Gatherings

Balancing security, privacy and cost

# Database of practical knowledge

D6.1

YEAR OF PUBLICATION
2024

AUTHORS
Judith Münch &
GATHERINGS
consortium

Funded by
the European Union

# 1 Database of practical knowledge

Surveillance practices threaten citizens' privacy in public gatherings but also have a social impact and economic cost. While individual security stakeholders can engage in surveillance practices and consequently collect citizens' personal data, collaboration between public and private stakeholders introduces a more complex scenario concerning privacy, public safety, data transfer, and transparency.

The GATHERINGS (common standards for security, privacy and cost of the surveillance of public gatherings) project focuses on improving the efficacy of surveillance in order to render public gatherings safer. It seeks to improve the fairness and transparency of surveillance by making it more privacy-friendly and boosting the feasibility of surveillance for involved stakeholders by making it more economically and socially cost-effective. A further purpose is to identify gaps in terms of awareness among professionals and citizens and to bring about international harmonisation of good practices and common standards concerning the privacy-friendly, socially sensitive, cost-effective surveillance of safer public gatherings.

As part of the project, awareness-raising programmes for local surveillance professionals and citizens will be developed. These programmes aim to raise awareness among surveillance professionals about the common standards for data management, data protection, and data sharing across EU Member States. Despite that, the awareness-raising programmes focus on the reduction of vulnerability and resilience strengthening of citizens in vulnerable/at-risk areas.

The preliminary English-spoken (but subtitled in the project languages) online awareness-raising programme for surveillance professionals is based on the key components of improved privacy, transparency and citizens' awareness, the security-privacy-cost evaluation matrix developed during the project and the common standards containing detailed guidelines on how to maximise privacy-friendly, transparent, cost-effective, and socially inclusive surveillance of public gatherings, which were also collected during the project.

The awareness-raising programme for citizens, civil society, and vulnerable groups aims to bring about enhanced knowledge about their rights, as well as about the way surveillance and data transfer are organised in their local settings.

As a basis for the awareness-raising programmes, needs and knowledge gaps among security professionals and citizens are identified. While doing so, surveillance practices and impacts on social and economic costs are considered. The following **database of practical knowledge is not claimed to be exhaustive.** It is based on the latest project's research status and especially takes the following research activities into account:

- A literature review focusing on the surveillance assemblages involved in the securitisation of public gatherings, exploring the technologies used, stakeholders involved and data transfer between involved stakeholders.
- Interviews with surveillance and security professionals (local authorities, police (including the police partners in the consortium) and the business community) in European cities about technologies used, stakeholders involved and data transfer between these stakeholders.
- An online survey mapping the effects of surveillance assemblages promoted at public gatherings and events, which are used to collect insights about how visitors of (spontaneous or planned) public events experience the surveillance and securitisation of these events.

Throughout these activities, needs and knowledge gaps on the surveillance of public gatherings were identified. These complementing findings are presented in this document.

While the project is still running and thus further research is conducted, this database of practical knowledge can be updated regarding new insights anytime.

# 2 Identified needs and knowledge gaps

In the following section, the needs and knowledge gaps from the literature review will be presented. Then, the methodology on the interviews with surveillance professionals, as well as the survey among citizens, is explained. Afterwards, the respective findings from the interviews and the survey are depicted.

## 2.1

# Findings from the literature review

At the beginning of the GATHERINGS project, a literature study was conducted. It focused on the surveillance assemblages involved in the securitisation of public gatherings, exploring the technologies used, stakeholders involved and data transfer between involved stakeholders. The data and information were acquired from scientific literature, government, and NGO reports. The consortium partners, VUB (Belgium), TRI (Ireland, UK), VIC (Austria), EIF (Bulgaria), and KEMEA (Greece), reviewed literature related to their own countries. A template was used to ensure the research was as standardised as possible for all partners contributing to the literature review. The template had to be filled out for each technology mentioned below. This template included providing information on the use of a certain technology in a specific country. In addition, it included information about the status, efficacy, and privacy-friendliness of providing security with the specific technology.

It was then shared among the project partners. Specific attention was devoted to how surveillance affects gender and cultural minorities differently, as compared to broader society.

**In particular, the actors involved and the technologies in use were considered for the literature review. These technologies were researched:**

- Facial recognition
- CCTV
- ANPR (fixed and mobile)
- Bodycams
- Drones
- Access control technologies and biometric techniques for access control
- Social media tracking
- Analogue surveillance
- Crowd control

## From the GATHERINGS Surveillance Impact Report (D2.1), we know:

1. **There are highly varied deployment patterns and regulations relating to surveillance technologies in public gatherings.** The same technologies can have different preferred uses and restrictions of use, depending on the country and its internal law enforcement processes and procedures. For example, bodycams are used for various purposes in the jurisdictions researched. In Greece, they are permitted to be used during high-risk demonstrations, contingent upon a specific order from the Attorney General. Such cameras are primarily used by the Traffic Police in Bulgaria, but plans are in place to extend their use to public events as well. In the UK, they are widely used by police officers, particularly by those who come into contact with the public.

2. **Each country has its own complex networks for data sharing, including between LEAs, other government agencies, and the private sector.** For example, Austrian LEAs can access CCTV data from private actors and request extended data retention permission from public bodies and private entities with public service mandates. In the UK, data collected by CCTV is shared between law enforcement agencies (LEAs) and other public and governmental bodies. In Greece, data collected through bodycams can be shared between the Hellenic Police, Fire Service, and Coast Guard as they all come under the Greek Ministry of Citizen Protection.

3. **There is uneven availability of information about technology use and justification of data sharing across countries.** For example, in Belgium, there is little provision for direct citizen access to police bodycam recordings, and the specifics of data transfer regulation need clarification. Access can be obtained indirectly through the Control Body on Police Services (COC) or, in criminal investigations, via a request to the public prosecutor or investigating judge. The exact number of CCTV locations operated by Austrian LEAs is not readily available, with the latest reliable figures from 2017 indicating 17 locations across Austria.[1] Similarly, the precise costs associated with bodycam deployment in Belgium need further investigation, especially regarding data storage. Information about the costs of different technologies is especially challenging to access.

[1] https://kurier.at/chronik/kameras-werden-wieder-abgebaut/243.543.107

4 **There are intricate relations between law enforcement and the private sector.** For example, in Belgium, The Camera Act of March 21, 2007 allows police access to third-party surveillance cameras in publicly accessible places that pose particular security risks, such as train stations and metro stations. In Austria, the Security Police Act (Sicherheitspolizeigesetz or SPG) authorises the use of video surveillance by third parties, including public bodies and private entities with public service mandates. These third parties must notify local LEAs of their CCTV presence and can be required to store footage for up to four weeks. In Belgium, LEAs can request licensed civilian UAV operators to assist in certain operations.[2]

5 **There is an ongoing, consistent set of social and ethical and social concerns around fairness, function creep, data security, and transparency.**

***Fairness:*** For example, studies have shown that facial recognition systems can have different success rates for different racial groups. During the Zaventem experiment, in which Belgian police trialled facial recognition, the software produced many false positives, especially in recognising individuals with certain physical characteristics such as skin colour, moustaches, beards, and glasses.[3]

***Function creep:*** Figures in Austria indicate that, even where facial recognition technology is warranted for serious crimes and terrorism, it is predominantly used to identify theft suspects.[4] Drones gained significant attention during the Covid-19 pandemic when they were used to enforce health measures, such as monitoring compliance at public markets and holiday parks.

***Data security:*** There are significant social and economic costs and vulnerabilities around data storage, especially on newer technologies with relatively untested systems like drones. Further, a growing number of surveillance technologies employed at different gatherings increases the number of technologies that process data and need to have their security measures assessed and assured.

***Transparency:*** In the UK, the Biometrics and Surveillance Camera Commissioner has called for urgent guidance with regard to good practice, sensible controls, and ethical oversight in relation to how they are used. In private use of cameras, the exact programme structure and algorithm are protected as trade secrets and are not disclosed, raising privacy concerns.

[2] Federale Overheidsdienst Binnenlandse Zaken. (2022). Ministeriële omzendbrief van 8 april 2022 betreffende het gebruik van drones door politie- en hulpdiensten. https://etaamb.openjustice.be/nl/omzendbrief-van-08-april-2022_n2022040594.html

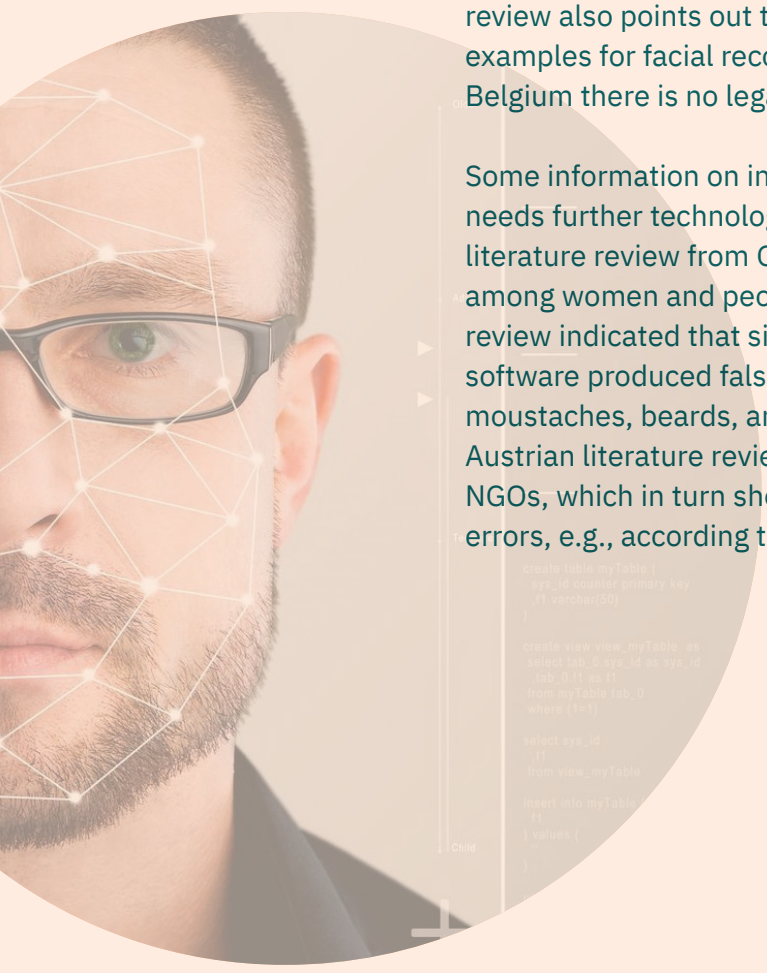
[3] http://extranet.greens-efa.eu/public/media/file/1/7297 (pp. 67-74)

[4] https://www.diepresse.com/6022800/polizei-setzte-gesichtserkennung-seit-einfuehrung-1574-mal-ein

In the following section, identified needs and/or knowledge gaps listed in the country-specific literature reviews are listed about each individual technology:

## Facial Recognition

Several needs and/or knowledge gaps regarding the use of facial recognition were identified throughout the literature review. No information on the economic costs of facial recognition was found in the countries studied. Also, the data transfer between LEAs was not always clearly indicated in the literature: the literature review for Belgium and Ireland could not give any information on that. Despite that, the literature review for Belgium especially points out the lack of transparency regarding the data transfer between LEAs and other public and governmental bodies. Another aspect is the availability of data, collected by facial recognition tools, back to citizens. As the literature from Austria and Greece indicates, information on these proceedings is unavailable. There is no empirical research available regarding privacy friendliness in Belgium, either. The Belgian literature review also points out that there is no concrete efficacy at providing security examples for facial recognition. This can be explained by the fact that in Belgium there is no legal basis for the use of facial recognition technology.



Some information on intersectional effects shows that facial recognition needs further technological development to give precise information: the literature review from Greece states, that difficulties in facial recognition among women and people of colour were observed. The Belgian literature review indicated that similar errors were observed: the facial recognition software produced false-positive results in recognising skin colour, moustaches, beards, and glasses. A similar observation was added to the Austrian literature review. There, references were made to publications by NGOs, which in turn showed that facial recognition systems are prone to errors, e.g., according to skin colour and gender.

## Traditional CCTV

While traditional CCTV is widely used, little information can be presented in the literature review with respect to the economic costs of CCTV (e.g., no data provision for Austria or Greece). For Austria, Belgium, Ireland, and the UK, there was no information on how data is transferred between LEAs. Further, in some countries, how data is transferred beyond LEAs to other public or governmental bodies is not transparent. Knowledge of data availability back to citizens is considered challenging, at least in Austria, where individuals are rarely actively informed about their rights and little information on that is given on the official websites of the Austrian Federal Police or the Austrian Ministry of Interior. In Bulgaria, the data is only shared with citizens when used as evidence in a case.

## Automatic number-plate recognition (ANPR)

ANPR is used as a surveillance measure in all countries in which literature was reviewed for purposes like traffic or border control. Almost no information on the unequal impact on certain social groups could be found. The exception is a case in Belgium: In Antwerp, surveillance cameras near synagogues are now used to survey illegal gatherings when originally intended to protect citizens from terrorist attacks[5]. No information on data transfer is provided for Austria, Belgium, and Ireland. No further content regarding privacy or data transparency for citizens can be given for Bulgaria, Ireland, and Austria.

[5] https://trends.knack.be/nieuws/houd-die-drones-in-hun-kot-2/

## Bodycams

Bodycams are used on many occasions across the surveyed countries except Ireland, where no information is provided in the literature review. But also here, knowledge gaps were identified. Once more, economic costs are not always available (e.g., in Austria, Belgium). Intersectional effects of the usage of bodycams are also not considered in the reviewed literature. Little information is provided on the availability of data for citizens (except Belgium). Further knowledge regarding the data transfer between LEAs and data transfer between LEAs and other public and governmental bodies is missing for Austria and Belgium.

## Drones

Drones are another relatively new but widely used surveillance measure e.g., for observing demonstrations or large public gatherings. For Ireland, no information on the usage of drones can be given. For Austria, there is no information available about the efficacy of providing security by using drones. Economic costs (in the UK) of drone usage cannot be found in the literature. The data transfer and the data availability back to citizens are often unclear (e.g., Austria, Belgium, Bulgaria, Greece).

## Listening devices & communication interception

One must mention that there are significant legal barriers against using listening devices and communication interception as a surveillance measure in the countries reviewed. For example, in Ireland, communication interception is prohibited for private purposes. For law enforcement purposes, it seems that such an interception must be in conformity with the Law Enforcement Directive (and GDPR), i.e., exceptionally authorised and where a party has a legitimate interest in recording a call[6]. The Austrian literature review also refers to the usage of IMSI-Catcher (to locate and track mobile phones), which might be applied for the interception of mobile communication in certain areas[7]. While, in general, the Austrian literature review mentions that using IMSI Catcher helps locate endangered individuals, in the Irish case, there is no information on the efficacy of providing security by using listening devices and communication interception. Overall, no information on the surveillance measure of listening devices and communication interception was provided in the literature review for the UK and Belgium. The literature also could not provide specific data on economic costs and the unequal social impact of the surveillance measure. Additionally, there is insufficient information regarding data sharing not only among Law Enforcement Agencies (LEAs) but also between LEAs and other public or governmental bodies. The availability of data to citizens is limited. In Greece, it is not possible for citizens to access this data. In Bulgaria, it is only possible when used as evidence. For other cases, the literature review did not find information on data availability for citizens.

[6] https://legalguide.ie/surveillance/#surveillance-and-interception-of-da

[7] § 53 Abs 3b & §§ 134ff stop Österreich, https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40263019/NOR40263019.html

## Access control technologies

Access control technologies are widely used. Nevertheless, there is little information on the applied access control technologies, as the literature reviews demonstrate. For Austria and the UK, no information is provided. The Bulgarian review indicates that the price varies according to the requirements and the technologies used, and the Greek review states that the costs of this surveillance measure are high. In the other countries, no data about economic cost is available. Information about the unequal social impact is seldom mentioned; only the Irish literature review indicates that authorisation for the use of access control technologies lies within LEAs and, therefore, weak checks against bias exist.

## Social media tracking

According to the review, no information on social media tracking as a surveillance measurement is available for Austria and the UK. For Greece, it is indicated that social media tracking is not used as a main tool, although it is indicated that there are low costs (without giving concrete numbers) for using such tools. The literature review from all countries shows that intersectional aspects are not considered in the literature, as the literature review did not bring up any information on the tracking of social media and a linkage to intersectional considerations while using such tools. The Bulgarian and the Belgian review did not consider any publications regarding privacy-friendliness. Further information on data transfer between LEAs and data transfer between LEAs and other public and governmental bodies is not given in the review for Ireland and Belgium.

## Analogue surveillance: patrolling and tracking individuals

While patrolling and the presence of LEAs in public spaces is common sense for all countries where the literature review was conducted, only vague information exists for almost every reviewed country. For Austria, the literature review gives no information on analogue surveillance. In the Irish case, no information could be provided regarding the privacy-friendliness, economic costs, intersectional aspects, data transfer between LEAs and data transfer between LEAs and other public and governmental bodies. But also in the Greek case, the information found during the literature review was vague, e.g., concerning economic costs, no concrete numbers could be mentioned, and the question of considering intersectional effects of analogue surveillance was not answered, which is the same for the Bulgarian case.

## Crowd control technologies

The Austrian and the Irish literature review do not offer any information on crowd control technologies, while the technology is used in the other countries. No public information exists about the technology's cost, social impact, data transfer between different operators, etc.

## Summary

Looking at the literature review from Austria, Belgium, Bulgaria, Greece, Ireland and the UK, there are several knowledge gaps regarding the use of surveillance measures like facial recognition, CCTV, ANPR, bodycams, drones, access control technologies, social media tracking, analogue surveillance and crowd control.

The main conclusion from this literature review is that there is a fundamental lack of public information concerning these surveillance technologies, their use, cost, and social impact, as well as the data transfer between operators (both LEA and non-LEA) and back to citizens.

According to the literature review, some surveillance measures were already part of research, and there is accessible information about them. It must also be considered that there is factual information on some aspects. For example, certain technologies need to be procured (bodycams or CCTV should be mentioned here as examples). This means that budget is available for procurement and has been/will be used. Institutions and organisations entrusted with the process of monitoring and the use of monitoring technology, therefore have information about the costs. However, it is a matter of how this information is published and/or cumulated to receive a broader picture of the usage of a certain surveillance technology. As it was analysed within the literature review, this form of information access and cumulation of costs is not clearly available. It could also be the case that for the reviewed country, no specific research on this behalf has been done so far, and nobody has requested this information from the responsible parties.

In general, we can conclude that there is almost no research in the countries involved in this literature review concerning intersectional aspects and unequal social impact of the surveillance measures studied. There clearly is a need for further research.

To conclude, it is almost impossible to avoid surveillance, yet very little information about their application is available. In the following sections, we present findings from interviews with professionals involved in surveillance assemblages across Europe and from a survey among citizens subjected to surveillance during events in public spaces.

## 2.2

# Methodological and overall demographic information on conducted interviews and survey

The methodology of the interviews and the survey "Citizens' Perceptions of Surveillance and Security Measures at Public Gatherings in Europe" are explained below to help readers better understand the data collection process. Before the needs and knowledge gaps, respectively, results are presented, information on the demographic data of the interviewees and survey participants is also depicted.

## Interviews

To gain practical insights into surveillance measures, interviews with surveillance and security professionals from local authorities, police (including police partners in the consortium) and the business community were conducted in spring 2024. All participants were based in Europe and were questioned about the technologies used, stakeholders involved and data transfer between these stakeholders.

A standardised questionnaire was previously developed within the consortium. Every partner was responsible for acquiring interview participants. The interviews were conducted in several languages according to the preferences of the interviewees by all consortium partners. Afterwards, the interviews were transcribed and translated into English. A unique and, at the same time, specific syntax was chosen: the participants were given country-specific codes and numbered consecutively. For example, AT01 was the first interview partner to conduct the interview with the Austrian consortium partner VICESSE. The abbreviation "BE" depicts interviewees talking to the Belgian consortium partner VUB, "DE" indicates the BayHfÖD from Germany, "BG" Bulgaria, "GR" Greece, "IR" or "UK" for interviewees talking to Trilateral, based in Ireland and the UK.

For a first analysis, a previously developed analysis template was used. The first analysis aimed to narrow down the results and statements according to each country of origin/working of the participants to get specific insights into the surveillance landscape there. This document relies on the country-specific analysis conducted using the developed analysis template.

For recruiting research participants, the GATHERINGS consortium relied on an elaborate guide on doing intersectionality and diversity-sensitive research. As stated within the info sheet, factors such as ethnicity, sexuality, gender, economic status, and (dis)ability are likely to be markers for significant socio-cultural differences. Recognizing these distinctions is crucial for comprehending the social phenomena examined in qualitative research, as well as for refining our research methodologies.[8]

[8] Allmark, P. (2023) Should research samples reflect the diversity of the population? J Med Ethics 2004;30;185-189. Doi:10.1136/jme.2003.004374.

**Thus, during the interview project phase, demographic data has been collected. The following tables give an overview of the interview sample:**

| | |
|---|---|
| **TOTAL NUMBER OF INTERVIEWEES** | 51 people |
| **GENDER DISTRIBUTION** | 41 identified as male,<br>10 identified as female |
| **EDUCATION**<br>(THERE WAS NO SELECTION GIVEN WHICH DEFINED "EDUCATION" PRECISELY. THUS, A WIDE RANGE OF TERMS WERE USED HERE) | •**PhD:** 6 people<br>•**Master:** 21 people<br>•**Bachelor:** 3 people<br>•**High school/ A levels:** 4 people<br>•**Others** (e.g., apprenticeship or undefined educational pathway labelled 'university', but no indication of the degree obtained): 16 people |
| **OCCUPATION**<br>(THERE WAS NO SELECTION GIVEN WHICH DEFINED "OCCUPATION" PRECISELY. THUS, A WIDE RANGE OF TERMS WERE USED HERE) | •**Members of Police:** 20 people<br>•**Professors:** 3 people<br>•**Event Organisers:** 2 people<br>•**Public authorities:** 5 people<br>•**Other security organisations** (e.g., Red Cross): 2 people<br>•**Others** (ranging from "CEO" to "director"; no specific job description was given in advance; thus, participants could describe their profession vaguely): 15 people |
| **AGE AVERAGE** | **~46 years**<br>(youngest interviewee: 28 years; eldest participants: 65 years) |
| **ETHNIC BACKGROUND** | Most participants indicated the same "ethnic background" as their nationality (e.g., Austrian nationality and Austrian ethnic background).<br><br>1 participant indicated "Central/Northern Europe", 1 participant indicated "black" and 1 participant indicated "Caucasian" and 6 participants indicated "White" from which 3 indicated to be "Irish White" and one indicated to be "British White" as ethnic background. 4 German participants did not specify their ethnic background at all. |

As it can be seen, the collected needs and knowledge gaps, which are mentioned in the next chapter, are biased. Since 4/5 of the participants are male, the statements on surveillance practices, impacts, etc., are mostly from a male perspective. The participants are well educated, too, and the average age shows that the participants have several years of (life) experience with an average of 46 years, with an interviewee aged 28 being the youngest participant and one aged 65 being the eldest.

The participants were asked to indicate their ethnic background, too. It should be noted here that the majority indicated their ethnic background to be the same as their nationality. Only a few interviewees distinguished by using different terms than their nationality to describe their ethnic background:

- 1 participant indicated “Central/Northern Europe”,
- 1 participant indicated “black” and
- 1 participant indicated “Caucasian” and
- 6 participants indicated “White” from which 3 indicated to be “Irish White” and 1 indicated to be “British White” as ethnic background.
- 4 German participants did not specify their ethnic background at all.

Although the interviewee sample does not depict diversity as desired, the GATHERINGS consortium is aware of it and “intersectionality”, referring to the fact that social identities (such as race, gender, class, sexuality, ability, etc.) intersect and interact to shape individuals’ experiences, perspectives, and access to resources, was taken into account during the recruitment. Nevertheless, the interviewee sample cannot be described as a cross-section of society confronted with surveillance, but it still offers valuable and interesting insights regarding the needs and knowledge gaps.

## Survey

The “Citizens perceptions of surveillance and security measures at public gatherings in Europe” survey was set up by the consortium partner VICESSE. It focuses on citizens’ perceptions of surveillance activities in the context of large public gatherings (commercial and non-commercial) as well as their impact on citizens’ feelings of security. A link and/or QR code was shared within the attending audience and people could voluntarily participate in the anonymous survey. The survey was spread among participants of gatherings, e.g., concerts.

The following findings are tentative since the study was not terminated when writing this document. By October 9, 2024 (due date of this first analysis), 257 people who agreed on using their data participated and answered the survey questions.

The following charts give an overview of the demographic data of the participants. It can be seen that male and female respondents took part in the survey almost equally. People who see themselves as belonging to a different gender or no gender are only slightly represented.

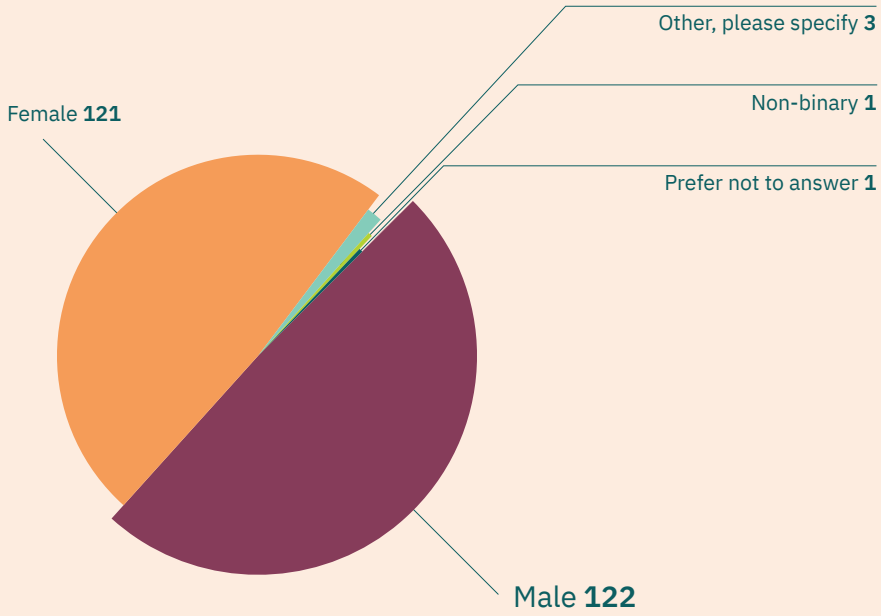



**Figure 1** What is the Gender you identify with? (some participants did not answer the question and also did not specify it clearly)

The group of people with disabilities is not represented strongly: 7 people said that they have a disability or impairment impacting their attendance of public gatherings:

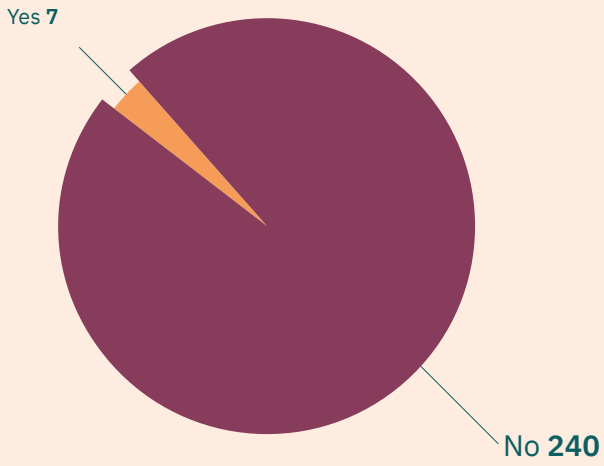



**Figure 2** Do you have any disabilities or impairments that impact your attendance of public gatherings? (some participants did not answer the question)

Regarding the age distribution, the survey can rely on a more diverse participant range. However, mostly younger people answered the survey: the biggest group of participants indicated to be between 18 and 30 years old.

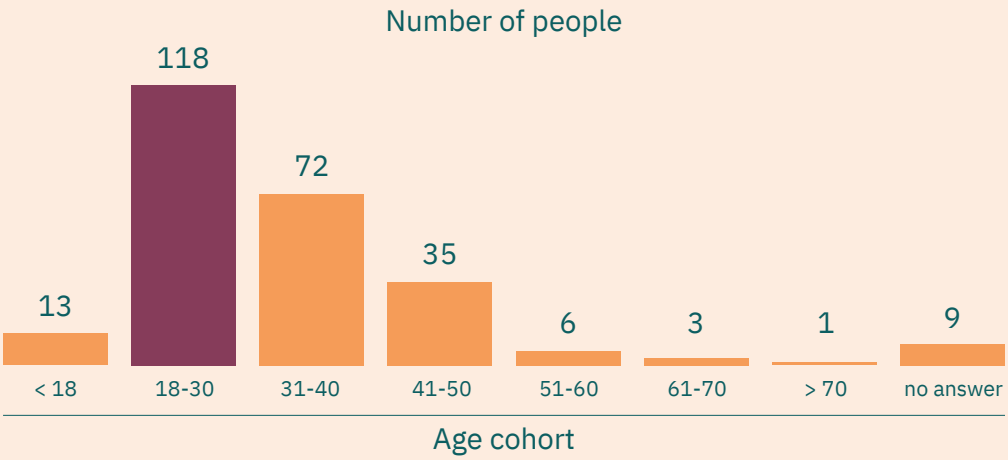



**Figure 3** Age distribution among survey participants

When looking at the ethnic and cultural background, the given answers are made mainly by people identifying themselves as white/Mediterranean:

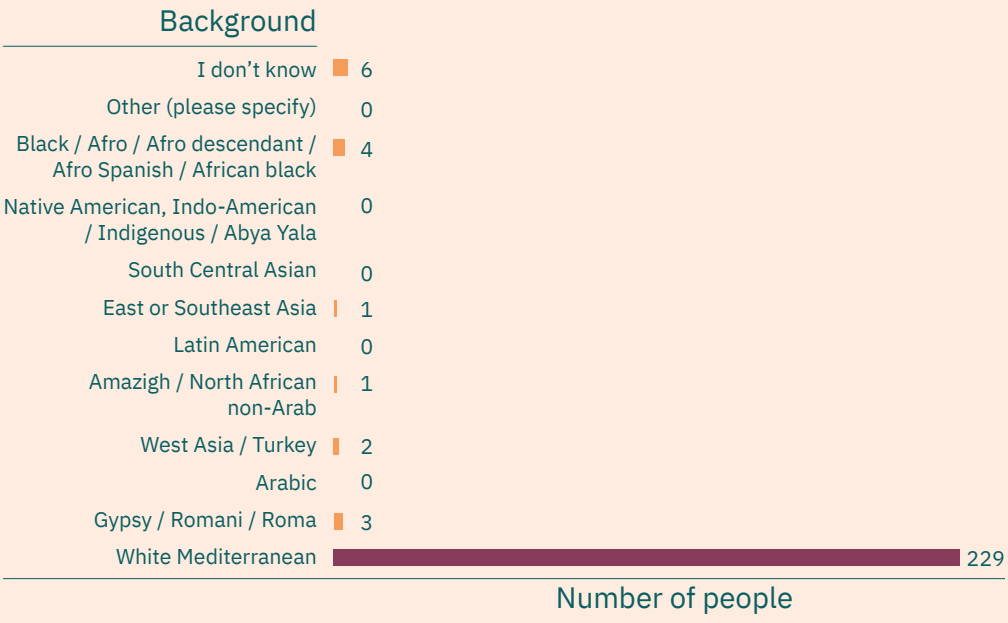



**Figure 4** What is the ethnic or cultural background you identify with (several answers allowed)?
(some participants did not answer the question)

As mentioned, the survey was not terminated when the first findings were added to this deliverable. Thus, the demographic landscape among the survey participants might change when the results are evaluated at the end of the survey. Nevertheless, it shows by now that the answers given so far are mostly made by younger white/Mediterranean people with no disabilities.

## 2.3 Findings from the interviews

For the first analysis, a developed analysis template was used. This analysis aimed to narrow down the results and statements according to each country of origin/working of the participants to get specific insights into the surveillance landscape there. This document relies on the country-specific analysis conducted using the developed analysis template. As the template shows, specific questions were asked, the answers to which were intended to reveal possible gaps in knowledge or unmet training needs. While looking at the answers from all consortium partners, the following findings from the interviews are summarised:

### Blurred definition of safety and security

The interviews were conducted in several languages spoken in the countries of the project consortium members (Belgium, Ireland/UK, Germany, Austria, Bulgaria, Greece). It then was stated that many languages lack distinct terms for “safety”:

> **“But unfortunately, if you look at, you know, doing Wikipedia search on safety and security, in most languages, it’s the same word for both. So, the language is not there and therefore the vocabulary isn’t there and therefore the understanding isn’t there and therefore the training isn’t there and therefore these concepts tend to get mixed and mashed together and unless you can clearly differentiate it, you’ll end up thinking that you’ve got a secure site. Yeah, it might be secure but it might not be safe.”** (Participant IR07)

This conflation of the terms “security” and “safety” seems to cause challenges in understanding and implementing appropriate measures for both, as they need different approaches and skill sets. Security is fundamentally about protecting against **intentional** threats or attacks. It aims to safeguard people, information, property, and systems from malicious actions. Conversely, safety focuses on accidents, failures, and other **unintended** events that can cause physical harm or damage through an understanding of crowd dynamics and crowd flows.

## Resistance to technology

A certain resistance to technology exists, which can be attributed to a lack of knowledge/uncertainty in the use of technology. Participant BG08 noted:

> **"Any new innovation inevitably meets resistance because they have not used them and they have not worked with them."**

This resistance extends to the public, where acceptance is perceived as a significant challenge. Participant GR07 illustrated this point:

> **"A lot of times when we go to install a CCTV system, we have reactions. We have reactions from the very bystanders of an organisation. They may be employees or whatever. And a lot of times those reactions are strong despite the fact that we always apply the law and ensure compliance."**

## Specific group needs

LEA and event organisers from Belgium mention that video surveillance treats all citizens fairly and protects them, including vulnerable groups. Of course, this only holds true when the technologies are used in a legal way by the relevant authorities.

> **In itself, I don't think a camera is going to contribute to some form of stigmatization. It's about what do you do with those images, how do you interpret those images, how do you look for solutions about those images? I think that's where the issue is."** (BE_07)

Next to the person interpreting the camera footage, interviewees are aware of the potential risks of biases, as the following respondent explained:

> **Bias. So, when you create data thanks to cameras or other things and you deliberately place it in those particular neighborhoods and then you go to work with that data for counts or patterns, we have a bias by definition. So that's definitely a very big danger."** (BE_04)

The participants point out that as long as there is a sign showing there is video surveillance, there is no violation of rights, including those of vulnerable groups.

> **With regard to disabled persons, persons with disabilities, etc. I suppose that to the extent that they also use television or other modern means of communication, they are aware that everywhere in public places there is video surveillance."** (BG_08)

As our demographic data show, the statements of disabled people are not presented very well here. Thus, the answers and statements above from LEA and event organisers should be treated with caution.

DE02 states that to some extent, people with disabilities, here people using a wheelchair were mentioned, are considered. It was the case that the event DE02 works for, which has a sandy underground and thus is not accessible by wheelchairs. Despite that, DE02 could not confirm that people with disabilities are especially considered in security plans. While some provisions exist for wheelchair users, other disabilities, such as visual impairments, hearing impairments, and cognitive disabilities, are largely neglected.

> **I was at a panel discussion on the subject of safety, where a representative of the deaf was also present. He said that he likes going to events and concerts, and the organiser said, "What are you doing there? You can't hear anything". He said he likes the feeling of the bass. (...) If something unexpected happens, like a sudden movement of 10.000 people at the same time, he might sense the change but not understand the cause, which could lead to panic."** (Participant AT01)

In addition, some interviewees discussed the need for safe spaces or code words for identifying and reporting sexual violence. While these concepts exist and are used in several countries, it was noted that women might hesitate to seek help from security personnel due to fear of further harassment or lack of trust. This is not a clear knowledge gap but can be summarised as a need to establish a trustworthy environment for people seeking help from security professionals.

## Data management practices – increased public awareness

Security professionals perceive growing awareness among the public about data security issues, but a gap remains in practical knowledge about how to protect oneself. IR_02 on data protection:

> **So, then you only five people in our field [of security] like yourself may and the concern about the things because we work in that area, we will be paranoid about security. But again, we know that I [sic], the innocent public, are [sic] being exploited in that space. So, it's a very interesting difference of perception in that way."**

Many individuals feel helpless or consider themselves unimportant as targets, leading to complacency in securing their digital identities.
There is a call for better understanding and visibility regarding where data is stored, how it is used, and ensuring it is properly deleted when requested.

## Data management practices – layered data protection measures

There is a concern that existing regulations like GDPR leave room for interpretation, allowing organisations primarily focused on profit to exploit loopholes (IR02). Participant IR02 also noted that policies alone are insufficient and that practical technical solutions are necessary to ensure that data privacy is maintained across different organisations and sectors.

## Training needs – security concepts

Security concepts are set up prior to an event or for a specific location, when analysing possible threats, and when aiming for a secure and protected environment for people around. Regarding needs and knowledge gaps in training, the differentiation between "security" and "safety" is pointed out once more. There is a recognised need for developing security concepts for events and/or public gatherings, with stakeholders pointing out the scarcity of such training programmes in Europe (AT02, IR07). In this regard, training programs should differentiate between safety and security skills. In terms of safety, practical and theoretical training in crowd management is considered essential.

## Training needs – continuous education on technology advancements

While some participants have received training, e.g., as this shows:

> **My first concern will be that we have that prepared with all the emergency services. That we have involved the firedepartment and police, our own events cell. And that inthis way we can put all the check marks on the safety measures that need to be taken according to a fixed sequence." BE_06,**

Others feel there is a need for continuous education, especially when new technologies or legislative changes are introduced (GR06, GR03, DE04).

> **[...]the security market is of course highly competitive on the one hand, and quite a niche. There aren't that many providers, because you can't make a lot of money with it, that's something to be said quite clearly. And in that respect, there is certainly still a need for additions, when I see what has already found its way into private technology. That is still a long way from security technology. I spoke earlier about intelligent video surveillance, so that there is something for security applications, at least for us in northern Germany. I don't think this product is available across Germany yet. But of course, that's not just to do with technical development, but ultimately our entire legal system is lagging technical development, so intervention measures are not possible at all."** (DE04)

> **What I think is that the use of reference and importance and investigation, is that if we have changes in the legislation, there should be further education."** (GR03)

There is a recognition of the need for theoretical and practical training in using surveillance technologies. Some interviewees mention receiving only theoretical seminars on using these technologies and express a desire for more hands-on, practical training (Participant GR02, GR06, GR03)

Operators receive regular "basic" (DE03) training, which is deemed sufficient by some, but there is room for improvement, particularly in AI and robots (AT01, DE01, DE02). This aspect also came up when the interviewees were asked about future developments of their work and will be mentioned later in this document again.

## Training needs – data protection

The challenge of managing and interpreting large volumes of data from surveillance systems is a significant concern. One participant (IR07) noted that while technology was expected to solve problems, it often overwhelmed operators with data they could not manage effectively.

While some security professionals reported having data protection training in place,

> **training courses regarding legal framework conditions are carried out regularly, because the law determines the tactics" (DE01),**

Several interviewees pointed out a lack of specific training in data protection and ethics. There is a call for more comprehensive and updated training programs to ensure personnel understand the importance of protecting personal data and comply with relevant regulations, as participants GR02 and GR06 emphasised. Training at the management level is particularly important to ensure staff understand their responsibilities under GDPR and the implications of non-compliance. This understanding is crucial, especially for systems used across multiple jurisdictions, according to Participant IR03. In general, updated continuous training is essential. Participant BG02 mentioned,

> **"I've gone through ethical behaviour training mostly for employees, but it's always helpful to update the knowledge periodically, so more trainings are needed."**

## The future – AI development

Security professionals believe that AI systems will become increasingly influential, especially in areas such as crowd management, behaviour recognition, mass data analysis for threat assessment, and intelligent video surveillance (IR08). However, there is a perceived lag in technology adoption for some countries compared to others (GR68).

Participants foresee the development of more privacy-preserving technologies within an ethical AI framework, striking a balance between enhanced capabilities and respect for individual and social rights (IR08). This balance is considered necessary for gaining and maintaining public trust.

The focus on data security is expected to grow, with more robust measures being implemented to protect against cyber threats. Compliance with data protection regulations like GDPR will remain a critical concern for event organisers (IR06). Here a potential need can be identified.

## The future – compulsory exam for crowd managers

Interviewees anticipate that competency exams for managing or hosting large events will soon become mandatory (IR06). This requirement ensures that only qualified individuals are responsible for overseeing crowd safety and management. The need for such stringent regulations and competency checks is expected to become apparent as more major incidents occur, highlighting a reactive approach to implementing regulatory changes.

## The future – slow standard adaptation

Rapid technological advancements make it challenging to keep standards up-to-date (IR11). There is a need to adapt standards to new technologies, e.g., network coverage (mentioned by Greek participants but also DE01). The increasing use of covert cameras for security purposes also presents challenges in terms of regulation and privacy protection:

> **"Legal problems, such as the unauthorised use of facial recognition software, etc., or if an event turns into a demonstration, the use of video surveillance is only possible on a rudimentary basis."** (DE01)

## The future – update practices to new psychological theories on crowd behaviour

The need to adapt practices to new psychological theories on crowd behaviour was discussed, too. It was mentioned that many current policies are based on outdated psychosocial theories that view crowds as irrational and prone to panic, with a focus on survival at any cost. In dangerous situations, people often respond with cooperation and coordination rather than chaos. This adjustment in understanding crowd behaviour could lead to more effective and humane crowd management practices in the future and thus is identified as a need and knowledge gap to develop surveillance practices for public gatherings further.

## 2.4 Findings from survey

As mentioned, the survey was not terminated when the first findings were added to this deliverable. In addition, no detailed analysis of the findings will be conducted here. Thus, only two questions and answers are discussed here.

The first question “Have you at any point during the event felt unsafe or experienced a situation which made you feel uneasy?” was answered by 5 out of 257 participants with yes. 5 people stated that they had a situation in which they felt uneasy. 6 people did not answer the question. The rest indicated they did not feel unsafe or experienced a situation that made them uneasy.

The second question inquired into the perception of the surveillance and security measures in place at the event the participant attended. To better understand the effects of these measures, the people were asked how these measures contribute to their feeling of security, from 1 (not at all) to 7 (very much). It was asked about technical measurements like CCTV or drones, as well as human measurements like the presence of police or searching bags. To get a first impression, only the margins, i.e., answers 1 (not at all) and 7 (very much), are considered here. After the survey has ended, all responses will be considered in a detailed analysis of the results.

| QUESTION | PEOPLE ANSWERING WITH 1 (NOT AT ALL) | PEOPLE ANSWERING WITH 7 (VERY MUCH) | NUMBER OF ALL AND NO ANSWERS (STATUS: 09/10/2024) |
|---|---|---|---|
| How does **CCTV** contribute to your feeling of security? | 50 | 30 | 53 |
| How does **CCTV with facial recognition** contribute to your feeling of security? | 66 | 37 | 49 |
| How do **drones** contribute to your feeling of security? | 56 | 30 | 52 |
| How do **access controls** contribute to your feeling of security? | 56 | 44 | 48 |
| How does **bag search** contribute to your feeling of security? | 56 | 46 | 44 |
| How does the **presence of the police** contribute to your feeling of security? | 13 | 78 | 45 |
| How does the **presence of private security** contribute to your feeling of security? | 32 | 58 | 50 |
| How does the **presence of first responders** contribute to your feeling of security? | 9 | 96 | 38 |

**Table 1** Sample questions and answers at the respective margins

So far, 257 people answered the survey. Looking at the number of responses to the question about the feeling of security when using certain surveillance measures, an average of 47 people did not answer the questions. So, around one fifth did not answer the questions. Thus, the answers at the margins 1 (not at all) and 7 (very much) weigh stronger.

The following section takes a closer look at the use of certain safety measures as examples: Concerning this, the 96 people answering the question agree very much that the presence of first responders contributes to their feeling of security, whereas only 9 people mentioned the presence of first responders does not at all contribute to their feeling of security. 78 people answering the question stated that the presence of the police contributes to their feeling of security, whereas 13 people stated that the presence of the police does not at all contribute to their feeling of security. Only 30 people mentioned that CCTV contributes very much to their feeling of security, whereas 50 stated the opposite (“not at all”). While asked about CCTV with facial recognition, 30 people also noted that this measurement contributes very much to their feeling of security, whereas 56 stated the opposite.

It turns out that the use of human resources as a ‘surveillance measure’, especially the presence of first responders and secondly the presence of the police, leads to a solid sense of security among the study participants.

The use of technical surveillance measures, e.g., CCTV with facial recognition or drones, is viewed more critically by the study participants. For some people, these technologies contribute very much to the individual feeling of security; for others, it does not at all contribute to that. The survey tried to receive some answers for the reasons behind their selection. Although people selected the answer that a specific surveillance measure does not at all contribute to their feeling of security, few participants specified their answers and explained their selection. Only 13 answers were given to this question, from which 4 given answers did not relate to the initial questions (” I don’t have any insecurities. “; “Everything was fine. “; “Nothing in particular!”; “There are to [sic] many genders. “; “There aren’t many people and the audience seems civilised.“) Although people selected the answer that a specific surveillance measure does not at all contribute to their feeling of security, few participants specified their answer and explained their selection.

## Here is an overview of the responses

> “Video surveillance does not inspire confidence in me, because I think there is rarely enough quality and coverage of the areas to cover possible security gaps. Often, faces are difficult to recognise only by this means.”

> “There was no physical check.”

> “I haven’t seen them [there was no further specification on which question the answer relates] yet.”

> “I don’t want there to be facial recognition.”

> “Most of the security companies are not suitable for this type of event.”

> “The measures [no further specification possible to which measure the answer relates] were not implemented.”

> “A large number of visitors.”

Referring to the overall topic of the GATHERINGS project, the people were asked to indicate whether they would consider the measures to be pervasive and affecting their privacy from 1 (not pervasive at all) to 7 (very pervasive). This should help to understand the effects of the measures better. The table below shows the given answer at the margins of the range and also depicts how many people did not answer the questions at all (on average, 62 people did not answer each question).

| QUESTION | PEOPLE ANSWERING WITH 1 (NOT AT ALL) | PEOPLE ANSWERING WITH 7 (VERY MUCH) | NUMBER OF ALL AND NO ANSWERS (STATUS: 09/10/2024) |
|---|---|---|---|
| Indicate whether you would consider **CCTV** to be pervasive and affecting your privacy. | 60 | 13 | 59 |
| Indicate whether you would consider **CCTV with facial recognition** to be pervasive and affecting your privacy. | 76 | 20 | 64 |
| Indicate whether you would consider **drones** to be pervasive and affecting your privacy. | 60 | 15 | 74 |
| Indicate whether you would consider **access controls** to be pervasive and affecting your privacy. | 61 | 27 | 60 |
| Indicate whether you would consider **bag searches** to be pervasive and affecting your privacy. | 60 | 32 | 53 |
| Indicate whether you would consider the **presence of the police** to be pervasive and affecting your privacy. | 18 | 50 | 60 |
| Indicate whether you would consider the **presence of first responders** to be pervasive and affecting your privacy. | 13 | 63 | 60 |
| Indicate whether you would consider the **presence of private security** to be pervasive and affecting your privacy. | 32 | 50 | 64 |

**Table 2** Sample questions and answers at the respective margins II

While looking at technical measures like CCTV and drones, there is a tendency for people to consider these measures not pervasive at all. On the other hand, more people indicate that the presence of police, first responders or private security is pervasive and affects their privacy.

When asked to specify what made them consider these measures to be pervasive, only 6 people contributed[9]:

- Invasion of privacy
- Control of personal data
- Find facial recognition critical because I don't know what happens to it then
- No baggage checks

[9] One person stated "I am not" and another "I saw them". These sentences do not give any further insight and are left out above.

It also shows a contradiction: on the one hand, first responders, for example, contribute very much to people's feeling of security. On the other hand, the presence of first responders was also indicated as very pervasive and affecting their privacy by 63 people out of 76 people, who answered the question. This is similar when looking at the contribution of police presence to the feeling of security: as mentioned before, 78 participants indicated that the police contribute to their feeling of security. At the same time, 50 participants answered that the presence of the police would be pervasive and affect their privacy.

The stated answers on the individuals' feeling of security can be interpreted as trust in a specific measure or no trust in this measure, e.g., 96 people answering the question agree very much that the presence of first responders contributes to their feeling of security, whereas only 9 people mentioned that the presence of first responders does not at all contribute to their feeling of security. If one continues to follow this interpretation, the question arises as to why some measures lead to a lower perception of safety and how to change this. Here, the specified answers can provide some insights, which prove the lack of trust, e.g., lack of trust in the technical capabilities of CCTV, lack of trust in the competence of a security company, concerns about the size of the event, concerns because some measures like physical check which probably was expected by the individual did not take place, concerns regarding the personal data and privacy.

# 3 Complementing the identified needs and knowledge gaps

In the survey, participants mentioned little information on data availability back to citizens, which we also identified as a gap in the literature review. This may suggest that there is a need for more transparency in order to improve trust in surveillance measures. However, as pointed out in chapter 2.3, vulnerable groups are not always considered. From the literature review, one can conclude that intersectional aspects and differential impacts have not been considered that much or at all in the literature so far. From the survey, we cannot say anything conclusive about this, considering that the sample is not very diverse (see chapter 2.2). From the interviews we can conclude that most of the professionals working in surveillant assemblages are not taking these issues into account; there is a clear knowledge gap regarding how surveillance measurements are perceived and how they affect social groups differently.

Throughout the project, further activities are planned to elaborate on citizens' views on surveillance measures. Three Living Labs are conducted to gain more insights. This mixed-method design will be finetuned by the consortium partners VUB, VIC, KEMEA and EIF and implemented in the form of three Living Labs in Bulgaria, Greece and Austria. Information about the needs, requirements, and issues from a variety of stakeholders, as well as about the felt experiences and vulnerabilities of specific user groups of public spaces are collected. One focus group of representatives from local LEA, public administration and business community; a focus group covering a diverse sample of citizens as users of public space and participants of public gatherings and events and a focus group covering gendered and cultured aspects of the securitisation and surveillance of public spaces, gatherings and events on vulnerable populations.

These focus groups may bring a deeper understanding of the attitudes and opinions held by different stakeholders in different countries, while presenting them information about surveillance and data transfer. By involving citizens in such an informed debate, it can be better understood how surveillance resonates with societal values held by different groups. It might also contribute to the aspect of intersection effects, which was identified as a knowledge gap so far (compare chapter 2.1). Despite that, the online survey (see chapter 2.4) will be analysed in depth as soon as it is terminated. It might be interesting to validate the identified needs and knowledge gaps with the findings from these research activities and/or to add new insights.

This database of practical knowledge will not only be supplemented by further research activities during the GATHERINGS project. The database helps to formulate the training needs for the awareness-raising programme of surveillance practitioners and the awareness-raising programme for citizens. While relying on the identified needs and knowledge gap, new information shall be published in the format of the awareness-raising programmes and thus contribute to deepening the understanding of surveillance, why and how surveillance is applied, and which obligations and rights lie within these measures to reach the surveillance target of secure public gatherings.

Gatherings

# Balancing security, privacy and cost

**CONSORTIUM**

VRIJE UNIVERSITEIT BRUSSEL

TRILATERAL RESEARCH Ethical AI

Hochschule für den öffentlichen Dienst in Bayern
Fachbereich Polizei

VICESSE

BM.I

.LPD

european institute

KEMEA

LOBA

**FOLLOW US**

@gatheringsEU

**CONTACT US**

info@gatherings-project.eu

**WEBSITE**

gatherings-project.eu

Funded by the European Union

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.