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

ICoCA Research Series

The International Code of Conduct Association (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 report is 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.

CONTENTS

EXECUTIVE SUMMARY

Private security companies (PSCs) are increasingly using advanced surveillance technology including sensors, facial recognition, behavioural biometrics and other intelligence gathering platforms such as drones to inform their guarding of physical assets. Beyond their traditional physical security services, PSCs are now taking on new profiles, including in the realm of cybersecurity driven by technological developments. Tech companies are also entering the private security market and offering security services such as surveillance or intelligence, alongside their own cybersecurity services.

Technology can be integrated into security systems in several ways. For example, Artificial Intelligence (AI) is increasingly used with CCTV systems to identify, track and, if necessary, remove or arrest suspected shoplifters; drones and other remote operated vehicles are used in the surveillance of sites, assets and border management to locate and identify migrants; open-source information is now being collected at a much larger scale, with automated Open Source Intelligence (OSINT) being able to search through multiple online sources of data simultaneously and possibly facilitate the occurrence of human rights violations (i.e. right to privacy, freedom of expression, etc.). These technologically enhanced operations are sometimes analogous to signals intelligence (SIGINT) operations carried out by state armed forces. In situations of conflict, these technologies can also be used to collect military intelligence and assist in making targeting decisions.

Whilst the integration of new technology may improve security services, it can give rise to risks in terms of respect for human rights and international humanitarian law (IHL), particularly in poorly regulated contexts and complex environments. Consequently, the private security sector would benefit from guidance and standards on how to use technology in a responsible way. The International Code of Conduct for Private Security Service Providers ("the Code") offers a unique pathway to achieving this. As part of its work in this area, ICoCA partnered with the ICT4Peace Foundation to produce a first Toolkit for the responsible use of ICTs in the private security sector ("the Toolkit").

This report is structured in four parts. The first part discusses how the Code applies to the use of technology. The next two parts highlight key current and emerging trends in security and the advanced technologies most commonly used by private security actors. The last part identifies priority legal and ethical challenges, drawing on the Code and the Toolkit to make some practical recommendations for private security providers. Finally, the conclusion presents a broad policy agenda for ICoCA, governments, civil society and companies to promote the responsible use of technology by private security providers.

INTRODUCTION

Traditionally, private security has been associated with guards patrolling perimeters or security vehicles transporting VIPs, cash or bullion. However, the face of the private security industry is rapidly changing. This transformation is being driven by the swift adoption and integration of advanced technologies alongside traditional methods to enhance security provision. Additionally, we are witnessing a major surge in the provision of new types of security services by technology companies.

Technological advancements place the private security industry at a crossroads. On the one hand, new technologies offer security providers the opportunity to improve the efficiency of traditional physical security operations and new capabilities allow for completely new services in the field of digital security. On the other hand, new technological developments also carry risks and can, in some circumstances, lead to violations of human rights and IHL. These risks are heightened in complex and high-risk environments – such as situations of armed conflicts, border management or preventing or countering violent extremism – and when technologies are deployed in countries with already weak oversight of the private security sector generally. In a global context where there is considerable political and commercial support for bringing technological solutions to security issues, relevant ethical and legal dimensions are easily overlooked.

The fast transformation of the security sector

Advanced technology offers new business opportunities for traditional "boots on the ground" PSCs, offering physical security services i.e. "companies primarily engaged in providing guard and patrol services, such as bodyguard, guard dog, parking security and security guard services".[1] They can expand and diversify their range of services, offering cybersecurity services for instance while maintaining existing guarding activities.

PSCs are adopting new modes of operation by increasingly utilising information and communication technologies (ICTs), including advanced surveillance technologies,[2] at an accelerating rate.[3]

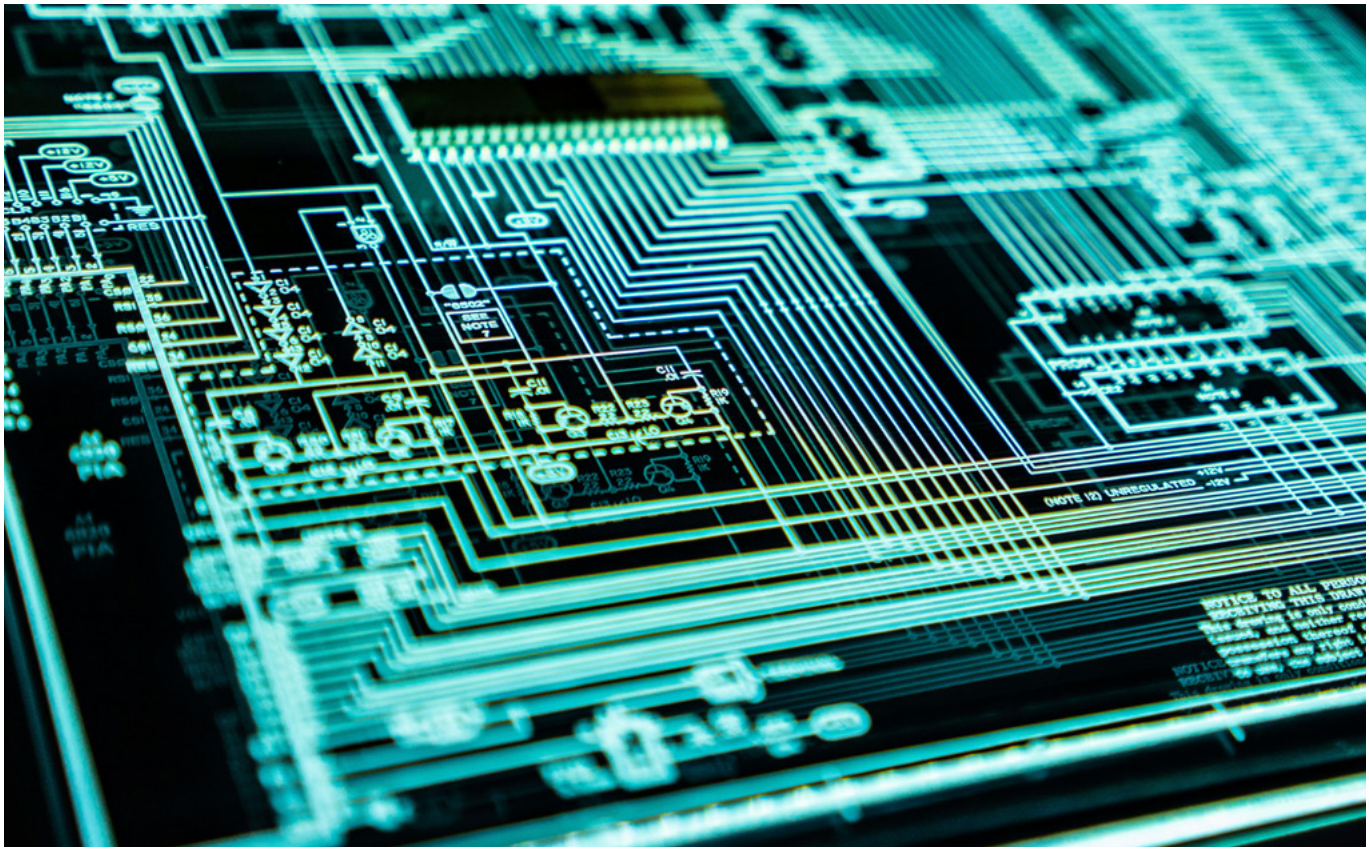
The use of ICTs enables PSCs to pursue new and enhanced security services such as cybersecurity, digital intelligence, tracking individuals using open-source data and employing AI for predictive security actions. These advancements are supplementary to traditional guarding missions, which in some places are also now being transformed using advanced technologies such as drones, advanced sensors and CCTV systems. Some PSCs have even shifted away from physical security services entirely, identifying technological solutions as the industry's primary growth area.

Beyond traditional security actors, tech companies are also playing a growing role in providing security services. The activities of these companies encompass services such as intelligence, surveillance or cybersecurity. They sometimes develop and produce the technologies they use themselves. While they may not fit our traditional perception of security and they do not define themselves as "PSCs", they are nonetheless delivering private security services.

1. Examples of services provided by these companies include the prevention of unauthorised activity or entry, traffic regulation, access control, and fire and theft prevention and detection. These services can be broadly described as the protection of personnel and/or assets. Other security services include roving patrol, bodyguard, and guard dog services. U.S. Bureau of Labor Statistics NAICS 561612- The U.S. Producer Price in Security Guards and Patrol.

2. The exact definition of ICTs is broad and can include a diverse set of technological tools, software and other products and services used to capture, transmit, store, create, secure, damage, delete, share or analyse information by electronic means. Surveillance technologies and ICTs, in their many forms, can inform both the guarding of physical assets and digital intelligence operations.

3. A comprehensive 2024 mapping study conducted by ICoCA comparing to 2022 results from the ICT4Peace Foundation found that each ICoCA Member provided at least one technology-based security services, with the use of technology being central to operations of most Members and Certified Members. 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/



Risks for human rights and international humanitarian law

With this evolution comes risk of abuses and violations of international human rights and IHL. PSCs and technology companies' collaborations with governments in electronic surveillance could violate the rights of individuals targeted. The way companies collect, store and transfer data may directly infringe on the right to privacy and may lead to persecutions of individuals and political, religious or ethnic groups. For instance, border security technologies and monitoring services could raise serious concerns surrounding the collection, processing and sharing of biometric data about asylum seekers and migrants.

Based on ICoCA's field observations and research, the private security sector remains largely unaware of the human rights and IHL risks associated with the use of emerging technologies. Many PSCs lack both the capacity and expertise to responsibly deploy advanced technologies, particularly when it comes to acquiring and managing large volumes of data, where legal requirements are often ambiguous. Disregarding legal and ethical standards can lead to severe consequences for commercial actors, with both private security providers and their clients potentially facing significant liabilities and reputational damage in the event of a breach.

While this concern extends across every industry collecting data today, private security frequently handles sensitive information related to individuals, clients and even national security matters. PSCs are typically hired to provide security to important persons or valuable assets, with heightened risks of attacks, thefts or other hostile acts.

The Code's relevance in the digital age of private security

The International Code of Conduct for Private Security Service Providers ("the Code"), adopted in 2010, articulates the responsibilities of private security companies under human rights and IHL to ensure the responsible provision of private security services.[4] The International Code of Conduct Association (ICoCA) was created in 2013 to serve as the main implementation mechanism for the Code.

4. While the Code focuses on the obligations of PSCs, the Montreux Document (2008) reaffirms the existing obligations of States under international law, in particular IHL and human rights law, relating to the activities of private military and security companies (PMSCs). International Committee of the Red Cross, Government of Switzerland, *The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict,* 2008, available at: shop.icrc.org/the-montreux-document-on-private-military-and-security-companies-pdf-en.html

The Code does not explicitly refer to the use of technology in its definitions of security services. However, 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. The Code explicitly imposes on companies that have joined ICoCA the duty to exercise due diligence to ensure compliance with the law and with the principles it contains, including the rights to freedom of expression, association and peaceful assembly and protection against arbitrary or unlawful interference with privacy or deprivation of property. All these rights, as this report will outline, are particularly vulnerable to abuse, whether inadvertent or otherwise, when using ICT-based security services.

Operationalising human rights standards

Over a decade after the adoption of the Code, now is the time to deepen our understanding of and address the implications of the growing importance of virtual security in relation to physical security, along with the associated gaps in oversight and standards. This entails the interpretation, clarification and possible updating of the provisions of the Code to explicitly cover the use of advanced technologies in security and cybersecurity operations.

Considering the above, ICoCA supported the ICT4Peace Foundation in developing a comprehensive Toolkit[5] to guide PSCs in the responsible use of technology while ensuring compliance with regulatory and human rights standards. It presents the legal, technical and ethical challenges associated with surveillance practices and data management and seeks to promote a human rights-centric approach to the use of new technologies in the private security sector. The Toolkit draws on the Code, relevant international law instruments, soft law as well as guidance documents issued by various organisations and best practices. Important work remains to be done reaching out to traditional and new security providers, disseminating the toolkit and strengthening regulatory and oversight mechanisms.

This report begins by a presentation of the relevant rules of the Code to help PSCs mitigate these risks (I). It then investigates the ongoing transformation of private security (II) and the main technologies being used, such as drones, robotics and AI-powered surveillance tools (III). The fourth part explores the main challenges for human rights and IHL associated with these technologies, presenting recommendations derived from the Toolkit (IV). The report concludes with a broader policy agenda aimed at promoting the responsible and ethical use of technology within the private security sector.

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


SECURITY

PART I.
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. This is why the International Code of Conduct for Private Security Service Providers was created in the first place: PSCs need guidance to implement strict and effective policies such as training their staff or ensuring access to grievances mechanisms, to prevent possible abuses. When PSCs operations involve the use of advanced technologies, they need to comply with all applicable national and regional legislations. However, the regulatory environment for the use of technologies by PSCs varies from one country to another, creating legal uncertainties for PSCs exporting their services or operating extraterritorially. In some contexts, there may be no national regulation and/or no oversight at all.

> *"Technology has advanced faster than regulation. Regulation for use of these technologies by states is behind and even further behind for security companies."*
> **Interviewee from a human rights NGO**

There is a growing sense that technology is evolving faster than the law, but this does not mean that security providers are operating in a legal vacuum. One of the interviewees submitted that "There is a continuous 'cat and mouse' game between regulation and technology [...] Is there a way to get ahead of the curve? If the current regulation and rules were already respected, we probably would have even much less need for even asking this question".

All stakeholders in the private security industry, PSCs and technology companies, regulators and civil society need to learn to navigate this new environment, develop their understanding of the use of technology by PSCs and understand the legal and ethical boundaries not to be crossed. The Code can provide such clarification and needs to be interpreted considering the evolutions of security, using the existing international law framework, national or regional legislations and best practices on data protection found in various sectors.

How does the Code define security services?

The Code is designed to regulate security services (such as arrest, detention, crowd management or maritime escorts, etc.) and to protect the rights of individuals affected by such services. It provides a non-exhaustive list of services that fall within its scope (see Box 1).

Responding to the market's demand, PSCs and tech companies alike are starting to integrate technology into security systems in several ways: AI is increasingly used with CCTV systems to identify, track and, if necessary, remove or arrest suspects; drones and other remote operated vehicles are utilised to identify and intercept migrants on their journey; open-source information is now being collected at a much larger scale, with automated Open Source Intelligence (OSINT) being able to search through multiple online sources of data simultaneously to provide intelligence.[6] Furthermore, many companies now offer cybersecurity services. How does this affect the application of the Code?

First, the Code does not specifically mention all the methods, weapons or technologies that private security companies may use in the provision of these services. Private security providers are still responsible for ensuring that any new means or methods they use in the provision of their security services is compatible with the Code's provisions, national and international norms.

This allows for a broader interpretation of its scope of application. The Code includes surveillance services under the entry "operational and logistical support for

6. Summary of Report No. 74 regarding automated OSINT by the Dutch Committee on the Intelligence and Services, Dutch Review Committee on the Intelligence and Security Services, 8 February 2022.

Security Services

Section B "Definitions" of the International Code of Conduct for Private Security Service Providers currently list a series of security services.

"Security Services include but are not limited to:

- guarding and protection of persons and objects, such as convoys, facilities, designated sites, property or other places (whether armed or unarmed),
- guarding and transporting prisoners, operating prison facilities, and assisting in operating camps for prisoners of war or civilian detainees,
- the checking, detention or searching of persons, searching of premises or containers and seizure of objects,
- counter-piracy services, armed or unarmed maritime escorts or onboard vessel protection,
- operational and logistical support for armed or security forces, including training and advice, intelligence, surveillance and reconnaissance activities,
- crowd management,
- operating and maintaining weapons systems,
- guard dog services,
- the recruiting and training of security personnel, directly or as an intermediary, for a company that offers private security services,
- and any other protective activity for which the personnel of companies are required to carry or operate a weapon in the performance of their duties."

armed or security forces (including training and advice), intelligence, surveillance and reconnaissance activities",[7] but that does not mean that surveillance could not also be interpreted outside the boundaries of this definition and considered as a means to an end, a tool used in the provision of other security services listed in the Code (such as a CCTV network used for the guarding and protection of persons and objects or smart sensors, video analytics, and artificial intelligence used for crowd control).

Furthermore, Article 25 of the Code 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, for example, 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 human rights violations, such as discriminatory practices.

While the Code does not explicitly include cybersecurity in the list of security services, it can be argued that human rights and IHL apply to cybersecurity operations anyway.[8] In 2021, the ICoCA General Assembly reviewed some of the provisions of the Code including the list of private security services in the Code. It decided that the inclusion of cybersecurity among the types of security services falling under the scope of the Code will be subject to further consultation.

The list of security services "includes but is not limited" to the ones mentioned in the Code; however, 1) technology's impact on security and its relation to human rights and IHL provisions has been so deep and pervasive that the extent to which technology is shaping the type of security services provided can no longer be ignored, and 2) the application of human rights and IHL to the use of technologies is complex and requires new specific instructions as well as specific indicators to assess the compliance of companies.

7. It is interesting to note that in 2011, the UN Working Group on the use of Mercenaries (UNWG) proposed a draft convention on PSCs and military contractors and mercenaries which included an expansion of the definition of security services, to include "any kind of knowledge transfer with security and policing applications, development and implementation of informational security measures and other related activities". Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, *Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council*, 13 May 2011, A/HRC/WG.10/1/2.

8. Human rights concerns may arise when private security companies engage in cybersecurity operations in complex and conflict-affected situations, independently or supplementary to the provision and use of ICTs in such environments. Cybersecurity services could, in some cases, amount to mercenary-related activities, as noted by the UN Working Group on the Use of Mercenaries (A/76/150). Given the widespread adoption of technology across industries and the growing importance of the cybersphere to state, non-state and private actors, it is important for States and businesses to also adopt best practices when contracting private cybersecurity services. 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. Indeed Article 21 of the Code 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." 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)

As a result, evidence-based recommendations on definitions, common standards and compliance indicators are needed. That is why, in line with the reflexion and consultation process initiated by the General Assembly in 2021, ICoCA could engage in a revision process aimed at addressing the new types of challenges, risks and regulatory gaps PSCs are confronted with in the digital age.

As a first step towards this renewed commitment to support companies in ensuring their compliance with human rights and IHL provisions, the following sections will offer an interpretation of how the Code applies to companies engaging in the provision of security services through technological solutions.

In which situations does the Code apply?

The Code applies to the actions and operations of Member and Affiliate companies.

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".*

The Code mentions a number of these actions and operations, including:

i. formally assisting states' law enforcement authorities;

ii. guarding, transporting, questioning or generally detaining individuals;

iii. apprehending persons in the case of an imminent threat of violence;

iv. selecting and vetting personnel and/or subcontractors;

v. providing personnel with initial and recurrent professional training on the Code and all applicable international and relevant national laws;

vi. ensuring personnel is properly trained in managing weapons, tools or technologies used in the provision of companies' services; etc.

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."*

In such environments, 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. In some cases, even when there are regulations in place, there may still be a lack of understanding and awareness regarding how they should be applied. 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. What this implies is that ICTs tools (e.g. surveillance systems[9]), which are now becoming increasingly relevant in shaping such operations, must be integrated into the Code's overall scope of application. This requires business actors to perform heightened human rights due diligence (hHRDD) in accordance with the UN Guiding Principles on Business and Human Rights (UNGPs).[10]

As technologies accelerate the growing dependence of public authorities on private companies for security

9. ICRC, "International humanitarian law and cyber operations during armed conflicts", *International Review of the Red Cross*, 102 (913), 2020, 481–492, available at: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf; UN Special Rapporteur Reports on Privacy and Freedom of Expression, *Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 2019, A/HRC/41/35, available at: https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur

10. 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

services (see below, Part II, Section on the Integration of Private and Public Security), it is important to highlight that Article 23 of the Code explicitly prohibits Member and Affiliate companies from derogating from the Code, even under pressure from "contractual obligations, superior orders or exceptional circumstances such as armed conflict, imminent armed conflict, threats to national or international security, internal political instability or any other public emergency". Despite these pressures, the Code reinforces the obligation to uphold its principles in all circumstances.

To which 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 obligations of security providers?

Article 4 of the Code states that:

> *"Member and Affiliate Companies affirm that they have a responsibility to respect the human rights of, and fulfil humanitarian responsibilities towards, all those affected by their business activities, including Personnel, Clients, suppliers, shareholders and the population of the area in which services are provided."*

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, private security providers 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" or "safety by design", and to engage in regular consultations with affected communities, even if these policies and actions are not explicitly outlined in the Code.

Indeed, as emphasised by Article 21 of the Code, 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.

> *"Member and Affiliate Companies will exercise due diligence to ensure compliance with the law and with the principles contained in this Code and will respect the human rights of persons they come into contact with, including, the rights to freedom of expression, association, and peaceful assembly and against arbitrary or unlawful interference with privacy or deprivation of property."*
> **(Art. 21)**

The Code does not only specify obligations for PSCs, but it also provides a framework for oversight and accountability. Administered by ICoCA, a multistakeholder initiative composed of governments, private security providers and civil society organisations, the Code requires authorisation, licensing, vetting and training, as well as monitoring and accountability. Meeting the requirements of the International Code of Conduct can help private security companies and their clients ensure that human rights are respected in the provision of security services. ICoCA is a risk-reduction mechanism in the security supply chain, conducting due diligence on its Members and Affiliates, monitoring their activities, certifying their operations, providing guidance and handling complaints. Furthermore, ICoCA regularly produces new guidance and training materials for security personnel, contributing to the prevention of abuses.

PART II.
How does technology transform private security?

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

How and what technology is being used by PSCs is continuously evolving. In response to growing security challenges and client demands for more sophisticated protection, PSCs are incorporating a range of innovative technologies into their operations. Including AI-integrated surveillance solutions to remotely piloted drones and biometric systems, these technologies offer PSCs the opportunity to enhance traditional security operations by opening new methods of operation. As technology continues to evolve, PSCs are capitalising on these advancements to deliver more responsive and adaptable services, further transforming our sense of how security is managed and deployed.

This section of the report presents some of the main trends in the transformation of the sector, providing examples from ICoCA Member companies in the first section (unless specified, other companies mentioned in this report are not ICoCA Members).

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

> *As of 2024, 100% of ICoCA Members report providing at least one ICT-based service – a 50% increase over two years.*

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 growth will continue in the coming years.[11]

This trend is well illustrated by the evolution of the use of technologies by ICoCA Member companies.

Categories of commercial security services using ICTs provided by PSCs[12]

- 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

Comparisons between the 2022 ICT4Peace Foundation mapping study on the use of technology by ICoCA Members and a 2024 internal ICoCA update found that:

- In 2024, 100% of ICoCA Member and Affiliate companies advertised providing at least one ICT-based service, such as digital apps for vehicle tracking or remotely monitored CCTV, with most offering multiple services.[13] In 2022, only 68.5% of ICoCA Members and Affiliates provided at least one ICT-based security service.[14] This represents a 50% increase over two years (during the same period, ICoCA membership also grew by 60%, from 92 to 154 Member and Affiliate companies).

11. Buzatu, 28.
12. Ibid.
13. Accurate as of September 2024 ICoCA Mapping study of the use of technology by Certified Members and Affiliate companies per their websites.
14. Buzatu, 28.

- Surveillance and remote monitoring using CCTV as well as other ICT applications such as apps on personal and company mobile phones, and in some cases drones, are the most advertised ICT-based services, with nearly 70% of 64 Certified ICoCA Member and Affiliate companies offering surveillance and remote monitoring.

- At least 25 ICoCA Member and Affiliate companies now provide specific cybersecurity services, often via separate departments from physical security operations, up from 10 in 2022.[15]

Consultations with ICoCA Members and Affiliates indicate that PSCs are expanding their security operations by incorporating more autonomous solutions, predictive analytics and sophisticated cybersecurity tools. Analysis of interviews conducted between April and September 2024 with a range of ICoCA Members, Affiliates and other industry stakeholders suggests that that this will undeniably raise new ethical, legal and human rights challenges, particularly concerning data privacy and accountability.[16]

An uneven deployment

Advanced technology is transforming the global private security ecosystem. However, it is important to observe from the outset that the deployment of new technologies and capabilities within the industry is unlikely to be uniform across regions or within countries, due to a variety of enabling factors and hurdles.

> *"There is definitely a move towards implementing more technical aspects of security [...] But in countries such as Iraq or Afghanistan, technology can only go so far."*
> **(Private security expert, UK)**

The use of advanced surveillance technologies and other ICTs is likely to become essential for security companies to remain competitive in a market where clients demand modern systems and equipment, particularly in the Global North. Some countries, such as China, are far ahead of the curve, as homegrown technologies have become widely available for both domestic use and export.[17] The rapid technological development has brought significant changes to China's private security industry, even impacting traditional security and service providers. Whereas security services were once mainly human-intensive, the industry has now undergone a transformation towards digitalisation.[18]

In other countries, several barriers to the adoption of technology exist. Companies are often unwilling or unable to issue devices such as tablets or smartphones to security guards because of implementation costs, low digital literacy among the workforce or clients' unwillingness to pay more for technology-enabled guarding services.[19] Moreover, guarding operations frequently take place in remote areas with limited access to electricity, phone reception and internet connectivity. Technology has been less widely adopted by PSCs in certain regions of Africa, where the security industry is composed of a majority of very small companies or where the national digital infrastructure required to support use of technology is lacking.[20] One interviewee mentioned that the military background of many security managers explains their reluctance to use technology, as they prefer to rely on human guarding. Others explain that clients are not requesting technologies because of the associated costs. The reliance of technologies on infrastructure, coupled with the often-prohibitive cost of satellite internet services, means that new technologies simply cannot be used in many environments.[21]

Uberisation of the security sector

Advanced technologies have enabled the uberisation of security services, allowing users to request assistance via a mobile application – for instance, if they feel threatened in a parking lot or are involved in a car accident. The concept of on-demand applies both to the provision of physical guarding services and to the payment structure for these services.

- One service, called Secura, allows users to request assistance from a range of PSCs and private ambulance companies using their mobile application. When a request is made, one of the many (armed or unarmed) PSCs that are partners of the *Secura* app respond.[22]

- Bsafe defines itself as an "Emergency Management System (BEMS), featuring an innovative dashboard with ground-breaking functions such as voice activation, live streaming, bidirectional communication, automatic audio and video recording and *Follow Me* features".[23]

15. Ibid.
16. These represent the most common concerns of those who participated in interviews with ICoCA, April-September 2024
17. Anonymous Testimony, ICoCA Workshop.
18. Anonymous interview conducted by ICoCA staff, July 2024.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.
23. https://www.secura.co.za/

Impact on the working conditions of security personnel

> *"With this new trend, some traditional providers may lose their jobs if they lack good education, training or familiarity with new technologies."*
> **(Private security expert, China)**

A major incentive for PSCs to adopt new technologies is their potential to supplement human security personnel, boosting efficiency. Technologies such as AI and machine learning can recognise patterns humans might not or enable the placement of sensors and cameras in areas that are difficult or costly to access. Technology can also enhance the safety of security officers, reducing their exposure to harm by enabling risks to be assessed remotely and improving communications on the job. The use of technology could also improve working conditions in other ways. For example, payments via apps can increase transparency, prevent supervisors from withholding salaries and ensure that remittances are actually paid to social security by employers (a major issue in some countries, where employers do not remit the funds[24]).

ICoCA has observed a global concern about the automation of labour across the sector.[25] As interviewees from private security trade unions noted, security workers are worried about being replaced by cameras and robots. Many fear that the rise in technology will make their jobs redundant, enabling employers in various industries to cut labour costs.[26] One security manager pointed out that clients may not yet fully grasp the potential of advanced technologies, but are likely to request their deployment once they become aware of the possibilities or when older systems become obsolete. The adoption of new technologies may also accelerate in response to labour shortages. For example, during the COVID-19 pandemic in Singapore, one company adopted new technologies such as CCTV to cope with the absence of the quarantined staff.[27]

PSCs managers are quick to respond that humans remain essential to their work, as engaging with the public often makes up a considerable part of the job.[28] At an ICoCA workshop in South Africa, executives from PSCs emphasised that the integration of technology is intended to assist – not replace – human security personnel.

A significant barrier to the implementation of technology is the lack of education and digital literacy among the work force. As the roles of security personnel become more complex, the training requirements for private security staff are also likely to be more demanding. Research conducted by ICoCA into the working conditions of private security personnel found that private security guards are offered substandard professional development and training programmes, a finding echoed by the personnel themselves.[29] The research identified various complex training needs, including relevant laws, use of force, human rights, first aid and, crucially, technology. If steps are not taken to ensure the effective integration of technology training, conditions in the industry could well deteriorate, with many staff at risk of redundancy. In many countries, security guards often lack secondary education.[30] PSCs will need to make significant investments in digital education to be able to support their continued growth in an increasingly technology-driven industry. This is especially true for those PSCs seeking to expand laterally into the cybersecurity sector while maintaining their physical security operations.

If technology can be effectively integrated into the industry, it may allow for a growing professionalisation of the sector and improve working conditions for guards, shifting their tasks from patrolling in the open to monitoring surveillance systems. This transition could also promote greater diversity in the security workforce, in terms of gender and age.[31] Companies are often reluctant to assign female security officers to arduous or more dangerous tasks, such as night shifts in isolated areas, but may be more inclined to employ them in roles such as monitoring surveillance systems in control rooms.

24. See ICoCA's surveys on working conditions in East Africa, available at: https://icoca.ch/working-conditions/
25. Ifeanyi Igbinijesu, "Is automation in the Private Security Industry something to be feared?", 12 September 2018, https://www.linkedin.com/pulse/automation-private-security-industry-something-feared-igbinijesu/?trk=pulse-article_more-articles_related-content-card
26. One survey reported that 20% of companies in the United States had already replaced at least some workers with technology, available at: https://www.cbsnews.com/news/how-many-companies-replace-workers-with-tech/
27. Chia Osmond, "Security industry faces manpower crunch, especially at dorms", *The New Paper*, 5 December 2021, available at: https://tnp.straitstimes.com/news/singapore/security-industry-faces-manpower-crunch-especially-dorms
28. Vigilance Blog, "New security technology: could it replace manpower?", 14 March 2018, available at: https://vigilanceprotects.com/news/2018/new-security-technology-could-it-replace-manpower
29. 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/
30. Anonymous Testimony, ICoCA Workshop.
31. Ibid.

The interface between technology and humans and its impact on compliance

The integration of technology can enhance accountability for both companies and their employees, potentially helping to prevent violence and abuse. Tools such as body cameras can also ensure greater accountability of security personnel.

However, there is often a tendency to idealise the potential of technology, leading companies to underestimate the risks associated with its use. There should be a clear understanding of both its added value and its potential risks.

Remote surveillance, for example, can foster moral detachment and reduce empathy among security staff. Surveillance technologies can dehumanise those being monitored by creating both physical and emotional distance. They can also contribute to the bureaucratisation and gamification of security services, eroding personal connection and respect for ethical guidelines and regulations. The use of robots for security tasks may be experienced as unsettling or even humiliating by members of the public directly affected by their deployment.

The collection and storage of data could heighten the risk of insider breaches. Recent research by ICoCA on the working conditions of security personnel has shown that poor labour conditions within the private security industry are a significant driver of misconduct and abuse. Disgruntled guards, in particular, may sell or leak sensitive information related to security operations.

Additionally, replacing human personnel with technology – such as drones or robots for patrolling – may result in the loss of human intelligence, reducing direct engagement with the public and impairing private security providers' understanding of social, political and cultural contexts. Such knowledge and interaction are key to de-escalate conflicts and ensure effective prevention. PSCs can be seen as mediators between communities and clients, and this role could be diminished by over-reliance on technology. Ultimately, this shift could lead to a decline in the overall quality of private security services. PSCs often provide employment opportunities for the local population, which helps build their social license to operate and enhances their legitimacy. Replacing human workers with technology risks undermining this legitimacy. While clients may seek the most cost-effective solutions, they may overlook the long-term consequences of such decisions.

Tech companies providing security services

A growing number of technology companies are now providing tech-based security products and services to clients who might have traditionally relied on the services of PSCs. These companies can operate as both technology producers (hardware and/or software) and service providers, offering support for the use and implementation of their products.

The war in Ukraine illustrates this trend, with companies like SpaceX or Microsoft directly providing the Ukrainian Armed Forces with intelligence or communications technology.[32]

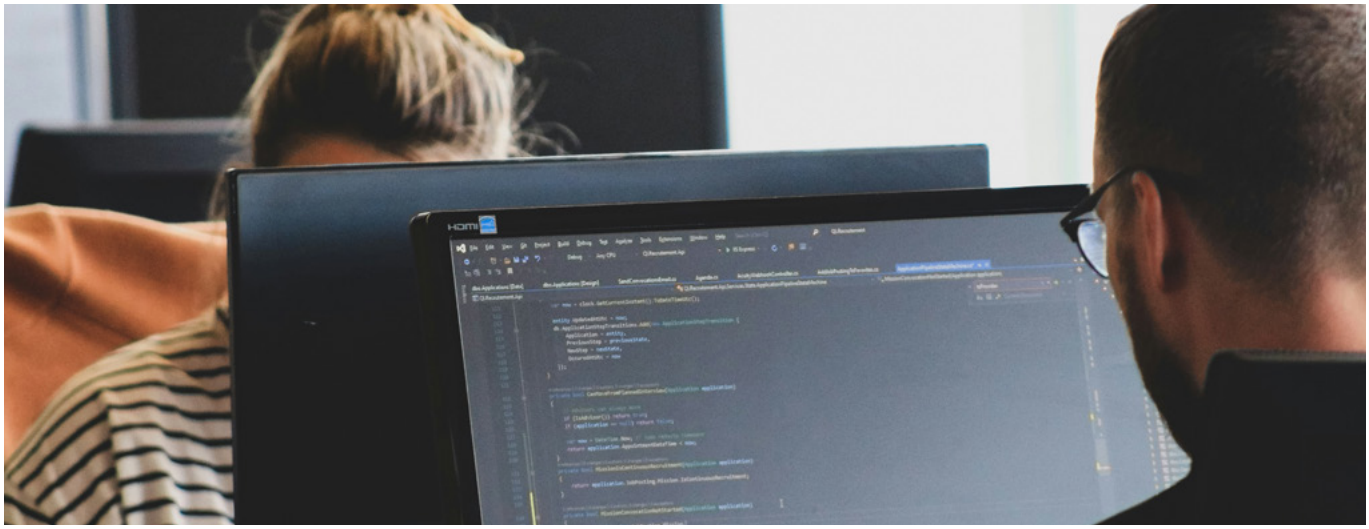
- *Palantir Technologies,* founded in 2003 as a response to the 9/11 terrorist attacks, utilises a range of ICTs and software solutions, such as AI-enhanced data analytics, to inform and augment security operations for state and private clients.

- Tech companies also provide security services to commercial entities. For instance, *Facewatch* offers a cloud-based facial recognition security system to combat shoplifting.[33]

Particularly promising is the use of open-source intelligence (OSINT) information and analysis, which processes information from public and legal data sources (such as social media, blogs, news outlets and the dark web) to serve specific functions. Applications in security are numerous, including detecting workplace security threats, protecting executives, conducting investigations, supporting prosecutions, gathering evidence, monitoring events, etc. OSINT can also be used to ensure the security of humanitarian organisations in conflict areas, collect information on violent incidents or disasters and assist in real-time rescue operations.

Private security companies may also be contracted for espionage (for instance with "mercenary spyware"), dis/mis-information operations and repression.[34]

32. "The original idea behind the study was to look at how 'traditional, boots on the ground' private security companies [...] were incorporating ICTs into physical security offerings. However, research and interviews painted a more complex portrait of how ICTs were being used by commercial actors in security-related activities and services, including anti-terrorism, intelligence-gathering, digital forensics and protection against cyberattacks." Foreword by Daniel Stauffacher, Anne-Marie Buzatu, p.iii.
33. https://www.facewatch.co.uk/
34. 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.



Integration of private and public security

> *"A lot has been left to the private security industry to deal with because if crimes happen, the police are not able to respond quickly."*
> **(Civil society organisation Member, Africa)**

The expansion of the security market and the evolving definition of security services raise new questions about transparency, accountability and the distinction between the civil and military sectors, as well as between the public and private sectors.

Public authorities and private industries are increasingly relying on private security services to support law enforcement tasks, including crowd control, counterterrorism and crime prevention. Interviewees noted a general trend toward greater state dependence on outsourced security solutions.

In recent years, the development and use of technologies have facilitated the growing integration of private and public security services. Public entities, such as the police and armed forces, have become progressively reliant not only on technologies provided by the private sector but also on tech-based security services, including intelligence and telecommunications.

Furthermore, in the digital era, the borders between public and private security are often porous: data collected by private actors can be shared with authorities and vice-versa, telecommunications systems can be used for both civilian and military purposes, as illustrated by several examples.

- *Project Pegasus:*[35] Recently, the UK's largest retailers agreed to fund a new biometric police operation that matches CCTV images of shoplifters with those in the police database.[36]

- ICoCA's research mission in Johannesburg observed how police and private security are now working hand in hand to monitor crime in the city. In recent years, South African PSCs have entered collaborative arrangements with the police under the umbrella of the Greater Gauteng Growth Together 2030 (GGT2030) programme. Having access to the same CCTV network across the city, PSCs contribute to the detection of crime. The CCTV system can locate and track stolen vehicles using their licence plates. The police and PSCs share information through social media platforms, such as WhatsApp groups, for quick updates on criminal activities. Private security armed guard patrols and intervention teams complement the work of the police. "Technological integrations, community involvement and belief in mutual objectives are starting to change the face of security."[37]

Emerging technologies challenge traditional notions of national sovereignty through cross-border military technology transfers, the use of big data in AI training, strategic dependencies on supplier nations, PSC operations across borders and global data management.

35. It should not be confused with the "Pegasus 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.
36. Borak Masha, "UK police, retailers partner to fight shoplifting with biometrics", *Biometric Update*, 11 September 2023, available at: https://www.biometricupdate.com/202309/uk-police-retailers-partner-to-fight-shoplifting-with-biometrics
37. Mkhululi Chimoio, "A new alliance in urban safety: how private security is reinventing crime combat in Johannesburg's Inner City", *Protection Web,* 7 November 2024, available at: https://www.protectionweb.co.za/police/a-new-alliance-in-urban-safety-how-private-security-is-reinventing-crime-combat-in-johannesburgs-inner-city/

PART III.
Which technologies do private security providers use?

This section presents the technologies currently most used in private security and those most likely to be used in the future, according to ICoCA's observations.

Surveillance, monitoring technology and AI

The development of surveillance and monitoring technology such as pressure sensors and CCTV technology has been foundational in the private security industry for years, but recent advancements have transformed their capabilities. Modern closed-circuit television (CCTV) systems can now include longer range, body-thermal imaging, facial and biometric recognition,[38] silhouette recognition and vehicle recognition, and in many cases can be monitored remotely over great distances. These systems are also evolving to meet societal shifts, such as the ability to recognise individuals wearing face masks – a significant advancement during and after the pandemic.[39] Surveillance using various digital methods can now identify a person based on characteristics such as their gait, voice or even the way they use a computer keyboard.

Surveillance and monitoring technology has moved beyond simple notification and identification and, through the power of AI integration, is now capable of extracting demographic details such as age, race and location. AI-powered facial recognition tools can detect detailed attributes, including ethnicity and regional features, raising both capabilities and concerns about privacy. Additionally, these systems can be integrated into larger cloud-based databases and used to identify individuals accused of shoplifting, notifying retailers in real time.

AI-based analysis of IP camera streams has introduced predictive policing, where machine learning models analyse patterns of behaviour to identify potential threats and security incidents. For example, security teams can now receive automated alerts for suspicious behaviours such as concealed shoplifting actions.

- *Dahua,* the world's second largest security camera manufacturer, lists AI-powered cameras on its own website that can detect "race", "skin colour" and even "Xinjiang/Tibet" facial features.[40]

- *Facewatch,* a UK-based company, utilises cloud-based facial recognition software and AI programmes integrated into CCTV systems to identify individuals accused of shoplifting, automatically notify stores of their presence when a match is detected and monitor their behaviour.[41]

- To monitor the 150 km of coastline in the Nord and Pas-de-Calais departments against illegal migration, The French company HGH has been contracted by the Ministry of the Interior to provide several SPYNEL infrared panoramic detection solutions. The aim is to establish a "smart border" based on advanced technologies to secure the coastline. "These systems allow for permanent and continuous surveillance in addition to the temporary surveillance means such as patrols, drones and airplanes."[42]

38. Ajay Sandhu and Kevin D. Haggerty, "Private Eyes: Private Policing and Surveillance", *Routledge Handbook of Private Security Studies,* 100–108, Routledge, 2015, available at: https://doi.org/10.4324/9781315850986-13; Christiane Wendehorst et al., *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces,* Policy Department for Citizens' Rights and Constitutional Affair, European Parliament, August 2021, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

39. Wudan Yan, "Face-mask recognition has arrived—for better or worse", *National Geographic,* 11 September 2020, available at: https://www.nationalgeographic.com/science/article/face-mask-recognition-has-arrived-for-coronavirus-better-or-worse-cvd

40. Donald Maye and Charles Rollet, *Dahua Race and Skin Color Analytic Cameras*, IPMV, 17 October 2022, available at: https://ipvm.com/reports/dahua-race-analytics

41. Mark Townsend, "'We'll just keep an eye on her': Inside Britain's retail centres where facial recognition cameras now spy on shoplifters", *The Guardian*, 29 July 2023, available at: https://www.theguardian.com/world/2023/jul/29/well-just-keep-an-eye-on-her-inside-britains-retail-centres-where-facial-recognition-cameras-now-spy-on-shoplifters

42. HGH, "HGH, partner in the 'Smart Border' project between France and the UK securing the coast against illegal immigration", 18 April 2023, available at: https://hgh-infrared.com/hgh-partner-smart-border-project-illegal-immigration/

Drones

The use of drones, also referred to as unmanned aerial vehicles (UAVs) and unmanned marine vehicles (UMVs), represents another major technological leap in surveillance technology. Drones can be used for a wide range of applications, from monitoring pipelines to offering anti-piracy services at sea, allowing PSCs to cover vast areas without deploying human personal (private security use of drones include mapping, search and rescue operations, real-time monitoring, crowd control, event security, access control, intruder detection, evidence collection, decontamination, facility security, traffic and route monitoring, crime detection and prevention, border surveillance and protection, etc.).

- *Ocean Infinity* employ UMVs for deep-sea security operations, reducing risks to human personnel while enhancing operational efficiency.[43] The company uses uncrewed deep-sea survey boats, enabling deployment of unmanned underwater security systems for defence, providing a "transformational alternative to traditional operations at sea to dramatically reduce risk to people".[44]

- Numerous companies advertise UAVs as part of their service offerings. For instance, a major South African company, *Fidelity Services Group,* uses drones in its response plans to residential and commercial property alerts. The drones serve both as a visible deterrent and a surveillance tool to track suspects, for example when patrolling pipelines and communications or power cables.[45]

PSCs, technology companies and defence contractors also play a critical role in operating drones, both lethal and non-lethal, on behalf of states. Military drones require significant resources for operation, including qualified staff and hardware. As a result, private security companies and/or military contractors are often contracted to fulfil these operational needs. While piloting military drones is left to states, PSCs often process intelligence and surveillance imagery collected by drones, thereby influencing targeting for lethal strikes.[46]

States may contract private companies to operate drones for border surveillance. Examples include the European agency Frontex tracking migrant boats crossing the Mediterranean Sea[47] and US authorities monitoring the US-Mexico border.[48]

Robotics

The use of robotics, as a distinct offering from drones, is another technology that may offer significant potential for PSCs.[49] Some companies are already replacing human security guards with robots in certain locations. These robots can patrol areas, detect intruders and suspicious activity, reduce false alarms, capture images, send data, and more. However, this practice remains limited, and its effectiveness is still debated,[50] though it is likely to increase as costs for acquiring and operating robots are decreasing.

- The tech company *Micron* promotes the use of security robots with the following arguments:

> *"Pity the poor security guard. In busy environments such as prisons and crowded shopping malls, they need to be everywhere at once. And in a more isolated setting – on the night shift in a lonely warehouse, for instance – they may struggle to stay engaged and alert. Security robots don't have these problems. Instead, they have artificial intelligence that works without getting tired or bored and streaming video to broadcast everything they see, bringing others on the scene no matter where they might be."*[51]

- In Singapore, a large PSC has begun using robots for traffic control around shopping malls, autonomously reminding vehicles to move along if stopped for too

43. "Survey Firm Ocean Infinity Buys Private Maritime Security Company", *The Maritime Executive*, 8 June 2021, available at: https://www.maritime-executive.com/article/survey-firm-ocean-infinity-buys-private-maritime-security-company
44. Ocean Infinity Defence, Safer Operations at Sea, available at: https://oceaninfinity.com/defence/
45. Ishveena Singh, "On-demand private security drones take off in South Africa", *DroneDj*, 25 May 2021, available at: https://dronedj.com/2021/05/25/private-security-drones-south-africa
46. Katharine Pena, "Accountability for Private Security Contractor Drone Operators on the U.S.-Mexico Border: Applying Lessons Learned from the Middle East", *Public Contract Law Journal 44*, no. 1, Fall 2014, 137-156, available at: https://www.wired.com/story/palantirs-gods-eye-view-of-afghanistan/
47. Frontex contracts out drone operation and development operations various companies; Welt Sichten. "Border security with drones and databases", *State Watch*, 27 February 2024, available at: https://www.statewatch.org/analyses/2024/border-security-with-drones-and-databases/
48. Katharine Pena, op. cit.
49. Indoor Robotic, "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", available at: https://www.indoor-robotics.com/blog/why-automated-security-robots-are-the-next-big-thing/
50. Cyrus Farivar, "Security robots expand across U.S., with few tangible results", *NBC News*, 27 June 2021, available at: https://www.nbcnews.com/business/business-news/security-robots-expand-across-u-s-few-tangible-results-n1272421
51. Micron Technology, "How security robots help make our lives safer", available at: https://sg.micron.com/insight/to-catch-a-thief-how-security-robots-help-make-our-lives-safer

long and providing a deterrent against breaking traffic rules when picking up and dropping off passengers.[52] In addition to traffic control, the robots' sensors and cameras can be used to patrol shopping centres and airports, detecting unwanted behaviour and using sirens and lights to deter it. Human security officers remain present and can intervene when necessary.

- *Ascento,* a Swiss start-up spun off from ETH Zurich, combines robots and AI in its autonomous security guards. These robotic guards are designed to patrol large private outdoor and indoor sites and are deployed by clients in sectors such as manufacturing, data centres, pharmaceutical production centres and warehouses. If the autonomous robot guard detects a security threat, such as an intruder, it can alert human security guards via its integrated app.[53]

Drones and other security robots represent a significant growth area in the adoption of technology by PSCs. According to the 2023 World Security Report produced by Allied Universal, 24% of the 1,775 chief security officers – or those in equivalent roles – surveyed stated that they plan to increase their use of drones, while 29% indicated plans to expand the use of security robots over the next five years to enhance both their physical and cyber security operations.

AI and machine learning integration for predictive security operations

AI is increasingly being used in the private security industry to enable further automation and increase the use of technologies such as drones and robots. It can also augment human decision-making by informing security personal and managers about how and which technologies are used. This has potentially significant implications for how technology will be deployed, especially in conflict-affected areas.

By utilising the vast amounts of data gathered through surveillance and monitoring technology, as well as potentially other existing data sets, AI can be used to inform predictive security operations. These operations may be similar to predictive policing or directly contribute to predictive policing conducted by law enforcement agencies. Predictive policing can be defined as "the application of analytical techniques – particularly quantifiable techniques – to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions".[54] It is primarily used to help prevent potential future crimes by forecasting them, or to reduce response time compared with human observation. There are two types of predictive policing: place-based and person-based. Place-based predictive policing uses pre-existing security data to identify places and times with a high risk of crime or security incidents. Person-based predictive policing attempts to identify individuals or groups who are likely to commit a crime or a security incident – or to be victim of one – by analysing risk factors such as past arrests or victimisation patterns.[55]

- *KeyCrime,* a company founded in 2007 and dedicated to using Artificial Intelligence to identify recurring patterns in serial crime, developed Italy's first predictive policing software, "Dynamic Evolving Learning Integrated Algorithm" (DELIA). Using statistical methods, "the application takes data from the latest crime and compares it with other crimes on the search for similarities". The Milan police department began trials in 2008, making the software one of the most established digital tools in Europe in this field, managed by KeyCrime. According to Algorithm Watch, the company went bankrupt following the introduction of new AI legislation prohibiting the use of AI for predictive policing.[56]

- *Smart Police* is an application that include a "predictive" module and was developed by the French startup *Edicia,* which, according to its website, has sold this software suite to over 350 municipal forces.[57]

- AI surveillance technology is spreading much faster and across a wider range of countries than experts had commonly understood. As of 2022, at least 97 out of 179 countries are actively using AI and

52. Gregg Greenberg, "Security Robots Patrolling a Mall Near You: Silicon Valley start-up Knightscope is rolling out security robots that can help take a bite out of the crime that costs the American economy $1 trillion every year", *The Street*, 17 January 2017, available at: https://www.thestreet.com/technology/security-robots-patrolling-a-mall-near-you-13956376
53. Ascento, Provided as a comprehensive Robotics-as-a-Service solution, available at: https://www.ascento.ai/#solution
54. Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith, and John S. Hollywood, Predictive Policing: *The Role of Crime Forecasting in Law Enforcement Operations,* Washington, DC: RAND Corporation, 2013.
55. Tim Lau, "Predictive Policing Explained", *Brennan Centre for Justice*, 1 April 2022, available at: https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained
56. Pierluigi Bizzini, "The Rise and Fall of a Predictive Policing Pioneer", *AlgorithmWatch*, 7 November 2024, available at: https://algorithmwatch.org/en/predictive-policing-pioneer-keycrime/
57. Edicia, Smart Police, Améliorez la tranquillité du citoyen au sein de l'espace public, available at: https://www.edicia.fr/fr/smart-police

big data technology for public surveillance purposes. This includes smart city/safe city platforms (64 countries), facial recognition systems (78 countries), smart policing (69 countries) and social media surveillance (38 countries).[58]

The integration of AI and machine learning to enhance predictive policing and security operations has the potential to revolutionise the private security industry, transforming it from a labour-intensive sector into a technology-driven one. While this shift offers several potential benefits, such as increased efficiency and reduced costs, it also poses significant risks.

Relying on AI for threat and risk assessment through machine learning means users may be unaware of how the recommendations are generated.

The likelihood of discrimination – whether intentional or resulting from poorly trained or inadequately developed AI and machine learning systems – is a major concern. This also emphasises the need to reinterpret the Code and the Montreux document in light of the growing involvement of technology companies in the private security industry, both as providers of technology and of services to private clients and states.

As part of the 2023 World Security Report produced by Allied Universal, 1,775 chief security officers – or those in equivalent roles – were asked which technologies they plan to utilise, either through internal investment or outsourcing to a security vendor, over the next five years. 65% said their company currently uses predictive technology to enhance security and intends to increase its use over the next 12 months. 42% said they plan to utilise various AI-powered systems within the next five years to improve their physical and cyber security operations.

The new EU Artificial Intelligence Act (AI Act), which came into force in 2024, prohibits several types of AI systems, such as the use of biometric categorisation systems inferring sensitive attributes; systems that deploy subliminal, manipulative or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm; that compile facial recognition databases under certain conditions; or that assess the risk of an individual committing criminal offences solely based on profiling or personality traits, etc.[59] The latter prohibition could significantly restrict the use of private predictive security services within the EU.

Cybersecurity

> *"Security isn't just about physical threats. It's also about electronic threats, the protection of commercial information and national security."*
> **(UK private security expert)**

The growth of cybersecurity[60] (i.e. how organisations and individuals protect ICT systems and digital information and reduce associated risks) within the private security industry is being driven by the widespread societal and economic adoption of technology. The transition to remote working and increasing reliance on digital information have heightened reliance on ICTs, introducing new vulnerabilities that cyber attackers can exploit. Consequently, the security concerns of organisations are no longer limited to physical assets but now extend to a wide range of cyber incidents and threats, such as phishing scams and ransomware attacks.

For example, according to the IBM® X-Force® Threat Intelligence Index, "Ransomware as a Service" (RaaS) accounts for 20% of all cybercrimes. RaaS refers to the practice of ransomware developers selling malicious code or malware to other hackers, known as "affiliates", who then use it to launch their own ransomware attacks.

This represents a growing area for PSCs to support clients in protecting their commercial information by responding to such incidents. 88% of chief security officers polled as part of the 2023 World Security Report said company leaders are now more concerned with cybersecurity than physical security threats, marking a significant shift in the industry.[61] As noted above, at least 25 ICoCA Member companies now provide cybersecurity services, compared to just 10 two years ago.

Cybersecurity services are generally considered to be defensive, aimed at securing the integrity of an

58. Steven Feldstein, *AI & Big Data Global Surveillance Index* (2022 updated), Version 4, June 2022, available at: https://data.mendeley.com/datasets/gjhf5y4xjp/4
59. *EU Artificial Intelligence Act*, Chapter II, Prohibited AI Practices, Art. 5, available at: https://artificialintelligenceact.eu/article/5/
60. *The National strategy for the protection of Switzerland against cyber risks* defines cybersecurity as a: "desirable state within cyberspace in which communication and data exchange between information and communication infrastructures function as originally intended. This state is achieved with measures of information security and cyber defence." *National strategy for the protection of Switzerland against cyber risks* (NCS) 2018-2022, available at: https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html
61. *World Security Report*, 2023, Allied Universal, 2023, p.5.

organisation's or individual's ICT systems and digital information. This can include cybersecurity incident response and digital forensics following a breach, identifying attackers and taking remedial action. Experts, however, emphasise that the distinction between defensive and offensive cyber operations is not always clear-cut. Cyber capabilities can also be used for espionage. Moreover, during armed conflicts, this distinction becomes irrelevant under international humanitarian law (IHL): when the conditions for direct participation in hostilities are met, both civilian attackers and defenders may lose their protection as non-combatants.[62]

In some cases, private cybersecurity companies directly provide both defensive and offensive capabilities to state actors involved in conflicts, thereby participating in warfare and blurring the distinction between civilian entities and combatants. Such cybersecurity providers risk becoming "mercenary-like" proxies.[63] During the Russo-Ukrainian war, private security companies have been significantly involved in cybersecurity operations on both sides. This trend of collaboration is not new: in 2016, US Cyber Command awarded a contract of USD 460 million to six private security companies that included support for offensive cyber operations.[64]

As PSCs continue to utilise a diverse range of advanced surveillance technologies, there will be a significant increase in the amount of information and data gathered and used by them. Such information can be highly sensitive, especially when it involves the use of facial recognition hardware and software, other biometric identification technology or the monitoring of electronic communications. Security guards and clients may also be unaware of the risks associated with their cell phones geo-location capabilities, which can reveal sensitive information such as personnel identities, patrol routines and security perimeter details.

As an insurance company recently remarked: "Security firms – tasked with safeguarding physical and digital assets – are becoming prime targets for cybercriminals because they handle confidential client data, have extensive IT networks and often lack the same cybersecurity measures as larger corporations. The irony is stark: the very entities designed to prevent breaches are increasingly vulnerable to cyber-attacks."[65]

- Consequences for PSCs can be severe. Beyond the unauthorised release of confidential information, cyberattacks can lead to financial losses, operational disruptions and the erosion of client trust. In 2022, G4S Australia was the victim of a cyberattack. Personal information of employees – including tax file numbers, bank account information and medical checks – was stolen and posted online in a ransomware attack. G4S provides services for prisons across Australia.[66]

- Beyond the theft of sensitive information, such cyberattacks can also temper with access controls or affect surveillance systems and security cameras. For instance, in January 2024, the Security Service of Ukraine reported that Russian-backed hackers had accessed residential security cameras in Kyiv to gather information on air defence systems, informing attacks on the region.[67]

62. Nils Melzer, *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*, ICRC, 2009, available at: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc-002-0990.pdf
63. Vibhu Mishra, "UN chief warns of 'cyber mercenaries' amid spike in weaponising digital tools", *UN News,* 20 June 2024, available at: https://news.un.org/en/story/2024/06/1151266
64. "Cyber Mercenaries and the Crisis in Ukraine", *Council on Foreign Relations,* 30 January 2018, available at: https://www.cfr.org/blog/cyber-mercenaries-and-crisis-ukraine
65. El Dorado Insurance Agency, "Cyber attacks on security firms: what we've learned from case studies", 16 September 2024, available at: https://www.eldoradoinsurance.com/security-industry-news/the-rising-threat-of-cyber-attacks-on-security-firms-lessons-learned-from-case-studies/
66. Josh Taylor, "Staff at security firm G4S on alert after tax numbers and bank details posted online following hack", *The Guardian*, 4 October 2022, available at: https://www.theguardian.com/australia-news/2022/oct/05/staff-at-security-firm-g4s-on-alert-after-tax-numbers-and-bank-details-posted-online-following-hack
67. Sinead Baker, "Russia hacked kyiv cameras", *Business Insider*, 3 January 2024, available at: https://www.businessinsider.com/russia-used-kyiv-surveillance-cameras-huge-missile-attack-ukraine-2024-1

PART IV.

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

This part examines key legal and ethical challenges posed by the use of advanced technologies in private security. It draws on the Code and Toolkit to formulate practical recommendations on how to translate the human rights obligations set out in the Code into actionable steps for companies.

To address the challenges of implementing the Code when using technologies, ICT4Peace and ICoCA produced a Toolkit to provide practical guidance to support the operationalisation of human rights obligations. The Toolkit is designed to help PSCs navigate the complexities of using technology while ensuring compliance with human rights standards and legal obligations. It offers essential best practices advice. By implementing the recommendations outlined in this guidance, PSCs can enhance their operational frameworks, mitigate risks and uphold the principles of democratic governance.

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 landscape of technology and 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.

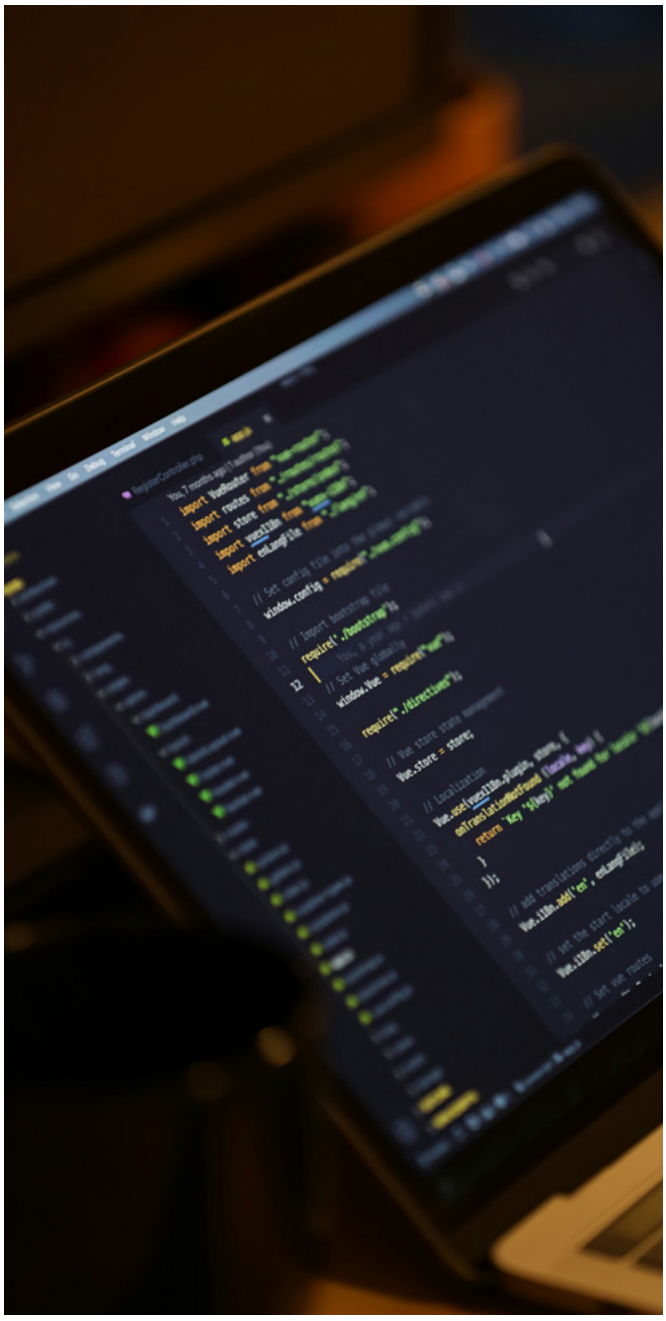
Surveillance and the right to privacy

> *"Privacy violations or breaches of data protection are just the gateway to other human rights violations: tracking people and intimidating them, exercising violence, harassing them, even killing them."*
> **(Interviewee from a human rights NGO)**

The US Department of Defence 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".[68] While

68. *DOD Dictionary of Military and Associated Terms*, 2021, available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

state authorities employ surveillance for law enforcement, border control and counterterrorism, the implications of mass surveillance – integrating CCTV, drones, tracking of social media use and meta data, and other tools – extends far beyond these functions. The potential harms are extensive, including invasions of personal privacy, a chilling effect on political activism, threats to democratic processes and the risk of personalised violence based on collected information.[69]



The impact of spyware developed and operated by private companies on behalf of states

A 2023 study conducted by the European Union Policy Department for Citizens' Rights and Constitutional Affairs, on behalf of the European Parliament, analysed the impact of Pegasus and similar spyware on fundamental values enshrined in Article 2 of the Treaty on European Union. These include respect for human dignity, freedom, democracy, equality, the rule of law and the protection of human rights – particularly for individuals belonging to minority groups – as well as privacy and data protection, and the integrity of democratic processes within Member States.

The study revealed that spyware systems such as Pegasus, developed by the Israeli NSO Group, facilitate invasive surveillance by remotely hacking mobile devices without the user's knowledge or consent, leaving minimal traces of their operation. This pervasive form of secret surveillance poses significant threats to individuals' privacy and data protection, as well as to fundamental rights such as freedom of speech, association and assembly.

Notably, the impact of spyware is especially detrimental to those in the public sphere, including journalists, politicians and activists. The mere fear of being monitored can deter individuals from seeking public office or effectively campaigning, thereby undermining democratic institutions and processes.

Concerns regarding state-led mass surveillance have surged in recent years, particularly following incidents such as the PRISM scandal involving Western intelligence agencies and the Pegasus revelations concerning the use of mercenary spyware.[70] However, much of the discourse has focused on state surveillance, with less attention given to the role of private security firms in these practices. By outsourcing surveillance functions to PSCs, states may

69. Paul Bernal, "Data gathering, surveillance and human rights: recasting the debate", *Journal of Cyber Policy*, 1(2), 2016, 243–264, available at: https://doi.org/10.1080/23738871.2016.1228990. And Amnesty International, *The surveillance industry and human rights: Amnesty International submission to united nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression,* 2019, available at: https://www.amnesty.org/fr/documents/ior40/5179/2022/en/

70. PRISM was a classified surveillance programme run by the US National Security Agency (NSA); it involved the collection of massive amounts of American and international individuals' private data held by private security companies justified under Section 215 of the Patriot Act. Edward Snowden, a former NSA contractor, leaked information regarding the programme in 2013, which led to a large public backlash against the US government and the NSA; Pegasus is a 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.

dilute their responsibilities, transferring both moral and legal implications to these private entities. As a result, PSCs can conduct surveillance activities on behalf of governments, businesses and individuals. This lack of transparency raises serious human rights concerns, as all forms of electronic surveillance have the potential to violate individuals' rights.

However, the involvement of tech companies in the provision of security is hardly a new phenomenon. As early as 1979, Prof. Michael T Klare spoke about an "International Repression Trade" to describe the trade in technologies used for social control.[71] In 1995, Privacy International published "Big Brother Incorporated",[72] a study of the international trade in surveillance technologies.

What is unprecedented is the potential scale and depth of the surveillance that the most recent technologies now permit. A 2024 report by the Geneva Centre 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".[73] The use of advanced surveillance by PSCs presents several significant risks. Interviews conducted as part of ICoCA's research show widespread apprehensions about technologies such as facial recognition, drones and AI-powered surveillance tools. Kutynska and Dei point out that the primary issue with drone usage lies in its potential to violate privacy.[74] These systems can allow governments and/or private actors to access personal data without the knowledge or consent of individuals, thereby infringing on their right to privacy.

Moreover, the integration of predictive security operations into these surveillance frameworks exacerbates existing risks, particularly regarding discrimination and privacy violations. For example, intrusive spyware such as Pegasus has reportedly been weaponised by governments to survey journalists, activists and political opponents.

- The company developing the spyware Pegasus, NSO Israel, initially marketed it as a tool for fighting crime and terrorism. However, this technology ended up being abused by government to target journalists, political dissidents and activists during the Azerbaijan-Armenia conflict.[75] A similar situation was noted for the Italian Hacking Team's technology being used in Ethiopia's internal conflict.[76]

The impact of surveillance on the right to privacy is profound. Video surveillance, location tracking, open-source data collection and large-scale data analytics can intrude into individuals' private lives, amassing vast quantities of data without explicit consent. This data is susceptible to misuse, mishandling and inadequate security measures, potentially resulting in significant breaches of personal information.

International human rights instruments affirm the right to privacy.[77] Article 17 of the International Covenant on Civil and Political Rights (ICCPR) stipulates that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

Continuous monitoring of individuals' activities poses a further threat to freedom of expression and political freedoms, fostering an environment of self-censorship where individuals may fear voicing their opinions or engaging in political activities.

71. Michael Klare, "The International Repression Trade", *Bulletin of Atomic Scientists*, November 1979.
72. Privacy International, *Big Brother Incorporated: A Report on the International Trade in Surveillance Technology and its Links to the Arms Industry*, London, 1995, available at: https://privacyinternational.org/sites/default/files/2017-12/Big_Brother.pdf
73. Geneva Center for Security Sector Governance and 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
74. Anastasiia Kutynska and Maryna Dei, "Legal regulation of the use of drones: human rights and privacy challenges", *Journal of International Legal Communication*, 8(1), 2023, 39–55, available at: https://doi.org/10.32612/uw.27201643.2023.8.pp.39-55.
75. Giulio Coppi, Natalia Krapiva and Rand Hammoud, "Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict", *Access Now*, 27 November 2023, available at: https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/
76. Human Rights Watch, "Ethiopia: Hacking Team Lax on Evidence of Abuse", 13 August 2015, available at: https://www.hrw.org/news/2015/08/13/ethiopia-hacking-team-lax-evidence-abuse
77. See also Article 12 of the Universal Declaration of Human Rights (1948); Article 16 on the Convention on the Rights of the Child (1990); Article 8 of the European Convention on Human Rights (1953); General Data Protection Regulation (GDPR) – Legal Text (2016) (GDPR, 2016/ 679).

Private security spying on Julian Assange[78]

In June 2012, Julian Assange, founder of WikiLeaks, sought refuge in the Ecuadorian Embassy in London to evade extradition to Sweden, where he faced allegations of sexual assault. Assange feared that once in Swedish custody, he could be further extradited to the United States due to WikiLeaks' publication of classified US documents, exposing him to potential prosecution in the US.

While staying in the embassy, Assange alleged that the Spanish PSC hired to protect the premises had been carrying out extensive spying against him. Court documents filed by Assange claimed that the PSC provided the CIA with audio and video recordings of his meetings with his lawyers and inner circle. Such actions would constitute violations of privacy laws as well as legal privileges and specific immunities. Spain's High Court began an investigation into the director of the PSC for the alleged unlawful activities of his company. Furthermore, in 2023, four American visitors to Assange filed a lawsuit against the CIA in a United States Federal Court, asserting that their privacy rights had been violated under the Fourth Amendment.

According to the Acting Director of University of New South Wales's Kaldor Centre for International Refugee Law, the PSC "set up a surveillance operation inside the Ecuadorian embassy: microphone, video cameras and eventually live-streaming, and it seems that everything was monitored, including lawyer-client meetings and the personal technical equipment of individuals who might be visiting Julian Assange at the embassy". Intelligence was then likely provided to the US authorities and the CIA.

Privacy International argues that the United Nations Guiding Principles on Business and Human Rights (the "UN Guiding Principles"),[79] unanimously endorsed by states through the UN General Assembly in 2011,[80] provide a clear mandate for states and companies alike to strengthen measures to respect, protect and fulfil human rights and fundamental freedoms, such as the right to privacy and freedom of expression. These responsibilities extend to all sectors, including the technology industry.[81]

ICoCA's Members and Affiliates are obligated to uphold human rights standards, including freedom of expression and privacy.[82]

The unchecked collection of sensitive data, misuse of biometric information and practices such as racial profiling can severely infringe upon fundamental rights. Such actions not only undermine personal liberties but also pose a threat to the rule of law and democratic governance. To address these concerns, it is imperative that both states and PSCs adhere to stringent regulatory frameworks that prioritise human rights protections, ensuring that the pursuit of security does not come at the expense of individual freedoms.

Surveillance and the rights of migrants

In recent years, states have increasingly contracted private security providers to deliver security services in relation with migration, both in terms of physical security (management of camps and borders) and digital security (surveillance).[83] The recent ICoCA report "Securing Dignity: The imperatives of responsible security in migration surveillance and detention"[84] highlights the risk of human rights violations when PSCs are involved in migration and border management. It specifically underscores the risks associated with the use of technologies in these contexts.

Securitisation:

The contracting of private security providers by government contributes to framing immigration primarily as a security issue rather than a humanitarian or socio-

78. The full description of the case is available on ICoCA Case Map: https://icoca.ch/case-studies/ongoing-case-private-security-company-accused-of-spying-on-julian-assange/
79. Office of the UN High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights*, 2011, available at: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
80. UN Human Rights Council, *Resolution on Human Rights and transnational corporations and other business enterprises*, UN Doc A/HRC/RES/17/4, 6 July 2011, available at https://undocs.org/en/A/HRC/RES/17/4.
81. Privacy International, *Safeguard for Public-Private Surveillance Partnerships*, December 2021, https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf
82. *The Code*, Article 21.
83. 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, responsibilities of tech companies operating in MENA*, available at: https://media.business-humanrights.org/media/documents/2022_Scrutinising_border_surveillance_in_MENA.pdf
84. ICoCA, *Securing Dignity: The imperatives of responsible security in migration surveillance and detention*, 2024, available at: https://icoca.ch/wp-content/uploads/2024/07/ICoCA-Policy-Brief-Securing-Dignity.pdf. See also UN Working Groups on Mercenaries, Report A/HRC/45/9, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/175/79/PDF/G2017579.pdf?OpenElement

economic issue, often advocating for militarised responses through advanced and dual-use technologies. As Daniela Irrera notes, "Even if not directly responsible, these companies are complicit in human rights violations and abuses committed by other actors, such as immigration and border authorities, through the security technologies they provide and their co-framing of migration as a security threat for which the solution lies in the security and military technical and technological tools that only they can provide".[85]

While surveillance technologies may be deployed under the pretext of saving the lives of migrants during their perilous journey, such technologies can inadvertently compel migrants to alter their routes, forcing them into even more dangerous situations as they attempt to evade detection. There is also a lack of transparency regarding how data is collected and shared by PSCs.

Externalisation

Contracting private security companies to use advanced technologies to monitor migration routes contributes to the development of state "externalisation" policies, under which border control no longer occurs at the physical borders of countries of destination but rather in countries of first arrival, transit or departure, or on international waters. As part of this practice, states are leveraging private security services to circumvent their obligations to uphold the principle of non-refoulement and to guarantee the human rights of those seeking asylum.[86]

- In October 2020, The Guardian reported that Frontex had awarded contracts to private companies to operate drones spotting migrant boats crossing the Mediterranean. Aerial footage was shared with the Libyan Coast Guard, which would intercept the boats, even when they were well outside of Libyan waters, and forcibly return them to Libya, where migrants allegedly face arbitrary detention and other human rights abuses.[87]

According to Daria Davitti, the European refugee "crisis" meets the conditions of a high-risk context as defined by the United Nations Guiding Principles on Business and Human Rights (UNGPs). This implies that both states and PSCs involved are under heightened human rights obligations when implementing the UNGP.[88]

85. Daniela Irrera, "The (ab)use of PMSCs in managing migration flows and the contradictions of the EU", *Private Security Conversations* blog, 20 November 2022, available at: https://blog.icoca.ch/the-abuse-of-pmscs-in-managing-migration-flows-and-the-contradictions-of-the-eu/

86. Panagiotis Loukinas, "Drones for Border Surveillance: Multipurpose Use, Uncertainty and Challenges at EU Borders", *Geopolitics*, 27(1), 2022, 89-112, available at: https://www.tandfonline.com/doi/full/10.1080/14650045.2021.1929182

87. Jasper Jolly, "Airbus to operate drones searching for migrants crossing the Mediterranean", *The Guardian*, 20 October 2020, available at: https://www.middleeasteye.net/news/libya-europe-migration-frontex-surveillance-deadly-fate; Antonio Mazzeo, "Border surveillance, drones and militarization of the Mediterranean", *Statewatch*, 6 May 2021, available at: https://www.statewatch.org/analyses/2021/border-surveillance-drones-and-militarisation-of-the-mediterranean/, See also "No rescue from above: Europe's surveillance in the Mediterranean leaves migrants to their fate", 30 January 2002, available at: https://www.middleeasteye.net/news/libya-europe-migration-frontex-surveillance-deadly-fate

88. ICoCA, "AGA 2021 Opening Plenary: The role of private security companies in migration detention," 29 November 2021, available at: https://icoca.ch/2021/11/29/aga-2021-opening-plenary-the-role-of-private-security-companies-in-migration-detention/. See also Daria Davitti, "The Rise of Private Military and Security Companies in European Union Migration Policies: Implications under the UNGPs", *Business and Human Rights Journal*, 4(1), 2019, 33-53.

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 can be used to discriminate against various categories of the population and the staff of PSCs themselves.

AI algorithms trained on biased data can disproportionately target certain racial or ethnic groups, perpetuating systemic inequalities and injustices.[89] This is particularly concerning in contexts where PSCs are contracted to perform law enforcement duties, as biased AI can exacerbate existing prejudices and result in the unfair treatment of vulnerable populations.[90] This may undermine due process, the right to a fair trial and the right to privacy.

- For instance, the Pegasus project in the UK mentioned above, which relies heavily on facial recognition technology to combat shoplifting, sparked controversy as human rights organisations claimed that it would wrongly criminalise certain categories of people.[91] Several human rights organisations urged retail companies to withdraw from this surveillance scheme, arguing that "Facial recognition technology notoriously misidentifies people of colour, women and LGBTQ+ people, meaning that already marginalised groups are more likely to be subjected to invasive stops by police or at increased risk of physical surveillance, monitoring and harassment by workers in your stores".[92]

Algorithms used for predictive policy may not be free from bias, potentially leading to racial profiling. The use of such algorithms also raises concerns regarding transparency. Furthermore, the privatisation of public safety risks weakening accountability and oversight mechanisms.[93]

The potential for discrimination in surveillance practices cannot be overlooked. Section 42 of the Code states that:

> *"Member and Affiliate companies will not, and will require that their Personnel do not, discriminate on grounds of race, colour, sex, religion, social origin, social status, indigenous status, disability, or sexual orientation when hiring Personnel and will select Personnel on the basis of the inherent requirements of the contract."*

To help address these challenges, the ICoCA-ICT4Peace Toolkit offers essential guidance on best practices to limit algorithmic bias.

89. Alexander Babuta and Marion Oswald, *Briefing Paper: Data Analytics and Algorithmic Bias in Policing*, RUSI, 16 September 2019, available at: https://assets.publishing.service.gov.uk/media/5d7f6b2540f0b61ccdfa4b80/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf
90. Rashida Richardson et. al, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice", *94 N.Y.U. L. REV. ONLINE 192,* 2019, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423
91. Mark Townsend, "Major UK retailers urged to quit 'authoritarian' police facial recognition strategy", *The Guardian*, 28 October 2023, available at: https://www.theguardian.com/technology/2023/oct/28/major-uk-retailers-urged-to-quit-authoritarian-police-facial-recognition-strategy
92. Liberty, "Joint letter to retail CEOs regarding Project Pegasus," October 2023, available at: https://www.libertyhumanrights.org.uk/wp-content/uploads/2023/10/Liberty-Joint-letter-to-retail-CEOS-regarding-Project-Pegasus-October-2023.pdf
93. Caroline Haskins, "Dozens of Cities Have Secretly Experimented With Predictive Policing Software", *Vice, 6* February 2019, available at: https://www.vice.com/en/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software

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

> *"Many of the security personnel have limited knowledge about digital safety, so even when handling digital tools they may not understand how to secure data or protect people's privacy".*
> **(Civic-tech expert, African human rights NGO)**

As private security actors increasingly adopt technology, they are more frequently handling sensitive information obtained through surveillance techniques, as well as from their own records, which may include data on their own staff, operations and clients. The ethical management of this information – encompassing how it is stored, used and ultimately deleted – remains a critical human rights concern that demands stringent regulation and oversight.[94] The right to be forgotten, as this is often colloquially referred to, and as was formally enshrined in the European Union's GDPR legislation, is fundamental to protecting broader human rights such as freedom of expression.

Once collected, PSCs must ensure that information is managed in compliance with legal standards to prevent misuse by clients, state authorities or other third parties.

Experts interviewed as part of this research raised serious concerns regarding data mining practices in weak regulatory environments, particularly in conflict zones. In such contexts, the risk of human rights violations escalates without robust corporate due diligence processes to ensure that data handling complies with international human rights law. These insights reinforce the necessity for transparency and accountability in how PSCs manage large-scale data analytics and biometric data collection, given the profound implications for individual rights.

Many national jurisdictions have begun to tackle the human rights issues related to data protection by enacting regulations that emphasise principles such as purpose limitation, fairness and transparency, and accountability. These principles ensure that personal data is collected and processed with respect for individual rights, as outlined in the EU GDPR, which applies to both EU-based companies and those outside the EU that process the data of individuals within the Union. However, as of 2021, only 66% of countries worldwide had similar legislation in place, with a further 10% having draft laws under consideration.[95]

94. UNHRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on surveillance and human rights*, 28 May 2019, UN Doc A/HRC/41/35, available at: https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur
95. Tar Davis, "Data Protection in Africa: A Look at OGP Member Progress", *Alt Advisory*, 2021, available at: https://altadvisory.africa/2021/08/12/data-protection-in-africa-a-look-at-ogp-Member-progress/

Additionally, cross-border data flows pose significant challenges for PSCs. Operating in complex environments often means that keeping data locally might expose sensitive information to violent or repressive actors. At the same time, jurisdictions like the EU prohibit data transfers to countries that do not meet specific data protection standards, further complicating PSC operations.

The application of POPIA in South Africa

Private security is a major industry in South Africa, where surveillance technologies are massively used by PSCs. Participants in the consultations conducted by ICoCA and ICT4Peace in South Africa mentioned that, although the country has adopted the Protection of Personal Information Act (POPIA), implementation measures for PSCs are still missing. A major issue relates to how private security personnel collect and manage personal information at the entrances of public and private properties, such as gated communities or official buildings. While such information was previously recorded in handwritten logbooks, it is now increasingly gathered using digital surveillance tools.

Recently, the Chairperson of South Africa's Information Regulator of South Africa, Advocate Pansy Tlakula, raised concerns about why access points to private properties require extensive personal information from visitors, and how this information is protected. "When you go into gated communities and office parks, what happens is they scan your licence disc, which contains a lot of personal information. They scan your driver's license and some even take your photo." However, POPIA specifies that only the minimum necessary personal information may be collected, and solely for a specific purpose. "How are they protecting it? Where does it end up? That disc has your name, home address and ID number linked to it," Tlakula stated, suggesting the adoption of a code of conduct for security providers.

Technology itself may offer part of the solution. The South African company At the Gate (ATG) advertises digital scanning systems that can be configured to conceal personal information on scanning devices or in reports stored on backend systems. These devices can be set not to retain any captured personal data. Once the information is scanned, it can be immediately encrypted and uploaded to secure cloud-based storage. This means security guards, other visitors, site managers and potential criminals have no access to the data stored on the devices.

Source: Hanno Labuschagne, Driving licence card scanner warning for estates, my broadband, 30 October 2024, available at: **https://mybroadband.co.za/news/security/567285-driving-licence-card-scanner-warning-for-estates.html**

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 already having a significant impact on the recruitment, working conditions, required skillset and training of security guards.

Many PSCs are already using surveillance technology to monitor their own staff, often as a cost-saving measure for supervision and oversight. However, such practices raise serious concerns about the right to privacy of security staff, similar to the ones associated with public surveillance. Since the COVID-19 pandemic and the generalisation of remote working, there has been growing acceptance of using surveillance tools to track employee performance. Nonetheless, this trend should not justify practices that unduly intrude into workers' privacy. According to the European Foundation for the Improvement of Living and Working Conditions, "The risk of breach of privacy and data protection rights becomes even more acute in the context of remote working. The provision of digital devices by employers for work and personal use leads to an increasing enmeshing of employees' private and working lives and results in the merging of personal with work-related data".[96] While technology can certainly improve working conditions of security workers, remote working may also blur the boundaries between work and personal life, disrupting workers' work-life balance.

The data collected by PSCs on their employees need also to be protected against possible hacking. Private security personnel and their families may be targeted by criminal gangs or enemy forces. The recent example of the Taliban gaining control of systems holding sensitive biometric data of security personnel left behind by Western donor governments in Afghanistan in 2021 is a case in point.[97]

Surveillance of workers may also infringe on their labour rights, notably the freedom of association of workers.

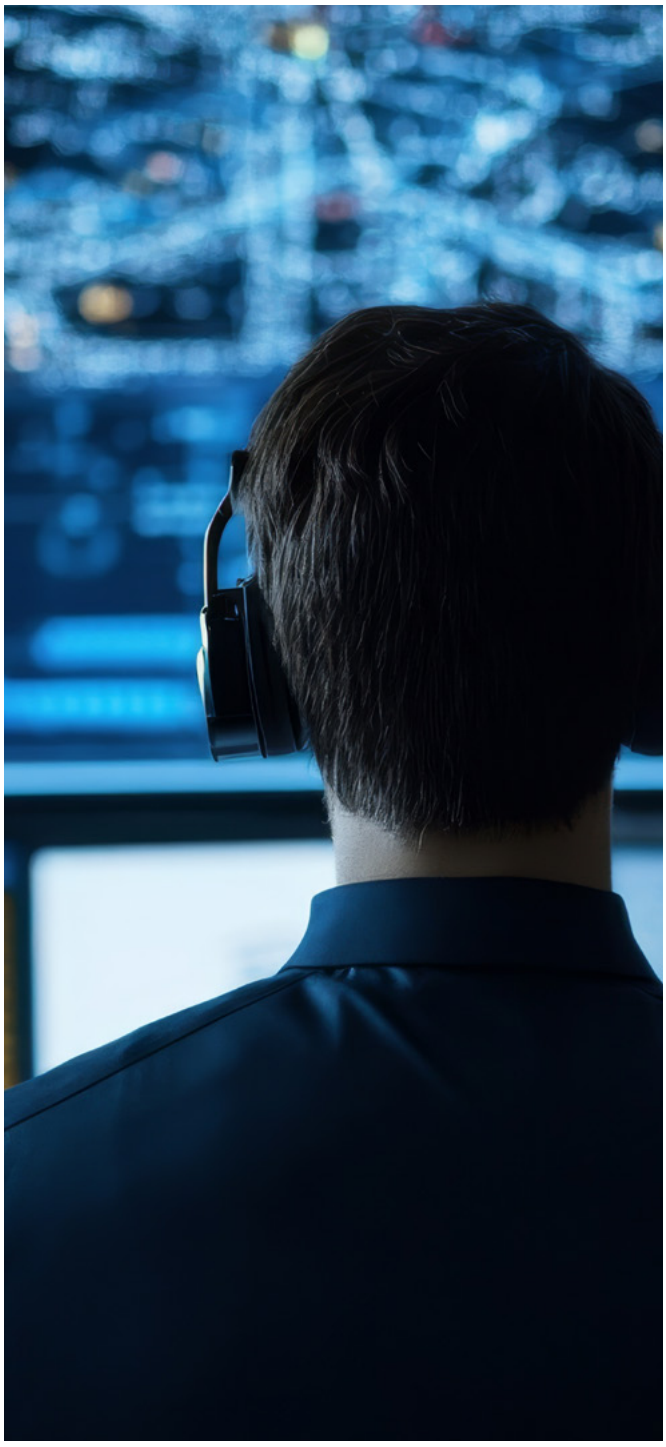
Finally, the use of new technologies raises significant concerns about workforce displacement in an industry where many workers already face precarious employment conditions. Guidance must be provided to enable PSCs to use technology to enhance security operations by complementing, rather than replacing, human personnel. This process will demand significant investment in training programmes to equip security

96. European Foundation for the Improvement of Living and Working Conditions, *Monitoring and surveillance of workers in the digital age*, available at: https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age

97. Human Rights Watch, "New Evidence that Biometric Data Systems Imperil Afghans: Taliban Now Control Systems with Sensitive Personal Information", 22 March 2022, available at: https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans

staff with the necessary skills to work with advanced technologies. Staff also need to be trained to respect human rights in their work, a training which is virtually absent today according to our interviewees.

Moving forward, stakeholders in the private security industry must aim to strike a balance between innovation and responsible use of technology, ensuring that technological advances lead to the professionalisation of the sector and safeguard the rights of workers and the public.



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.

PART V.
Bridging the gap: 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 role of ICoCA

In view of the increasing number of tech companies involved in surveillance activities, David Kaye, the UN Special Rapporteur on Freedom of Opinion and Expression, emphasised the need for a "co-regulatory governance" framework which, involving the "meaningful participation from State, business and civil society actors", may provide "a blueprint for human rights accountability in the private surveillance industry".[98] Kaye specifically cites ICoCA as a model to follow.

Indeed, as multi-stakeholder initiative bringing together representatives of industry, states and civil society, ICoCA provides a model of co-governance for the private security industry. The UN Working Group on the issue of human rights and transnational corporations and other business enterprises advocates for such a model to "operationalise the human rights responsibilities of the sector and set out practical guidance and standards for the responsible provision of cyber services".[99]

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.[100]

The above-mentioned report by the Geneva Centre for Security Sector Governance and Privacy International highlights the urgent need for collaboration among international and national non-governmental organisations, civil society, industry stakeholders and state actors to improve the governance of privatised surveillance. It recommends that this effort should be grounded in frameworks like the Montreux Document and the Code.[101]

In its recently adopted strategic plan for 2024-2030,[102] ICoCA dedicated one of its 5 strategic goals to the technological transformation of the industry: "Goal 4: Establish standards for respecting human rights and using new technologies by private security providers, integrating these into the International Code of Conduct." The impact it seeks is "a private security industry that employs new technologies in a manner that enhances its contribution to global security and stability while respecting human rights and ethical standards, including the right to privacy". ICoCA's strategy aims to: (i) further adapt and enlarge its platform to all the new actors technology is bringing into 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.

Ensuring respect for human rights by new security actors

> *"Co-regulatory governance that involves meaningful participation from State, business and civil society actors may provide a blueprint for human rights accountability in the private surveillance industry".*
> **David Kaye, UN Special Rapporteur on Freedom of Opinion and Expression[103]**

98. 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
99. 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
100. ICT4Peace, pp. 55-57.
101. Geneva Center for Security Sector Governance and Transparency International, p. 25.
102. ICoCA, ICoCA 2024-2030 Strategic Plan, December 2024, available at: https://icoca.ch/2025/01/22/shaping-the-future-of-responsible-private-security/
103. David Kaye, paras. 61-64.

The lines are increasingly blurred between tech companies providing security-related services and traditional PSCs providing guarding services. As discussed above, the International Code of Conduct for Private Security Service Providers does apply to both, as its scope covers "Private Security Companies and other Private Security Service Providers" (Article 1). However, many tech companies may not be fully aware of their responsibilities when delivering services that fall within the scope of private security.

This raises a broader question: should the governance of private security expand to include industries that produce security technologies and cyber services, and not just those that use them in operations? Are clients of these new types of security actors sufficiently aware of the human rights and legal risks involved?

It is because of this lack of awareness and clarity that urgent action is needed to regulate the use of advanced technologies in the provision of security services. By engaging in a review process of its Code and committing to closely monitor technological developments in the sector, ICoCA aims to lead the way, offering its multi-stakeholder governance structure as a platform to set clear standards for the protection of human rights in security services that utilise technology.[104]

Recommendations: ICoCA could support the expansion of technology's governance in the private security field by:

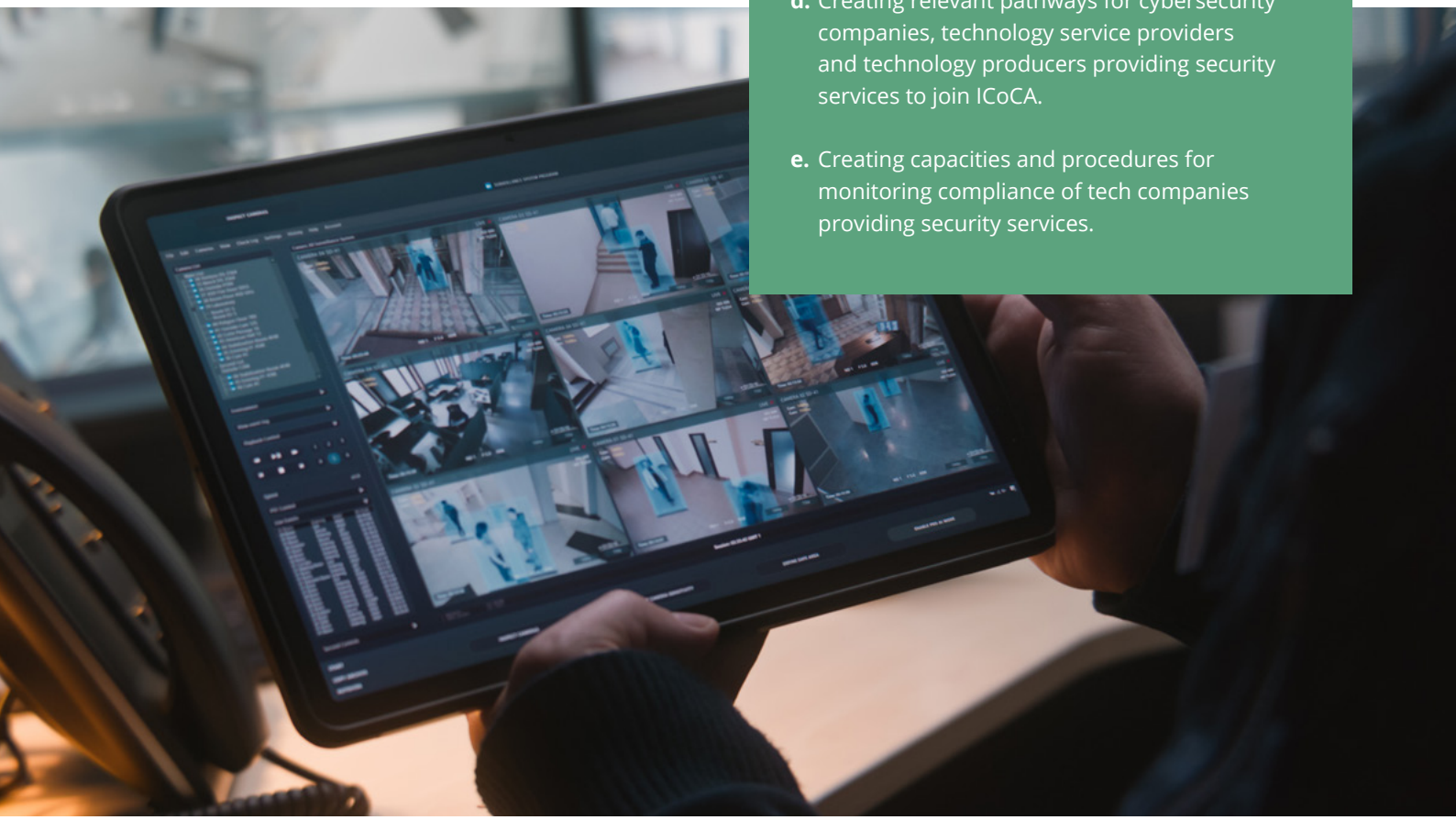
a. Engaging in a dialogue with public authorities, cybersecurity companies, technology service providers and technology producers to identify possible risks, gaps and needs in terms of regulation and oversight

b. Engaging in a dialogue with CSOs and networks or coalitions of CSOs 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.



104. ICT4Peace, pp. 55-57

Implementing the Code

Implementing the provisions of the Code would go a long way towards ensuring the responsible use of technologies. Best practices already exist (see the Geita Gold Mine case box) and could be replicated.

Recommendations: 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.

Best practice: Surveillance at the Geita Gold Mine (Tanzania)

Following a series of serious violent incidents with the local community, the management of the Geita Gold Mine in Tanzania undertook a comprehensive review of its security arrangements. Prior to 2014, the mine's security relied heavily on the police and on the use of force or threat thereof for both deterrence and enforcement. Incursions were frequent and serious incidents reportedly commonplace. Since 2014, the mine has implemented an innovative, integrated security strategy to safeguard its personnel, assets and extracted gold. This revised approach, called the "Five Point Plan – Community Enhanced Security", incorporates the use of technologies to reduce risks. Its key elements include:

- Removing people from risk and risk from people, to minimise the potential for conflict.
- Defining the role of communities in complementing security initiatives.
- Defining the role of both private and public security in supporting the community-enhanced security model.
- Deploying trained, skilled and equipped rapid reaction teams to improve incident response and handling.
- Optimising technology versus manpower through the use of appropriate technologies to reduce risk and improve efficiencies.

CCTV is used extensively, including high-end thermal cameras with long range capability (up to 10 km) and night-vision sensitivity. These systems reduce the reliance on physical patrols, as CCTV towers are strategically placed at regular intervals along the site's boundary to enable wide-area surveillance and proactive threat detection.

Surveillance cameras are also installed in all vehicles and bodycams are being introduced to aid investigations, particularly in response to potential allegations of human rights abuses by security guards.

While there is no physical border such as wall or fence, the CCTV towers along with beacons and painted boulders essentially act as boundary markers, established in agreement with local communities. The absence of a physical perimeter has helped foster trust and improve relations between the community and the company. This technological infrastructure also supports the mine's community policing programme, enabling community police to log and report intrusions systematically. The overarching aim is to use technology to improve operational efficiency, minimise human intervention and, crucially, reduce the risk of collusion – which now represents the most significant remaining challenge, following marked improvements in community relations.

Out of this experience, three main best practices can be recommended:

- Leverage technology to compliment physical security arrangements – CCTV and other tools can replace the need for physical barriers.
- Use technology responsibly, including to build accountability of the security guard force – for example, through deployment of bodycams.
- Ensure the surrounding community are engaged and understand how technology tools are being deployed around the site.

Note: This case is presented in detail on the ICoCA Case Map available at: **https://icoca.ch/case-studies/geita-gold-mine/**

Interpreting and reviewing the Code

The question of revising the Code was addressed during a consultative workshop organised by ICoCA in March 2025. It was agreed that the Code is a living document that must be interpreted in light of the evolving landscape of private security, even if it does not explicitly mention specific technologies. Additionally, should the Association decide to initiate a revision process, participants recommended structuring the discussions around several key guiding principles:

1. Anticipating the specific human rights and international humanitarian law (IHL) risks that may arise from the use of technologies could serve as a framework for determining which provisions need to be amended or added to the Code.

2. The original focus of the Code was on preventing physical violence and coercion by private security providers. However, with the growing use of advanced technologies, it is crucial to place greater emphasis on civil and political rights, as well as other human rights that may be violated by new types of security operations enabled by these technologies. This includes rights such as privacy, freedom of expression and non-discrimination. While these rights are already referenced in the Code, a revision process could further underscore their protection.

3. Rather than attempting to list and regulate every possible technology, the Code could introduce a provision requiring security providers to ensure that any new weapons, methods or security technologies comply with its standards and other relevant national or international norms. This provision would obligate companies to review the legality of new weapons, tactics or technologies before deploying them in security operations. Beyond the Code, a similar rule could be incorporated into national legislation and regulatory mechanisms, such as licensing procedures for security companies.

4. The transformation of security services could be reflected in the Code, with two key considerations: first, how existing security services are being delivered through new methods and the changes and risks this may introduce; and second, the emergence of new services, such as cybersecurity. While the list of security services in Section B of the Code is non-exhaustive, it remains overly narrow. To ensure the Code stays relevant to emerging security providers, it could include key terms like digital technologies, data protection and cybersecurity, extending its scope beyond traditional private security companies."

Recommendations: 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.

CONCLUSION

The rapid development of technology presents both significant opportunities and complex challenges for private providers of security services. While these technological advancements may offer enhanced operational efficiency and effectiveness, they also pose critical human rights risks.

The increased reliance on tools of surveillance, AI-driven decision-support systems or predictive policing can be beneficial for security operations but, if not managed responsibly, may have serious implications for individual rights and democratic systems. As traditional PSCs adopt these technologies, tech companies enter the security market and new security services emerge, there is an urgent need for responsible use and stringent regulatory frameworks to mitigate the human risks associated with this transformation.

By prioritising the responsible use of technology and embedding human rights considerations into their operational frameworks, PSCs and their clients can better navigate the complex intersection between security and individual freedoms, ultimately contributing to a safer and more equitable society.

The Toolkit for the Responsible Use of Technology supports PSCs in addressing the challenges of integrating AI and other advanced technologies into their operations while ensuring compliance with human rights standards and legal obligations. By implementing the Toolkit's recommendations, companies can strengthen their operational frameworks, mitigate risk and uphold principles of democratic governance. This can also help PSCs build trust with clients and the communities they serve.

The Toolkit represents an important step toward responsible regulation but, as technology continues to evolve, so too must the guidance. The Code and existing governance and monitoring mechanisms should be continuously reviewed and interpreted in light of emerging risks to human rights and IHL. Ongoing collaboration between PSCs, policymakers and regulators is essential to establishing strong oversight mechanisms for private security in the digital age – mechanisms that protect not only individuals and assets but also uphold human rights and ethical standards.

Acknowledgements

Author: Vincent Bernard

Research Assistant: Samuel Pennifold

Special thanks to Souhail Belhadj-Klaz, Florie Barbotte, Anne-Marie Buzatu, Leo Colonnello, Elena Fecchio, Chris Galvin, Alice Iynédjian, Tom Mather, Antoine Perret, Anna Sadilova, Ebrima Touray, Eliza Urwin and Jamie Williamson.

ICoCA, 2025

The Responsible Security Association

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