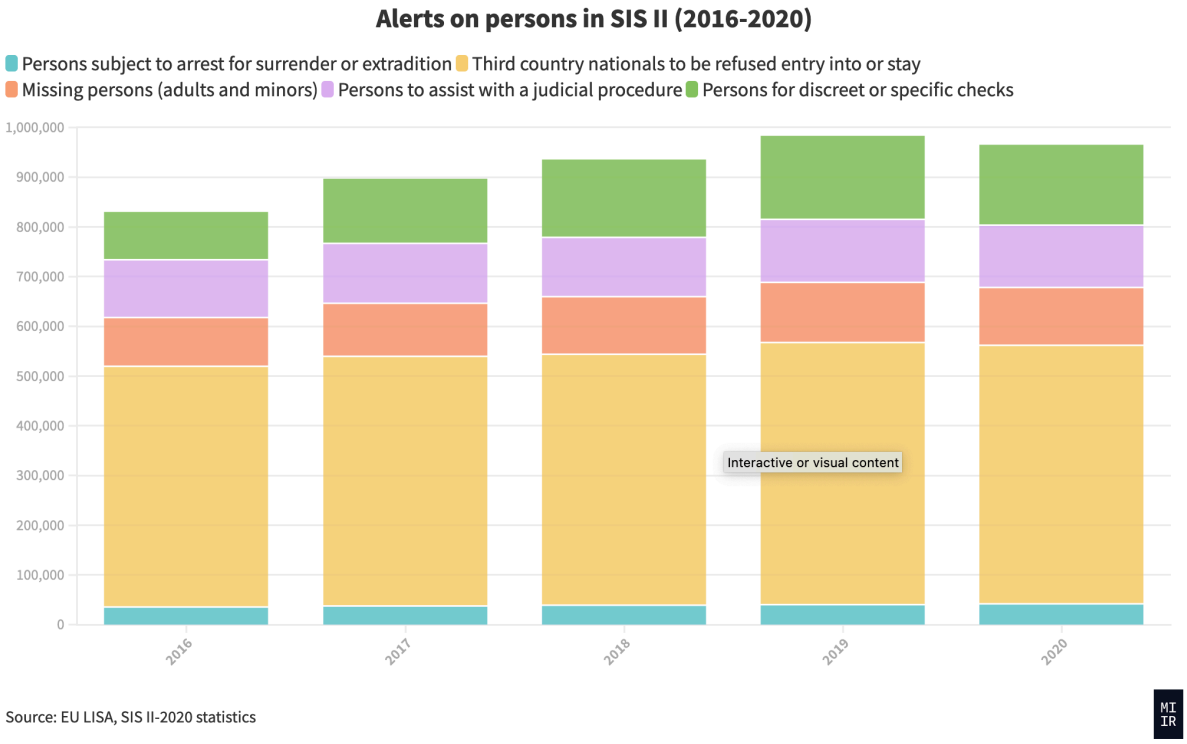
EU, fleeing disasters, violence, war or political persecution, are considered risk factors that need to be assessed and categorised.

MIIR's journalistic team within the Panelfit project (Participatory Approaches to a New Ethical and Legal Framework for ICT) undertook to penetrate the different EU data recording and surveillance systems, to study their legislation and the data collected in the different databases, to identify the human-rights risks also created by the interoperability of these systems, based on numerous interviews with experts in the field, researchers, activists, lawyers, NGOs and migrants. In the first part of the research we present a brief overview of the main surveillance systems.

## Description of the recording systems and personal databases

### 1. SIS-II Schengen Information System

The oldest database. Its purpose is to monitor the movements of third-country nationals in the Schengen areas. It was originally established in 1995 to be updated in its second version in 2013 and from the following months provisions incorporated in 2018 will enter into force. It is the largest IT system in Europe, operating in 26 EU member states (Cyprus is not included but is expected to join) and in Switzerland, Norway, Liechtenstein and Iceland.  Under the SIS II regulations, data (names, surnames, dates of birth, and other alphanumeric information) of third-country nationals subject to return decisions, data on refusal of entry or stay of persons in the Schengen area, and objects (e.g. cars, weapons, lost documents, passports, etc.) are collected and processed for the purpose of police and judicial cooperation. The provisions of the SIS II Regulations allow for the application of biometric identification of persons based on facial recognition technology. It is used both by police authorities and by immigration and asylum authorities. If a person applies for asylum, the authorities can search the SIS to see if there is an alert for him or her. Alerts can be issued for persons wanted for arrest or control, persons under surveillance by law enforcement authorities, persons who do not have the right to enter or stay in the EU, persons wanted for judicial assistance and missing persons (adults and children).




The SIS II system in 2019 set a record with 18 million searches per day by all competent authorities entitled to access it. In fact, this number is three times higher than the number of searches in 2014 (6 million searches per day). Indicative of the widespread use is the introduction at the end of 2020 of the Automated Fingerprint Identification System (AFIS) application, enabling searches by States and through fingerprints and introducing automatic checking and comparison with existing searches.

However, indicative of the targeted expanded use of the system to identify undocumented migrants is that of the 964,720 alerts issued in SIS II in 2020, more than half were for third-country nationals who had been refused entry and stay within Schengen. This has been the case consistently over the years, as the table of alerts 2016-2020 shows.

## 2. VIS – Visa Information System

It was gradually put in place from 2011 and the development of the system was completed in 2016. The system is used by the 30 Schengen states together with Bulgaria, Croatia, Cyprus and Romania. The purpose is to allow these countries to exchange data on short-stay visas and to facilitate visa checks at border crossings. The competent asylum authorities can access the VIS. In 2018, the European Commission presented a proposal to revise the VIS in order to broaden its scope. The proposed rules suggest that the VIS should also include data on long-stay visas.

**VIS: Use of biometrics, searches and access**

**68 million facial images stored in the VIS**
By the end of 2019

**69 million fingerprints sets stored**
By the end of 2019

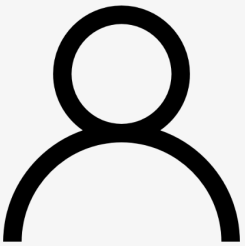
**100 million records capacity**
By the end of 2019

**7 million biometric searches in 2019 (2018: 8 million)**
Searches in 2019

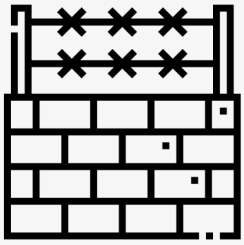
**17 million biometric authentications in 2019 (2018: unchanged)**
Searches in 2019

**25 million alphanumeric searches in 2019 (2018: 23 million)**
Searches in 2019

**116 national authorities granted access**
Access



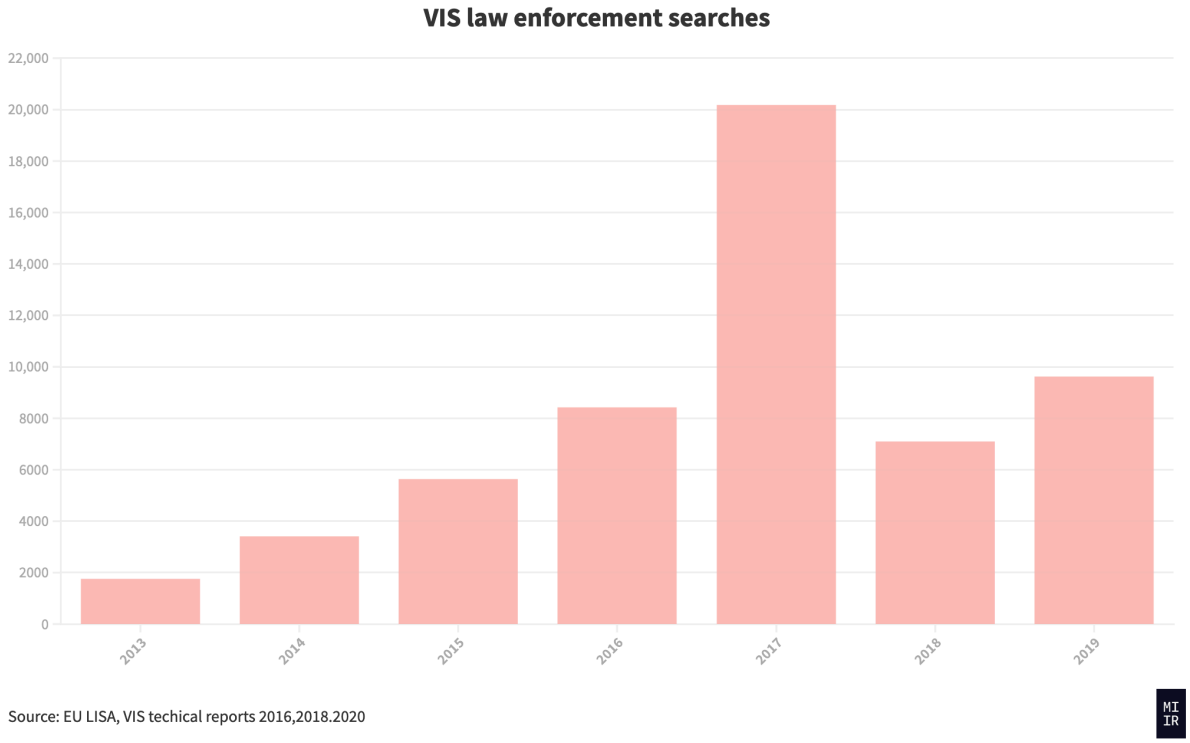
**458.000, total number of end-users accessing VIS**
Access



**84 million border checks (visa verification and identification)**
Border checks

The system stores fingerprints and a photograph of visa applicants/holders, as well as personal data included in their applications, such as surname, home address, information on visa status and bank data (proof of deposit). “Without this the visa will not be granted. This is implicitly a class discrimination: if you are rich you can travel, if you don't have money they will not reasonably give you a visa (‘low-tech discrimination’). The amount depends on each member state," says researcher Georgios Glouftios.

Automated biometric identification is already used in the VIS on the basis of the fingerprints collected. In 2019, 7 million biometric searches were carried out and 17 million biometric identity checks were carried out, the latter mainly at border stations. At airports, authorities check third-country nationals travelling to Europe to ensure that their fingerprints match those on their individual file in the VIS system, which is compulsorily set up prior to travel.  Police authorities can search the VIS to see if a person who has previously applied for a visa is involved in criminal activity. It can also be used by asylum authorities.




Another element that exacerbates the privacy concerns of citizens and organisations towards these systems is the extended access by agencies and people from all services. It may be true that every year the authorities in each country that are entitled to access the database are published in the EU Journal. But this alone is not enough, as the number of end-users who may have access to individuals' personal data is uncertain. For example, in the VIS system a total of 116 national services and authorities, including law enforcement authorities, have permission to create, modify and delete data – and the number of end-users reaches the astronomical figure of 458,000 employees, who all have access to this sensitive personal data.

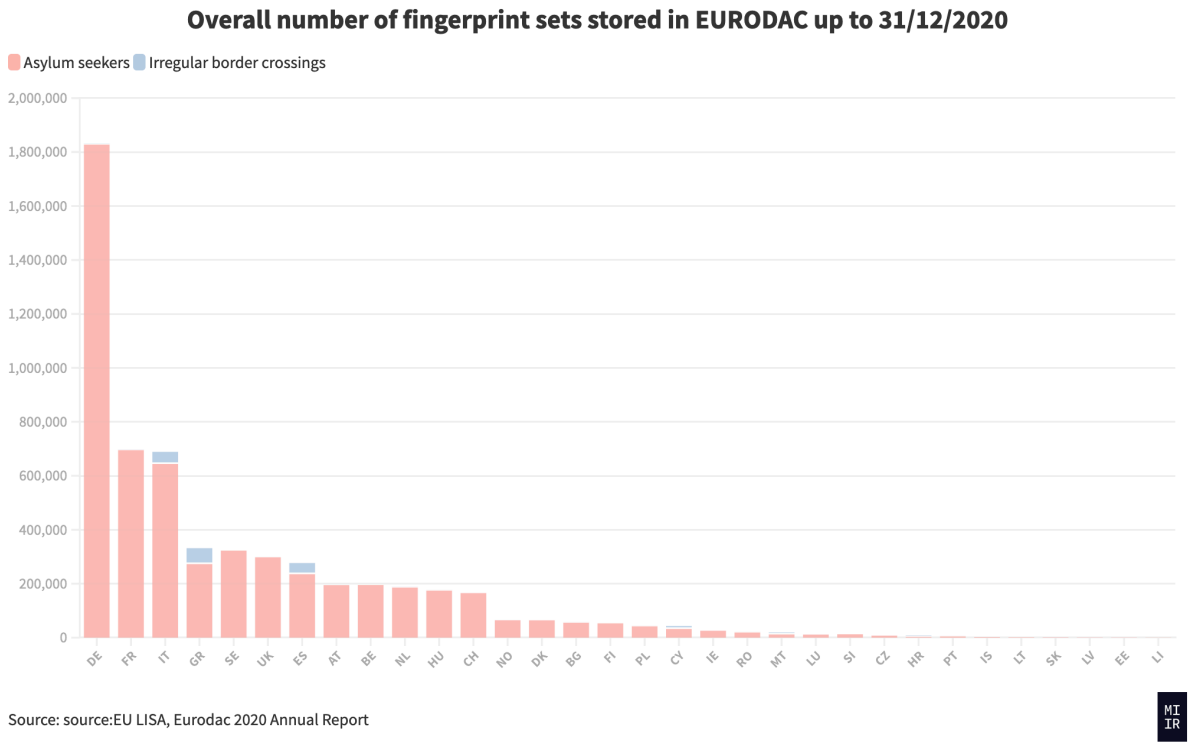
## 3.Eurodac

The European system for the comparison of fingerprints of asylum seekers (EURODAC) became operational in 2003, as the first IT system allowing the storage of fingerprints in a database at EU level. The purpose of the system was to make it easier for EU countries to determine responsibility for examining an asylum application by comparing the fingerprints of asylum seekers and third-country/non-EEA nationals with a central database. In addition, the purpose was to enable law-enforcement authorities, under strict conditions, to search Eurodac for the investigation, detection and prevention of terrorist or serious criminal offences. So far it only stores biometric characteristics, and does not even record someone's name. When an asylum seeker or a third-country/non-EEA national is found illegally in an EU country, then the EU country can consult Eurodac to see if the person has previously applied for asylum in an EU country or has already been arrested while trying to enter the EU illegally.

EURODAC is currently under review. The proposed revisions provide for the interaction of EURODAC with other EU IT systems in asylum, return and resettlement procedures. In this context, EURODAC will be used, inter alia, for the control of migration flows and the detection of secondary movements of third-country nationals in an irregular situation.

However, figures show that the collection and storage of fingerprints of third-country nationals or stateless persons is also common practice. In particular, member states transmitted a total of 644,926 fingerprint sets to EURODAC in 2020. Of these, 62% represent fingerprint datasets of applicants for international protection, 25% represent fingerprints of a third-country national or stateless person found to be illegally staying in a member state, while 13% are those of the same groups found illegally crossing the external border.

The new proposal, if adopted, would introduce a mandatory requirement to collect and store the fingerprints of third-country nationals or stateless persons found to be illegally staying in Europe. In addition, the volume of personal data collected will be radically increased. The proposed provisions will allow the collection of a wide variety of biographical and biometric information in addition to that already collected, such as images of persons, names, date and place of birth, and nationality.




The almost 6 million fingerprints accumulated in EURODAC at the end of 2020 do not belong exclusively to asylum seekers, but also to migrants that host states have classified as "irregular border crossers", who are not entitled to access asylum procedures. On 31/12/2020, when the registration was made, they only accounted for almost 155,000 (3%), but the fingerprints of this category are automatically erased from the database after 18 months, unlike those of asylum seekers, which are stored for 10 years. For example, the corresponding proportion for them at the end of 2016 was 13%. It should be noted that since July 2015, the EURODAC database has also been accessible to the police services of the countries and Europol in the name of preventing and investigating offences related to terrorism and serious crime.

It is noteworthy how Germany, although not a country of first reception like Italy and Greece, nevertheless appears to accumulate the vast majority of biometric data among the 32 Segen countries. This is due to the fact that a large majority of the migrants who came to Europe especially with the 2015 refugee crisis applied for asylum for the first time in Germany, and not in the countries at the entry points of the European borders. In the biometric storage ranking, the countries following Germany are France, Italy, Greece, Serbia, the United Kingdom and Spain.

It is also striking that Greece is the "leader" among the 32 countries in the collection of fingerprints of migrants who are not entitled to access to asylum. This amounts to 56,000 (i.e. one third of the total of this category in EURODAC) out of a total of 331,609 fingerprints registered by Greece at the end of 2020. The remarkable Greek first place is linked to the process of data recording and screening in Greek reception centres for migrants entering the country.

The first official stage of registration, in addition to checking the relevant documents that the person may be carrying (passport, identity card, other documents) is the examination/interview/interrogation by either Greek police or FRONTEX personnel, the so-called screening. "The purpose of this procedure is to ‘calibrate’ the identity of the person, i.e. data such as age, nationality, place of origin, family relations, and it is done in cooperation with FRONTEX translators", says Vassilis Vlassis, a post-doctoral researcher on surveillance technologies at the University of Informatics in Copenhagen. He has conducted a field study on asylum and screening procedures in the reception centres in Chios and Lesvos. "In interviews I have done," he continues, "with people who were screeners at VIAL, in Chios, it turned out that a lot of data is examined: speech, pronunciation, spelling, clothes, jewellery, of course mobile phone photos etc., all are examined and taken into account in the conclusion that the screener will draw: ‘I know that Syrians spell Mohamad like this and never like that, while Moroccans spell it like this, but never like that’ I was told. Instinct, intuition also play their part. Sometimes, as soon as they walk through the door, you immediately have an opinion, and then you seek to validate it, as one of the auditors also said," recounts Vlasis. In conclusion, the way in which this data takes shape is multifactorial and has strong performative elements, yet it can nevertheless have a decisive impact on the future of the migrant who joins EURODAC. "The coordinator of the FRONTEX mission to the Greek islands in 2016 himself told me: 'the result of the screening does not constitute a scientific fact. It is a working hypothesis, the best we can do and what we are working with'", recounts Vlassis.

### 4. EES (European Entry/Exit System)

Established in 2017 and expected to be fully operational in May 2022. It collects data on all third-country nationals regardless of whether they need to apply for a visa or not. It records and stores the date, time and place of entry and exit of short-stay visa holders and travellers who are exempt from the visa requirement while crossing the EU border. The system aims to replace the passport stamp procedure by allowing the processing of biometric data of individuals. It will also record the length of someone's stay and create automated alerts for situations of "overstaying" in a country. National law enforcement authorities and Europol will be able to access this database.

### 5. ETIAS – (European Travel Information and Authorisation System)

Created in 2018 and the goal is to be fully operational by December 2022. According to EU declarations, it is "a largely automated IT system that will be set up to identify security, irregular migration or high epidemic risks posed by visitors travelling to Schengen states who are not subject to visa requirements. [...] Third-country nationals who do not need a visa to travel to the Schengen area should apply for a travel authorisation through the ETIAS system before travelling." It is yet another example of the EU treating people planning to travel to Europe as risk factors. It will not store any kind of biometric information. However, different categories of data will be collected, such as the applicant's surname, nationality, country and city of residence, home address, email address and phone number, educational status (primary, secondary, higher or no education).

In practice, the ETIAS system will work in much the same way as the ESTA system in the US.

## 6. ECRIS-TCN (The European Criminal Records Information System that concerns Third-Country Nationals)

Originally created in 2012, ECRIS allows for the efficient exchange of information between member states regarding criminal convictions in the EU. Most of the information exchanged concerns European citizens. The revised European Criminal Records Information System will now include a central database of information on convictions of third-country nationals and stateless persons (ECRIS-TCN) and is expected to be operational in 2022. Both biographical and biometric data of convicted third-country nationals, stateless persons and EU citizens who are third-country nationals and have been convicted in a member state are stored within ECRIS-TCN. These data include categories such as full names, place and date of birth, nationality, gender, identity numbers, as well as fingerprint data collected in accordance with the legislation of the member state during the criminal proceedings. The facial images of convicted persons will also be stored in the system if the legislation of the convicting member state allows the collection and storage of facial images of convicted persons. The database will be available on the internet and authorities will be able to easily search it with a positive/negative search mechanism: a positive search result will identify the member states from which complete criminal record information on a particular person can be obtained.

ECRIS has been used around 3 million times a year to exchange information on previous criminal convictions. Around 30 % of the cases in which criminal records information is requested are answered positively.

According to the Meijers Commission, a group of law professors, researchers, judges and lawyers working to ensure that European legislation respects the rule of law and guarantees fundamental rights for all, the ECRIS-TCN regulation is the first European legislation to treat as third-country nationals European citizens who are also nationals of a third-country.

## Interoperability of systems

The servers of all these systems are located in Strasbourg. There the servers are managed by the EU-Lisa service. When we think of border controls and mobility checks we usually think of Frontex, but Frontex is not the main player in these databases. EU-Lisa, the European Agency for the Operational Management of Large-Scale Systems in the Area of Freedom, Security and Justice, has been operating since 2012, is based in Tallinn, Estonia, but its operational centre is in Strasbourg. It has coordinated the testing of the Smart Borders pilot project and subsequent actions, analysis of results and reporting on this project, in close cooperation with the participating EU countries and the European institutions. EU-Lisa is responsible for the operational management of EURODAC, SIS II, VIS and Entry-ExitSystem, while ensuring information security and data protection.

In 2019, the EU adopted two regulations putting in place a legal framework requiring the interoperability of 6 of the databases described above (VIS, SIS II, Eurodac, Entry-Exit System, ECRIS-TCN and ETIAS). The objective is to implement the general data interconnection system by the end of 2023.

While the European Commission presents interoperability as a natural progression, in practice this is not the case, as many of the existing databases are not yet fully operational.

## "Point of no return"

According to the European Data Protection Supervisor, the EU legislator's decision to make these systems interoperable would mean a "point of no return", with profound implications for the right to privacy of people entering the EU. A new central database containing information on millions of third-country nationals, including their biometric data, would have new and improved access to information systems.

Four more data collection platforms across the EU will become operational or are planned to expand their scope over the next two years. The European Search Portal (ESP) will enable national and EU competent authorities, when they are unable to identify an individual or have doubts about the identity provided, to be able to initiate a query by submitting biographical or biometric data to ESP, which will search the 6 databases simultaneously. The Biometric Matching Service will create and store templates from all biometric data recorded in the underlying systems. The Common ID Repository (CIR) will store an individual record for each person enrolled in the systems, which will contain biometric and biographical data. Finally, the Multiple Identity Detector will be able to cross-check identities across all systems.

As stated in the Technological Testing Grounds report by the EDRI Network and Refugee Law Lab authored by Petra Molnar, this single interoperability framework provides a favourable infrastructure for many automated decision-making processes that put human rights at risk. Statewatch director Chris Jones, author of the report “Automated suspicion: the EU's new travel surveillance initiatives”, said: "The enthusiasm among EU and member state officials for using new techniques and tools on unsuspecting travellers is worrying, as they increase the risk of discrimination, may lead to further errors in decision-making and will hand over more personal data to governments. People should think more about how their governments treat foreigners – otherwise they too may be treated as suspects rather than citizens."

It is also noteworthy that there is a complete absence of any impact assessment by the legislature on the human-rights impact of the new interoperable systems and on the resources and scope of the independent authorities that control these systems, so as to hold them to account.

One of the pitfalls of technological development is that we tend to believe that it will increase efficiency and help achieve the goals for which it was designed. Too often, this is not the case. A first major issue that arises has to do with the quality of the data being entered into some of the aforementioned databases we have presented. "For example, according to a report recently published by the European Court of Auditors, there is a major problem with the quality of the data entered into the Schengen Information System. And quality here can refer to both biometric data and alphanumeric data. For example, it may happen that a police officer in a member state misspells the name of a wanted person when entering an alert into the system or enters a person's name in the data field dedicated to surnames," says researcher Georgios Glouftios. If a person is registered in a database with an incorrect name or other poor quality data, two problems can arise. The first concerns false negatives: wanted or suspected persons are not identified by the system simply because their names are not correctly stored in the database. The other problem is false positives, meaning the incorrect identification of a person. For example someone is being checked by the police for whatever reason and by mistake his/her name looks very similar or the same as a bad alert stored in a system. In this case, he/she may run into trouble precisely because the system incorrectly identifies him/her as a wanted person.

"I think there are three main problems in terms of the accuracy of the technologies applied for border security. First, poor data quality. Second, lack of data completeness. And third, and this is more about future developments, biased data and potentially biased security decisions," says Georgios Glouftios.

* Quote from the "Technological Testing Grounds, Migration Management Experiments and Reflections from the Ground Up" (EDRi, refugee law lab, November 2020, author Petra Molnar)

## Trapped in a digital surveillance system

**Abstract:** The impact of surveillance systems on vulnerable populations, money for Frontex drones, and monitoring the movement of citizens within the European area.

**Author:** Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

**Link:** Available starting from 26 April 2022

**Text:**

At the Greek Consulate in Istanbul, one morning in 2016, Erkan, a Turkish citizen of Kurdish origin, crosses the threshold of the building to address the Greek authorities. He was seeking a visa to enter Greece in order to flee Turkey at a time when the Erdogan regime was stepping up persecution, particularly against the leadership and members of the opposition HDP party and its Kurdish supporters. The Greek consular authority, however, rejected the visa request and Erkan was forced to remain in Turkey.

Orestiada Evros, 4 years later. Erkan was arrested at the Greek-Turkish border as he attempted to enter Greek territory and was taken to court. The court sentenced him to 4 years in prison without suspension and a 10,000 euro fine on charges of re-entering the country. But Erkan had not re-entered Greece.

What had happened? In front of Greek judges, Erkan sought asylum from Greece for persecution by the Erdogan regime, but was told that his name was on the National List of Unwanted Aliens (EKANA) and the Schengen Information System (SIS II, the largest information exchange system between Schengen countries), with a note that he had been banned from entering the country for 7 years. Because of his inclusion on these lists, he was taken first to Komotini prison and then to Corfu prison.

"We were trying to find out what had really happened" recounts Erkan's lawyer and Human Rights 360 attorney, Eugenia Kouniaki. "My client had never entered Greece before and was suddenly convicted of re-entering the country. Initially, I contacted the police authorities, the Director of the Asylum Service in Athens, where he replied that my client had been included in the EKANA and SIS II because his visa had been rejected by the Consulate in Istanbul."

The truth was quite simply to be found in the operation of the Single European Visa Information System (VISA-VIS) and SIS II. The Greek consulate that processed Erkan's application entered the visa refusal in the VIS system and in SIS II at the same time. From then on, this record was enough to get him on his way to prison, even if he sought international protection.

"Even when I asked for his removal from the undesirable list and SIS II, as Erkan was an asylum seeker, the Greek police refused," Kouniaki describes. "Apart from the fact that my client did not know that he was on the list, when we tried to find out why his visa was refused in 2016, we received the vague answer 'for falsifying some documents'. When we attempted to find out what documents were claimed to have been falsified, we could not check what they were. Fortunately, in the appeal that we filed for a delay in implementing the sentence, the judges accepted our arguments, and after a year he was released from prison."

However, after all this unfair treatment and imprisonment, he preferred to leave the country "because he believed that he would never find justice," Kouniaki concludes.

### Burning fingers to avoid identification in EURODAC

Erkan's story may sound outrageous, but unfortunately it is not the only one linked to the consequences of surveillance technologies and biometric data systems for migrants. In the report "Technological Testing Grounds: migration management experiments and reflections from the ground up" (EDRi, Refugee Law Lab, November 2020), author Petra Molnar, a lawyer and member of EDRi

(European Digital Rights), has collected a multitude of interviews with asylum seekers in Brussels who came into contact with mobility control systems during their journey to safety in Europe.

Caleb, a married man in his 30s, describes his experience of the asylum process by saying he felt "like a piece of meat with no life, just fingerprints and iris scans". Another migrant, Esche, describes her encounter with drones in the Mediterranean and the English Channel with a devastating quote the moment she saw them in the sky: "now we have flying computers instead of more asylum".

The most unpleasant story is told by Negassi, a 20-year-old from Ethiopia: 'I am tired and I want to go to England' he says after being stranded in Brussels for nearly two years, undocumented, and earlier the same in Nuremberg for 5 years. But this is not his first time in Belgium, as he was deported to Germany before when he was arrested in a park in Brussels, where he was sleeping rough. When his biometric data was taken by the Belgian police, his fingerprints showed a hit on the EURODAC system, which stores and identifies the fingerprints of asylum seekers, identifying him as a first-time asylum seeker in Germany. So they sent him back because of Dublin II, which stipulates that the first host country has to process the claim.

Negassi acknowledges that the process of collecting biometric data is invasive to the body, but asks: "How can I refuse when the police handcuff me, take me to the station and force me to give my fingerprints?" he tells Molnar. He has friends who have gone so far as to burn their fingers to alter their fingerprints and avoid identification. "However, that doesn't solve the problem" for Negassi, as no identification usually means a longer detention period.

"There is a very important aspect that is not discussed enough in the public debate," Petra Molnar tells us, "and it concerns the fact that these surveillance technologies cause trauma to people who are not even familiar with the technology. The migrants I spoke to all had a strong belief within them that they were experiencing racist and discriminatory treatment through their contact with these systems."

This is why it is even more important, he continues, "in terms of the rampant use of these technologies, that there is accountability, oversight and governance. We need to focus on what kind of governance structures need to be developed to ensure that these technologies, which are a human-rights risk, do not cause trauma to people."

The accountability part, however, does not seem to be enhanced by the way these systems are developed. The involvement of private companies in the security and defence industries further complicates matters. "There is a very problematic relationship of private companies and state institutions working together under the guise that states themselves cannot develop these technologies in-house", points out Molnar. "So huge public resources are directed to big companies to develop

them. But also from a legal point of view, it creates the problem of what some call 'responsibility laundering' when something goes wrong. In these cases, as we have seen, the state says 'it is not our problem because we did not develop this technology'. And the private company for its part retorts that 'the state management of the tools is to blame'."

But public budgets for the industrial complex of migration management and border control are substantial, Molnar points out. "Of all that money in such a problematic technology that inflicts trauma, imagine if it went to education, legal services, housing. Why don't states, instead of pouring so much money into surveillance technologies, think about how to use it for social inclusion?"

## The European Border Surveillance system (Eurosur) and the money for drones

Perhaps the most interesting system for migration issues is Eurosur, which produces maps of both territorial/land and maritime borders. It is operated by Frontex and allows for the exchange of maps between states regarding border controls at sea. "The development of Eurosur was launched in 2007, but it reaches the European Parliament for the first time at the end of 2012, after hundreds of millions have been spent and its design has been completed, effectively presenting the institution with a fait accompli. Due to the lack of transparency, the research in the relevant directorates of the European Commission is largely captured by the priorities of the security-industry complex", journalist Apostolis Fotiadis reported in his book "Border Merchants".

When it was first developed it was promoted as a "humanitarian technology", a system that would allow the authorities of each member state to conduct search and rescue operations. The idea was that "we use maps, we get information from satellites and also from drones, to perceive migratory flows, for example from Africa to Europe, so that we can rescue people at sea". The problem is that Eurosur creates so-called pre-frontier pictures. These are maps that focus on the area before the border, before a ship arrives at the maritime border, for example Greece. "Mainly they do it to organise pull-back operations, because for example the Italian authorities can share data with the Libyan authorities so that the Libyan authorities can take back the migrants. They know that push-backs are not allowed, so the solution is pull-backs. That's why Libya is funded," explains Georgios Glouftios, a lecturer at the University of Trento, to MIIR.

For the creation of the pre-frontier maps, Frontex also cooperates with the European Union Satellite Centre (EU SatCen), which provides it with satellite imagery, aerial photographs and other related services. The Eurosur database also records incidents occurring at the EU maritime borders, although member states have not been obliged until now to upload data from incidents at border checkpoints in a systematic and organised manner (this changed with an implementing regulation in April 2021). Which means that there is no complete and methodical recording of incidents, blurring the overall picture of incidents at the external borders. A fact that is also admitted by the European Commission in the Eurosur evaluation report (September 2018).

Frontex's second report in 2018 on the operation of Eurosur recorded over 184,000 incidents in the period from December 2013 to the beginning of 2018, with the vast majority (147,827) relating to migratory flows.

**Events inserted in Eurosur 2013-2018**

| Eurosur Node | Crisis | Irregular migration | Related crossborder crime | Other | Total events |
|---|---|---|---|---|---|
| Member State | 66 | 83,845 | 20,641 | 686 | 105,238 |
| Frontex | 80 | 63,982 | 12,231 | 3029 | 79,322 |
| Total | 146 | 147,827 | 32,872 | 3715 | 184,560 |

Source: Frontex

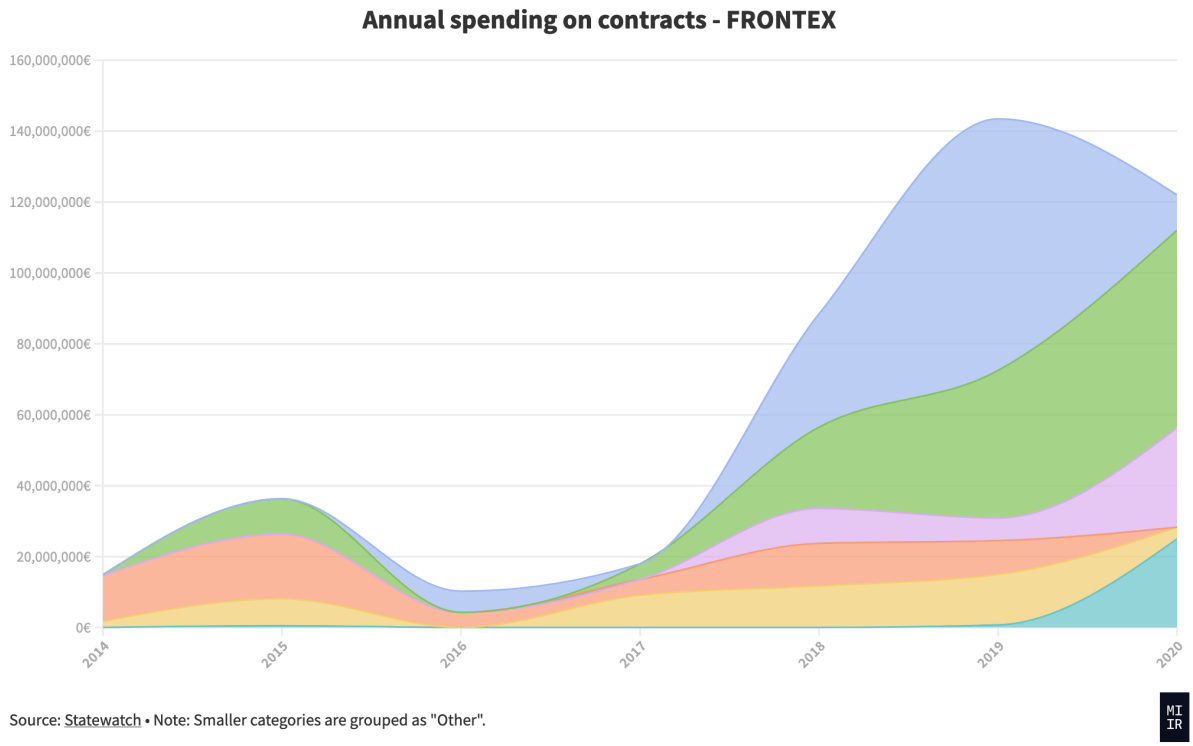
MI IR

In February 2022, the French government announced that it would install additional cameras along the Channel coast to help monitor migrants hoping to cross the stretch of water to the UK. The cameras are being paid for by the British government. In December 2021, the Italian navy delivered a new shipment of containers with surveillance equipment to Libya to monitor migration in the Mediterranean (source: Altreconomia research magazine, February 2021 issue). Additional "trap cameras" for cars and people have also been placed at or near the border between Italy and Slovenia along the so-called Balkan route.

## Eyes in the sky

Frontex confirms that it uses "a set of services falling under Eurosur, the information exchange framework designed to improve the management of Europe's external borders" (source: infomigrants.net, "Digital borders: EU increases use of technology to monitor migration", 18.2.2022). It states that most of this monitoring is carried out "by aerial surveillance by manned and unmanned aircraft, with satellite imagery devices and collection of vessel positions through positioning systems".

According to a recent in-depth survey ("Funds for Fortress Europe: spending by Frontex and EU-LISA", January 2022) by the non-profit organisation Statewatch, Frontex spends most of its annual budget on maritime and aerial surveillance, alongside deportations (chartered and scheduled flights for the return of migrants). According to data analysis carried out by Statewatch, between 2014-2020 Frontex together with the European agency EU-LISA (which oversees large-scale mobility-control information systems) spent a combined €1.9 billion on contracts with private IT companies and the security and defence industry. Of this money about half a billion (€434 million) was managed by Frontex with more than €100 million going to contracts with private companies related to air surveillance. This included a €50 million contract with the Airbus consortium – one of the leading trans-European companies in the aerospace and defence industry – and the Israeli company Albeit, which supplies 85% of the Israeli army's drones.




https://public.flourish.studio/visualisation/9014574/

In the same period, Frontex seems to have had a profitable relationship with three other air surveillance service providers: the Canadian CAE Aviation, the British Diamond-Executive Aviation (DEA) and the Dutch EASP Air. As a consortium they won 8 contracts worth a total of €57 million (not counting the contracts they have signed alone for other security and control services to Frontex).

The same trend continued in 2021 with €84 million – i.e. one sixth of Frontex's annual budget – going to air surveillance services.

In the deportation process, Frontex has worked with the Polish eTravel SA on a €30 million contract to provide travel services (booking and ticketing services) for the scheduled return flights. It has also worked with the British multinational Air Charter Service Limited and the Norwegian AS Aircontact in flight chartering for the same purpose.

London-based Privacy International in July 2021 published its findings on how an increasing number of companies are "developing satellites capable of tracking and selling their data to border agencies". The organisation concluded that while "such surveillance can save lives, it can also facilitate pullbacks or be used to persecute asylum seekers".

The use of all these surveillance technologies also has a deeper consequence, underscores Antonella Napolitano, network coordinator of Privacy International. "On the one hand, it contributes to the

criminalization of the migrant's person, and at the same time it turns him into a data hub, from the beginning of the journey from the country of origin to the evaluation of biometric data in the EU. The aim is to fully record his movement and track him until the next steps within the European area. Indeed, if he is found trapped because of a wrong recording or decision within these systems where his data is stored, this error follows him for the rest of his life."

This notion is not unconnected to the risk of extending surveillance to the whole range of travel, whether for tourism or work. Moreover, Napolitano points out, "the very interoperability of the systems is a good example of how a system developed to monitor migratory movements can then be extended to everyone, as these systems are progressively extended to all travellers entering the European area, but also to EU citizens moving within the EU".

"Being potentially considered a 'criminal by default', a concept reflected in the management of surveillance technologies, cannot leave anyone indifferent," Napolitano concludes.

## Passenger Name Record: the monitoring of intra-EU movements

The Passenger Name Record (PNR) concerns the recording of all data of passengers moving within European territory, regardless of whether they come from a third country. What does this system collect? Name, nationality, when we travelled, where from, where to, our email, our address. Apart from that, one can find out our travelling companions, possibly some data related to our stay such as hotel reservations, whether we travelled for business or personal reasons. It can probably even find out in an extreme case our religion, as the system even records the meal we ate during our flight. This meal may contain 'interesting' facts about us, e.g. if we eat kosher we are Jewish, if we don't eat pork it means we are Muslim. It may also reveal if someone has allergies.

The PNR is accessible to the police authorities of each country. "And this is where the problems start. There is a European directive on how personal data can be processed through the PNR system. This European legislation must be transposed into national law in each country. The problem is that we have some failures in the transposition of this directive in different countries, such as Greece," says lawyer Kostas Kakavoulis, a member of Homo Digitalis, to MIIR. As he explains, "the European directive says that each member state shall establish or designate an authority which is responsible for the prevention, detection, investigation and prosecution of serious terrorist offences. So we are talking about an authority that is either established from the outset or exists and is given this competence. In Greece, the legislature has given this competence to a department within the Directorate of Information Management and Analysis of the Greek Police. So we are not talking about an authority but a directorate of the Greek police. It is absurd for the body which holds the data, the police, to ask for access to this data from a department within the police. If it is subject to hierarchical control or if there are pressures in general, it is rather doubtful that a department of the Greek police will refuse to provide other departments of the Greek police with data that they need, even if it were necessary to do

so. In France this is not the case, as a special independent authority has been set up for PNR data. In Greece any police force can have uncontrolled access to PNR data anywhere, anytime. There is no record anywhere of who requested which data, when and for what purpose. And there is no classified access policy. You only need to be a member of the police force to access this data."

In Greece, the organisation Homo Digitalis (member of EDRi), in an open letter to the parliament, underlines that "the data in question can reveal the pattern of a person's movements, such as the time of travel, the place of departure and arrival, his/her email and address, as well as a person's travelling companions, but possibly even related hotel reservation data, etc., thus revealing information on business or personal travel and even the person's social circle, such as friends or companions".

The organisation notes that in the draft law submitted in 2018 in Greece there was:

- lack of a system for recording access to PNR data
- lack of prior judicial control over the provision of PNR data to pre-trial and other authorities
- the retention period of PNR data is not limited to the strictly necessary period

Four years later, the same shortcomings remain.

The organisation stressed that PNR data of minors transferred should be described clearly and accurately, and that any data transferred should not reveal either religious beliefs or information about the passenger's health.

## Automation and surveillance in Fortress Europe

**Abstract:** Artificial intelligence and algorithms are at the heart of the EU's new mobility-control regime. High-risk automated decisions are being taken on human lives. It is an emerging multi-billion-euro unregulated market with dystopian 'smart' applications.

**Author:** Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

**Link:** Available starting from 26 April 2022

**Text:**

In late June 2020, Robert Williams, an African-American resident of Detroit, was arrested at the entrance of his home in front of his two young daughters. No one could tell him why. At the police station, he was informed that he was considered a suspect in the 2018 robbery of a store, as his face was identified by store-security surveillance footage. The identification was based on an old driver's licence photo. After thirty hours in custody, Robert Williams was eventually released. The cynical confession of the Detroit police officers was disarming: "the computer probably made a mistake."

A similar incident occurred in June 2019 to Michael Oliver, also an African-American Detroit resident, who was arrested after the alleged identification of his face on a security-camera video. He was taken to trial, where he was eventually acquitted three months after his arrest.

Similarly, in a test study of Amazon's Rekognition software, the program incorrectly identified 28 members of Congress(!) as people who had previously been arrested for a crime. The misidentifications overwhelmingly involved blacks and Latinos. But do not assume that this only happens in the US.

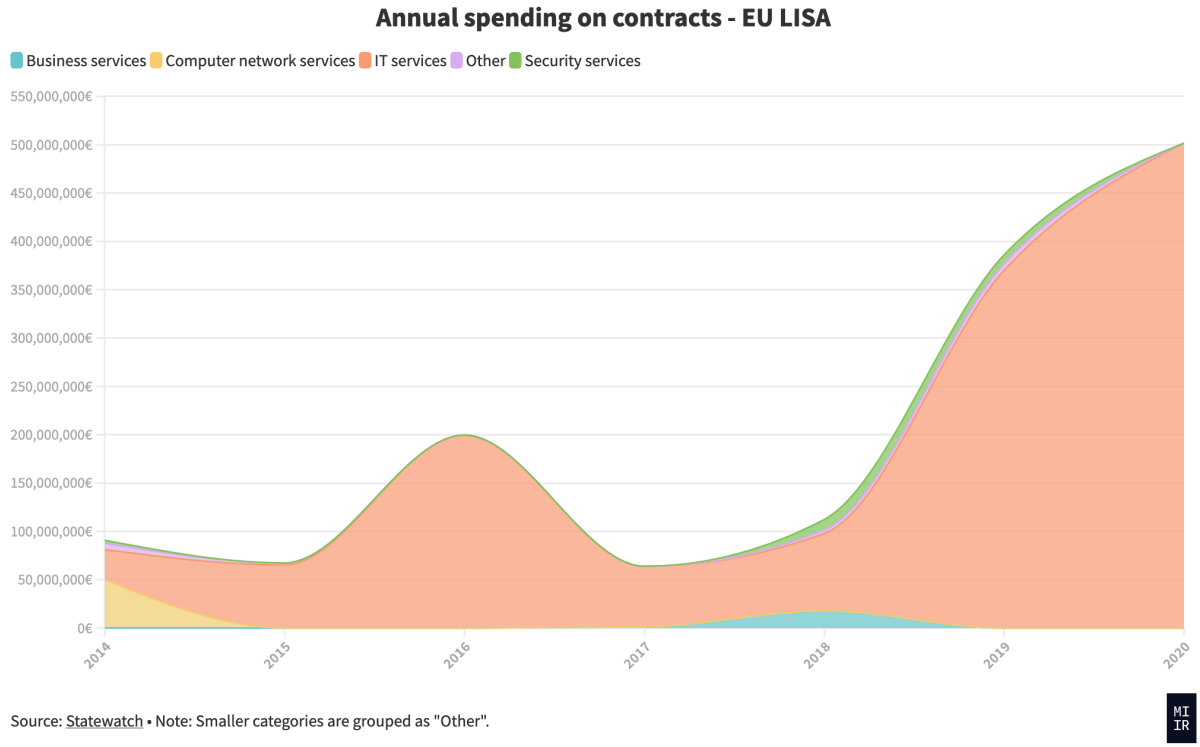
As discussed in the previous two parts of MIIR's research on "Europe's Digital Fortress Walls", the EU, as part of a new architecture of border surveillance and mobility control, has in recent years introduced a number of systems to record and monitor citizens moving around the European space. The EU is using different funding mechanisms for research and development, with an increasing emphasis on artificial intelligence (AI) technologies, which can also use biometric data. Between 2007 and 2013 (but with projects running until 2020) the most relevant of these was the Seventh Framework Programme (FP7), followed by Horizon 2020. These two programmes have funded EU security projects worth more than €1.3 billion. For the current period 2021-2027, Horizon Europe has a total budget of €95.5 billion, with a particular focus on 'security' issues. Technologies such as automated decision-making, biometrics, thermal cameras and drones are increasingly controlling migration and affecting millions of people on the move. Border management has become a profitable multi-billion-euro business in the EU and other parts of the world. According to an analysis by TNI (Border War Series), the annual growth of the border-security market is expected to be between 7.2 % and 8.6 %, reaching a total of USD 65-68 billion by 2025.

The largest expansion is in the global Biometric Data and Artificial Intelligence (AI) markets. The biometrics market itself is projected to double its turnover from $33 billion in 2019 to $65.3 billion by 2024. A significant part of the funding is directed towards enhancing the capabilities of EU-LISA (European Agency for the Operational Management of Large Scale IT Systems in the Area of Freedom, Security and Justice) which is expected to play a key role in managing the interoperability of databases for mobility and security control. The activities of this supercomputer are funded by:

- a grant from the general budget of the EU.
- A contribution from the member states related to the operation of the Schengen area and Eurodac related measures.
- direct financial contributions from member states.

Chris Jones, Executive Director of the non-profit organisation Statewatch, has been following the money trail starting in Brussels for several years. He explains that "EU-LISA projects are usually run by consortia of private companies, public bodies and universities. Private companies receive the largest sums, more than public bodies." A recent Statewatch study (Funds for Fortress Europe:

spending by Frontex and EU-LISA, January 2022) highlights that around €1.5 billion was directed to private contractors for the development and strengthening of EU-LISA in the period 2014-2020, with the largest increase occurring after 2017 and the peak of the refugee crisis.




https://public.flourish.studio/visualisation/9014422/

## The surveillance oligopoly

One of the most important contracts signed in 2020, worth €300 million, was between French companies Idemia and Sopra Steria for the implementation of a new Biometric Matching System (BMS). These companies often win new contracts as they have agreements for the maintenance of the EES, EURODAC, SIS II and VIS systems. Other companies that have been awarded high-value contracts for EU-LISA-related work are Atos, IBM, and Leonardo – for €140 million – and the consortium Atos, Accenture and Morpho (later Idemia) which in 2016 signed a contract worth €194 million. Data collected by Statewatch also shows cooperation – usually through joint ventures – in the expansion of the EU-LISA system with companies of Greek interests, such as Unisystems SA (owned by the Quest Group of former President of the Association of Greek Industrialists Th. Fessa), which signed a €45 million contract in 2019. Similarly, European Dynamics SA (owned by Konstantinos Velentzas) participated in a €187 million contract awarded in 2020, and Luxembourg-based Intrasoft International SA (previously owned by Kokkalis interests) is participating with five other companies in a €187 million project in 2020.

**Contracted companies (by contract size) - EULISA**

Search...

| Company name | Sum of all contracts | Number of contracts | Address |
|---|---|---|---|
| Sopra Steria Benelux SA/NV | 604,954,007 € | 6 | 15/23 Avenue Arnaud Fraiteur, Brussels, Belgium |
| Atos Belgium NV | 573,501,690 € | 4 | DA Vincilaan 5, Zaventem, Belgium |
| Idemia Identity & Security SAS | 302,550,000 € | 1 | 2, place Samuel de Champlain, Courbevoie, France |
| Accenture NV/SA | 271,786,039 € | 8 | boulevard de Waterloo 16, Brussels, Belgium |
| Morpho SAS | 194,450,000 € | 1 | 11 boulevard Gallieni, Issy-les-Moulineaux, France |
| ARHS Developments SA | 187,000,000 € | 1 | 13 Boulevard du Jazz, Belvaux, Luxembourg |
| European Dynamics Belgium SA | 187,000,000 € | 1 | 15, rue Belliard, Brussels, Belgium |
| European Dynamics Luxembourg SA | 187,000,000 € | 1 | 12, rue Jean Engling, Luxembourg, Luxembourg |
| European Dynamics SA | 187,000,000 € | 1 | 209, Kifissias Ave. & Arkadiou Str, Athens, Greece |
| Everis Belgique SPRL | 187,000,000 € | 1 | rue de SPA 8, Brussels, Belgium |

1 / 5

Source: Statewatch

https://public.flourish.studio/visualisation/9468645/

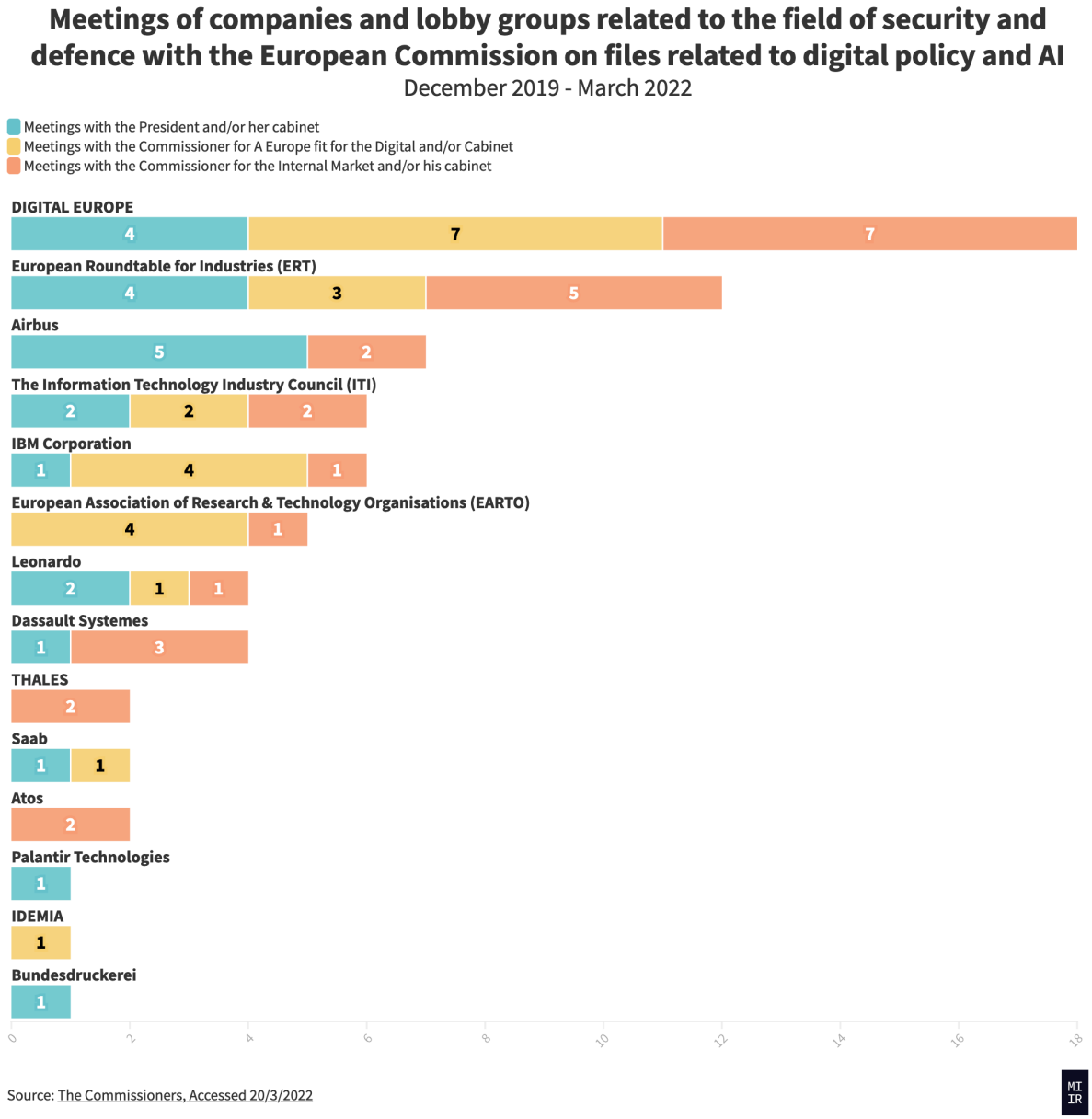
EU-LISA's relationship with industry is also illustrated by the frequent holding of joint events, such as the "roundtable with industry" to be held on 16 June 2022 in Strasbourg. This will be the 15th consecutive such meeting and will bring together EU bodies, representatives of mobility management systems, and individuals. "There are extensive, long and very secret negotiations between member states and MEPs whenever they want to change something in the databases. But we don't know what the real influence of the companies running these systems is, whether they are assisting in what is technically feasible and how all this interacts with the political process," says Statewatch's Chris Jones. The content of the contracts signed between the consortia and EU-LISA also remains unknown, as it is not published.

## The new frontier of AI and the pressures on the EU

In April 2021, the European Commission published its long-awaited draft regulation on artificial intelligence (AI ACT). The consultation process is expected to take some time. This important piece of legislation exceeds 200 pages and which will be – among other things – a refinement of the data protection legislation (Directive 680/2016). There is expected to be considerable pressure exerted by companies and operators in the sector until the bill is submitted in its final form to the European Parliament.

MIIR has investigated the records of official meetings on AI and digital policy issues between European Commission President Ursula von der Leyen, Commissioner Margrethe Vestager (“A Europe Fit for the Digital Age”), Commissioner Thierry Breton (Internal Market) and their staffs

between December 2019 and March 2022. It emerges that at least 14 agencies, private sector giants and consortia of companies related to the security and defence sector met with key representatives of the European Commission 71 times in 28 months to discuss issues related to digital policy and AI. Most meetings with the Commissioners were held by DIGITALEUROPE, an organisation representing 78 corporate members, including major defence and security companies such as Accenture, Airbus and Atos. Other consortia were also identified to be lobbying heavily, such as the European Round Table for Industries (ERT) which represents a number of defence and security companies such as Leonardo, Rolls-Royce and Airbus.




https://public.flourish.studio/visualisation/9083043/

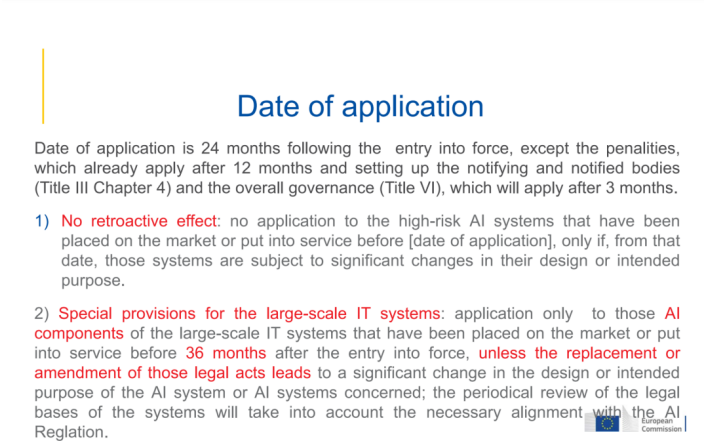
## High-risk systems

The proposal for the European regulation (COM/2021/206 final) adopted in April 2021, gives a good overview of the AI systems and applications that are expected to be regulated, and the risks of their

unregulated operation at Europe's entry points. As stated: “[...] it is appropriate to classify as high-risk AI systems intended to be used by the competent public authorities responsible for tasks in the areas of immigration management, asylum and border control as polygraphs and similar tools or for detecting the emotional state of an individual; for assessing certain risks presented by natural persons entering the territory of a member state or applying for a visa; for assessing certain risks presented by natural persons entering the territory of a member state or applying for a visa; for assessing the risk of a person's personal data [...]”

## The critical parameter

The scope of the field where 'high-risk' AI systems can be applied seems wide. Despite hopes that a new directive will regulate how they operate, there is one parameter that may remove this possibility. As revealed in an internal presentation by the European Commission's internal review that took place in May and was brought to light by Statewatch, the new regulation, if passed, will come into force 24 months after it is signed and will not apply to all systems, as it is not expected to be retroactive to those on the market before the effective date.




"It's like he's clearly saying, 'yes, we should control the use of artificial intelligence and machine learning in a responsible way. But we won't do it for the systems we're already building because... we have other ideas for them...'," comments Chris Jones. The issue is also addressed in the joint statement issued under the auspices of the EDRI digital rights network in November by 114 civil society organisations, highlighting that "no reasonable justification for this exemption from the AI regulation is included in the bill or provided". In the Communication, they call on the Council of Europe, the European Parliament and member state governments to include in the final bill safeguards for accountability that will guarantee a secure framework for the implementation of AI systems and, most importantly, the protection of the fundamental rights of European citizens.

## Robo-dogs in action: Algorithms and nightmarish research projects

"There is a great effort by EU institutions and member states to increase the number of deportations. The EU has poured money and resources and these databases to essentially say 'we want to help remove these people from European soil'," Statewatch's Chris Jones points out. Indeed, automation and the use of industry-pushed algorithmic tools are already playing an important role at Europe's entry points, raising many questions about safeguarding the rights of refugees and migrants. It is not only the profiling that worries those who criticise these EU projects, but also the quality of the data on which this process is based. "It looks like a 'black box', where we don't know exactly what's inside," says refugee law specialist and anthropologist Petra Molnar, who focuses on the risk of automation without a human factor in decision-making when it determines human lives.

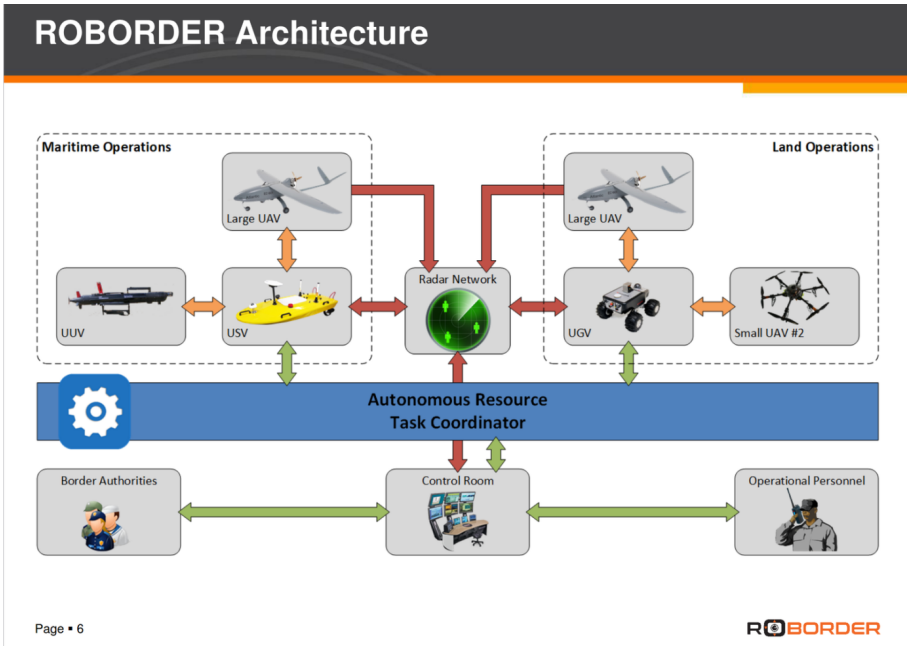
Some of the major pilot systems funded in the past few years include the following:

**iBorderCtrl – "smart" lie detectors:** Combines facial matching and document authentication tools with AI technologies. It is a "lie detector", tested in Hungary, Greece and Latvia, and involved the use of a "virtual border guard", personalised for the gender, nationality and language of the traveller – a guard asking questions via a digital camera. The project was funded with €4.5 million from the European Union's Horizon 2020 programme, and has been heavily criticised as dangerous and pseudo-scientific (“Sci-fi surveillance: Europe's secretive push into biometric technology”, The Guardian, 10 December 2020; “We Tested Europe's New Lie Detector for Travelers – and Immediately Triggered a False Positive”, The Intercept, 26 July 2019).

It was piloted under simulated conditions in early July 2019 at the premises of TRAINOSE in a specially designed area of the Security Studies Centre in Athens. Before departure the traveller had to upload a photo of an ID or passport to a special application. They then answered questions posed by a virtual border guard. Special software recorded their words and facial movements, which might have escaped the attention of an ordinary eye, and in the end the software calculated – supposedly – the traveller's degree of sincerity.

On 2 February 2021, the European Court of Justice ruled on a lawsuit brought by MEP and activist Patrick Breyer (Pirate Party) against the privacy of this research project, which he called pseudo-scientific and Orwellian.

**Roborder (an autonomous swarm of heterogeneous robots for border surveillance):** This aims to develop an autonomous border surveillance system using unmanned robots including aerial, maritime, submarine and ground vehicles. The whole robotic platform integrates multimodal sensors in a single interoperable network. From 28 June to 1 July 2021, the final pilot test of the project, in which the Greek Ministry of National Defence is participating, took place in Greece.




**Foldout:** The €8.1 million Foldout research project does not hide its aims: "in recent years irregular migration has increased dramatically and is no longer manageable with existing systems". The main idea of the project, piloted in Bulgaria and being rolled out in Finland, Greece and French Guinea, is to place motion sensors on land sections of the border where terrain or vegetation makes it difficult to detect an irregular crossing. With any suspicious movement, human or vehicle, there will be the possibility of sending a drone to that point or activating ground cameras for additional monitoring. The consortium developing it is coordinated by the Austrian Institute of Technology (which has received €25 million from 37 European projects).

Among the organisations lobbying for these projects at the European level, we met EARTO, a consortium of research centres and project beneficiaries in various fields, including security. These included KEMEA in Greece, the Fraunhofer-Gesellschaft (140 EU-funded research projects, including Roborder) and the Austrian Institute of Technology (Foldout).

Many of the Horizon 2020 research projects (Roborder, iBorderCtrl, Foldout, Trespass, etc.) have been described by their own authors as still "immature" for widespread use. However, the overall shift in the European Union's approach to the use of AI for mobility control and crime prevention can be seen in the ever-increasing funding of the European Security Fund. One such project is the supply of thousands of mobile devices by the Greek police that will allow citizens to be identified using facial recognition and fingerprinting software. The total cost of the project, undertaken by Intracom Telecom, exceeds €4 million and 75% comes from the European Security Fund.

## The Samos "experiment"

"Borders and immigration are the perfect laboratory for experiments. Opaque, high-risk conditions with low levels of accountability. Borders are becoming the perfect testing ground for new technologies that can later be used more extensively on different communities and populations. This is exactly what you see in Greece, right?", asks lawyer Petra Molnar. The answer is in the affirmative, both for the north and the south of the country.

On the island of Samos on Greece's south-eastern border with Turkey, at the new migrant camp which the Greek government is almost advertising, two special pilot systems called YPERION and KENTYROS are being put into operation.

YPERION is an asylum management system for all the needs of the Reception and Identification Service. It processes biometric and biographical data of asylum seekers, as well as of the members of NGOs visiting the relevant structures and of the workers in these structures. It is planned to be the main tool for the operation of the Closed Reception Centres (CRCs) as it will be responsible for access control, monitoring of benefits per asylum seeker using an individual card (food, clothing supplies, etc.) and movements between the CRCs, and accommodation facilities. The project includes the creation of a mobile phone application that will provide personalised information to the user, to act as their electronic mailbox regarding their asylum application process, with the ability to provide personalised information.

KENTYROS is a digital system for the management of electronic and physical security around and within the premises, using cameras and AI behavioural analytics algorithms. It includes centralised management from the Ministry of Digital Governance and services such as : signalling perimeter breach alarms using cameras (capable of thermometry, focus and rotation) and motion analysis algorithms; signalling of illegal behaviour alarms for individuals or groups of individuals in assembly areas inside the facility; and use of unmanned aircraft systems to assess incidents inside the facility without human intervention.

"KENTYROS uses cameras that have a great ability to focus on specific individuals, cameras that can also take someone's temperature. The most important thing is not that KENTYROS will use this image for security reasons, it is that behavioural analysis algorithms will also be used, without explaining exactly what it means," says lawyer and member of Homo Digitalis, Kostas Kakavoulis. As he points out, "an algorithm learns to come to certain conclusions based on some data we have given it. Such an algorithm will be able to distinguish between the fact that person X may have increased aggressive behaviour, and may attack other asylum seekers or guards, or may want to escape from the accommodation facility illegally. Another use of behaviour analysis algorithms is lie analysis, which can judge whether our behaviour and our words reflect something that is true or not. This is mainly done through the analysis of biometric data, the data that we all produce through our

movement in space, through our physical presence, through our physical appearance and also the way we move our hands, the way we blink, the way we walk, for example. All these may seem insignificant, but if someone can collect them over a long period of time and can correlate them with the data of many other people, they may be able to come to conclusions about us, which may surprise us, about how aggressive our behaviour can be, how much anxiety we have, how afraid we are, whether we are telling the truth or not." In the current legislation, it is prohibited to process personal data without the possibility of human intervention.

Lawyer Petra Molnar has recently been researching the effects of AI applications on the control of migration flows. She was in Samos at the opening of the new closed reception centre. "Multiple layers of barbed wire, cameras everywhere, fingerprint stations at the rotating gate, entry-exit points. Refugees see it as a prison complex. I will never forget that. On the eve of the opening I was at the old camp in Vathi, Samos. We talked to a young mother from Afghanistan. She was pushing her young daughter in a pram and hurriedly typed a message on her phone that said: 'If we go there, we'll go crazy'. And every time I look at the camps with these systems, I realise that it embodies that fear that people have when they're going to be isolated, and surveillance technologies are used to further control their movements."

Médecins Sans Frontières described the new structure in Samos as a "dystopian nightmare". They were not alone. "The KENTYROS system is framed by the use of highly intrusive technologies to protect privacy, personal data as well as other rights such as behavioural and motion analysis algorithms, drones and closed circuit surveillance cameras. There is a serious possibility that the installation of the YPERION and KENTYROS systems may violate the European Union legislation on the processing of personal data and the provisions of Law 4624/2019", the NGO Homo Digitalis points out. The Hellenic Human Rights Association, HIAS Greece, Homo Digitalis and a Lecturer at Queen Mary University of London Dr Niovi Vavoula filed a request before the Greek Data Protection Authority (DPA) on 18 February 2022 for the exercise of investigative powers and the issuance of an Opinion on the supply and installation of the systems. On Wednesday 2 March 2022, the Authority commenced an investigation of the Department of Immigration and Asylum in relation to the two systems in question.

## The automation fetish

"The problem is that authorities, and politicians, are beginning to perceive advanced data analytics as factors in some kind of objective and unbiased knowledge about security issues, because they have this aura of mathematical precision. But artificial intelligence and machine learning can actually be very accurate in reproducing and magnifying the biases of the past. We should remember that poor quality data will only lead to bad automated, biased decisions," says researcher George Glouftios.

[1] These have been summarized; full descriptions are available in the grant agreement document.

[2] At the start of the project, these were: (1) informed consent; (2) commercialization of data; and (3) security/cybersecurity issues.

[3] Available at: http://guidelines.panelfit.eu/understanding-data-protection/

[4] Facebook post: 159 people reached; First tweet: 811 impressions, 2 likes, 1 retweet; Second tweet: 1,841 impressions, 6 likes, 7 retweets; ECSA newsletter, July 2020: 438 opens (21.9% of subscribers); ECSA mailing list of 600+ individual and organisations.

[5] The PANELFIT guide to responsible research and innovation provides more information for this group.

[6] Art. 21 of Directive 2013/33/EU (Recast Reception Conditions Directive). See: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/vulnerable-person_en

[7] While this guide focuses on Europe, many of the types of vulnerability are experienced elsewhere. At the same time, there are further causes and types of vulnerability found outside of Europe.

[8] For example, 'refugees' are a vulnerable group, but 'being poor' and 'being homeless' are a description of someone's state at a given time and in a given context.

[9] This stands for lesbian, gay, bisexual, transgender, queer, intersex and asexual.

[10] See: www.theguardian.com/world/2020/may/19/hungary-votes-to-end-legal-recognition-of-trans-people

[11] The Sámi are the only European people on the UN's list of Indigenous Peoples.

[12] See: www.iwgia.org/en/sapmi.html

[13] There are free online tools that perform photosensitive epilepsy analysis; see, for example, www.w3.org/TR/WCAG20-TECHS/G15.html; Mozilla's website also has a section on accessibility solutions for developers: https://developer.mozilla.org/en-US/docs/Web/Accessibility/Seizure_disorders