Civil Society and Digital Security in the Age of AI

A field dossier on information and data security

The same technology strengthens defense on one side and makes fraud cheaper on the other. This dossier offers civil society a calm framework for living with both realities at once.

SECURE-CS · FIELD DOSSIER
ERASMUS+ KA220-YOU
ISTANBUL · DECEMBER 2025

PROJECT
SECURE-CS: Civil Society Initiatives Strengthened with Information and Data Security

REFERENCE NO / PROGRAMME
2023-1-TR01-KA220-YOU-000161230 · Erasmus+ KA220-YOU (Cooperation Partnerships in Youth)

PREPARED BY
Gülşen Nişli · Expert Researcher, on behalf of ANKA Gelecek ve Yenilik Derneği (Project Partner)

FUNDING
Co-funded by the European Union

Getting started

Most associations have no server room. They have a laptop, a few email accounts, a member list built up over the years, and project folders sitting in the cloud. When the daily work looks this simple, the phrase "information security" sounds like a concern for large companies. Yet that same laptop holds young people's identity details, parents' signatures, volunteers' phone numbers, and the reputation an organization has earned over years. There is more to lose than it seems.

SECURE-CS, in full *Civil Society Initiatives Strengthened with Information and Data Security*, is a partnership that takes the responsibility behind this simple picture seriously. Carried out under the Erasmus+ Cooperation Partnerships in Youth (KA220-YOU) action, the project has been working since December 2023 to strengthen the digital, cyber-security and data-protection skills of organizations active in education, youth and sport. Six partner organizations work side by side through meetings and trainings that stretch from Türkiye to Norway and from Belgium to North Macedonia. The project has two concrete outputs: a curriculum and toolkit for building digital-security capacity through civil society, and an online platform on which organizations can test their own digital-security readiness. Through dissemination events held until the project ends, this body of work aims to reach more than three hundred participants.

This dossier places a current debate alongside that effort: artificial intelligence. Written by expert researcher Gülşen Nişli on behalf of ANKA Gelecek ve Yenilik Derneği, it aims to be neither a celebration of technology nor a doom scenario. We have tried to explain how artificial intelligence touches civil society's security agenda, in the language of people working in the field and with the data at hand.

THIS DOSSIER AT A GLANCE	
F-01	**Shifting ground.** AI is no longer the exception; most organizations use it in some form, often without any written rule.
F-02	**Two sides of the coin.** The same technology lowers breach costs on defense and makes phishing cheaper and more convincing on attack.
F-03	**Civil society in the crosshairs.** Being small is not being invisible; the data held and the trust earned are values in their own right.
F-04	**Data protection as a promise.** Türkiye's KVKK and the European Union rules can be read as the legal form of respect owed to beneficiaries.
F-05	**Small steps.** Ten measures that ask for habits rather than budgets, and a self-assessment platform where organizations can test themselves.

RECORD: GROUND ASSESSMENT

78%

ORGANIZATIONS USING AI IN AT LEAST ONE BUSINESS FUNCTION IN 2024; 55% A YEAR EARLIER (STANFORD HAI, 2025)

88%

ORGANIZATIONS REPORTING AI USE IN MCKINSEY'S 2025 GLOBAL SURVEY

233

AI-RELATED INCIDENTS RECORDED IN 2024; ANNUAL INCREASE OVER 56% (STANFORD HAI, 2025)

FILE 01

Shifting ground: As AI stops being the exception

The hardest part of talking about artificial intelligence is not getting caught between hype and dismissal. At one end sits a tale of magic that will solve every problem; at the other, the label of a passing fad. The figures confirm neither; they say something calmer: this technology has settled into the way organizations do their daily work.

According to Stanford University's 2025 AI Index report, 78 percent of organizations used artificial intelligence in at least one business function in 2024; a year earlier that figure was 55 percent. McKinsey's 2025 global survey points to a similar picture, with a usage rate reaching 88 percent. This is not a declaration of revolution but an assessment of the ground: artificial intelligence is no longer an unusual choice but an ordinary tool.

Civil society is not outside this picture either. Between the first draft of a project report, the translation of a social media post, and the proofreading of an event text, artificial intelligence has long taken its place at many associations' desks. The problem is not the use itself; it is that the use often happens without a written rule, a shared judgment, or a security filter.

The same reports also record the other side of the coin: according to data compiled by Stanford, the number of AI-related incidents reported in 2024 reached 233, an increase of more than 56 percent over the previous year. As use spreads, the side effects become visible too. The next file looks at how these two trends, adoption and risk, grow at the same time in the field of security.

RECORD: TWO FRONTS

$4.88

MILLION: AVERAGE COST OF A DATA BREACH, A RECORD HIGH, UP 10% (IBM, 2024)

$2.2

MILLION: AVERAGE PER-BREACH SAVING FOR THOSE USING SECURITY AI AND AUTOMATION EXTENSIVELY (IBM, 2024)

60%

PARTICIPANTS DECEIVED BY FULLY AI-GENERATED PHISHING EMAILS (HEIDING ET AL., 2024)

FILE 02

Two sides of the coin: One technology, two fronts

Artificial intelligence has an odd property in cyber-security: it sits on both sides of the table. Defender and attacker draw from the same shelf. So the question is not whether AI is good or bad for security, but in whose hands and with what care it works.

On defense: noticing earlier, losing less

IBM's 2024 cost of a data breach study found that a breach cost organizations on average 4.88 million dollars, a 10 percent increase over the previous year and the highest level measured to that point. The study's less-discussed finding is this: organizations that used artificial intelligence and automation extensively in their security processes lost on average 2.2 million dollars less per breach, and detected and contained breaches in markedly less time. When set up correctly, the technology turns into an early-warning system that catches an incident before it grows.

On attack: phishing got cheaper and sharper

The same capabilities also work in malicious hands. In an experiment published in the Harvard Business Review in 2024 and run by researchers including Fredrik Heiding and Bruce Schneier, phishing emails generated entirely and automatically by AI deceived about 60 percent of participants, the same level as emails crafted by hand by human experts. Moreover, automating the process cuts the cost of a phishing campaign by more than 95 percent. A cheaper and more convincing attack means more attacks.

RECORD: CASE + HUMAN

68%

BREACHES INVOLVING A NON-MALICIOUS HUMAN ELEMENT (VERIZON, 2024)

<60s

MEDIAN TIME TO FALL FOR A PHISHING EMAIL (VERIZON, 2024)

$25

MILLION: SUM TRANSFERRED VIA A SINGLE DEEPFAKE VIDEO CALL (CNN, 2024)

CASE NOTE · FEBRUARY 2024 · HONG KONG

Everyone in the meeting was fake. A company's finance employee approved a transfer of about 25 million dollars on the instruction of the finance director seen in a video call. Every executive in the meeting was an imitation whose voice and image had been generated by AI; the company was later confirmed to be the international engineering firm Arup.

The lesson of the case is behavioral, not technical: image and sound can no longer count as proof of identity on their own. Requests for money or data, whatever the amount or urgency, should be verified through a second channel.

The human side completes the picture. According to Verizon's 2024 data breach investigations report, 68 percent of breaches involve a non-malicious human element: a wrong click, sending to the wrong recipient, a well-meaning reply to a fake request. The same report notes that the median time to fall for a phishing email is under one minute.

The 2024 threat landscape report of the European Union Agency for Cybersecurity, ENISA, confirms the same trend at an institutional scale: social engineering is on the rise, and AI-fed forms of information manipulation are now tracked as a separate heading. The target of an attack is often not the system but the person at its controls; so the first layer of defense is not technology but the habit of verification.

> Defender and attacker draw from the same shelf. The difference lies not in the technology, but in whose hands and with what care it works.

This two-front picture is not an abstract expert debate for civil society. That is exactly the subject of the next file: where do organizations with small budgets and valuable data stand in this equation?

RECORD: TARGET ANALYSIS

600M+

ATTACK ATTEMPTS FACED BY MICROSOFT CUSTOMERS EACH DAY (MICROSOFT, 2024)

MICROSOFT'S THREAT INTELLIGENCE RANKS THINK TANKS AND CIVIL SOCIETY ORGANIZATIONS AMONG THE SECTORS MOST TARGETED BY STATE-LINKED ACTORS.

FILE 03

Civil society in the crosshairs: Being small is not being invisible

There is a sentence often heard in civil society: what is there to steal from us? The answer cannot be found by looking in the safe, because that is not where to look. A youth association's archive holds identity photocopies, parental consent forms, health declarations, bank receipts, and contact lists of vulnerable groups. Each of these is a value in its own right to someone with bad intentions. So are the organization's name and trust: a fake donation appeal sent from a hijacked association account can spend, in minutes, the trust built over years.

Nor is there room for illusion about scale. Microsoft's 2024 Digital Defense Report notes that its customers face more than 600 million attack attempts each day; the same report notes that think tanks and civil society organizations are among the sectors most targeted by state-linked actors. Most attacks, however, single out no one in particular: automated scans find weak passwords and unpatched systems, whoever they belong to. The hand that tries the door does not read the name on the sign.

What also makes civil society fragile is its own way of working. Volunteers come and go; accounts are shared; work runs from personal phones and home computers; the domain and admin panel of a finished project are left exposed, assigned to no one. None of this is a fault; it is the reality of the field. But each is a door that can be closed with a small adjustment.

> Most attacks do not look at an organization's size; they look for an open door. Being small offers no protection; being orderly does.

RECORD: LEGAL FRAMEWORK

6698

TÜRKİYE'S PERSONAL DATA PROTECTION LAW (KVKK): ASSOCIATIONS ARE DATA CONTROLLERS TOO

72h

EXPECTED TIME TO NOTIFY THE AUTHORITY OF A DATA BREACH UNDER BOARD PRACTICE

2026

START OF MOST HIGH-RISK SYSTEM OBLIGATIONS UNDER THE EU AI ACT (AUGUST)

FILE 04

Data protection as a promise made

A young person's parental consent form is not merely a document; it is the signed form of a family's trust in the organization. Reading data protection law not as a burden but as the legal counterpart of that trust makes the work both easier and more meaningful. The rule is the written form of a duty of care.

In Türkiye the framework is drawn by the Personal Data Protection Law No. 6698, and associations are data controllers under this law. Its practical meaning can be summed up in a few sentences: tell people clearly why their data is being requested, use the data only for the stated purpose, never collect more than necessary, do not keep data once its purpose is served but erase it, and if a breach occurs, do not conceal it. Under Board practice, data breaches are expected to be notified to the Authority within 72 hours of becoming known. The soundest principle is the simplest: data you do not collect cannot leak.

The European dimension is not far off either. In Erasmus+ partnerships, participant lists, photographs and reports travel across borders, which naturally raises the matter of alignment with the European Union's data protection principles. In 2024 a further layer was added: the European Union Artificial Intelligence Act entered into force as Regulation (EU) 2024/1689 and graded AI systems according to the risk they carry. Prohibitions on unacceptable-risk practices took effect in February 2025 and obligations for general-purpose models in August 2025; most obligations for high-risk systems will, per the timetable, begin to apply in August 2026.

For civil society the message here is not memorizing legislation; it is knowing what the tool being used actually does, not letting go of human oversight, and being transparent. These three attitudes match the core of both the KVKK and the European framework, and they form the backbone of the steps in the next file.

RECORD: ACTION FORM

66%

EXECUTIVES WHO EXPECT AI TO HAVE THE BIGGEST IMPACT ON CYBER-SECURITY NEXT YEAR (WEF, 2025)

37%

ORGANIZATIONS WITH A PROCESS TO ASSESS AN AI TOOL'S SECURITY BEFORE DEPLOYMENT (WEF, 2025)

FILE 05

Small steps: What actually works in the field

The World Economic Forum's 2025 Global Cybersecurity Outlook sums up well the gap between awareness of the issue and institutional readiness: 66 percent of executives think artificial intelligence will have the biggest impact on cyber-security next year; yet only 37 percent of organizations have a process to assess an AI tool's security before deploying it. The awareness is there; the habit is not. This gap is exactly where SECURE-CS works.

None of the ten steps below requires expensive software; they all ask for decision, order and a little consistency. Even if the organization is a team of one, the list is the same. The boxes were left empty on purpose: this page is designed not to be read but to be ticked.

- ☐ 01 **Turn on multi-factor authentication everywhere.** Use a second verification step on all critical accounts, above all email, cloud storage, social media and banking; on its own this step defeats most account-takeover attempts.
- ☐ 02 **Switch to a password manager.** Remembering a separate, strong password for each account is not possible; a password manager turns this into an organizational habit and does away with shared passwords floating around on paper.
- ☐ 03 **Make updates automatic.** Turn on automatic updates for the operating system, browser and add-ons; most known vulnerabilities are exploited because they were left unpatched even though a fix had been available for months.
- ☐ 04 **Take backups and test the restore.** Keep more than one copy of important data, at least one on a different medium; once a year, actually restore it and see that it works, because an untested backup is no backup.
- ☐ 05 **Keep an account inventory and revoke access on departure.** Keep a single list of which account is held by whom and with what permissions; when a volunteer or staff member leaves, closing their access should be as natural a step as the farewell coffee.

RECORD: ACTION FORM

THE ONLINE COUNTERPART OF THIS FORM: TAKE YOUR ORGANIZATION'S DIGITAL SECURITY SNAPSHOT THROUGH THE PROJECT'S SELF-ASSESSMENT PLATFORM.

civilsociety security.net

- [ ] 06 **Verify money and data requests through a second channel.** Confirm transfer and information requests that arrive by email, message or video call by calling back a known number, ignoring the pressure of urgency; in an era when voice and image can be imitated, this one-sentence rule saves a great deal.

- [ ] 07 **Simplify permissions.** Rather than every permission for everyone, give each person only as much access as their work requires; close unused administrator accounts and shared sessions.

- [ ] 08 **Write a one-page rule on AI use.** Put in writing which information may and may not be entered into the tools, who reviews the output before it is published, and how AI assistance is to be indicated where needed; one page is enough.

- [ ] 09 **Have an incident plan ready.** When something goes wrong, keep on a single page who is to be called, which passwords are to be changed, and, if necessary, how a breach is to be reported; the moment of crisis is not the moment to write a plan.

- [ ] 10 **Test yourselves at regular intervals.** Security is not a one-off project but a habit of periodic review; an annual self-assessment keeps the picture up to date.

If you want to see what these steps look like in your own organization, you can take its snapshot through the project's digital security analysis platform at **civilsocietysecurity.net**. All project information and publications, including the curriculum and toolkit, are gathered on the project website at **civilsocietysecurity.com**; both outputs are open to the whole ecosystem.

RECORD:
CONCLUSION

6

PARTNER ORGANIZATIONS · TÜRKİYE, BELGIUM, NORWAY, BOSNIA AND HERZEGOVINA

2

CORE OUTPUTS: A DIGITAL-SECURITY CURRICULUM/TOOLKIT AND AN ONLINE ANALYSIS PLATFORM

2026

YEAR THE PROJECT WILL BE COMPLETED (30 JUNE)

CLOSING

In closing

In this dossier we have tried to describe an unrelenting technology without alarm. Because experience in the field says this: security is built by order, not by panic. Tools will change, models will be renewed, and today's talked-about threats will be replaced by others. What will not change is the fact that we hold people's data in trust, and the care owed to that trust.

The SECURE-CS partnership shows that this care can be learned and shared. Six organizations working in different countries and at different scales meet at the same conclusion: digital security is not a product but a habit acquired as a team. The curriculum, the toolkit and the self-assessment platform stand ready as the starting materials of that habit.

The rest begins at each organization's own desk: by setting up a password manager, by drawing up a permissions list, by making a verification phone call. Small steps, for exactly this reason, should not be underestimated.

> Technology changes; the care shown to a trust does not. Security is not a product but a habit acquired as a team.

ANNEX · A

References

CNN. (2024, February 4). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'.* https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

European Commission. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024.* ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Heiding, F., Schneier, B., & Vishwanath, A. (2024, May 30). *AI will increase the quantity - and quality - of phishing scams.* Harvard Business Review. https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

IBM. (2024). *Cost of a data breach report 2024.* IBM Security. https://www.ibm.com/reports/data-breach

Personal Data Protection Law, Law No. 6698. (2016, April 7). *Official Gazette* (No. 29677). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

McKinsey & Company. (2025). *The state of AI: How organizations are rewiring to capture value.* QuantumBlack, AI by McKinsey. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

Microsoft. (2024). *Microsoft digital defense report 2024.* Microsoft Security. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Stanford University, Institute for Human-Centered Artificial Intelligence. (2025). *Artificial intelligence index report 2025.* Stanford HAI. https://hai.stanford.edu/ai-index

Verizon. (2024). *2024 data breach investigations report.* Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum. (2025). *Global cybersecurity outlook 2025.* WEF. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

ANNEX · B

Project Details

PUBLICATION TITLE

Civil Society and Digital Security in the Age of AI: A field dossier on information and data security

PUBLICATION TYPE

Project dissemination publication / field dossier

PROGRAMME / ACTION

Erasmus+ · KA220-YOU (Cooperation Partnerships in Youth)

PROJECT REFERENCE NO

2023-1-TR01-KA220-YOU-000161230

GRANT MODEL

Lump Sum · €250,000.00

PROJECT DURATION

01.12.2023 - 30.06.2026

PROJECT WEBSITE / ANALYSIS PLATFORM

civilsocietysecurity.com · civilsocietysecurity.net

COORDINATOR

SETA - Foundation for Political, Economic and Social Research (Türkiye)

PLACE AND DATE / LANGUAGE

Istanbul, December 2025 · English

PREPARED BY

Gülşen Nişli · Expert Researcher, on behalf of ANKA Gelecek ve Yenilik Derneği (Project Partner)

ROLE OF ANKA

Project Partner

PARTNERS

BRAVO - Bosnian Representative Association for Valuable Opportunities (Bosnia and Herzegovina) · TtB (Norway) · SETA Foundation for Political, Economic and Social Research (Belgium) · Türkiye Youth Foundation - TÜGVA (Türkiye) · ANKA Gelecek ve Yenilik Derneği (Türkiye)

SUGGESTED CITATION · APA 7

Nişli, G. (2025). *Civil society and digital security in the age of AI: A field dossier on information and data security* [Project publication]. SECURE-CS: Civil Society Initiatives Strengthened with Information and Data Security (Erasmus+ Project No. 2023-1-TR01-KA220-YOU-000161230). ANKA Gelecek ve Yenilik Derneği.

DISCLAIMER

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 or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

OPEN TO THE WHOLE ECOSYSTEM
SECURE-CS · 2025