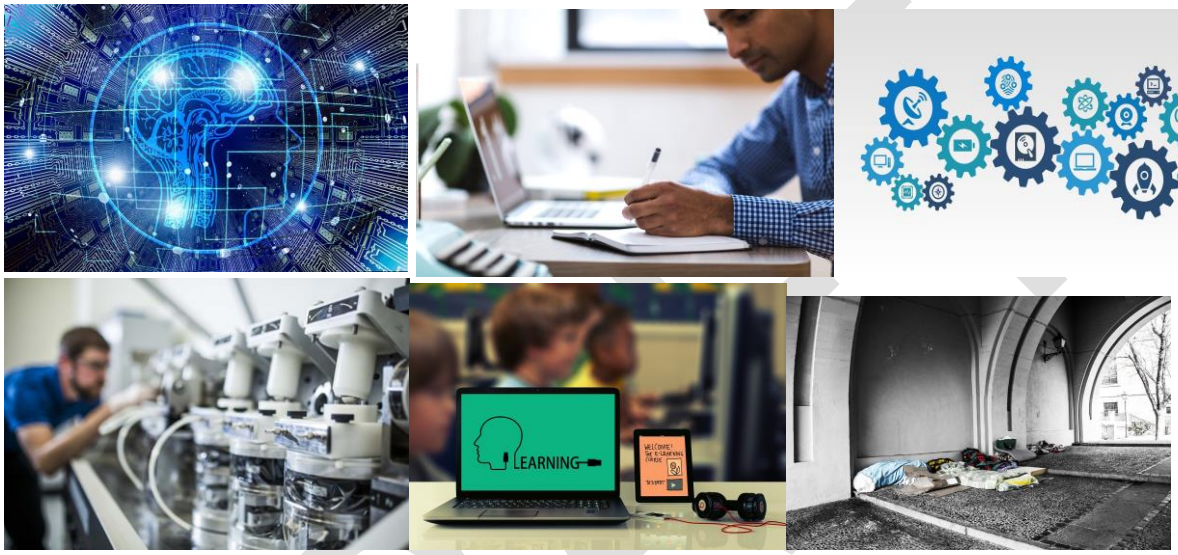
ICTs, data and vulnerable people: a guide for citizens



DRAFT

PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Contents

DRAFT

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.

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'[1] 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.

Contact

Aliuska Duardo
UPV/EHU, GI.Derecho y Genoma Humano/Law and the Human Genome R.G
Edificio de Biblioteca, Local 6A7
48940 Leioa
Biscay, Spain
E-mail: aliuska.duardo@ehu.eus
Tel: +34 94 601 7105
www.panelfit.eu

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

DRAFT

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'.

DRAFT

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 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 secure 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 a disadvantage 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'.

DRAFT

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. 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.

DRAFT

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. 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. 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. 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.

DRAFT

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

DRAFT

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

DRAFT

- 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 is also subjective. 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 themselves 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.

DRAFT

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? The EU[2] has defined vulnerable persons as:

> *"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,[3] as well as people experiencing certain types of vulnerability.[4] 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.

DRAFT

[2] 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

[3] 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.

[4] 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.

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.

DRAFT

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 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	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.

DRAFT

victims of female genital mutilation		
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[5] 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.[6]	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.

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

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

DRAFT

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[7]	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	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

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

DRAFT

	Finland do not fulfil their stated objectives of guaranteeing the human rights of the Sámi people.[8]	project is targeting the Sámi people.
Ethnic minorities	Ethnic minorities in a country often face discrimination and may exhibit a higher prevalence 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.

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

DRAFT

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).[9]
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.

[9] 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

DRAFT

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.	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.

DRAFT

	They may also have young families, and hence have an increased level of vulnerability (e.g., financial).	
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.

DRAFT

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	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

DRAFT

	nature of such events makes it difficult to prepare for them, leaving people less resilient.	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.

DRAFT

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.

[FIGURE 1 – to be drawn]

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

[FIGURE 2 – to be drawn]

FIGURE 1	**FIGURE 2**
Data subjects	**Data controllers**
Who? *All citizens, including vulnerable citizens and those who have responsibility for vulnerable citizens*	**Who?** *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? 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	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

DRAFT

data protection authority.	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.
	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?

DRAFT

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. If you are keen to find out more about these subjects, we recommend the following.

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

DRAFT

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

While written many years ago, this article by Liesl Graz for the **Red Cross** covers many of the themes addressed in this guide, with real-life examples of people living with vulnerability. Available in English. www.redcross.int/EN/mag/magazine1997_3/2-7.html

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/

DRAFT

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.

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

DRAFT

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, 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

Funding

This guide was funded by the European Union's Horizon 2020 research and innovation programme, through the PANELFIT project (grant agreement No 788039).

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).

Funded by the Horizon 2020 Framework Programme of the European Union

© PANELFIT Consortium (2021)

This work is licensed under a CC BY 4.0 license:
https://creativecommons.org/licenses/by/4.0/

DRAFT