A GUIDE TO INVESTIGATING HIGH-RISK TECHNOLOGIES:

FROM IDENTIFICATION TO ADVOCACY

SHARE FOUNDATION 2026.

"A GUIDE TO INVESTIGATING HIGH-RISK TECHNOLOGIES: FROM IDENTIFICATION TO ADVOCACY"
SHARE FOUNDATION
MARCH 2026
PUBLICATION EDITORS: Danilo Krivokapić and Andrej Petrovski
AUTHOR: Mila Bajić
LANGUAGE AND TRANSLATION EDITOR: Milica Jovanović
DESIGN AND LAYOUT: Olivia Solis Villaverde
ILLUSTRATIONS: macrovector on Freepik

This publication was funded partially by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.

CC LICENSE
ATTRIBUTION-SHAREALIKE CC BY-SA
This license lets others remix, tweak, and build upon your work even for commercial purposes, as long as they credit you and license their new creations under the identical terms. This license is often compared to "copyleft" free and open source software licenses. All new works based on yours will carry the same license, so any derivatives will also allow commercial use. This is the license used by Wikipedia, and is recommended for materials that would benefit from incorporating content from Wikipedia and similarly licensed projects.

WHAT

In the digital environment, high-risk technologies are automated systems used to collect data about people, make decisions, manage behavior, and more. What makes them high-risk is a combination of three factors: lack of transparency in how they work, insufficient legal regulation of their use, and the potential to harm fundamental human rights. In practice, these can include facial recognition systems (mass biometric surveillance), algorithms deciding access to social services, or generative AI used to spread disinformation and deepfakes.

HOW

This methodology offers a structured approach to investigating high-risk technologies in conditions of limited access to data and institutions. It is designed for civil society organizations, investigative journalists, and activists who want to identify, document, and challenge the use of these systems – regardless of whether they are introduced by the state or the private sector.

WHY

High-risk technologies are typically introduced without public debate, and their use remains in the shadows until visible consequences emerge. By the time harm is documented, the technology is already deeply embedded in the system. That's why early detection of risks – before they become normalized – is a key task for civil society and the media.

WHO

When state institutions introduce high-risk technologies into public systems and services without proper oversight or accountability, civil society organizations, investigative media, and the activist community become the main line of defense for the public interest. Their task is clear: systematically document, analyze, and inform the public about risks – before opaque deployments become the norm and before harm to citizens and society becomes irreversible.

RESEARCH PRINCIPLES

Researching high-risk technologies requires a careful and responsible approach. Several core principles should guide the entire process.

HUMAN RIGHTS-BASED APPROACH

- → use international human rights standards as the framework for risk analysis
- → pay special attention to vulnerable and marginalized groups, who are more exposed to rights violations
- → examine whether the technology was preceded by an impact assessment on privacy and fundamental rights, and whether safeguards are in place

PROACTIVE THREAT IDENTIFICATION

- → focus on early detection of emerging risks
- → develop the capacity to recognize patterns of technological harm
- → build systems for rapid response to identified threats

COLLABORATION AND KNOWLEDGE SHARING

- → build partnerships with civil society, technical and legal experts, and affected communities
- → jointly develop and share resources, knowledge bases, and research tools
- → establish coordinated response mechanisms

ETHICAL DATA PRACTICES

- → protect the privacy of contacts and sources; informed consent must be ensured whenever personal data is collected
- → use secure and transparent research methods
- → verify collected information to ensure accuracy and maintain transparent and open databases

INTERNATIONAL HUMAN RIGHTS STANDARDS:

→ European Convention on Human Rights

→ Article 8, Right to respect for private and family life

→ EU Charter of Fundamental Rights

→ Article 7 (privacy) and Article 8 (data protection)

→ International Covenant on Civil and Political Rights

→ Article 17, Right to privacy

→ UN General Assembly Resolution 68/167

→ Right to privacy in the digital age

RISK CLASSIFICATION SYSTEM

DEFINE RELEVANT RISK CATEGORIES

- → human rights violations
- → economic exploitation
- → environmental impact
- → spread of disinformation
- → ...

ASSESS THE SEVERITY OF POTENTIAL RISK:

Very low | Low | Moderate | High | Very high

based on: the impact of potential harm and the likelihood that harm will occur

EXAMPLE OF A RISK MATRIX

Risk = Impact × Likelihood	IMPACT: 1	IMPACT: 2	IMPACT: 3	IMPACT: 4	IMPACT: 5
Likelihood: 1	Very low (1)	Very low (2)	Low (3)	Low (4)	Moderate(5)
Likelihood: 2	Very low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
Likelihood: 3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Likelihood: 4	Low (4)	Moderate (8)	High (12)	High (16)	Very high (20)
Likelihood: 5	Moderate (5)	High (10	High (15)	Very high (20)	Very high (25)

DEVELOPING RESEARCH QUESTIONS

LEGAL FRAMEWORK

→ Is there a comprehensive legal framework regulating the use of high-risk technologies?

→ Is there an independent oversight body (e.g. data protection authority)?

→ Were proper legal changes made before implementation?

→ Are there international standards that restrict or prohibit such technologies?

→ In Serbia, there is no specific law governing high-risk technologies. Regulation relies on strategic and ethical documents that are not legally binding.

→ The relevant documents are the **Artificial Intelligence Development Strategy (2025-2030) and the Ethical Guidelines for the Development, Application, and Use of Trustworthy and Responsible Artificial Intelligence (2023)**, which highlight the need to pay special attention to the development and deployment of high-risk AI systems, and to their potential impact on citizens' rights. However, these documents are only a general framework and set of guidelines, but do not introduce binding rules, bans, or mechanisms for oversight and enforcement.

→ As a result, the protection of rights in the context of high-risk technology use is achieved indirectly, relying on general legislation governing the protection of human rights and personal data.

PRACTICAL USE

→ Have there been cases where the use of high-risk technologies led to privacy violations, data breaches, or other infringements of citizens' rights?

→ Is there public information on which high-risk technology systems are in use, how they work, and for what purposes?

→ Are there mechanisms through which citizens can seek the protection of their rights, request a review, or access decisions and processes involving high-risk technologies?

MEDIA COVERAGE

→ Do media report on these technologies responsibly and objectively?

→ What narrative dominates – tech optimism, critical scrutiny, or sensationalism?

→ Does reporting support informed public debate or just repeat official narratives and manufacturers' marketing messages?

WARNING SIGNS

PHYSICAL CHANGES

→ new cameras and sensors in the streets

→ new high-tech equipment in public institutions

→ "smart system" signs and notices

POLICY CHANGES

→ novi propisi o prikupljanju podataka ili nadzoru

→ new rules on data collection or surveillance

→ government contracts with tech companies, public procurement

→ changes to the terms of use and privacy policies of public digital services

NEWS AND ANNOUNCEMENTS

→ AI use in public administration

→ partnerships with tech companies

→ tech projects funding announcements

→ public consultations (tenders) on new systems

IDENTIFICATION CHECKLIST

Technology	What it looks like	Where to find it	Rights at risk	Examples
Facial recognition systems	Sensor-equipped cameras	Streets, city buildings, public spaces	Right to privacy, freedom of movement, freedom of assembly and association	Surveillance cameras on Belgrade streets
AI decision-making systems	Softverske platforme	Banka, zdravstvo, penziono, socijalne službe	Protection from discrimination, protection of personal data	Social Card system
Cameras with AI analytics	Regular cameras labeled 'smart'	Traffic junctions, parks, streets	Right to privacy, freedom of assembly	Oko sokolovo (Falcon Eye)
Digital identification systems	Self-service kiosks, apps, document readers	City offices, banks, hospitals	Right to privacy, personal data protection	IS COVID-19, IZIS

→ Serbia's healthcare system has shown serious failures in protecting the most sensitive patient data. The Integrated Health Information System of the Republic of Serbia (IZIS), set up by the Ministry of Health in 2017, was compromised from the very beginning: all medical staff with access to the system were given the same password, exposing patient data to potential misuse.

→ A few years later, at the start of the COVID-19 pandemic, the COVID-19 Information System was set up to store sensitive medical data of all people who were infected or had contact with infected individuals. This system was also poorly secured: access credentials were publicly available online for a full eight days.

→ Both cases point to a systemic problem: data security in the public sector falls well below standard, while a culture of accountability is virtually non-existent.

GATHERING INFORMATION

Information about high-risk technologies can be gathered in several ways: through freedom of information requests, by searching publicly available sources, through direct inquiries to institutions and companies, and by researching public procurement procedures.

FREEDOM OF INFORMATION REQUESTS

All public authorities are legally required to uphold the public's right to know. This includes ministries, city and municipal administrations, state-owned companies, as well as private entities that carry out public interest activities or receive significant public funding. The most effective requests are specific: instead of asking general questions, request particular documents such as contracts, minutes, decisions, or impact assessments. It is also helpful to clearly define the time period the request covers.

Referring to publicly available information that is indirectly related to the request increases the chances of getting a response. It shows that the requested document likely exists. If a public authority fails to respond within the legal deadline, a complaint can be filed with the Commissioner.

EXAMPLE:

The website of the Personal Data Protection Commissioner provides clear information on who you can send freedom of information requests to, how to submit them, and how to file a complaint:

→ What you can request, how, and from whom

→ Freedom of information request form

PUBLIC PROCUREMENT

There is almost always a paper trail, at least as an entry in tender documentation available on the Public Procurement Portal. The portal centralizes all public procurement procedures in the country and allows you to search by institution, subject of procurement, or supplier. It provides information on tender conditions, supporting documentation, as well as details on who was awarded the contract and under what terms.

Since publishing this information is a legal obligation, the data on the Portal is verified and can serve as a key starting point for research – especially for identifying who manufactures or supplies the technology in question, who is responsible for its implementation, and how much funding has been allocated to the project.

APPEALS TO THE COMMISSIONER

A complaint can be filed with the Commissioner if a public authority rejects, ignores, or delays a request, sets an unjustifiably high fee, or otherwise prevents access to information. The complaint must be submitted within 15 days of receiving a response, or once the legal deadline has passed without a response.

However, complaints to the Commissioner are not possible against decisions of the National Assembly, President, Government, Supreme Court of Cassation, Constitutional Court, National Bank, or Public Prosecutor's Office — in those cases, administrative court proceedings are the only option.

EXAMPLE:

→ In 2019, When Serbia's Ministry of Interior published a 2019 impact assessment on video surveillance, civil society organizations and activists raised concerns about its intrusiveness and disproportionate nature. The Commissioner then confirmed those concerns, ruling that the assessment had not been prepared in line with the Personal Data Protection Law.

INDEPENDENT RESEARCH

The starting point of any investigation is mapping the information that is already available. Sources can be grouped into two categories: media content – news articles, broadcasts, podcasts, investigative stories – and official documents published by institutions themselves, such as annual reports, impact assessments, strategies, and tenders.

Both are useful, but in different ways: media sources help you understand the public narrative and key actors, while official documents provide insight into how institutions justify their use of particular technologies.

WHERE TO FIND INFORMATION

Type of information		Where to access
Laws and regulations	→	Official Gazette website
Project planning	→	City and urban planning documents
Tenders	→	Public Procurement Portal
Annual reports	→	Agency websites
Analyses and reports	→	Civil society organization websites
News and announcements	→	Media websites

TIP:

→ Technology company websites may contain information about specific projects and clients that is not available anywhere else, including technical specifications, references to government contracts, and photos of installations. These pages can be changed or removed without notice, so it is important to archive the content as soon as you find it (for example, using archive.org or tools for saving pages locally). When the SHARE Foundation published information from Huawei's website about the Safe City project in Belgrade, the page was taken down within 10 hours.

→ Patents can be a useful source of information about the technical capabilities of the system being investigated: they can reveal how the technology works, what it is designed for, and who is developing it. Patent databases are publicly available and searchable, but interpreting technical documentation often requires expert input.

FROM DATA TO ACTION

ANALYSING AVAILABLE INFORMATION

Collected data is not enough on its own; what matters is what can be concluded from it and how those conclusions are documented. When internal documents are available, such as impact assessments or contracts, it is useful to carry out both legal and technical analysis: legal analysis examines compliance with applicable regulations, while technical analysis assesses whether the system works as described. The same approach can be applied to other sources – press releases, media reports, tenders – to reconstruct how the decision to deploy the technology was made and how it is being justified.

EXAMPLE:

→ Analysis of the data processing impact assessment on personal data protection in the use of video surveillance systems by the Ministry of Interior | SHARE, Partners Serbia, and BCBP, 2019

BEFORE STARTING THE ANALYSIS, IT IS USEFUL TO CLARIFY A FEW THINGS:

- → What is the goal of the analysis? What are we trying to establish?
- → How will we define the problem? Which aspects of the technology will we focus on, and why?
- → Which sources are credible and available to us for research?
- → Who can contribute to the research process – technical experts, lawyers, journalists, affected communities?

When data is not publicly available, the starting point is to map what already exists – media analyses, civil society reports, academic research, or the experiences of activists. This makes it possible to identify where gaps remain and where new contributions would be most useful. A few questions can help guide this process: Is it known what the technology is used for, who acquired it, and under what conditions? Is the same or similar technology used in the region – and what can be learned from those experiences? Are there people directly affected by the use of the technology who can speak about its consequences?

Consulting colleagues often brings valuable perspectives that might otherwise be overlooked. Conversations with experts in digital rights, cybersecurity, or other relevant fields provide technical and legal insights that strengthen both the arguments and the credibility of the findings. First-hand accounts from people who have directly experienced the harmful effects of high-risk technologies also help humanize the issue and make abstract risks more tangible. This is equally valuable for both research and media reporting.

Comparative research can be especially valuable when a domestic case has not yet produced documented consequences. Experiences from other cities, countries, or sectors can show how a particular technology is typically introduced and justified, what consequences have been recorded, and which arguments have proven effective in challenging its use.

EDUCATIONAL MATERIALS

Knowledge gathered through research only has value if it is accessible and understandable to those it is intended for. Reports and analyses are the foundation, but research often needs to be adapted for different audiences: educational materials help new generations of researchers and activists get up to speed more quickly, while documents aimed at decision-makers need to be more concise and focused on clear recommendations.

EXAMPLE:

→ At the end of 2023, the SHARE Foundation published a book on biometrics as one of the first comprehensive overviews of the global use of biometric surveillance systems. The book was the result of a years-long effort to ban facial recognition surveillance in Belgrade – bringing together accumulated knowledge, experience, and lessons learned, and presenting biometric surveillance as a systemic issue that goes beyond a single city, country, or continent.

→ Two years later, in 2025, a book on spyware was published – another pioneering effort to document surveillance and challenge the growing ambitions of social control.

RAISING AWARENESS

Once findings are documented and the position is clearly defined, the next step is shaping the message. Effective communication requires clarity: what the core issue is, who is affected, and why it matters to the wider public. The message should be clear and concrete, so it resonates beyond a narrow circle of experts and activists.

KEY MESSAGE ELEMENTS

WHAT DID WE FIND?

→ Basic facts about the technology or system uncovered, presented clearly and concretely: the wider public should understand what it is and why it matters.

WHY DOES IT MATTER?

→ What are the concrete consequences for individuals and the wider community – legal, financial, social, psychological? A clear answer helps people see the issue as their own and join calls to protect their rights.

WHERE IS IT HAPPENING?

→ The geographic scope of the technology's deployment – whether it affects a specific location, neighborhood, region, or the entire country. Specifying the scale helps people understand how widespread and harmful it may be.

WHO IS INVOLVED?

→ Which actors are behind the deployment and use of the technology? Which companies, public authorities, or foreign governments are involved?

COMMUNITY ENGAGEMENT

The public can get involved in different ways – from sharing information on social media to submitting requests and complaints, taking part in public consultations, or organizing protests. It is important to offer clear and accessible ways for participation, tailored to different levels of engagement. The media can be key allies at this stage: by contributing to investigations, reporting on findings, or supporting campaigns, they significantly expand the reach of the message and help bring early warnings from civil society to a wider audience, especially on issues the public may not yet be aware of.

EXAMPLE:

→ During the #hiljadekamera campaign (2019-2021), citizens were invited to photograph cameras across Belgrade and send the coordinates to the SHARE Foundation team, which added the data to a publicly available database. The result was a list of verified smart camera locations several times longer than the official list published on the Ministry of Interior's website. The campaign played a key role in exposing the scale of surveillance in the city.

ADVOCACY

Advocacy turns research findings into pressure for change directed at institutions, decision-makers, or the broader public. The strategies should be developed simultaneously across multiple levels: local, national, and international, as the same argument may carry different weight depending on who it is directed at and when.

LOCAL AND NATIONAL ADVOCACY

Local advocacy begins with understanding the community – its specific concerns, how it consumes information, and how familiar it already is with the issue. Local media that are trusted by the community are often the most effective channel for putting the issue into context and connecting it to people's everyday lives. Direct community involvement – through discussions, surveys, or sharing information – matters for another reason too: people affected by these technologies are rarely asked for their views. The sense of participation in itself helps build support and strengthens the advocacy position.

At the national level, building coalitions is key: acting together with civil society organizations working on related issues carries more weight than individual voices. A coalition makes it possible to develop shared positions,

prepare proposals for legal reforms, file joint complaints or criminal reports, and coordinate engagement with international bodies.

INTERNATIONAL ADVOCACY

International advocacy strengthens the legitimacy of domestic initiatives and increases pressure on public authorities that are reluctant to respond to citizens' demands. International mechanisms, relevant bodies, and comparative practice from other countries can strengthen arguments and help guide further advocacy efforts. Drawing attention to issues and specific cases beyond national borders reduces the risk of abuses being covered up. Cooperation with international organizations and media increases visibility and enables the exchange of experience.

All three levels of advocacy should reinforce one another through consistent messaging and coordinated action – local support adds credibility to national efforts, while alliances at the national level strengthen the international position.

ISBN 978-86-89487-20-6

SHARE FOUNDATION 2026.