



Gatherings

Balancing security,
privacy and cost



Surveillance Impact Report D2.1

YEAR OF PUBLICATION
2024

AUTHORS
Iohana Voicu,
Joshua Hughes,
Christopher Nathan



Funded by
the European Union

This document is pending approval from the EC and may be subject to modifications. Any information contained here is provisional and should not be considered final until official approval is granted.

1 Introduction

This Surveillance Impact Report aims to **showcase how surveillance assemblages work “on the ground”, the effects surveillance has on citizens’ privacy, and which socio-economic costs these assemblages produce.** The report includes a summary of research findings from the GATHERINGS Project, carried out on topics related to mapping and evaluation of surveillance practices of public gatherings EU-wide. The report is designed for the use of, among others, surveillance professionals, local authorities, law enforcement agencies, representatives of local communities, and civil society organisations.

The GATHERINGS Project is a research project funded through the European Commission’s Horizon Europe programme (Project No. 101121200), which runs from 2023 to 2026. The project’s ambitions are: 1) to improve efficacy of surveillance practices to make public gatherings safer (increasing fairness and transparency of surveillance practices by making it more privacy-friendly, while also making it more cost-effective, both economically and socially); and 2) to identify awareness and training gaps on surveillance of public gatherings among local citizens and security professionals, and support harmonization of good practices and common standards with regards to privacy-friendly, socially sensitive, cost-effective surveillance of public gatherings.

A core component of the present report consists of findings from a major study of security professionals across Europe on the impacts and costs of public gatherings surveillance, and a series of desk-based research efforts conducted to answer these questions.

Between March and July 2024, the GATHERINGS project conducted 51 semi-structured interviews with safety and security professionals in multiple European countries (Ireland, the UK, Bulgaria, Austria, Germany, Greece, and Belgium). These include law enforcement agents, local authorities, event organisers, employees of public and private companies, and security consultants. The interviews aimed to understand and map the experiences of security professionals regarding concerns, technologies used, stakeholders involved, and data transfers related to large gatherings. The selection of respondents was designed to ensure a complex overview of what surveillance entails for various stakeholders.

Findings from the interviews were grouped under the following overarching themes and sub-themes:

THEME	SUB-THEMES
SAFETY AND SECURITY CONCERNS	Unclear definition of safety and security; Main safety concerns; Main security concerns; Cybersecurity
SAFETY AND SECURITY MEASURES	Technological measures; Non-technological measures
PERCEIVED IMPACTS	Public sense of safety; Privacy; Chilling effect; Resistance to surveillance technology; Importance of public debate; Specific group needs
STAKEHOLDERS INVOLVED	Event organisers; Private security providers; Police/Law Enforcement Agencies (LEA); Local governmental authorities; Transport Representatives; Local residents; Emergency services; Attendees
TRAINING NEEDS	Technology use; Security concepts; Crowd management; Ethical AI; Data protection
DATA MANAGEMENT PRACTICES	Increased public awareness; Increased event organisers interest; Layered data protection measures
THE FUTURE	Enthusiasm for technology development; Update practice and skills in crowd management; Slow standard adaptation; Update practices to new psychological theories on crowd behaviour

Additionally, the report summarises desk research efforts conducted, including:

- A literature study of three building blocks of surveillance assemblages
- Research efforts on the identification and analysis of legal concepts, frameworks and national legislations applicable to personal data protection.
- Preliminary preparation for interviews with surveillance and security professionals.
- Mapping of socio-economic costs of surveillance practices and intersectional effects on vulnerable social groups
- Identification of key components of security, privacy and socio-economic cost.

The findings reported are structured into three main sections: *Surveillance Assemblages, Safety and Security, and Vulnerabilities and Surveillance*. Each section addresses surveillance impact from a different perspective. The first section, Surveillance Assemblages, aims to clarify the three building blocks forming the foundation of a surveillance assemblage, and looks at the relation between surveillance deployments and privacy impact. The second section, Safety and Security, looks at defining the nuances which distinguish the two concepts and showcases why defining them is important when considering measures for a public gathering. The third section, Vulnerabilities and Surveillance, provides an overview of current challenges surrounding diversity among public gathering attendees and the legal context in response to them.

Research standing at the foundation of this report, further informs upcoming GATHERINGS project work on the development of:

- a) a security-privacy-cost evaluation matrix.
- b) an awareness-raising programme tailored both for local surveillance professionals, and citizens.
- c) three policy dialogues with EU and national policymakers, leading to the formulation of a set of legal recommendations.
- d) an EU Handbook on Surveillance of Public Gatherings.

The Surveillance Impact Report is designed for the use of, among others, surveillance professionals, local authorities, law enforcement agencies, representatives of local communities, academics, civil society organisations and citizens.

2 Surveillance assemblages

KEY MESSAGE:

The concept of a ‘surveillance assemblage’ helps us to think about surveillance practices in a holistic way.

2.1

Privacy and assemblages

A common finding of the GATHERINGS project's interview study outlined challenges faced by security professionals to deploy public gatherings surveillance while ensuring individuals' privacy. Respondents highlighted risks of data breaches, as well as a need to manage event participants' perceived violation of the sense of privacy. One interviewee raised concerns about the unintended or repurposed use of collected data, stressing the risks of linking personal data across various aspects of an individual's life. These risks question the feasibility of the "right to be forgotten" and the ethical use of analytics in the context of a security assemblage.

Research findings emphasized the importance of the right to be informed when we are subject to video surveillance, as well as potential misuse of the surveillance system by the operators. The chilling effect on public behaviour is a direct potential side-effect needing to be considered when establishing various surveillance options during an event. The knowledge of being watched can alter how people behave in public, potentially stifling free expression and peaceful assembly. This highlights the need to balance safety with privacy. One participant explained,

“We need to balance safety against privacy, (...), and this is why, fortunately, we have the European Court of Justice, which is able to answer questions when it's unclear which of the rights, safety or one of the other rights should prevail” (practitioner, IE).

To ensure a fair management of security assemblages set in place temporarily, security professionals stressed the importance to reassess temporary security measures on a regular basis. If this process is not set in place, there is a risk of temporary security measures becoming permanent, which could erode freedoms over time with no legal basis. These processes are particularly important in the context of major events like the Olympics, where heightened security measures are often justified but need to be carefully managed to prevent long-term negative impacts on civil liberties.

Some security professionals interviewed stated that surveillance risks are directly dependent on the security operator's legal and ethical use of the technology deployed. As one participant noted, as long as the security-responsible employee did his/her job properly, following the legal guidance, there was no risk in the surveillance process. However, if there was any breach or violation of the legal guidance, and the employee would try to hide it, that's where the human risks would materialize:

“If an employee does his job and respects the legal framework, there is no problem. It's a problem if there is a violation of the law and the person wants to hide it” (security practitioner, BG).

The diversity of issues raised under the privacy rights scope illustrate a lack of a common, standardized approach across Europe on the concept of *Privacy*. Moreover, the intricacies of privacy rights are dynamic in the context of technological advancement. As research found, ‘Early debates on privacy began at the end of the nineteenth century, when the potential intrusion of photography and the (tabloid) press was first recognised. When contrasted with the concerns that we face today due to the smart devices surrounding us, collecting data, and influencing our opinions and behaviour, the old worries look quite innocent.’ (Roessler & DeCew, 2023). The ongoing history of our ideas about privacy is disorienting because it involves simultaneous normative, social, and technical shifts.

A classic, broad approach to privacy was built on the right to be let alone. Articulated by Warren and Brandeis (1890), early concepts defined privacy as the right to enjoy a personal realm free from interference by others. This perspective strongly influenced legal frameworks throughout the years, particularly in the context of tort law in the United States, framing privacy as a defence against unwarranted exposure or intrusion. In Europe, the concept was embedded with Article 7 of the Charter of Fundamental Rights of the European Union, which ensures respect for private and family life. The value placed on privacy in the EU shapes EU directives and regulations to minimize data collection, and prevent unnecessary intrusions into individuals’ lives.

A narrower approach to privacy centres on control over personal information. Privacy is based on an individual’s ability to control the collection, use, and dissemination of their personal information. Some argue that this definition of privacy is essential since it supports correlated values, such as trust, intimacy, and freedom in personal decision-making (Fried, 1968). This approach is also embedded at the core of the EU General Data Protection Regulation (GDPR), implemented in 2018. It empowers EU citizens to significantly control and manage their personal data, including rights to access, rectify, and erase personal information. The GDPR’s emphasis on consent, transparency, and the right to be forgotten underscores this philosophical stance.

Other specialists and academics take on an extensive perspective on privacy, which goes beyond the control of personal information, sometimes emphasising the need to positively empower individuals, rather than merely delegate them the task of agreeing to legalistic ‘terms and conditions’ documents (Solove & Hartzog, 2024). Another example is given by Nissenbaum (2004), who argues that privacy should be understood within the context of specific social situations, each governed by norms about

what information is appropriate to share. Privacy is breached when these norms are violated, even if the individual has control over their information. Her approach does not aspire to provide a single unifying definition of privacy but rather defines a *right* to privacy as a *right* to ‘appropriate flow of personal information’.

Our approach in GATHERINGS focuses on the specific issue behind any given concern labelled ‘privacy’. For example, we specify whether the root issue is a data security concern, a chilling effect, a right to control of data, and so forth. The concept of privacy deployed by itself can confuse readers by insufficiently distinguishing one issue from others.

2.2

Surveillance deployments

KEY MESSAGE:

There is a persistent set of social and ethical concerns around the use of surveillance technology, and there are complex and uneven deployments.

A simple way to explain how surveillance as a whole is deployed for public gatherings is through the lens of the surveillance assemblage concept. This concept’s application to security was notably discussed by Haggerty and Ericson (2017), drawing on the work of philosophers Gilles Deleuze and Félix Guattari (1988). A surveillance assemblage is a concept used to describe the union of different surveillance systems into an integrated network. Its application encourages us to think about the processes, functions, and effects of surveillance as a whole, in a rounded way. Rather than focusing on how, for example, a particular CCTV camera, or the use of drones, affects a population, the idea of a surveillance assemblage leads us to consider the functioning and effects of a surveillance structure, including the way that data is transferred on from its collection point, and the uses that may be made of this information in the future.

For the scope of the GATHERINGS project, we consider that a **surveillance assemblage** (Haggerty and Ericson (2017)) consists of three components:

- The **stakeholders** involved.
- The **technology** deployed; and
- The **processes** for transferring data between stakeholders.

Stakeholders in public gatherings will include event organisers, police, local authorities, emergency services, private security, transport services, local residents, and attendees. Core **technologies** include CCTV, drones, body-worn cameras, open-source intelligence, and access control. Security professionals interviewed as part of our study showed enthusiasm for the technological advancements available to the industry, such as AI-enhanced behaviour monitoring, crowd density monitoring, and holistic crowd understanding technologies. Regarding the **transfer of data**, we found that professionals perceive a growing awareness among the public about data security issues, but that a gap remains in practical knowledge about how people can protect themselves against the undesired use of their personal information. Many feel helpless or consider themselves unimportant as targets, leading to complacency in securing their digital identities.

The GATHERINGS project has sought to outline security assemblages and their application to public gatherings surveillance with the support of publicly available material, by focusing on the security context of core project partner countries Ireland, the UK, Bulgaria, Austria, Greece, and Belgium. **In doing so, preliminary work identified the following core focus topics, which form a backdrop for the rest of the study:**



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.



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.



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 (Schreiber, 2017). Similarly, the precise costs associated with bodycam deployment in Belgium need further investigation, especially regarding data storage. Information about costs of different technologies is especially challenging to access.



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 (Federale Overheidsdienst Binnenlandse Zaken, 2022).



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 trialed facial recognition, the software produced many false positives, especially in recognising individuals with certain physical characteristics such as skin colour, moustaches, beards, and glasses (The Greens/EFA, 2021).

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 (Die Presse, 2021). 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: 'like any potentially intrusive technology that can be used to watch and collect information about people, there must be consistent 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.

3 Safety and Security

KEY MESSAGE:

There is a valuable distinction between 'safety' and 'security'.



3.1

Safety and Security Concepts in Public Gatherings

Within the context of this report, safety involves preventing unintentional harm or accidents, that are often related to hazards in the environment, while security looks at guarding against intentional threats by people or groups that aim to cause harm or gain unauthorised access. (El-Kady et al, 2023)

This distinction is useful because, although it is sometimes missed, there are possible tensions between safety and security. For example, efforts to counter a known security threat can create crowd control bottlenecks. It is important to understand which elements stakeholders are responding to, especially where such tensions exist, and what the rational responses are to any trade-offs.

Security professionals participating in our study highlighted that language is key in shaping understanding and implementation of safety and security measures. One of the main difficulties in defining the two concepts is a lack of a standard approach across Europe, where many languages lack distinct terms for “safety” and “security” and often use them interchangeably (Blokland, Reniers, 2019). This linguistic overlap leads to confusion and blurs the distinctions between the two concepts. As one security practitioner explained:

“But unfortunately if you look at, you know, doing a Wikipedia search on safety and security, in most languages, it’s the same word for both. So the language is not there, [...] the vocabulary isn’t there, [...] the understanding isn’t there, [...] 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” (security practitioner, IE.).

This conflation seems to cause challenges in understanding and implementing appropriate measures for both security and safety, as they need different approaches and skill sets. Though the terms can often be used loosely and interchangeably, the meanings behind the concepts of security and safety are not fully analogous (Rigterink, 2015). 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. Conversely, security is fundamentally about protecting against intentional threats or attacks. It aims to safeguard people, information, property, and systems from malicious actions.

As Boustras and Waring (2020) outlined, ‘safety’ includes a wide range of sub-domains (e.g. food safety, sports safety, chemical/radiations hazards, hearing damage, occupational or specific sector safety (construction, chemicals, nuclear etc.), public safety, transportation safety, and its often strongly related to health and environment either in relation to major hazards or lesser risks. Regarding safety, a security professional stated:

“it is important that there is some kind of consideration of how people get there? How do they get away again in a regulated manner? How do they get away in an emergency? What are the routes? How do visitors move around the event site? What happens in which emergency? Who are the people who make decisions and take action? How does communication work between the organisers and the security services?”
(security practitioner, AT).

In contrast, ‘security’ defines several levels and interconnected types of risks, as it includes sub-domains of national security, public order, corporate security, transportation security, industrial, residential, and personal security. Moreover, ‘security’ includes a wide-range of connected topics such as cybersecurity, physical security, identity protection, fraud, counter-terrorism, hate-crimes etc. (Boustras and Waring (2020)).

To understand the concept of ‘security’ and its intricacies, Rigterink (2015) proposes distinguishing between four concepts included under the ‘security’ umbrella – technical safety, perceived safety, technical security and perceived security. The four concepts look at security and safety from two perspectives – aggregate threats brought on to a group of people, and individual threats brought to a single individual. Security indicators outline the overall effects on a group of people, while safety indicators focus on the effects of a threat on an individual. Technical security encompasses the freedom of threats of some group of individuals (using as indicator the average probability an individual member of a group will be subjected to a particular threat), whereas perceived security looks at perceived freedom from threats (of a group of individuals/ to the aggregate entity). Technical safety encompasses individual freedom from threats (using as average probability that an individual will be subjected to a particular threat), whereas perceived safety looks at perceived individual freedom from threats (to the individual).

3.2

Key Safety Considerations

KEY MESSAGE:

A consistent set of safety considerations for public gatherings is centred on crowd management.

Security professionals' engagement throughout this project emphasized that ensuring the safety and well-being of attendees is a primary focus in the context of large event planning and execution. As one interview respondent from Greece noted, the main concern is first of all placed on the protection of human life.

The first safety consideration in a public gathering is centered on **crowd management**, as one professional put it - "how will they behave and what can happen as a result?", explaining that the focus is on the management of all human participants (the attendees, the composition of the event or the assembly) (practitioner, EL). This includes managing visitor flows, preventing mass panic, and ensuring sufficient emergency exits.

Project primary research findings (interviews study) showcased an important distinction made by practitioners in the concepts and terminology related to crowds - crowd management and crowd control- which can also be often used interchangeably in literature. Thus, we found that the concept of crowd control was often adopted by LEAs, while crowd management was adopted by first responders. While crowd control is a strict security concept, looking at ways to contain crowd movement, crowd management was understood as a means to guide the flow of the crowd at a certain location.

Several respondents noted that crowd management is inextricably linked to the location where an event takes place. One professional highlighted that a distinction must be made between, for example,

“a festival meadow where you can build as many evacuation gates into your fence as possible and, for example, a city festival where you have to work in the context of the city and are thus much more limited” (security practitioner, BE).

For the latter case, an important concern is that everything is prepared as well as possible with all partners involved. As another security professional showed: 'In other words, how many people use which areas in which time unit. We very often see at events, for example, that the entrance is undersized because there are too few gates for cost reasons, there are too few security staff and there can be congestion. You always have higher crowd densities in front of stages anyway, but they are usually intentional,

so it's important to differentiate between intentional and unintentional density. In crowd management, there is actually one value that is relevant, the so-called limit density, which is reached at six people per square metre. They have more than that in front of stages, where people expect it and it doesn't bother them. But if, for example, they reach the same density in the inflow or outflow that they have in front of a stage, and the audience there is not prepared to be confronted with this density, it can quickly turn into panic' (security practitioner, AT).

We summarise the five main safety concerns as showcased through our research:



Overcrowding and crowd management: Overcrowding can be the cause of crushes or stampedes, which can result in serious injuries or fatalities. This risk is exacerbated in situations where crowd dynamics are poorly understood or managed. Ensuring smooth and controlled movement of people was reported as critical, and a lack of coordination can disrupt the flow, leading to bottlenecks and gridlocks. Properly planned and executed crowd management strategies help maintain a steady and safe movement of attendees, preventing dangerous build-ups.



Crowd panic: Large gatherings are vulnerable to panic-inducing incidents. For instance, a sudden loud noise or scream can trigger chaos and accidents. One such example was given by an interviewee:



This occurred during the 2010 Remembrance Day commemoration event in Amsterdam, where a loud scream caused widespread panic and resulted in 87 injuries.”(security practitioner, IE)



Extreme weather conditions: Extreme weather conditions, such as high temperatures, intense rainfall and floods can pose significant risks to the health and safety of attendees. Interview study respondents stressed that providing safe spaces during such conditions are key to preventing heat-related illnesses and other weather-induced health hazards.



Environmental hazards: Specific environmental factors, such as insect bites and challenging settings (e.g. caves), can pose health risks to attendees. Managing these hazards involves preventive measures and ensuring that medical assistance is readily available.



Infrastructure safety: Infrastructure-related safety concerns focus on having safe infrastructures, protecting them at events, and ensuring proper stewarding.

3.3

Key Security Factors

KEY MESSAGE:

Security concerns include a wide range of elements, with varying degrees of seriousness.

When mapping security concerns related to public gatherings surveillance, the primary issues identified during our research involves managing tensions between participants, ranging from minor disputes to more significant conflicts and anti-social behaviours, as well as addressing hooliganism. Security practitioners highlighted that provocateurs often use the anonymity of the crowd to instigate violence. Notably, terrorism was seldom mentioned as the major concern by the interviewees across countries, though the example of the Manchester bombing at the Ariana Grande concert in 2018 was used by a practitioner from Austria to highlight the potential threat and the challenges faced by security personnel in identifying and addressing suspicious behaviour. Risks levels among countries were not perceived as equal. As one practitioner noted,

“Ireland is perceived to have lower threat levels compared to other European countries, particularly the UK.’ The primary concern in Ireland was focused more on safety and crowd dynamics rather than high-level security threats such as terrorism (security practitioner, IE).

Issues like anti-social behaviour and drug use are considered significant but are managed through safety protocols rather than high-security measures. Other European countries maintain a wider, more complex range of active risks monitored during active gatherings, due to their own social and cultural context.

In addition to these traditional security concerns, a new theme emerged on **cyber security**. This includes protecting against cyber threats that could disrupt event operations or compromise personal data that are collected to access the event (e.g. ticketing) or during the event (e.g. CCTVs). Cyber threats such as hacking into digital systems, cutting off power, or hijacking display screens to spread fear can cause real harm. These scenarios are no longer hypothetical and, as one practitioner from Ireland noted, need to be planned for, as they can lead to loss of control over the event and significant danger.

3.4

Safety and Security Measures

3.4.1

Technology-based

KEY MESSAGE:

Professionals perceive a number of technologies as useful aids, including CCTV, drones, body-worn cameras, and access control.

Venues hosting large crowds often implement complex networks that involve **multiple layers** of security, including surveillance. For example, airport security includes technologies used by personnel from the airport itself, border patrol, and national security agencies. Likewise, large events employ **multi-layered technologies** used for different goals. Depending on the type of the event and the level of risk, different types of technologies are adopted for safety as well as for security purposes to

- 1) prevent accidents.
- 2) monitor crowd flows.
- 3) identify asks for help or anti-social behaviours.
- 4) communicate.
- 5) control access.

Security professionals expect technology advancements to ‘make [the job] easier’ for them, as one interview respondent mentioned. Technologies are reported to bring about more accuracy, reduced subjectivity, quicker emergency response times, reduction in personnel required, increased customer experience, and better access to evidence in case of criminal activities.

CCTV cameras are the technology solution most commonly used to monitor public gatherings, especially as a combination of fixed and mobile CCTV cameras. This combined use is necessary due to temporary setups of stages or food stands, for example, that can block lines of sight from regular, fixed cameras. CCTV data can be used for post-incident analysis to help resolve crimes and safety issues, or for real-time decision-making through mobile operations centres. In these centres, different stakeholders (e.g. police, first aid emergency teams, private security agents) monitor live footages and can coordinate real-time safety and security responses. As one practitioner notes:

“In general, the means of video surveillance are extremely useful (...). Through the means of video surveillance, it is possible to analyse the dynamics of the crowd, of the group, of the audience, to identify risky places, and risky groups, in order to somehow manage the crowd, so that security and safety for people are created.” (security practitioner, BG.)

Research findings also show that in LEA practice, CCTV is also used to identify perpetrators of anti-social behaviours and crimes.

Video surveillance is perceived to have the function of prevention, as event attendees are less likely to commit any crimes or escalate a situation when they are aware of being recorded. An interview respondent confirmed,

“It has been proven that when a technical tool of video surveillance is used the attendees’ actions are limited, i.e. fewer crimes are committed. The fact that people are being recorded, leads to a faster solution of a situation and the latter does not escalate towards the police officers.” (security practitioner, BG).

However, there is always an awareness of the well-documented chilling effect on public behaviour, whereby the knowledge of being watched can alter how people behave in public, potentially stifling free expression and peaceful assembly.


Drones are highly valued for their flexibility and ability to provide aerial video streams of large, open areas. Research found that, due to their versatility, drones were used across-Europe for multiple purposes. They are often used for monitoring visitor flows (crowd management or crowd control), and avoiding pressure points if a panic situation were to arise, so that authorities have an overview for quick response. As one interview respondent mentioned,

“We previously used a helicopter for this, but it’s now much easier with the drone.” (security practitioner, AT).

This approach is especially true when drones are equipped with thermal imaging cameras and night vision. Drones distinguish themselves from traditional camera surveillance which is not the best tool for crowd control, as a participant explains:

“The use of drones- that is the first time that I actually see a technology that makes it possible to monitor very locally, certainly at night, the density of the public in a certain area of a square, for example. So that micro level, that we lack with the cell phone data that we track, where we can only look in those large groups. That we now effectively have qualitative info with those drones that is much more qualitative than camera use. Camera use towards a crowd is not interesting. Because of the oblique perspective, that very quickly becomes a mush of people, of heads and of shoulders.” (security practitioner, BE).

Notwithstanding, drones can also be useful for following up on specific incidents and gathering evidence, especially when used in a ‘duo’ formation. In this, one drone is used to maintain a good overview and another drone can zoom in on a specific incident. A security practitioner interviewed explained the approach:



“Then we are in the story of drones, certainly drones in pairs, one of which is flexibly deployable at that time to quickly assess a location. There, of course, we’re going to be able to go and see what’s going on long before maybe emergency services or crews are on the scene there. And of course, (...) we also have potential evidence.” (security practitioner, BE).

Lastly, drones are also utilised to transport objects and to identify injured or missing people quickly, as an interview responder notes:

“Drones will certainly also change a lot. Our colleagues in [location] have a drone unit and last year at [event] they used the drone for the emergency services for the first time (...). It was said that there was an emergency at a food stall, they immediately zoomed in and saw that there really was a person lying on the ground. We told the paramedics, you have to go 20 meters further forward, because sometimes they just can’t see where the actual scene is because of the people standing there.” (security practitioner, AT).

Body-worn cameras are used primarily by police to record incidents, serve as evidence when needed and, as a means of accountability for the officer wearing it. Body-worn cameras are therefore mainly useful retrospectively since the footage is usually not live-streamed due to the high cost. During large events, it was reported that the placement of the body-worn camera is an additional consideration to address, to avoid filming only the abdominal or chest level of attendees. However, an important added value is the audio that traditional camera systems don’t have. One interview respondent exemplified:

“For us, you really have to say that a big advantage is the evidence. It’s a huge thing for us, because at the last [event], we had this guy who rolled around on the floor with another guy, (...), and wanted to attack me too. Then he was arrested, and it was all on [body worn] camera.” (security practitioner, AT).

Open-source intelligence is used by law enforcement authorities (**and in some cases private security actors**) to determine the risk profile of a particular event and to choose appropriate safety and security measures. Information gathered from various online and offline sources helps create a picture that forms the basis for operational planning. An interview respondent noted:

“**So looking at the forums, looking at the performers themselves, looking at their entourage, their supporters (...), the permanent security staff looking at how other venues have dealt with that performer seeking intelligence from other groups. (...). The supporters and the public can be enormously useful, even by using forums and chat groups and social media.**” (security practitioner, IE).

Another example was given by a security professional from Belgium:

“**Software to consult open-source data is very important. It is useful to know if there is a buzz on the internet regarding all registered events up to that point. However, the same buzz can also exist for unregistered events, providing a warning that something might happen. This is when the team responsible for administrative information takes action.**” (security practitioner, BE).

Access control technologies include traditional metal detectors and applications used to manage individual access through digital ticketing. AI-based metal detectors and perimeter security measures are used to detect weapons and other prohibited items. These technologies are perceived to reduce the reliance on manual checks and are perceived to improve both security and the customer experience. An interview respondent confirmed that customer experience is reported to be improved by higher throughput and less false alarms, frictionless security as well as less subjective searchers as

“**We are no longer relying on ... a relatively low paid CCTV analyst who has beef with the [subject, or]...identifying [with the subject]... So I think it becomes much less subjective, which is great.**” (security respondent, IE).

3.4.2

Non-Technology-based

KEY MESSAGE:

Technologies are an aid, but they are secondary to crowd management plans and appropriate visibility of security personnel.

Despite technology being seen as a useful aid or tool, it is considered secondary to crowd management and crowd control plans, and to the physical presence of security staff and police officers and communication among them. Research found that effective policing is seen to depend on the human element and direct interaction, which technology cannot replace. As one interview respondent showed:

“Technology is a useful tool, but it is a tool. Always the basic investment and planning and design is based on the physical presence of police officers.” (security practitioner, EL).

Another respondent reiterated that the people in the field are the key security and safety measure, and that it is vital clear to establish communication channels between the relevant actors for an event.

Human observation and visibility of the security staff and police are the primary non-technological measures for providing security at public gatherings. Additionally, interview respondents added the police would also involve dog units where relevant, as it was a measure to increase the ‘feeling of security of the participants’ in certain contexts, as well as serve as a deterrent of crime. As a respondent notes:

“Visibility is important, so I would say that everyone at the exhibition centre always sees that we [the police] are there. That increases security and, what do you call it, acts as a deterrent, because some people think twice when they say they’re going to come straight to me, so I’d rather not do it. But if it is, you should also, well, de-escalate, so you shouldn’t escalate further, let’s put it that way, if it arises.” (security practitioner, AT).

In addition to the benefits of police visibility, the ‘invisibility’ of policing also provides benefits. The added value of teams in **plainclothes** is cited as effective for securing gatherings in public spaces. Direct contact with people is highly valued by the police as it significantly improves communication and relationships between officers and the community. A respondent notes:

“The deployment of teams in civilian clothes. We are very much in favour of that. Then, of course, you want to choose the right people, because you don’t need people who are going to be freewheeling around the festival for three days, twelve hours at a stretch. Serious people who are aware of their task and blend into the crowd in small teams and also sense the atmosphere, listen to radio communications and are actually in the right place before the incident breaks out to intervene immediately.”
(security practitioner, BE.)

Another respondent added:

“I’m actually an advocate of foot patrols. [...]. And I personally think that it has an extreme added value because you get into dialogue with the public. Not just at events now but also in general when you’re out and about in good weather because people are much more likely to approach you if you’re walking or cycling than if you’re sitting in a police car with dark windows. You don’t really notice much anymore actually.” (security practitioner, AT).

To maintain a non-threatening presence to the public’s perception, there are some perspectives that favour officers wearing a civilian uniform and carrying minimal weapons. A security practitioner emphasised:

“There is one thing that I personally would like to see: not too martial. There have sometimes been instructions to enter a shopping centre with an assault rifle after terrorist attacks, which I personally find inappropriate. [...] Yes, I want to be seen, but I want to have more access to the population and talk to people a bit about what they need, what they would like. And not this extremely martial approach. [...] I was in [recently attacked city] after the attacks, I was there at a conference, a meeting like that. You feel like you’ve walked through a military camp. It has a threatening effect on the population. [...]” (security practitioner, BE.)

Beyond the police, the event staff also play a crucial role by physically participating in and supervising events. Their presence allows for quick responses to potential incidents. One respondent reported that

“The service personnel who participate in the gathering, [ensure] the safety of the people who participate in the gatherings, [as well as] the surrounding shops, buildings, properties, in general of the socio-economic life of the place.” (security practitioner, EL).

4 Vulnerabilities and surveillance

KEY MESSAGE:

The differential impact on vulnerable communities is not always sufficiently analysed.

One of the main foci of the GATHERINGS project is the unequal impact of surveillance on **vulnerable communities**. A key point that has come from research conducted so far in the GATHERINGS project is that we not only can talk about how people from vulnerable groups or those presenting diverse characteristics might interact with policing and security actors, but we can also think about how certain people can be specifically vulnerable to surveillance, especially over-surveillance, as a distinct area of analysis. It is well known that not all social groups are treated equally by law enforcement in all places all of the time. For example, experts convened by the United Nations High Commissioner on Human Rights (2021) have noted the presence of ‘racism, gender-based and other forms of discrimination’ in relation to policing of protests across the globe. Academic research also notes that new technologies deployed in public spaces can be biased or discriminatory effects on people based on colour, gender, sex, race, nationality, religion, disabilities etc. (Wittkower, 2018). As such, the assessment of how vulnerabilities and technologies interact with the surveillance of public spaces is an important focus in the GATHERINGS project.

Amnesty International has reported on several occasions on the risk of inaccurate results and racism influencing technology outputs; for example, facial features of African American, Asian, and especially indigenous peoples are more likely to be misidentified than white ones. An example of the negative consequences of using biased technology constituted the arrest of Robert Williams, a person of colour wrongfully arrested by the police in 2020 in Detroit based on facial recognition identification tool (Amnesty International, 2023).

Vulnerabilities were specifically discussed with our interview respondents who had a range of different perspectives; general overarching points are now provided before focusing on specifically vulnerable groups. Some respondents noted that the presence of different groups needed to be assessed as part of the overall situation being considered for securing an event. For example, rival political protests are likely to be subject to a greater level of surveillance than if there was no friction expected between those groups. Interviewees who provide private security recognised that by placing groups under increased surveillance, the people present can also be subject to more policing. For instance, younger people being regularly surveilled socialising in public more frequently than others looking after families at home or working long hours. Another example was a neighbourhood that had been subject to social upheaval resulting in increased surveillance and over-policing. One suggestion to mitigate discriminatory effects was offered by one respondent who suggested focussing gathered surveillance data toward intelligence-based policing to identify high-risk individuals, locations, objects, or other entities rather than focusing on social groups.

Yet, several police officers were resistant to the idea that people could be unequally vulnerable to surveillance. Many police officers and private security actors interviewed suggested that nobody is especially vulnerable to CCTV or

video surveillance suggesting that there is no difference in how attendees of gatherings are recorded, especially where the surveillance is lawful, and the public is informed of it. However, several of these officers provided examples of unequal treatment of certain groups, of which criminals were mentioned by multiple interviewees:

“As long as you don’t look for problems yourself, you have no reason to feel stigmatised [by being surveilled].”
(security practitioner, BE).

This potentially suggests that some of this perspective might be focused on the technology itself rather than a holistic view of a wider policing/security operation, or that the apparent equal vulnerability to surveillance applies to innocent attendees of gatherings.

The theme of **technological neutrality** was also foregrounded by a CEO of a technology company who did not accept any responsibility for what police did with the systems they provided. However, this was contrasted by other interviewees in private security and city councils who recognised both that stigmatisation was possible and that the operationalisation of biases can be due to the choices made by the surveillants. One city official gave an example of being present in a command centre where an over-zealous police officer informed them of city council staff taking unscheduled breaks, having watched them on CCTV. Taking an overarching perspective, one private security actor suggested that the biases of surveillors should be taken into account when planning security measures.

It is also worth noting that **the time at which a person is vulnerable to surveillance does not start and end with the gathering they are attending.** For example, persons organising a protest might be subject to background checks, football supporters’ groups might be engaged by specialist teams to gather intelligence, and open-source intelligence might be monitored by police. Events such as pop concerts or those of national significance with a very dedicated group of attendees who camp out prior to the event might need surveillance or support available for those arriving early who could be vulnerable without shelter. Further, vulnerabilities might extend after an event where surveillance data is reviewed and analysed, especially where it is used in police action or court proceedings.

Another key theme highlighted in interviews is that, **people who are generally vulnerable to police actions, are typically also vulnerable to surveillance.** For example, people from poorer background with experience of interacting with police might stay away from certain events or areas where they would be subject to heavy surveillance. However, some groups, such as football fans might be targeted for trust-building activities by police to facilitate a more collaborative approach to policing; yet, this is not extended to other potentially vulnerable groups.

4.1

Groups especially vulnerable to surveillance

Interviewees and surrounding research highlighted that vulnerabilities to surveillance could be grouped in terms of gender, intersectionality, and sexuality; disability, and neurodiversity; those from an ethnic minority or with a migration background; political groups; children; known offenders; police and security actors themselves. Themes also emerged around the employment of AI technologies being associated with an expectation of increased vulnerability to both surveillance and police action. A major issue with the presence of these vulnerabilities in relation to surveillance systems is that they can enable such groups to be socially ‘sorted’ into categories arising from stereotypes or prejudices and can ‘verify identities, assess risk, assign worth’ to persons placed in those categories, potentially leading to long-term social differences and outcomes for different groups (Lyon, 2003). An important part of social sorting is the observing of differences through surveillance, and so there is an increased risk where a group is especially vulnerable to surveillance.



4.1.1

Gender, intersectionality, and sexuality

KEY MESSAGE:

An understanding of sexualised, gendered, and sexuality-relevant issues and clear mitigation strategies is required for all security and surveillance personnel.

Undesirable impacts of surveillance on people due to their gender, sexuality, and other intersectional aspects were noted by several interviewees, though intersectionality itself was not directly mentioned by interviewees. The concept of intersectionality was first developed by Crenshaw who highlighted how black women experience both race and gender discrimination, and so interact with the world differently from both black men and white women (Crenshaw, 1989; 1991). It is an approach that can enable analysis of different intersecting and interacting power dynamics that affect people differently (Crenshaw, 1991). Berg and Mann (2023) outline how intersectionality can be applied to policing, starting with understanding how different forms of discrimination affect vulnerable groups, reflecting on biases in one's own position, critically assessing how systems and strategies used can affect vulnerable groups, and employing intersectional diverse people in the development and deployment of new practices. One example of intersectional issues provided in the interviews involved a police officer acknowledging that despite profiling being unlawful, young males are often subject to a greater level of surveillance than their behaviours would warrant compared with other groups. An intersectional approach would involve inviting that officer to understand the effect of this on young males, their potential role in it, the practices surrounding such decisions and how they could be improved.

The lack of awareness for sexualised violence means that girls and women may not only feel unsafe at public gatherings, but also that attempts to access support might be additionally traumatic and not actually help them. In project interviews, security professionals discussed the need for **safe spaces or code words** for identifying and reporting sexualised violence, targeting women in particular who can then be provided with support. An interviewee mentioned:

“We have an initiative in the [country] which is [...] ask for Angela, where there are code words that honourable people can use where you define within your site safe spaces”

However, another respondent noted that women might hesitate to seek help from security personnel due to fear of further harassment or lack of trust. All personnel involved in public gatherings must be aware of these codes to provide appropriate assistance. The same respondent continued:

“On the one hand, training is also about knowing all the emergency codes, because I say, if someone now turns to uniformed staff with: “Where is Panama?”, “Is Louisa here?”, if they don’t know that, I experienced it myself at an event where I happened to overhear it on the security radio, where a 16-year-old girl went to a steward: “Where is Panama?”, who radios to the operations centre: “There’s someone standing there and keeps asking where to go to Panama”, and the head of operations from the security service radios back: “Explain the way to [the] Airport”. (Event medical staff, AT.) Where victims are recognised and supported, several interviewees recognised the importance of having (safe) spaces to provide victim support services, though one senior police officer noted that this should be separated from police operations. (Security practitioner, BE).

Some interviewees suggested that the use of surveillance systems could provide some level of **deterrence to sexual violence**, as well as an ability to observe and intervene early. However, the majority of police officers interviewed focused on the ability of surveillance technologies to **record and preserve evidence** of physical acts of sexual harassment and violence. Several also noted that sexual harassment is often verbal, and no sufficient technology has been developed to help respond to that in a public events context. The development of a technology to analyse behaviours and detect ‘habitual body movements’ of persons engaged in sexual violence and other crimes is one proactive approach suggested by an interviewee (private security actor, EL). Though this would be challenging to create as such behaviours are non-uniform.

In terms of sexuality, this was only mentioned as an aside in interviews. One respondent noted that whilst the city council they work for had celebrated their LGBTQ community, sexuality was not something specifically considered within their event plans. Whilst this might indicate that people from the LGBTQ community are not seen as specifically vulnerable by surveillance professionals, due to the prevalence and regularity of events such as Pride there are many opportunities to take the needs of this community into account in event planning.

4.1.2

Disability, neurodiversity

KEY MESSAGE:

There are widespread opportunities to take stronger account of diverse disabilities and neurodiversity.

A major issue highlighted was the **insufficient consideration of people living with disabilities** in event security and surveillance plans. One respondent said:

“While some provisions exist for wheelchair users, other disabilities, such as visual impairments, hearing impairments, and cognitive disabilities, are largely neglected.”
(Event support staff, AT)

Another security respondent said

“I was at a panel discussion on the subject of safety, where a representative of the deaf was also present, who 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.” (Event medical staff, AT)

An additional undesired consequence that was discussed in relation to vulnerable groups was that of lack of provision for people with disabilities. For event attendees in wheelchairs, they are usually required to use designated areas for wheelchair users rather than spend the event with their friends or at the front of the stage, hence hindering them from attending the event as they would wish. One respondent noted that they regularly experience wheelchair users arriving at events and asking to be supported to sit in stands rather than the designated area for wheelchair users. Such requests are typically rejected as staff would be unable to ensure safe evacuation routes if people with physical disabilities are unable to move as quickly as others. A police officer noted that when they need to respond to an incident involving someone presenting psychiatric issues, this requires a minimum of three officers, often for some time. This suggests a theme that supporting those with disabilities can be seen as **additional effort using up resources, rather than an essential part of the planning for an event or gathering.**

Yet, there is an awareness on understanding and planning for the specific risks associated with the type of crowd expected at an event. Different performers attract different audiences, which influences the required safety and security measures. For instance, the crowd management strategies for a large-scale music concert would differ significantly from those for a well-supported sports team playing a match due to the different demographics and behaviours of the attendees. Tailoring security measures to the specific characteristics of the crowd ensures that all potential risks are adequately addressed, and appropriate protections are in place for vulnerable groups.

Despite an awareness of the needs of people with disabilities, in the organisation, security, and surveillance of events, the needs of people with disabilities are rarely considered adequately. Few security concepts exist regarding the inclusion of people with disabilities. Where there is such consideration, the focus is upon wheelchair use, while other disabilities are given relatively little attention (be that people with reduced sight, hearing impairments, cognitive impairments, etc.). People with disabilities can be especially vulnerable to surveillance because they might not be made aware of the existence of surveillance as no efforts might be made to make this information available in an accessible way.

Following on from recent research, there is an opportunity for event planners to consider more closely how they can make their events in general, including their security and safety aspects, more accommodating to different disabilities (Mostafa, 2021). Consider, for example, the provisions that can be made for autistic people, modeling on the work behind Dublin's Autism Friendly City initiative (As I Am Ireland, n.d.). Actions might include:

- Provision of quiet spaces or sensory escape areas.
- Use of clear and predictable signs.
- Sensory zoning in crowd safety management.
- Pre-event familiarisation.
- Communication with crowds where possible through clear and non-intrusive visual cues, rather than alarms or announcements (Hamzehlou, 2024; Pisello, et al., 2024; Hara and Bigam, 2024).

Such policies can have significant effects on inclusion at relatively low or even negligible cost.

4.1.3

Ethnicity and migration background

KEY MESSAGE:

People from ethnic minorities or with a migration background have been over-policed and discriminated against, profiling should be avoided and community or pro-active policing approaches could be alternatives.

Ethnicity was mentioned by several interviewees in relation to areas where people from ethnic minorities tend to live, or migration background. Several interviewees noted that neighbourhoods have been stigmatised where a lot of people from ethnic minorities reside there, and this has led to a cycle of increased surveillance and policing. There is significant evidence demonstrating that people of colour are policed differently to their white counterparts, often resulting in **over-policing and over-surveillance** of ethnic minorities, especially at anti-racism protests such as Black Lives Matter (Privacy International, 2020).

The presence of immigrants from outside Europe was discussed in varying terms. Asylum seekers and immigrants were noted to have made a contribution to their local communities. Some police officers did acknowledge the possibility that surveillance of people from migrant communities could be discriminatory. One officer noted that native locals were willing to inform police about potential criminality by immigrants, leading to further police action.

Another issue related both to migration background and women is how police responded to incidents such as those in Cologne on New Year's Eve in 2015 where dozens of women were sexually harassed by male migrants (BBC News, 2016). One police officer who responded to the project admitted that when something similar occurred in their location, their local police force felt they had no option but to profile males of an apparent immigrant background whilst an event was ongoing to avoid further harassment of women. This was followed-up by taking a **community policing-informed approach** and visiting migrant groups to explain what behaviours, according to the police, were considered acceptable in their location. These biased approaches clearly indicate how ethnic minorities can be subjected to over-policing and over-surveillance.

Other police forces have taken a **pro-active policing approach** by increasing the level of lighting in normally dark areas so as to reduce hidden areas.

4.1.4

Political groups

KEY MESSAGE:

It is important that police are aware of the surrounding context of gatherings and the groups present to be able to take account of relevant issues. This should not fall into profiling.

In the introduction to this section we mentioned that some groups are often monitored more closely than others, and this is often the case where there are rivalries between political groups, or where politics is intertwined with other aspects such as football. For example, several police officers gave examples of European football games held in a 'neutral' location that can involve football teams representing areas that either are, or have been, involved in armed conflicts. One respondent noted that, increase monitoring can often fall into **profiling** of the groups who are present:

“Yes, it may not be the politically correct thing to say, but that’s what happens, you know.” (Private security actor, IE)

Further, police officers noted that whilst violent political protests and counter-protests from the extreme left or extreme right are generally rare, seemingly innocuous protests and gatherings can be hijacked by more extreme political factions. Local politics can also be relevant and link to global issues, several officers noted that ongoing conflict between Hamas and Israel had stoked tensions between different groups and that this was especially relevant where, for example, a mayor had sought to support a particular group, leading to protests of the mayor’s position.

Police expressed a need to be aware of the surrounding contexts and not just of a particular gathering, but of different groups that might operate in or around other gatherings, and what their goals might be. One police officer described a protest in response to the mayor mentioned above as an

“Administrative opportunity to take an extra look at some target groups.” (Security practitioner, BE)

Although profiling is mentioned above and in highly-charged protest/ counter-protest situations might lend themselves toward a robust police response akin to riot policing, one police officer was very clear that placing **plain clothes police officers** within gatherings allowed police to stay aware of how a situation was evolving and enabled them to **respond early to reduce the frequency of tensions increasing**. Further, a respondent involved in

private security highlighted the benefits of engaging with groups who might experience friction in advance to better understand their needs within the context of a gathering so that this can be taken into account. The **generation of trust** between such groups and the police was also something highlighted as beneficial by police both in interviews and in other research activities.

4.1.5

Children

KEY MESSAGE:

Children can have specific vulnerabilities that need to be taken into account with flexible response plans.

Children's issues were only briefly referred to by a small number of respondents. One important point mentioned was that as younger children are unable to make their own decisions, they are **reliant upon their caregivers to protect them and this extends to situations of surveillance** that might occur at a gathering. One interviewee who organises events did note the importance of family-friendly areas and plans for lost children to be reunited with caregivers. Though one plan for reuniting lost children involved placing a child on stage with a microphone so they can appeal to their caregivers, potentially increasing their vulnerability to surveillance despite good intentions. Another important point made regarding children is that whilst typical children under 13 might need more care than typical children who are 15-16, there are a **wide range of maturities** and so plans for dealing with children need to be flexible enough to manage this.

4.1.6

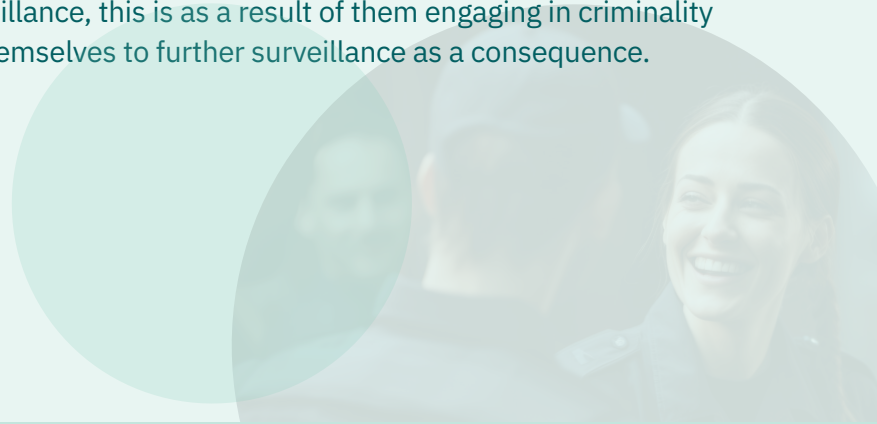
Known offenders

KEY MESSAGE:

Police are likely to maintain an awareness of known offenders recognised in gatherings and policing of their actions needs to be appropriate to deter and avoid ongoing offending whilst not displacing it to other areas.

One group that might obviously be vulnerable to surveillance are known offenders. Several police officers who were interviewed noted that frequent pickpockets can become **known to police and so are often surveilled**; this might be via video surveillance or plainclothes officers, both of which are useful for **identifying and tracking offenders**, and recording evidence.

The importance of a robust response to pickpockets at events was highlighted by one officer to prevent an offender from being dealt with quickly and returning immediately to the event to continue offending. Yet another interviewee noted that an especially strong response to pickpockets or other ‘low-level’ crime can, rather than deter offending, simply displace criminality to outside the event area meaning that the security plan for an event needs to expand geographically. Police officers who have engaged with the project have mentioned that although they might maintain an awareness of known offenders, they are **unlikely to intervene unless criminal behaviour is demonstrated** and whilst that awareness might mean a known offender is vulnerable to surveillance, this is as a result of them engaging in criminality and so exposing themselves to further surveillance as a consequence.



4.1.7

Police officers and security actors

KEY MESSAGE:

Police and security actors are also vulnerable to surveillance, but it can serve a protective function to support establish the truth of a situation.

A group that is often under surveillance, but under-recognised is the police and security actors themselves. For example, **a law enforcement officer could be captured on video surveillance** as they move around an event space, filmed by disgruntled members of the public opposing their action, on the body-worn cameras of themselves and colleagues as well, as other surveillance measures. One interviewee from a security regulator noted that they sought to exclude people with a criminal background from their industry. Whilst this could be seen as appropriate gatekeeping by some, it also prevents others moving on from a regrettable past.

Whilst vulnerability to surveillance is seen as a negative in other parts of this analysis, in terms of police and security actors it is also **protective**. As one police officer said of body-worn camera footage,

“It serves as a defence for the actions of police officers. We have had reports of corrupt practices, of unethical behaviour, and after reviewing the video recordings, we find that the reports are false, that is, they do not support what the applicant claims, so they protect the police services.” (Security practitioner, BG).

4.1.8

Vulnerabilities and future technologies

KEY MESSAGE:

There is significant concern that biases associated with use of AI technologies will make current discrimination worse, and this needs to be tackled using both human and technological measures.

Several interviewees noted fears that the increasing use of AI in the policing of gatherings could **increase biased decision-making** against ethnic minorities, as well as impact people’s privacy, with one remarking

“Certain profiles simply stand out, and then you very quickly find yourself in that ethnic profiling story [...] I suspect that [discrimination driven by AI bias] is just an extension of whatever happens physically on site.” (Event planner, BE)

Another significant issue with AI use, suggested by one interviewee from the private security sector, is that there is **little training on bias given to security actors** outside of airports. This would likely change where AI is used to replace some tasks currently conducted by humans, leaving the remaining people to deal with especially challenging issues:

“We are going to have less security staff but much higher trained because they’re gonna be using systems to manage exceptions.” (Engineer, IE.)

Another interviewee remarked that it would be important for decision-making to not be made on the basis of algorithmic processing alone, recalling earlier points made that people involved in policing gatherings need to be aware of the wider context (Smith and Mann, 2024).

4.2

Legal context of vulnerability

KEY MESSAGE:

The concept of vulnerability is having increased relevance in GDPR and LED jurisprudence, suggesting that recent organisers should determine measures for protecting vulnerable individuals.

This section includes an analysis of the specific legal aspects devoted to the protection of **vulnerable communities** in the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).

Contrary to the notions of **privacy, data protection, and transparency**, the concept of **vulnerability** itself is not enshrined in the European Convention on Human Rights or the EU Charter of Fundamental Rights. While recognition of its importance is reflected in the jurisprudence of the European Court of Human Rights, the Court has never conceptualised vulnerability in the field of private life, privacy, or data protection, though prominent voices argue that vulnerability is at the heart of privacy and data protection regimes (Malgieri and Niklas, 2020).

The notion of **vulnerable natural persons** (sometimes referred to as vulnerable persons) is mentioned once in the GDPR (more specifically in recital 75) and three times in the LED (in recitals 39, 50, and 51). Recital 39 of the LED refers to the notion in relation to **transparency (the right of access and the right to be informed)**: ‘In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of **vulnerable persons such as children.**’

Both the GDPR and the LED refer to vulnerability in the context of the **Data Protection Impact Assessments**:

‘The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: [...] where personal data of **vulnerable natural persons, in particular children**, are processed [...]’ (Recitals 50 and 51, LED; Recital 75, GDPR).

While vulnerable persons are not defined in the legal texts, they are ‘often defined as persons at higher risks (in terms of likelihood and severity) of damages to their rights and freedoms’ (Malgieri and Niklas, 2020). The legal

texts do, however, consequently refer to **children** as a possible category of vulnerable natural persons. Legal scholarship has revealed that reference to children as vulnerable persons points to two manifestations of vulnerability, namely **decisional vulnerability** and **outcome vulnerability**. Where decisional vulnerability refers to the observation that ‘some subjects should be protected for their limited capacity to understand and give consent’, outcome vulnerability refers to the observation that ‘some subjects should be protected for higher risks of material or non-material damages’ (Malgieri and Niklas, 2020).

Following the rationale that vulnerability can manifest in multiple ways, Article 29 Working Party (WP29) lists other categories possibly at risk (employees, mentally ill, asylum seekers, the elderly, a patient) and argues that a key factor in the identification of vulnerability is the presence of a power imbalance between data subject and data controller:

‘Data concerning vulnerable data subjects (recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties as opposed to the processing performed by their employer, when it is linked to human resources management. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns a more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.’ (Article 29 Working Party, 2017).

In acknowledging the importance of power imbalances, the WP29 echoes prominent voices in the debate who argue that ‘privacy and data protection regimes are manifestations of the idea that all individuals are vulnerable to power imbalances.’ (Malgieri and Niklas, 2020).

Following the risk-based approach to vulnerability, both the GDPR and the LED offer useful provisions to attend to the different manifestations of the notion of vulnerability as explained above. More specifically, the notion of **data protection by design** (Article 25 of the GDPR and Article 20 of the LED) and the data protection impact assessment (Article 35 of the GDPR and Article 27 of the LED) seem adequate to address vulnerability in a more nuanced and inclusive manner.

The principle of data protection by design confers upon the controller the obligation to take into account the ‘the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons’ and to ‘implement appropriate technical and organisational measures, which are designed to implement data-protection principles’. (Article 25 of the GDPR and Article 20 of the LED) This should be done ‘both at the time of the determination of the means for processing and at the time of the processing itself’. (Article 25 of the GDPR and Article 20 of the LED) In case of a ‘high-risk data processing, including the case where the data subjects can be considered vulnerable’ the data protection impact assessment requires ‘a systematic description of the processing, an assessment of necessity and proportionality, an assessment of risks and description of measures envisaged to mitigate such risks’ (Article 35 of the GDPR and Article 27 of the LED). Taken together, both provisions confer upon the data controller the obligation to autonomously determine measures for protecting vulnerable individuals.’¹

The above analysis of the notion of vulnerability in the legal framework for data protection in the European Union suggests that the identification of a power imbalance between the data controller and the data subject (or, in the context of public space surveillance, **surveilled** and **surveiller**) is a useful approach to the notion of vulnerability that extends the example of children to include any case where a power imbalance between data subject and data controller is present. This more nuanced and inclusive understanding of vulnerability attends to both manifestations, decisional vulnerability and outcome vulnerability. Within the existing legal framework, the principle of data protection by design and the data protection impact assessment were identified as suitable legal instruments to take this more nuanced and inclusive understanding of vulnerabilities into account in the surveillance of public spaces.

¹ idem

4.2.1

Differences in national legislation: Austria, Belgium, Bulgaria, Germany, Greece, Ireland

In order to attain a better understanding of national legislation in research partner countries regarding surveillance, an analysis of Member State law applying the Law Enforcement Directive and other relevant legislation was conducted. As the LED allows Member States some margin of appreciation in applying the Directive in the national law, there are some variations and not all national legislation covers all areas considered. An annex is provided to show Member State law examined.

In relation to the **right of access** and **the right to be informed**, Belgium, Germany, and Bulgaria apply an indirect system of right of access, meaning access is requested indirectly via the Data Protection Authority (Dimitrova & De Hert, 2024). However, Ireland, Germany, and Greece apply a direct system of right of access meaning that data-subjects can request access to their personal data from the data controller directly.

Under the LED, only a **competent authority** can process personal data for law enforcement purposes (Article 1(1), LED). Such authorities are defined as:



Any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or



Any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (Article 3 (7), LED)

Data protection legislation of Ireland and Austria took the wording found in the LED and do not delineate further, leaving a very broad definition that does not specify whether a competent authority should be a public and/or private entity. Bulgaria's Personal Data Protection Act requires a competent authority to be a public entity. Whilst the Greek data protection legislation does apply to both public and private entities, and the German Federal Data Protection Act places public security with public and private bodies (Vogiatzoglou & Marquenie, 2022: 21), neither defines a competent authority. The clearest delineation of what a competent authority means is provided in Belgium where data protection legislation lists all entities who can process personal data as a competent authority.

As noted above, **vulnerable groups** under the LED have a focus on children. In Ireland, the Policing, Security and Community Safety Act 2024 makes the prevention of harm and protection of people who are vulnerable or at risk an objective of An Garda Síochána (the national police and security service of Ireland), and defines such persons as children, those with a physical disability, injury, or illness, a mental disorder, or an intellectual disability. Bulgaria's Child Protection Act specifies the rights of the child and child protective measures and refers to the GDPR's definition of 'personal data' to elaborate on information related to children.

In terms of **surveillance beyond law enforcement**, reference is made to children and employees as categories requiring extra-legal protection. In relation to the positioning of surveillance cameras by private bodies, with Belgium's Camera Act (Article 10) providing: 'Surveillance cameras may not produce images that violate a person's intimacy, nor be aimed at gathering information about philosophical, religious, political, trade union affiliation, ethnic or social origin, sexual life or state of health.'

5 Conclusion

This Surveillance Impact Report showcased a summary of research findings on how surveillance assemblages work, the effects surveillance has on the privacy of citizens, and their cost.

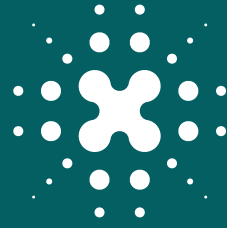
The report touched on main topics in analysing surveillance impacts, such as safety and security concerns, safety and security measures, perceived impacts, stakeholders involved, the role of training needs and data management practices.

Key messages of this report include:

- The concept of a ‘surveillance assemblage’ helps us to think about surveillance practices in a holistic way.
- There is a persistent set of social and ethical concerns around the use of surveillance technology, and there are complex and uneven deployments.
- There is a valuable distinction between ‘safety’ and ‘security’. In the absence of a clear definition of each concept, tensions may appear among stakeholders’ interchangeable use of the terms, which leads to difficulties in implementing the appropriate measures for each situation.
- There is a consistent set of safety considerations, centred on crowd management, to be considered at all times.
- There is a range of security concerns with varying degrees of seriousness to be accounted for by all security practitioners in organising a public gathering.
- Security professionals perceive a number of technologies as a valuable aid in conducting their work, including CCTV, drones, body-worn cameras, and access control.
- Technologies are an aid, but they are perceived as secondary to crowd management plans and appropriate visibility of security personnel.

- The differential impact on vulnerable communities is not always sufficiently analysed. An understanding of sexualised, gendered, and sexuality-relevant issues and clear mitigation strategies is required for all security and surveillance personnel. There are widespread opportunities to take stronger account of diverse disabilities and neurodiversity .
- People from ethnic minorities or with a migration background have been over-policed and discriminated against, profiling should be avoided and community or pro-active policing approaches could be alternatives.
- It is important that police are aware of the surrounding context of gatherings and the groups present so as to be able to take account of relevant issues. This should not fall into profiling.
- Children can have specific vulnerabilities that need to be taken into account with flexible response plans.
- Police are likely to maintain an awareness of known offenders recognised in gatherings and policing of their actions needs to be appropriate to deter and avoid ongoing offending whilst not displacing it to other areas.
- Police and security actors are also vulnerable to surveillance, but it can serve a protective function to support establish the truth of a situation.
- There is significant concern that biases associated with the use of AI technologies will make current discrimination worse, and this needs to be tackled using both human and technological measures.
- The concept of vulnerability is having increased relevance in GDPR and LED jurisprudence, suggesting that recent organisers should determine measures for protecting vulnerable individuals.

These outputs inform further project work on the development of 1) a security-privacy-cost evaluation matrix, 2) an awareness-raising programme tailored both for local surveillance professionals, and citizens, 3) three policy dialogues with EU and national policymakers, leading to the formulation of a set of legal recommendations; 4) an EU Handbook on Surveillance of Public Gatherings.



Gatherings

Balancing security, privacy and cost

CONSORTIUM



FOLLOW US

 @gatheringsEU

CONTACT US

info@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.

WEBSITE

gatherings-project.eu