The Responsible Security Association

ICoCA

ENSURING RESPONSIBLE SECURITY IN THE DIGITAL AGE

The application of the International Code of Conduct for Private Security Service Providers to Advanced Technologies

Policy Brief

The Responsible Security Association

ENSURING RESPONSIBLE SECURITY IN THE DIGITAL AGE

The application of the International Code of Conduct for Private Security Service Providers to Advanced Technologies

Policy Brief

CONTENTS

INTRODUCTION 6

PART ONE: How does the Code apply to advanced technologies? 8

PART TWO: How does technology transform private security? 10

PART THREE: Which technologies do private security providers use? 12

PART FOUR: What are the main challenges for human rights and international humanitarian law? 14

CONCLUSION 20

ACKNOWLEDGEMENTS 23

About ICoCA

ICoCA, the Responsible Security Association, is the leading international organisation committed to improving human rights standards in the private security industry. ICoCA's mission is to promote responsible, transparent and accountable private security practices worldwide that respect human rights, international humanitarian law and the rule of law, safeguarding communities through robust oversight, collaboration and capacity building.

The Association serves as the governance and oversight body for the International Code of Conduct for Private Security Service Providers (the "Code"), which articulates the responsibilities of private security companies to raise private security standards, particularly in complex environments. ICoCA's work is grounded in international frameworks, including the UN Guiding Principles on Business and Human Rights, international humanitarian law and the Montreux Document. It supports the 2030 Sustainable Development Goals, particularly Goal 16 (peace, justice and strong institutions) and Goals 5, 8 and 10 (human rights and labour standards).

With a global and diverse membership of governments, civil society organisations, private security providers and their clients, ICoCA mitigates risks associated with poor security practices in global supply chains and environments where abuses may occur.

ICoCA and the Responsible Use of Technologies

The responsible use of technologies in private security is one of ICoCA's key strategic priorities. The aim of this workstream is to provide guidance on the responsible use of technologies for private security providers, tech companies and users of private security, with an emphasis on human rights protection. It will also contribute to a review of the current governance mechanisms and norms regulating private security, considering the transformation of the industry and the technological, legal and political environment in which it operates.

In recent years, ICoCA has organised several consultations with experts on this issue. It partnered with ICT4Peace, a Geneva based think tank, to conduct a mapping study on the use of information and communications technologies (ICTs) in security services provided by commercial technology and security providers, and to produce a Toolkit for companies on the responsible use of these technologies in the security field, drawing on broad consultation across the sector.

This policy brief summarises a longer report based on research and field missions conducted by ICoCA and ICT4Peace, as well as a series of interviews and workshops held in 2024 with over 50 experts, private security companies (PSCs) and civil society organisations, focusing on the challenges and best practices in the use of advanced technologies. The recommendations were discussed at a consultative workshop with 20 experts in Geneva on 26 March 2025.

The research and workshop were made possible by grants from the Swiss Federal Department of Foreign Affairs and the UK Foreign, Commonwealth and Development Office.

INTRODUCTION

This policy brief takes stock of the transformative changes reshaping the private security industry, driven by the integration of advanced technologies. This transformation calls for a review of the governance and regulation of private security in the digital era.

These technologies are revolutionising the scope and methods of private security companies (PSCs), enabling them to expand from traditional physical "boots on the ground" services to digital intelligence operations and cybersecurity. Concurrently, tech companies are entering the security sector, further blurring the lines between physical and virtual security services. This evolution presents both opportunities for improved security services and significant challenges, particularly regarding human rights and legal compliance in complex and poorly regulated environments.

The use of technologies such as AI-enhanced surveillance systems, drones and open-source intelligence platforms by PSCs raises critical ethical, legal, human rights and international humanitarian law (IHL) concerns. In contexts such as conflict zones, border management or law enforcement, these technologies have been used to track individuals, collect sensitive data and support operations that mirror state-level intelligence activities. They are also widely used for policing, monitoring employees at the workplace or guarding private properties. Such practices risk infringing on privacy and other civil and political rights, enabling arbitrary detention, curtailing workers rights or exacerbating existing inequalities.

According to ICoCA field observations and research, the sector is largely unaware of the human rights and IHL risks posed by using technologies. Even worse, most PSCs lack both the ability and the knowledge to responsibly engage in the use of advanced technologies, especially in the acquisition and management of substantial amounts of data, where legal requirements can be unclear.

The International Code of Conduct for Private Security Service Providers (the Code), developed to regulate PSCs' activities, applies to the use of technologies. The operations of PSCs, such as surveillance or intelligence, are covered broadly in both the spirit and commitments of the Code, notwithstanding the means and methods they use to provide these services. However, the Code had not yet been interpreted with tech in mind. Recognising this need, the International Code of Conduct Association (ICoCA), in partnership with ICT4Peace, has recently developed a Toolkit[1] for the responsible use of technology in the private security sector, guiding PSCs in the responsible use of technology while ensuring compliance with regulatory and human rights standards. The Toolkit provides practical guidance for PSCs to align their use of technology with international legal frameworks, offering tools to mitigate risks and promote ethical practices.

This policy brief explores four key areas. After restating the relevance and clarifying the application of the Code to the use of advanced tech, it examines the shift from traditional guarding services to technology-driven security operations and the transformation of the sector with tech companies entering the market. It highlights some of the key challenges posed by advanced surveillance technologies and the collaboration between private security providers and states, including violations of privacy, data misuse and potential abuses in conflict and law enforcement contexts.

Adapting the regulation and governance of private security to the digital age also represents a challenge for ICoCA. Significant efforts will be needed in the coming years to disseminate the Toolkit, strengthen oversight mechanisms, review the Code and reach out to new actors in security with a view to safeguarding human rights in the era of digital security. The final part of the brief discusses the question of the implementation of the Code to new technological realities, emphasising the need for interpretation, clarification and regulatory updates to address the industry's evolving landscape.

1. The Toolkit is available at: https://icoca.ch/2024/11/11/toolkit-launch-responsible-technology-use-by-the-private-security-sector/

PART ONE

How does the Code apply to advanced technologies?

Operations by PSCs can pose significant risks for the respect of human rights and IHL, especially when they occur in a context of diminished accountability and oversight. When states outsource security functions such as surveillance to PSCs, it creates a grey area in which legal responsibilities can become diluted, leading to potential human rights or IHL abuses.

To address these challenges, all stakeholders — PSCs, technology companies, regulators and civil society — must navigate this evolving landscape, develop a deeper understanding of technology's use in private security and clearly define the legal and ethical boundaries. While PSCs must comply with existing regulations, including strict data protection laws that carry severe sanctions for breaches, the varying regulatory environments and uncertainties in cross-border operations further complicate compliance.

How does the Code define security services?

The Code does list a series of services that fall under its scope.[2] Amongst them, the category that is most relevant to the use of technologies in private security is surveillance services, understood to be an instance of "operational and logistical support for armed or security forces". However, the Code also states that the list of security services it applies to "includes but is not limited" to the ones it mentions. Indeed, since the Code explicitly prescribes that "Member and Affiliate Companies will comply, and will require their Personnel to comply, with applicable law which may include international humanitarian law and human rights law as imposed upon them by applicable national law, as well as all other applicable international and national law" (Art. 21), technological security services that are deemed to fall within IHL's scope, such as cybersecurity services,[3] are also subjected to the Code's provisions.

In which situations does the Code apply?

Article 13 specifies that the Code "articulates principles applicable to the actions and operations of Member and Affiliate Companies while performing Security Services — including when operating in complex and otherwise high risk, unstable or fragile environments — where there is a risk of human rights abuses and/or violations of international humanitarian law and/or civilian harm".

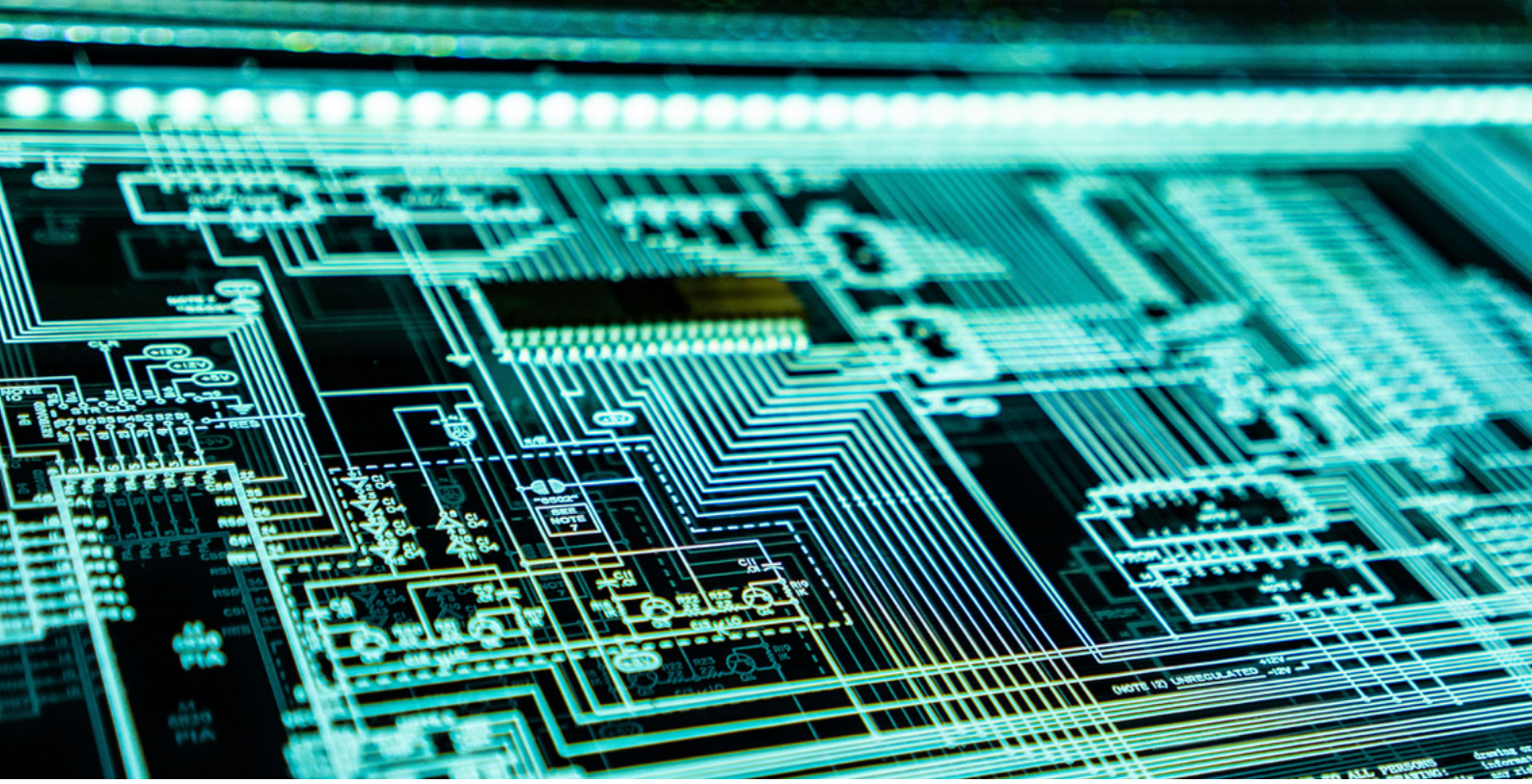
In complex environments,[4] the need for clear-cut definitions, common standards and evidence-based recommendations is even more urgent, as they are often characterised by a lack of regulation and/or limited oversight over the use of technologies in the provision of security services.

That is why the Code and the Toolkit can become important tools to provide guidance on how to operationalise human rights in the field of technological security services, supporting security providers, their clients and regulators in the effort to prevent human rights abuses. The Code requires Member states and companies to conduct comprehensive assessments to identify, prevent and mitigate potential human rights impacts linked to PSC operations.

2. International Code of Code for Private Security Service Providers, Section B, "Definitions", available at: https://icoca.ch/the-code/

3. The International Committee of the Red Cross has concluded that, as with "traditional" methods of conventional warfare and security services, cybersecurity services must comply with IHL and therefore falls within the scope of the Code, even though it is not specifically listed in it. (International Committee of the Red Cross, "International humanitarian law and cyber operations during armed conflicts", ICRC position paper, November 2019, available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts)

4. Section B of the Code provides the following definition of complex environments: "any areas experiencing or recovering from unrest or instability, whether due to natural disasters or armed conflicts, where the rule of law has been substantially undermined, and in which the capacity of the state authority to handle the situation is diminished, limited, or non-existent."



To which type of companies does the Code apply?

While they may not consider themselves to be PSCs, an increasing number of technology companies are delivering private security services. Pursuant to Article 1 of the Code, the Code applies to both "Private Security Companies and other Private Security Service Providers". Section B of the Code defines Private Security Companies and Private Security Service Providers (collectively "PSCs") as "any company (as defined in this Code) whose business activities include the provision of Security Services either on its own behalf or on behalf of another, irrespective of how such company describes itself".

Thus, tech companies providing security services such as intelligence, cybersecurity or surveillance do fall under the definition of PSCs established by the Code.

What are the legal obligations of security providers?

Article 4 of the Code underlines that Member and Affiliate companies have a responsibility to respect the human rights of all those affected by their business activities (personnel, clients, suppliers, shareholders, affected populations).

While ICT and technological tools can enhance companies' operational efficiency, they also pose significant challenges to fundamental rights, especially the rights to privacy, freedom of expression and self-determination; risks that are often exacerbated for marginalised groups.

To mitigate these risks, Article 21 of the Code emphasises that Member and Affiliate companies must exercise due diligence to ensure compliance with the law and the Code's principles, being particularly careful as to respect human rights, especially those that could be violated through the use of surveillance technologies. To mitigate these risks, PSC's must align with the principles of the Code, focusing on its overarching goals rather than interpreting it strictly. This approach could encourage them to implement policies like 'transparent data governance' even if this is not explicitly outlined in the Code. The Code does not only specify obligations for PSCs, but it also provides a framework for oversight and accountability. Administered by ICoCA, the Code requires authorisation, licensing, vetting and training, as well as monitoring and accountability. ICoCA conducts due diligence on its Members and Affiliates, monitoring their activities, certifying their operations, providing guidance and handling complaints. It regularly produces new training materials for security personnel, contributing to the prevention of abuses.

Furthermore, Article 25 states that: "Member and Affiliate Companies will take reasonable steps to ensure that the goods and services they provide are not used to violate human rights law or international humanitarian law, and such goods and services are not derived from such violations." This provision could apply to the collection of personal data in the context of surveillance operations. PSCs must ensure that such data is not used by their clients to commit violations of the law.

PART TWO

How does technology transform private security?

> *"Clients of security are now demanding technological solutions, so the market adapts."*
>
> **Private security expert, UK**

This section of the policy brief presents some of the main trends in the transformation of the sector.

A fast-developing trend: the case of ICoCA Member companies

> *In 2024, 100% of ICoCA Member and Affiliate companies advertise providing at least one ICT-based service. They were only 68.5% just two years before.*[5]

PSCs are increasingly using advanced technologies to supplement their traditional services: ICoCA Affiliate and Member companies (i.e. Affiliates, Transitional Members and Certified Members) have noted a significant increase in the use of ICTs in the provision of security services over the past 5-7 years, with the Covid-19 pandemic accelerating this shift. They also report that, according to their projections, this trend will continue in the coming years. Surveillance and remote monitoring dominate, with nearly 70% of 64 Certified companies advertising these services. Cybersecurity offerings have also grown, from 10 companies in 2022 to 25 in 2024. Interviews reveal that PSCs are adopting autonomous solutions, predictive analytics and advanced cybersecurity.

Categories of commercial security services using ICTs provided by PSCs

- Video Surveillance and Monitoring
- Industrial Control Systems / Supervisory Control and Data Acquisition (ICS/SCADA)
- Location Tracking
- Drones
- Access Control
- Security Apps
- Intelligence Services
- Automotive Cybersecurity
- Health Care Security
- Cybersecurity Services
- Threat Assessment Services
- Robots
- Surveillance Tech
- Data Analytics

5. Anne-Marie Buzatu, "From Boots On The Ground To Bytes In Cyberspace: A Mapping Study On The Use Of Information Communications technologies (ICTs) In Security Services Provided By Commercial Actors", ICT4Peace, Geneva 2022, available at: https://ict4peace.org/activities/from-boots-on-the-ground-to-bytes-in-cyberspace-a-mapping-study-of-the-use-of-icts-in-private-security-services-provided-by-private-commercial-actors/

An uneven deployment

Adoption varies by region due to factors like costs infrastructure and workforce readiness. In countries with limited digital infrastructure, adoption is slower.

Uberisation of the security sector

Mobile apps now enable an uberisation process of the security sector. On-demand security services connect users with PSCs or private ambulances, offering flexibility and responsiveness.

Working conditions of security personnel

The impact on security personnel is multifaceted. First, security workers fear displacement by automation, such as cameras and robots. Traditional security personnel risk job loss due to their replacement by technology but also insufficient education or digital skills. Advanced training in Artificial Intelligence (AI), cybersecurity and digital literacy is increasingly critical for the evolving demands of the industry. However, positive impacts on efficiency and safety improvement can be noted as AI, sensors and remote tools reduce risks to personnel. Payment apps and similar technologies improve transparency, address salary disputes and ensure that social security are paid.[6] Also, body cameras and other tech help prevent misconduct and improve accountability. Tech integration promotes professionalisation[7] and diversity by creating less physically demanding roles.

The interface between technology and humans and its impact on compliance

The integration of technology in private security can enhance accountability and help prevent abuse — such as through the use of body cameras. However, its potential is often idealised, leading companies to underestimate associated risks. Technologies like remote surveillance and security robots can dehumanise interactions, reduce empathy and undermine ethical behavior. They may also contribute to data breaches, especially in an industry where poor working conditions can lead to insider threats. Replacing human personnel with machines reduces valuable human intelligence and weakens community engagement, which is essential for conflict prevention and trust-building. Ultimately, over-reliance on technology may lower the quality of services and harm the legitimacy and social value of PSCs.

PSCs emphasise that human interaction remains essential for effective security services and recognise that remote surveillance can reduce empathy and moral accountability by fostering physical and moral distance, as well as bureaucratising security provision.

Tech companies providing security services

Beyond traditional “boots on the ground” private security companies, technology companies also offer security products and services such as surveillance systems and open-source intelligence (OSINT) tools. Examples include SpaceX providing intelligence and Palantir using AI-enhanced analytics. OSINT applications are diverse, supporting tasks like threat detection, evidence gathering and disaster response.

Integration of private and public security

Governments rely more on private sector technologies and services (e.g., intelligence, telecommunications) through collaborative models. Partnerships between police and PSCs are fast developing. Integration of tech into security and data sharing between public and private entities contributes to blur the civil-public boundaries in the field of intelligence, law enforcement and national security. It raises issues of transparency and accountability. Examples include retailers funding biometric police operations, shared citywide CCTV networks for crime detection, or the usage of “mercenary spyware”.[8]

6. See ICoCA’s surveys on working conditions in East Africa available at: https://icoca.ch/working-conditions
7. ICoCA, “When the abused becomes the abuser: Poor working conditions in the private security industry undermine human rights compliance”, 2023, available at: https://icoca.ch/working-conditions/
8. Mercenary spyware is software that can read information and communications on smartphones and avoids security features such as end-to-end encryption by accessing the data before it is encrypted.

PART THREE

Which technologies do private security providers use?

Surveillance, monitoring technology & AI

The private security industry has long relied on surveillance and monitoring technologies like CCTV or pressure sensors. Recent advancements have transformed these tools into sophisticated systems with extended capabilities, including long-range body-thermal imaging, facial and biometric recognition, even mask recognition, particularly used in post-pandemic contexts. These technologies are often AI-integrated, enabling demographic profiling, predictive policing and real-time notifications for retail security. Concerns around privacy and algorithmic biases, especially with the capacity to identify ethnic features through facial recognition, highlight the ethical complexities of their use.

Drones & Robotics

Drones, unmanned aerial vehicles (UAVs) and unmanned marine vehicles (UMVs) enhance surveillance efficacy, reducing reliance on human personnel and reaching vast, inaccessible areas. PSCs and other technology companies may be involved in the operations of drones, lethal and non-lethal, on behalf of states. They can be contracted to operate drones and process surveillance data for border surveillance for instance.

The use of robotics, distinct from drones, is another technology that may offer significant potential for PSCs.[9] It offers capabilities like patrolling, intrusion detection and real-time data transmission. While adoption is limited and its effectiveness debated, costs are decreasing, driving growth. Robots, such as those used in Singapore for traffic control and patrolling, complement human guards by enhancing surveillance and deterrence. Companies like Ascento are pioneering AI-enabled robots for large-scale facility security.

Drones and other security robots represent a massive growth area for the use of technology by PSCs. As part of the 2023 World Security Report produced by Allied Universal, 1,775 chief security officers (CSOs) — or those in equivalent positions — were asked what technologies they plan to utilise (either by investing internally or outsourcing to a security vendor) over the next five years. Among them, 24% said they plan to increasingly

9. "Automated Security Robots (ASR) are autonomous machines (ground-based or flying) that are primarily used to enhance the safety and security of various spaces through surveillance and monitoring. They combine self-navigation with visual and thermal imaging to collect and analyse data while patrolling indoor and outdoor spaces. The data goes back to a central control hub in real-time which uses artificial intelligence to assess and report any credible threats or safety risks." https://sasasurveillance.com/why-automated-security-robots-are-the-next-big-thing/

utilise drones and 29% said they plan to increasingly utilise security robots over the next five years to improve their physical and cyber security operations.

AI & Machine Learning Integration

AI is revolutionising private security by automating surveillance, supporting decision-making, enhancing predictive security operations and supporting technologies like drones and robots. Predictive policing analyses data to identify high-risk locations or individuals, improving crime prevention and response time.

As part of the 2023 World Security Report produced by Allied Universal, 65% of the CSOs said their company currently uses predictive technology to enhance security and they intend to increase its use over the next 12 months. 42% said they plan to utilise various AI-powered systems over the next five years to improve their physical and cyber security operations.

While AI adoption brings efficiency and cost benefits, it also raises risks, including potential biases and misuse, especially in conflict-affected areas. The EU AI Act (2024) bans certain AI systems, including those relying solely on profiling to predict criminal behaviour. The restrictions highlight the need to adapt frameworks like the Code or the Montreux Documents to address AI's growing role in private security.

Cybersecurity

Cybersecurity is driven by the increasing reliance on ICT and digital information, alongside vulnerabilities from remote work and digital operations. This has expanded security concerns from physical threats to cyber incidents like phishing or ransomware. Notably, 88% of CSOs surveyed in 2023 ranked cybersecurity as a greater concern than physical security. Services such as incident responses and digital forensics are key offerings, helping clients address breaches and identify attackers. For example, the rise of "Ransomware as a Service" (RaaS) — responsible for 20% of cybercrime — presents opportunities for PSCs to assist clients in protecting sensitive commercial data.

Moreover, PSCs themselves increasingly handle vast amounts of sensitive data through advanced surveillance and biometric technologies, necessitating robust cybersecurity measures to ensure data integrity and privacy.

PART FOUR

What are the main challenges for human rights and international humanitarian law?

ICT4Peace and ICoCA developed a Toolkit to address the legal and ethical challenges posed by technology use in private security. Building on the Code, the Toolkit provides actionable recommendations to help PSCs translate human rights obligations into practical actions. By implementing these best practices, companies can navigate the complexities of technology, mitigate risks and strengthen compliance with legal and democratic governance standards.

The ICoCA & ICT4Peace Toolkit on the Responsible Use of Technology in Private Security

This Toolkit serves as a go-to resource for private security companies (PSCs) of all sizes, helping them navigate the evolving technology landscape, including information and communication technologies (ICTs), and their impacts on human rights. Designed for a wide range of PSC stakeholders, from security professionals and managers to human rights officers, compliance teams, technology teams and government and civil society groups, it empowers PSCs to use technology responsibly, ethically and with respect for human rights.

The Toolkit consists of 12 interconnected but independent tools, each addressing a specific aspect of technology use in the private security industry:

- **Tool 1:** Human Rights Challenges Posed by ICTs in Private Security Companies
- **Tool 2:** Responsible Data Collection Practices
- **Tool 3:** Best Practices for Data Storage
- **Tool 4:** Best Practices for Data Security
- **Tool 5:** Best Practices for Data Destruction
- **Tool 6:** Surveillance and Monitoring
- **Tool 7:** The Challenge of Algorithmic Bias in Private Security
- **Tool 8:** Emerging Technologies and Future Trends in Private Security
- **Tool 9:** Accountability and Transparency
- **Tool 10:** Freedom of Expression
- **Tool 11:** Labour Rights in the Digital Age
- **Tool 12:** Right to Remedy and Effective Grievance Mechanisms

The Toolkit provides PSCs with practical guidance drawing on key principles and standards, including the Code, the Voluntary Principles on Security and Human Rights (VPs), the United Nations Guiding Principles on Business and Human Rights (UNGPs), the European Union General Data Protection Regulation (GDPR) and other relevant data protection laws.

Surveillance and the right to privacy

The U.S. Department of Defense defines surveillance as the "systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means".[10] While state authorities justify surveillance for law enforcement, border control and counterterrorism, the growing use of mass surveillance technologies — including CCTV, drones, metadata tracking and AI tools — raises significant concerns about privacy, political freedom and democratic integrity.[11] Outsourcing surveillance to PSCs reduces state accountability and heightens the risk of human rights violations, as these entities operate with limited oversight and often without adequate transparency or regulation.

Scandals such as PRISM and Pegasus spyware have highlighted state surveillance abuses, but the role of PSCs remains underexamined. States increasingly outsource surveillance to PSCs, delegating responsibilities without ensuring accountability. These companies often operate with limited oversight, conducting activities for governments, businesses or individuals, which raises serious human rights concerns.

Private sector involvement in surveillance is not new. Reports from the 1970s to today document the global trade in surveillance tools. However, modern technologies like facial recognition, drones and AI-powered systems amplify the scale and depth of surveillance. These tools allow for mass data collection without consent, infringing on privacy and enabling misuse. Predictive policing and spyware like Pegasus exacerbate discrimination and suppression of dissent, targeting journalists and activists.

Surveillance undermines privacy, as guaranteed under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and fosters self-censorship, restricting political expression and participation. The misuse of biometric data, location tracking and large-scale analytics compound these threats, enabling discrimination, profiling and data breaches.

International frameworks like the UN Guiding Principles on Business and Human Rights, along with the Code, emphasise the obligation to uphold privacy and freedom of expression. However, unchecked surveillance jeopardises these rights and threatens democratic governance.

In recent years, states have increasingly contracted private security providers in the provision of security services in relation with migration, both in terms of physical (management of camps and borders) and digital security (surveillance).[12] The recent ICoCA report "Securing Dignity: The imperatives of responsible security in migration surveillance and detention"[13] highlights the risk of human rights violations when PSCs are involved in migration and border management and specifically mentioned the risks associated with the use of technologies.

Governments increasingly contract PSCs for migration management, framing it as a security issue rather than a humanitarian one. This approach often relies on advanced technologies, promoting militarised solutions. PSCs, while not directly responsible, may be complicit in human rights violations by enabling and reinforcing these practices. Surveillance technologies, intended to protect migrants, often push them into riskier routes to avoid detection. Externalisation policies shift border control to transit countries, undermining obligations like non-refoulement and asylum rights. For example, Frontex contracts with PSCs to operate drones in the Mediterranean, sharing footage with the Libyan Coast Guard, which forcibly returns migrants to Libya, where they face detention and abuse. The European refugee crisis exemplifies a high-risk context under the UNGPs. This means that PSCs involved in this situation are under heightened human rights obligations when implementing the UNGPs.[14]

10. DOD Dictionary of Military and Associated Terms, 2021, available at: https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf
11. A recent report on private surveillance by the Geneva Center for Security Sector Governance and Transparency International states that "Private surveillance for security and/or military purposes is conducted by a wide range of actors beyond the classical security sector, including private investigators, software developers and communication operators. Such technology has a significant impact on human rights." Geneva Center for Security Sector Governance, Transparency International, "Understanding private surveillance providers and technologies within the wider framework of private security governance", 2024, p. 11, available at: https://www.dcaf.ch/understanding-private-surveillance-providers-and-technologies
12. A recent report by the Business & Human Rights Resource Centre stated that surveillance technology companies are "deeply implicated" in human rights abuses against migrants across the Middle East and North Africa (MENA). "Scrutinising Migration Surveillance, human rights responsibilities of tech companies operating in MENA", 2022, available at: https://media.business-humanrights.org/media/documents/2022_Scrutinising_border_surveillance_in_MENA.pdf
13. ICoCA, "Securing Dignity: The imperatives of responsible security in migration surveillance and detention", 2024, available at: https://icoca.ch/migration/. See also the UN Working Groups on Mercenaries report A/HRC/45/9, 2020, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/175/79/PDF/G2017579.pdf?OpenElement
14. United Nations Human Rights Office of the High Commissioner, "Guiding principles on business and human rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", 2011, available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

Recommendations on surveillance

ICoCA-ICT4Peace Guidance

Proportional Surveillance: Ensure that all surveillance activities are necessary and proportionate to the specific security objectives, avoiding excessive monitoring that infringes on personal privacy or freedom.

Data Minimisation and Retention: Collect only the data required for security purposes and implement clear policies on data retention and deletion to prevent the accumulation of unnecessary or outdated data.

Transparency and Communication: Clearly inform individuals about the use of surveillance through signage or notifications to foster transparency and trust.

Regular Audits and Oversight: Conduct periodic reviews and audits of surveillance systems to ensure they comply with human rights standards and remain effective in meeting security goals. Establish both internal and external oversight mechanisms.

Privacy-Enhancing Technologies: Use technologies that include privacy safeguards, such as anonymisation or pseudonymisation, to limit the risk of misuse or abuse of surveillance data.

Strong Data Governance: Develop robust data governance frameworks that outline how surveillance data will be collected, stored, accessed and deleted, with clear access control measures to prevent unauthorised access.

Human Rights Impact Assessments: Regularly conduct impact assessments to evaluate how surveillance practices affect individual rights and adjust practices as necessary to minimise negative impacts.

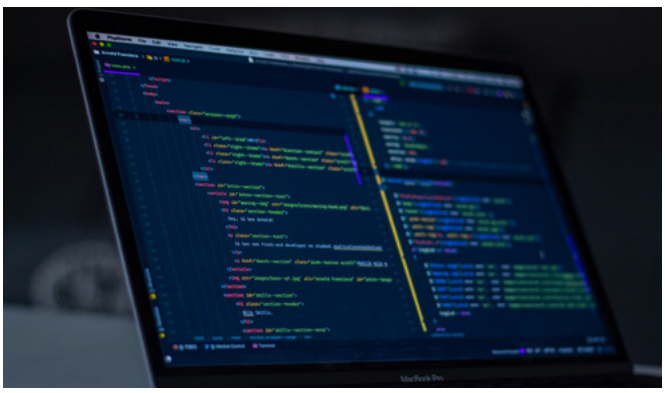
Training and Awareness: Ensure that all personnel involved in surveillance activities are trained on the ethical use of these technologies and understand the importance of balancing security needs with privacy rights.

Stakeholder Engagement: Engage with governance mechanisms such as ICoCA and affected stakeholders, such as clients, employees and communities, to address concerns and ensure surveillance practices are accepted and understood.

Algorithmic bias and the right to non-discrimination

Surveillance technologies risk perpetuating discrimination against marginalised groups, including within private security personnel. AI algorithms trained on biased data can disproportionately target racial or ethnic groups, exacerbating systemic inequalities. This concern is amplified when security providers perform law enforcement duties, as biased AI may lead to unfair treatment, racial profiling and infringements on privacy and due process rights. For example, the Pegasus project in the UK, which used facial recognition to combat shoplifting, drew criticism for its potential to misidentify people of color, women and LGBTQ+ individuals. Human rights groups argued that this could lead to invasive policing and harassment, urging companies to withdraw from the initiative.

Predictive policing algorithms also face transparency and accountability challenges, raising concerns about racial profiling and bias. The privatisation of public safety further complicates oversight of these technologies. The Code prohibits discrimination on any grounds, requiring equitable hiring and operational practices in its Article 42. The Toolkit provides PSCs with actionable guidance to ensure AI integration aligns with human rights and legal standards, addressing algorithmic biases.



Recommendations on algorithmic bias

ICoCA-ICT4Peace Guidance

Anti-bias Training: Implement ongoing training programmes to educate all relevant personnel on algorithmic bias, its impact on security operations and how to detect and mitigate bias in AI systems.

Diverse Data Training: Ensure that AI systems are trained on diverse, representative data sets to avoid biases that disproportionately affect certain groups based on race, gender or other characteristics.

Bias Audits and Continuous Monitoring: Regularly conduct audits of AI systems to identify and address potential biases. Implement continuous monitoring to catch emerging biases as systems are updated or retrained.

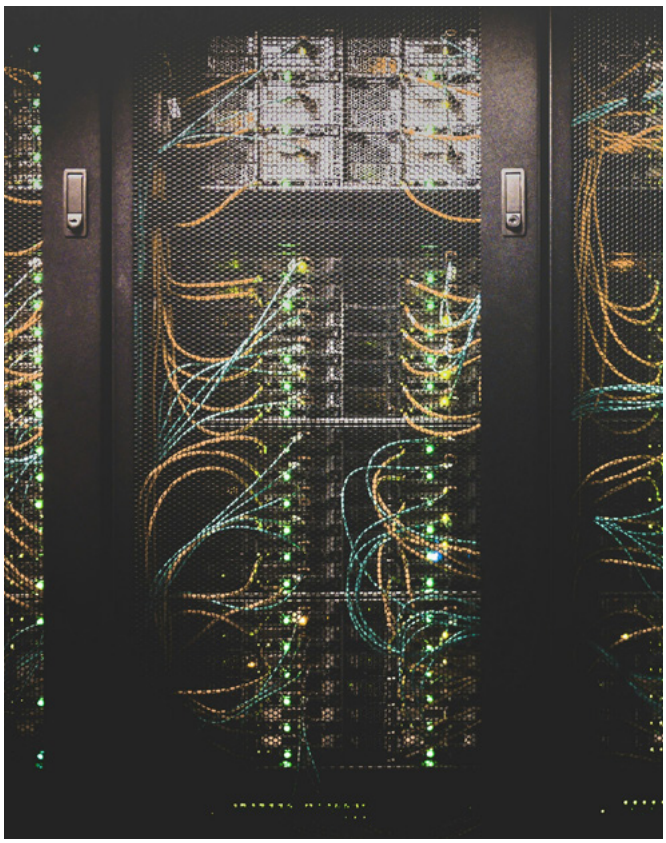
Transparency in AI Use: Provide clear and accessible information about how AI systems are used in security operations, including potential risks of bias. Engage with stakeholders, including employees and affected communities, to foster transparency and trust.

Human Oversight: Maintain human oversight in critical AI-driven decisions to ensure accountability and mitigate potential harms caused by biased outcomes. Clearly define roles for those responsible for reviewing AI decisions.

Ethical Framework for AI Deployment: Develop and implement a comprehensive ethical framework for AI use, aligned with human rights principles and international standards. This should include fairness constraints in AI algorithm design and policies for addressing identified biases.

Stakeholder Engagement: Engage with government mechanisms such as ICoCA and stakeholders, including clients, employees and communities, to ensure AI systems are aligned with their values and concerns and that bias mitigation efforts are inclusive.

Data protection and the right to be forgotten



As PSCs increasingly adopt technology, they manage sensitive information obtained through surveillance and from internal records, including data on staff, operations and clients. The ethical management of this data — its storage, use and deletion — remains a critical human rights concern requiring strict regulation and oversight. The "right to be forgotten," as enshrined in the EU GDPR, is essential to protecting human rights, including freedom of expression. PSCs must ensure compliance with legal standards to prevent misuse by clients, state authorities or third parties.

Experts highlighted concerns over data mining in weak regulatory environments, particularly in conflict zones, where the risk of human rights violations is higher without proper corporate due diligence. These insights reinforce the need for transparency and accountability in PSCs' handling of large-scale data and biometric collection, given the significant implications for individual rights.

Many national jurisdictions are addressing data protection by enacting regulations focused on principles such as purpose limitation, fairness, transparency and accountability. The EU

GDPR, which applies to companies worldwide processing data of EU individuals, is a key example. Cross-border data flows also present challenges for PSCs. Operating in complex environments can expose sensitive information to repressive actors, and jurisdictions like the EU prohibit data transfers to countries lacking adequate data protection standards, complicating PSC operations.

Without effective oversight, sensitive data may be exploited for unethical purposes, contributing to mass surveillance or repressive government actions. Prioritising human rights in data protection strategies is essential for safeguarding individual liberties.

To address these concerns, PSCs should adopt guidelines that prioritise ethical data management, as outlined in the ICoCA-ICT4Peace Toolkit.

Recommendations on data protection

ICoCA-ICT4Peace Guidance

Privacy by Design: Embed privacy considerations into data systems from the beginning and conduct regular privacy impact assessments and audits.

Data Minimisation: Collect only necessary data and establish clear data retention schedules to delete data when no longer needed.

Purpose Limitation: Use data solely for the purposes specified during collection and implement technical safeguards to prevent misuse.

Informed Consent: Ensure individuals give clear consent for data collection and provide easy options to withdraw consent or to access personal data.

Data Security: Apply robust security measures, including encryption, to protect sensitive data throughout its lifecycle.

Cross-border Compliance: Ensure data transfers comply with local laws, supported by data transfer agreements and impact assessments.

Data Governance: Establish clear governance structures with dedicated privacy officers to oversee compliance.

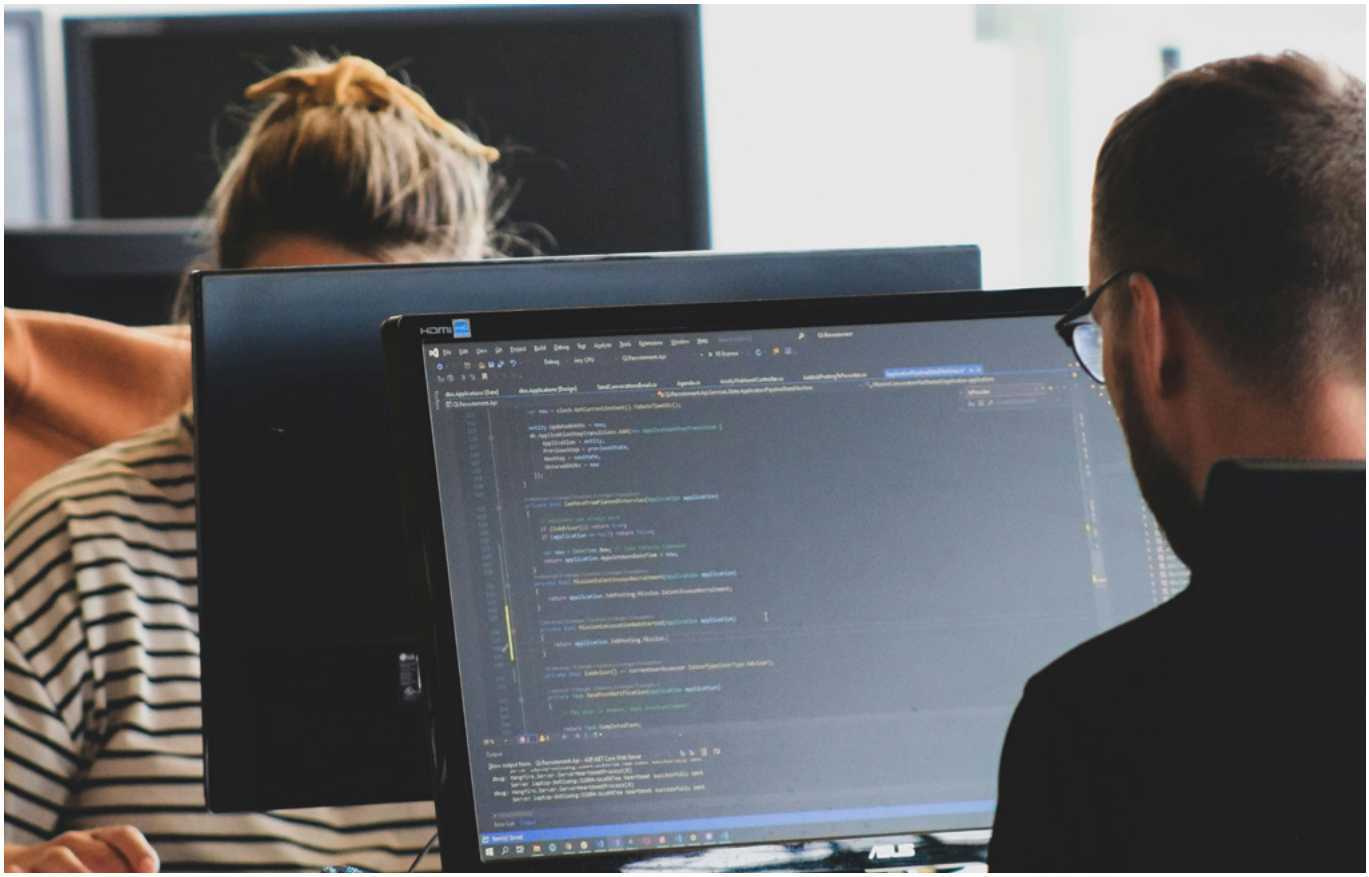
Employee Training: Regularly train staff on responsible data handling, consent and the importance of data minimisation.

Labour rights of security personnel

The adoption of technology by PSCs is transforming recruitment, working conditions, skill requirements and training for security staff. PSCs may be tempted to use surveillance technology on their own staff to save costs of supervision and monitoring for instance. However, this carries significant risks on the right to privacy of the security staff, similar to the ones that public surveillance entail, as well as risks for labour rights such as freedom of association.

Data collected on employees must be protected from cyber threats and the use of advanced technology may lead to workforce displacement in an already precarious industry. To address this, PSCs should focus on complementing human staff with technology, rather than replacing them, and invest in training programmes to equip workers with the skills needed to work with these technologies while respecting human rights.

Moving forward, stakeholders must balance technological innovation with responsible practices to ensure the sector's professional growth and the protection of both workers' and public rights.



Recommendations on protecting labour rights in the digital age for PSCs

ICoCA-ICT4Peace Guidance

Inclusive Adoption: Ensure all employees have access to the necessary technical tools and training to prevent inequality and promote equitable opportunities.

Transparent Monitoring: Develop clear policies outlining the scope and purpose of employee monitoring to balance operational needs with privacy rights.

Freedom of Association: Ensure that digitalisation does not hinder employees' ability to form or join labour unions and engage in collective bargaining.

Flexible Work Arrangements: Introduce policies that support work-life balance, especially in remote work contexts, to prevent burnout and overreach into personal lives.

Upskilling and Reskilling: Provide ongoing training programmes to prepare employees for evolving technological roles, mitigating job displacement risks due to automation.

Stakeholder Engagement: Collaborate with employees, labour unions and other stakeholders to align digital practices with labour rights and address concerns effectively.

Data Protection: Protect employee data through robust governance and regulatory frameworks emphasising security, transparency and compliance with privacy laws.

Human Oversight in Digital Tools: Maintain human oversight in critical decisions made by automated systems, ensuring accountability and fairness in outcomes.

Grievance Mechanisms: Implement accessible systems for employees as well as civilians to report concerns or violations related to digital transformation and labour rights.

Continuous Improvement: Regularly review and update policies to remain aligned with technological advancements and international labour standards.

CONCLUSION

Bridging the gap: the role of ICoCA in promoting responsible security in the digital age

> *"ICoCA can play a very important role by developing basic norms, providing good practices and enhancing capacity to monitor human rights violations by PSCs using ICT technology."*
>
> **Private security expert, China**

The challenges posed by technology in the private security sector are multidimensional and involve actors across the whole governance spectrum (international, national, private and public). What this means is that any strategy aiming to uphold and enhance human rights accountability in the field must be grounded on a "co-regulatory governance" framework involving the "meaningful participation from State, business and civil society actors" (David Kaye, the UN Special Rapporteur on Freedom of Opinion and Expression).[15] Kaye specifically cites ICoCA as a model to follow.

Indeed, by providing a model of co-governance for the private security industry, ICoCA is in a unique position to "operationalise the human rights responsibilities of the sector and set out practical guidance and standards for the responsible provision of cyber services".[16] As ICT4Peace's 2022 report also highlights, ICoCA's Code and multi-stakeholder governance process could provide an updated framework with principles and standards for the protection of human rights for security services utilising ICT.[17]

In its recently adopted strategic plan for 2024-2030, ICoCA dedicated one of its 5 strategic goals to the technological transformation of the industry: "Establish standards for respecting human rights and using new technologies by private security providers, integrating these into the International Code of Conduct." ICoCA's strategy aims to: (i) further adapt and enlarge its platform to all the new actors technology is bringing in the industry; (ii) promote instruments like the Toolkit to support security providers' compliance with human rights, IHL and the Code's provisions; (iii) review the Code and help develop regulatory and governance frameworks that promote human rights and ethical business conduct and that the international community can use as references.

(i) Ensuring respect for human rights by new security actors

As suggested by ICT4Peace in its recent report[18], ICoCA could support the expansion of technology's governance in the private security field by:

a) Engaging in a dialogue with public authorities, cybersecurity companies, technology service providers and technology producers to identify possible risks, gaps and needs in regulation and oversight.

b) Engaging in a dialogue with civil society organisations which are actively involved in the monitoring of human rights and advanced technologies and encourage them to join ICoCA.

c) Engaging in a dialogue with clients of cybersecurity companies, technology service providers and technology producers with a view to sensitise them on the respect of international standards.

d) Creating relevant pathways for cybersecurity companies, technology service providers and technology producers providing security services to join ICoCA.

e) Creating capacities and procedures for monitoring compliance of tech companies providing security services.

(ii) Implementing the Code

To support PSCs and other external stakeholders, ICoCA could undertake the following:

a) Promote the existing Toolkit in various fora and among private security providers and their clients.

b) Make the Toolkit accessible through an online platform and trainings, ensure it is adaptable and customisable by companies, and develop a feedback mechanism to keep it up to date.

c) Develop a research project on the transformation of private security, monitor trends and identify risks and best practices, including through a number of case studies.

d) Develop human rights indicators and incorporate them into its monitoring of Member and Affiliate companies.

e) Develop and provide further training resources and guidance to Member and Affiliate companies on safeguarding the rights of workers and the public when using advanced technologies.

f) Enable the exchange of best practices and cooperation among private security companies that have joined ICoCA to promote the responsible use of advanced technologies.

(iii) Interpreting and reviewing the Code

ICoCA could initiate a Code revision and update project:

a) Conduct research on the sector's transformation by identifying relevant case studies, incidents, best practices, applicable legislation, priority areas and challenges. Engage with experts, private security providers, civil society organisations, governments, clients and technology companies to gather diverse insights.

b) Based on this research, propose a process for interpreting and revising the Code to reflect current developments and changes in the sector.

15. David Kaye, "Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 28 May 2019, A/HRC/41/35, paras. 61-64, available at: https://digitallibrary.un.org/record/3814512?ln=en
16. United Nations General Assembly (UNGA), "Issue of human rights and transnational corporations and other business enterprises, report of the Working Group on the issue of human rights and transnational corporations and other business enterprises", 21 July 2020, A/75/212., para 97, available at: https://digitallibrary.un.org/record/3879218?ln=en
17. Anne-Marie Buzatu, pp. 55-57.
18. Ibid.

Acknowledgments

This policy brief is based on the research report “Ensuring Responsible Security in the Digital Age: The application of the International Code of Conduct for Private Security Service Providers to Advanced Technologies”, authored by Vincent Bernard, Senior Policy Advisor, with the support of Samuel Pennifold, Research & Policy Intern.

International Code of Conduct Association
Geneva, Switzerland
secretariat@icoca.ch
www.icoca.ch