

**Thematic Report on new technologies, including information and communications technology; and their impact on the promotion and protection of human rights in the context of assemblies, including peaceful protests.**

1. **Law, policies and programmes that have been developed to address the impact of new technologies, including information and communications technology, on human rights in the context of assemblies, including peaceful protest.**

To the knowledge of the Special Rapporteur (SR) on the rights to freedom of peaceful assembly and of association (FoAA), no international laws have been developed or passed on the impact of new technologies on human rights in the context of assemblies, including peaceful protest. However, the SR has stated in his reports that international law protects the rights to FoAA, whether exercised in person, through technologies of today, or through technologies that will be invented in the future. Existing international human rights norms and principles should not only dictate State conduct, but also be the framework that guides digital technology companies’ design, control and governance of digital technologies; whether we are examining hard law or soft law. In previous reports, the SR has recognized that digital technology is integral to the exercise of the rights of FoAA.[[1]](#footnote-1)

The rights to FoAA are protected in article 20 of the Universal Declaration of Human Rights and in articles 21 and 22 of the International Covenant on Civil and Political Rights. An “assembly” can be defined as an intentional and temporary gathering in a private or public space for a specific purpose. Although an assembly has generally been understood as a physical gathering of people, it has been recognized that human rights protections, including for freedom of assembly, may apply to analogous interactions taking place online.

The General Assembly has also called upon all States to “ensure that the same rights that individuals have offline, including the rights to freedom of expression, of peaceful assembly and of association, are also fully protected online, in accordance with human rights law”.[[2]](#footnote-2)

While these rights are not absolute, the Special Rapporteur has stated in his reports that the freedom to access and use digital technologies for the exercise of FoAA should be viewed as the rule, and the limitations as the exception. The general norm should be to permit the open and free use of the Internet and other digital tools.[[3]](#footnote-3)

Technology serves both as a means to facilitate the exercise of the rights of assembly and association offline, and as virtual spaces where the rights themselves can be actively exercised.[[4]](#footnote-4) Indeed, such technologies are important tools for organizers who seek to mobilize a large group of people in a prompt and effective manner, and at little cost, and also serve as online spaces for groups of people that are marginalized by society and are confronted with restrictions when operating in physical spaces. The SR on the rights of FoAA has called upon States to ensure that everyone can access and use the Internet to exercise these rights, and that online associations[[5]](#footnote-5) and assemblies[[6]](#footnote-6) are facilitated in accordance with international human rights standards.

Furthermore, the Human Rights Council (HRC) has recognized that although an assembly has generally been understood as a physical gathering of people, human rights protections, including for freedom of assembly, may apply to analogous interactions taking place online.[[7]](#footnote-7) In addition, the HRC has emphasized that States have the obligation to respect and fully protect these rights online as well as offline and has called on States to “ensure effective remedies for human rights violations, including those related to the Internet, in accordance with their international obligations”.[[8]](#footnote-8)

The SR notes the increased use of the Internet, in particular social media, and other information and communication technology, as basic tools which enable individuals to organize peaceful assemblies. However, some States have clamped down on these tools to deter or prevent citizens from exercising their right. In this connection, the SR refers to a recent report of the SR on the promotion and protection of the right to freedom of opinion and expression, in which he recommended, inter alia, that “all States [should] ensure that Internet access is maintained at all times, including during times of political unrest”.[[9]](#footnote-9)

The Guiding Principles on Business and Human Rights have been adopted by the High Commissioner for Human Rights. In the document, companies’ responsibilities to respect human rights, including the global framework for assessing digital technology companies, is highlighted. Guiding principles 11 and 24 recognize that business “should respect human rights” by avoiding infringing on the human rights of others and by addressing adverse human rights impacts with which they are involved.[[10]](#footnote-10) Therefore, to fulfil this obligation, business enterprises should have in place human rights policies and processes, including a policy commitment to meet their responsibility to respect human rights; a human rights due diligence process to identify, prevent, mitigate, and account for how they address, their human rights impacts; and processes to enable the remediation of any adverse human rights impacts that they cause or to which they contribute.[[11]](#footnote-11)

The digital age has opened new space for the enjoyment of the rights of FoAA. There are numerous examples across the globe which demonstrate the power of digital technology in the hands of people looking to come together to advance democracy, peace and development. However, the digital revolution has also brought a range of new risks and threats to these fundamental rights.

Laws criminalizing access to and use of digital tools are increasingly being adopted, in a diverse range of countries. These laws establish criminal liability in often vague and ill- defined terms, allowing for arbitrary or discretionary application and resulting in legal uncertainty. As such, they fail to meet the legal standards for permissible restrictions under articles 21 and 22 of the Covenant. The following domestic laws are mentioned as a non-exhaustive list of examples to address the advantages and challenges of the digital age within the domestic realm. Examples include cybercrime laws, antiterrorism laws, surveillance laws, and laws against protests.[[12]](#footnote-12)

Regarding Cybercrime Laws, the prohibition against the use of electronic devices “to ruin communal harmony or create instability or disorder or disturb or is about to disturb the law and order situation”[[13]](#footnote-13), found in the Digital Security Act 2018 of Bangladesh, for example, grants officials excessive discretion to determine what would constitute unlawful conduct and to pursue criminal actions against individuals based on arbitrary and subjective grounds. Other cybercrime laws give wide-ranging power to governments to block websites deemed critical of the authorities, such as those belonging to human rights defenders[[14]](#footnote-14), based on broadly defined concepts of national security.

Regarding the Antiterrorism Laws, mandate holders have raised concern on several occasions about the excessively broad language often used in antiterrorism legislation[[15]](#footnote-15). Although the SR is aware that States have an interest in protecting national security and public safety, which are legitimate grounds for restricting the right of FoAA, these laws often are drafted in ways that give opportunities for abuse. For example, many laws include broad and subjective concepts in the definition of terrorism, such as “widespread terror through political extremism”, “serious social disturbance”[[16]](#footnote-16), “disrupting public services”, “inciting violence at demonstrations” and “creating fear amongst the public to jeopardize the solidarity” of a country.[[17]](#footnote-17) The vagueness of the concepts makes it extremely difficult to determine with reasonable certainty what kind of conduct (online and offline) would be considered “terrorism”.

In addition, regarding the Surveillance Laws, the mandate holders have stressed that overly broad and vague surveillance laws often fail to target specific individuals on the basis of a reasonable suspicion.[[18]](#footnote-18) For example, the Investigatory Powers Act 2016, of the United Kingdom of Great Britain and Northern Ireland, contained vague language that allowed authorities to target a group or category of people without requiring each target of the surveillance to be individually identified. Other forms of surveillance law give enormous license to States to monitor citizens’ online activities, such as the Telecommunications and Other Legislation Amendment Bill, of Australia, which includes provisions that would grant authorities unfettered powers to compel companies to facilitate access to encrypted user data for security agencies and weaken encryption technologies.[[19]](#footnote-19) The risks of abuse are increased given that many existing laws and regulations governing surveillance do not keep pace with rapid changes in surveillance technology and its potential uses.

In regards of the Media anti-fake news Laws, during consultations with civil society, concerns were raised about the broad language used in Cambodian interministerial decree No. 170 of 28 May 2018, which prohibits online activities “intended to create turmoil in society”. This provision grants authority’s excessive discretion to prohibit a wide range of activities online, including sharing photos and videos of police abuse against protesters, disseminating messages calling for peaceful demonstrations, and political campaigning. The rules also impose severe penalties, and civil society organizations face the risk of being shut down for disseminating prohibited content, which is disproportionate and incompatible with the right to freedom of association. In addition, these restrictions are imposed through a government decree, adding to legality concerns.[[20]](#footnote-20)

Finally, with reference to the Demonstrations Laws, in the Russian Federation, for instance, the “Yarovaya Law” introduced overly broad amendments to the Criminal Code that prohibited “inducing, recruiting or otherwise involving” others in the organization of “mass unrest”. Publishing statements on the Internet is considered an aggravating factor. Similarly, in Kazakhstan, the Criminal Code forbids providing “assistance” to “illegal” assemblies, including by “means of communication”.[[21]](#footnote-21) The broad language of these provisions unduly limits the rights to freedom of peaceful assembly, association and expression, by potentially making it a crime to promote, discuss, seek or link to information regarding a protest event.

1. **Effective uses of such technologies as enablers of the exercise of human rights in the context of assemblies, including peaceful protest (e.g. how new technologies have facilitated the organization of assemblies, including peaceful protests).**

Digital technologies have brought remarkable opportunities for the enjoyment of the rights of FoAA; by serving both as tools through which these rights can be exercised “offline” and as spaces where individuals can actively form online assemblies and associations[[22]](#footnote-22), digital technologies have vastly expanded the capacities of individuals and civil society groups to organize and mobilize, to advance human rights and to innovate for social change. These tools should be seen by the authorities “as an excellent opportunity to interact with a large and diversified audience prior to and during peaceful assemblies, with a view to sensitizing them on their role and functions, and ultimately building or reinforcing trust among the population”[[23]](#footnote-23). Likewise, States should recognize the value of technology to facilitate people’s rights to public participation. Therefore, the SR welcomes efforts by many governments to establish online platforms through which those interested can submit and collect signatures for petitions on government policies and legislative action.

An individual or association’s website is an important means for the individual or association to advocate for a cause; to raise issues of public concern and contribute to public debate; to report human rights violations; to publish research; to seek, receive and impart information and ideas of all kinds; to build coalitions and networks with other organizations, including from abroad; to engage in fundraising; to recruit members and volunteers; and to interact with international and regional human rights bodies.[[24]](#footnote-24)

The role of social media in mobilizing people to the streets is well known. During his visit to Armenia in 2018, for instance, the SR heard several stories of how social media platforms, live-streaming tools and communication apps had played a key role in the “velvet” revolution of 2018 that had led to the resignation of the Prime Minister. The hashtags #MyStep and #MerzhirSerzhin had been used to share information, and mobilize citizens and gather their support, circumventing the government-controlled media. Many youth movements across the world are supported by social media, as demonstrated by the #RoadSafetyMovement in Bangladesh, the #FeesMustFall campaign in South Africa, and the #FridaysForFuture and #ClimateStrikes global movement.[[25]](#footnote-25)

Individuals can now use online spaces to participate in a virtually connected civil society. Women activists, for example, use the Internet to connect and to exchange strategies, including across borders, and as a space for organizing.[[26]](#footnote-26) The #MeToo movement is perhaps the most notable recent example. In 2017, survivors of sexual violence used social media platforms to share personal stories of sexual harassment and abuse and to call for gender equality in the workplace, under the hashtag #MeToo. Within a year, the hashtag had reportedly been used more than 19 million times[[27]](#footnote-27) both by survivors and by supporters of the cause. Although the movement began in the United States, women also joined in France (#BalanceTonPorc), in the Arab world (#AnaKaman), in India (#MeTooIndia), in Ukraine (#IAmNotAfraidToSayIt) and in Mexico (#MeTooMexico) also joined.

Furthermore, through the use of social media, e-petitions and crowdfunding platforms, civil society organizations have been able to reach new audiences, spread information, attract members and find funding in ways that were previously impossible or extremely costly. Similarly, digital technologies have become increasingly important for labour unions to perform their core functions, including organizing protests, keeping in touch with members and providing spaces for discussion and decision-making.[[28]](#footnote-28)

Additionally, several civil society groups have taken advantage of technology to innovate in addressing social problems. The Eyewitness project has developed technologies to enhance the capacity of civil society actors and individuals to document and record human rights abuses. Platforms such as Signal and Crabgrass have been developed to enhance security of civil society groups’ digital communications. Meanwhile, dominant online platforms such as Facebook, Twitter and YouTube have become the gatekeepers to people’s ability to enjoy the rights of FoAA, wielding enormous power over whether individuals and civil society actors can access and participate in the democratic space.[[29]](#footnote-29)

These examples demonstrate a remarkable range of uses of digital technology for the enjoyment of the rights of peaceful assembly and association, and the interplay between offline and online spheres. The Special Rapporteur observes that the rights of FoAA are often seamlessly exercised online and offline. For example, many associations have offices and people meet face-to-face. At the same time, they use digital technology to carry out daily activities and as a space to convene online discussions and assemblies. Similarly, associations primarily based online can also hold in- person discussions and assemblies. The extent of the online and offline activities depends on the association’s membership, strategies and goals. Simply stated, international law protects the rights of FoAA, whether exercised in person, or through the technologies of today, or through technologies that will be invented in the future.[[30]](#footnote-30)

1. **The human rights challenges posed by interferences with the availability and use of such technologies in the context of assemblies, including peaceful protests (e.g. through networks disruptions, blocking of internet services or restrictions on secure and confidential communications).**

The digital age has opened new space for the enjoyment of the rights of FoAA. There are numerous examples across the globe which demonstrate the power of digital technology in the hands of people looking to come together to advance democracy, peace and development. However, the digital revolution has also brought a range of new risks and threats to these fundamental rights.[[31]](#footnote-31)In this regard, the SR has observed how, over the past decade, States have used technology to silence, surveil and harass dissidents, political opposition, human rights defenders, activists and protesters, and to manipulate public opinion. Governments are ordering Internet shutdowns more frequently, as well as blocking websites and platforms ahead of critical democratic moments such as elections and protests. A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world. While the role that technology can play in promoting terrorism, inciting violence and manipulating elections is a genuine and serious global concern, such threats are often used as a pretext to push back against the new digital civil society. [[32]](#footnote-32)

The mandate holder is concerned about the variety of measures and tactics that are used by States to control and impede access to and use of digital technology for the exercise of the rights of FoAA. Laws that criminalize online content continue to proliferate, leading to a significant chilling effect on advocacy and mobilization. Numerous jurisdictions have resorted to shutting down access to communications networks and services during elections and public demonstrations, and blocking websites belonging to civil society groups, including human rights organizations. Demonstrating a sophisticated grasp of emerging technical tools, some States, and malicious third-party actors, have increased use of digital surveillance and online harassment against civil society actors, human rights defenders, opposition political leaders and those who plan to stage peaceful public assemblies. All of this has significantly reduced the space in which people can defend and promote shared interests. Notably, the HRC has expressed concern about “the emerging trend of disinformation and of undue restrictions preventing Internet users from having access to or disseminating information at key political moments, with an impact on the ability to organize and conduct assemblies”.[[33]](#footnote-33)

The SR believes network shutdowns are in clear violation of international law and cannot be justified in any circumstances. Shutdowns fail to meet the established test for restrictions on the right to peaceful assembly found in article 21, and for restrictions on the right to freedom of association under article 22 (2), of the Covenant. In most cases, network shutdown orders lack a legal basis. Where a legal basis does exist, shutdown orders are often coupled with broad and vague provisions and lack adequate independent oversight. While these measures are typically justified on grounds of national security and public order, they are a disproportionate and generally ineffective, means of achieving those legitimate aims.[[34]](#footnote-34)

In general, the blocking of entire websites is an extreme, disproportionate measure that severely limits the ability to carry out these activities, and therefore undermines the exercise of FoAA. In many cases these measures appear to improperly target dissent, and as such, cannot be justified as pursuing a legitimate aim. The SR considers that to prohibit an individual or association from publishing material online “solely on the basis that it may be critical of the government or the political social system espoused by the government” is inconsistent with the rights of FoAA.[[35]](#footnote-35)

Furthermore, blockingof entire websites of human rights organizations and political opposition parties has become increasingly common in many parts of the world, including in countries of the Middle East and North Africa region. For example, in the United Arab Emirates and in Saudi Arabia, authorities routinely block websites containing online criticism. Websites belonging to civil society organizations and human rights groups are particularly targeted, such as the Saudi #Women2Drive campaign, blocked in 2013. Similarly, Egyptian authorities have blocked several websites of human rights organizations.[[36]](#footnote-36) The firewall employed in China systematically blocks access to thousands of websites and online content based outside China containing key terms such as “democracy” and “human rights”.[[37]](#footnote-37) In this regard, the SP is concerned that access to new communications technologies, in particular the Internet, or to specific websites, has allegedly been temporarily blocked prior to, during or after peaceful assemblies (e.g., in Algeria, China and Egypt). The mandate holder also warns against possible abusive use of laws governing the prevention and fight against offences linked to information and communications technologies, which “should be applied only as an exception to the general norm of permitting the open and free use of the Internet, like all other forms of communication; only very few qualified and clearly legislated exceptions should be permitted”.[[38]](#footnote-38)

In addition, the capacity to use communication technologies securely and privately is vital to the organization and conduct of assemblies. Restrictions to online access or expression must be necessary and proportionate and applied by a body independent of any political, commercial or other unwarranted influences, and there should be adequate safeguards against abuse.[[39]](#footnote-39) The practice of blocking communications, impeding the organization or publicizing of an assembly online, rarely satisfies these requirements. In some States, laws of general application may have a disproportionate impact on the assembly rights of certain groups, whether intentionally or inadvertently. For example, laws governing the prevention and combating of offences linked to information and communications technology have the potential to be applied in ways that hinder the organization of peaceful assemblies. Youth, being the largest demographic of social media users, are particularly affected by restrictive Internet access policies. The SR warns that restrictions to information and communications technologies should be applied exceptionally. The general norm should be to permit the open and free use of the Internet and other forms of communications.[[40]](#footnote-40)

1. **The human rights challenges posed by the use of new technologies, including information and communications technology, in the context of assemblies, including peaceful protests (e.g the use of surveillance and monitoring tools by the authorities, including biometrics-based recognition technology to identify protestors).**

States often impede the exercise of the freedoms of assembly and association online through restrictions that are not necessary or proportionate considering the specific threats invoked. Some examples of this include the use of surveillance using digital technologies, social media taxes, body-worn cameras, commercial spyware and monitoring tools by the authorities.[[41]](#footnote-41)

The use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited. Surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision.[[42]](#footnote-42)

Furthermore, women and lesbian, gay, bisexual, transgender and intersex persons are at particular risk of facing these attacks. For example, the Government of Egypt reportedly identified and arrested lesbian, gay, bisexual, transgender and intersex activists by infiltrating and surveilling their activities on social media platform Grindr.[[43]](#footnote-43) Authorities in Brazil used Tinder to form relationships and then conduct surveillance on women activists engaged in protests. Furthermore, in Thailand, women human rights defenders were subjected to extensive discrediting, harassment campaigns and death threats in blogs and on social media.[[44]](#footnote-44) These attacks take particular forms, which include the dissemination of doctored pictures, usually of a sexualized and gendered nature; the spreading of information designed to discredit, often full of harmful and negative gender stereotypes; violent hate messages and threatening messages on social networks, including calls for gang rape and for murder; and breaches of privacy, including hacking into family members’ computers and phones and exposing the phone number, the home address and personal and family photos. The mandate holder echoes the findings of the Special Rapporteur on violence against women, its causes and consequences, that online abuse against women is a direct attack on women’s visibility and full participation in public life and should be duly investigated and punished.[[45]](#footnote-45)

The SR is concerned that the recent imposition of taxes for the use of social media in some countries may disproportionately affect vulnerable peoples’ ability to exercise the right of FoAA and that these “social media taxes” may raise concerns of necessity or proportionality. For example, the social media tax in Uganda “disproportionately and negatively impacts the ability of users to gain affordable access to the Internet, and thus unduly restricts their right to freedom of expression and their rights of FoAA, particularly so for low-income citizens, for whom purchasing 1 GB of data per month will cost nearly 40 per cent of their average monthly income”[[46]](#footnote-46). While there may be legitimate economic rationales for these taxes, States should take measures to ensure that the taxes do not disproportionately impede the ability of individuals to communicate with other members of society and widen the digital divides.

The appropriate use of body-worn cameras by law enforcement personnel in the context of assemblies could assist the work of internal investigations or civilian oversight mechanisms. Such technology is in its infancy, and delicate balancing of potential intrusions into privacy should be considered, but at this stage there seems to be potential to promote accountability, where adequate safeguards are in place.[[47]](#footnote-47)

The SR was concerned to hear, during his visit to Oman, that the authorities had reportedly employed a variety of tactics to clamp down on and control the use of information and communications technology. There are widespread reports that authorities systematically hack into online accounts and hijack them and flood social media such as Twitter with an endless stream of hashtag references, thus disrupting discussion on specific topics. The example of the Omani Group for Human Rights is instructive. In addition to online surveillance, authorities reportedly went as far as preventing the group members from communicating on WhatsApp. Voice over Internet Protocol services such as Skype are blocked in Oman, a situation that the SR experienced firsthand. The SR reiterates that States have the obligation to ensure that online assemblies are facilitated in accordance with international human rights standards.[[48]](#footnote-48)

Finally, the use of commercial spyware, such as FinFisher monitoring technology and the Pegasus spyware suite, to launch cyberattacks against civil society actors is another example of this trend. Well-documented reports have linked the Pegasus spyware suite to spyware attacks against activists and human rights defenders in Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia and the United Arab Emirates, among others.[[49]](#footnote-49) These attacks allow hacking into, and watching in real time, their communications, location and activities [[50]](#footnote-50), and can affect targets both within a State or extraterritorially.[[51]](#footnote-51)

1. **The impact on human rights of the use of new less-lethal weapons and ammunition technology in the context of assemblies, including peaceful protests.**

The principle of legality requires that States develop a domestic legal framework for the use of force, especially potentially lethal force, that complies with international standards.[[52]](#footnote-52) The normative framework should specifically restrict the use of weapons and tactics during assemblies, including protests, and include a formal approval and deployment process for weaponry and equipment.[[53]](#footnote-53)

The principle of precaution requires that all feasible steps be taken in planning, preparing, and conducting an operation related to an assembly to avoid the use of force or, where force is unavoidable, to minimize its harmful consequences. Even if the use of force in a particular situation complies with the requirements of necessity and proportionality, but the need to use force could reasonably have been prevented from arising in the first place, a State may be held accountable for a failure to take due precautionary measures. Training should include techniques of crowd facilitation and management consonant with the legal framework governing assemblies.[[54]](#footnote-54) States must ensure that their law enforcement officials are periodically trained in and tested on the lawful use of force, and on the use of the weapons with which they are equipped.[[55]](#footnote-55)

In the context of the right of FoAA on the basis of a risk assessment, equipment for law enforcement officials deployed during assemblies should include both appropriate personal protective equipment and appropriate less-lethal weapons.[[56]](#footnote-56) Weapons and tactics should allow for a graduated response and de-escalation of tensions. Accordingly, the provision of a firearm to law enforcement officials with no less-lethal alternative other than a baton is unacceptable. Where necessary, officials must be appropriately protected with equipment, such as shields, helmets and stab- and/or bulletproof jackets, with a view to decreasing the need for any use of weapons by law enforcement. Equipment and weapons that cannot achieve a legitimate law enforcement objective or which present unwarranted risks, particularly in the circumstances of an assembly, should not be authorized for use.[[57]](#footnote-57)

States are required to procure less lethal weapons for use in appropriate situations, with a view to increasingly restraining the application of means capable of causing death or injury.[[58]](#footnote-58) Less-lethal weapons must be subject to independent scientific testing and approval, and used responsibly by well-trained law enforcement officials, as such weapons may have lethal or injurious effects if not used correctly or in compliance with international law and human rights standards. States should work to establish and implement international protocols for the training on and use of less-lethal weapons.

Regarding the Business Enterprises, they have a responsibility to respect human rights, including in the context of assemblies. This requires that businesses avoid causing or contributing to adverse human rights impacts through their own activities, and address adverse human rights impacts in which they are involved.[[59]](#footnote-59) This extends to impacts that are directly linked to the operations, products or services of a business, such as where a business supplies less-lethal weapons or equipment or surveillance technologies which are used in the policing of assemblies. The trend towards the privatization of public places, such as shopping malls, pedestrian precincts and squares, means that assemblies commonly occur on property owned by business enterprises, sometimes referred to as privately owned public space. While private landowners generally have the right to determine who may access their property, the rights related to assembly may require positive measures of protection even in the sphere of relations between individuals.[[60]](#footnote-60)

A growing range of weapons that are remote controlled are becoming available, particularly in the context of the policing of assemblies. Great caution should be exercised in this regard. Where advanced technology is employed, law enforcement officials must, at all times, remain personally in control of the actual delivery or release of force.[[61]](#footnote-61)

The SR is aware of the efforts to further elaborate international legal standards with respect to the management of assemblies and acknowledges in this regard the current discussions on the development of Guidance on less-lethal weapons (LLWs) and related equipment in law enforcement under the auspices of the Geneva Academy and the Institute for International and Comparative Law in Africa (University of Pretoria), that intend to provide guidance on the lawful and responsible design, production, procurement, testing, training, transfer, deployment, and use of LLWs and related equipment.

1. See A/HRC/20/27 and A/HRC/38/34. [↑](#footnote-ref-1)
2. See General Assembly Resolution 73/173. [↑](#footnote-ref-2)
3. A/HRC/23/39, para. 76. [↑](#footnote-ref-3)
4. A/HRC/29/25/Add.1, para. 53. [↑](#footnote-ref-4)
5. A/HRC/20/27, para. 52. [↑](#footnote-ref-5)
6. A/HRC/29/25/Add.1, para. 34. [↑](#footnote-ref-6)
7. See Human Rights Council Resolution 38/11. [↑](#footnote-ref-7)
8. See Human Rights Council Resolution 38/7. [↑](#footnote-ref-8)
9. A/HRC/17/27, para. 79. [↑](#footnote-ref-9)
10. OHCHR, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (United Nations Human Rights Office of the High Commissioner 2011).

Principle 11 and 24. [↑](#footnote-ref-10)
11. A/72/162, para. 86 (c). [↑](#footnote-ref-11)
12. A/HRC/41/41, para. 32. [↑](#footnote-ref-12)
13. See BGD 4/2018 [↑](#footnote-ref-13)
14. See, for example, EGY 13/2017. [↑](#footnote-ref-14)
15. A/HRC/26/29, para. 59. [↑](#footnote-ref-15)
16. See BRA 8/2015. [↑](#footnote-ref-16)
17. Asian Forum for Human Rights and Development (Forum-Asia), Instruments of Repression: A Regional Report on the Status of Freedoms of Expression, Peaceful Assembly, and Association in Asia, pp. 84 and 89. [↑](#footnote-ref-17)
18. See A/HRC/35/28/Add.1. [↑](#footnote-ref-18)
19. See AUS 5/2018. [↑](#footnote-ref-19)
20. Inter‐American Commission on Human Rights, “Second report on the situation of human rights defenders in the Americas” (OEA/Ser.L/V/II. Doc. 66), para. 165. [↑](#footnote-ref-20)
21. A/HRC/29/25/Add.2, para. 57. [↑](#footnote-ref-21)
22. See A/HRC/29/25/Add.1. [↑](#footnote-ref-22)
23. A/HRC/23/39, para. 74. [↑](#footnote-ref-23)
24. A/66/290, para. 39. [↑](#footnote-ref-24)
25. A/HRC/41/41, para. 22. [↑](#footnote-ref-25)
26. A/HRC/35/9, paras. 23–24 [↑](#footnote-ref-26)
27. Pew Research Center, “How social media users have discussed sexual harassment since #MeToo went viral”, 11 October 2018. [↑](#footnote-ref-27)
28. Jeffrey M. Hirsch, “Worker collective action in the digital age”, West Virginia Law Review, vol. 117 (2015), pp. 921–959; and Klaus Schoemann, “Digital technology to support the trade union movement”, Open Journal of Social Sciences, vol. 6, No. 1 (2018), pp. 67–82. [↑](#footnote-ref-28)
29. A/HRC/41/41, para. 4. [↑](#footnote-ref-29)
30. Douglas Rutzen and Jacob Zenn, “Assembly and association in the digital age”, International Journal of Not-for-Profit Law, vol. 13, issue 4 (December 2011), p. 67. [↑](#footnote-ref-30)
31. A/HRC/41/41, para. 2. [↑](#footnote-ref-31)
32. A/HRC/41/41, para. 3. [↑](#footnote-ref-32)
33. See Human Rights Council Resolution 38/11. [↑](#footnote-ref-33)
34. See A/HRC/29/25/Add.2. [↑](#footnote-ref-34)
35. A/66/290, para. 39. [↑](#footnote-ref-35)
36. See EGY 13/2017. [↑](#footnote-ref-36)
37. See also Rebecca MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom (Basic Books, 2012), pp. 31–47. [↑](#footnote-ref-37)
38. A/HRC/20/17/Add.1, para. 105; A/HRC/23/39, para. 73 [↑](#footnote-ref-38)
39. A/HRC/17/27, para. 69 [↑](#footnote-ref-39)
40. A/HRC/23/39, para. 76; A/HRC/26/29, para. 36 [↑](#footnote-ref-40)
41. A/HRC/41/41, para. 50. [↑](#footnote-ref-41)
42. A/HRC/41/41, para. 57. [↑](#footnote-ref-42)
43. Article 19, “Apps, arrests and abuse in Egypt, Lebanon and Iran”, February 2018. [↑](#footnote-ref-43)
44. See, for example, THA 6/2017. [↑](#footnote-ref-44)
45. See A/HRC/38/47. [↑](#footnote-ref-45)
46. See UGA 3/2018. [↑](#footnote-ref-46)
47. A/HRC/31/66, para. 92 [↑](#footnote-ref-47)
48. A/HRC/29/25/Add.1, para. 34 [↑](#footnote-ref-48)
49. See, for example, the Citizen Lab, “Hide and seek tracking NSO Group’s Pegasus spyware to operations in 45 countries”. [↑](#footnote-ref-49)
50. See LBN 2/2018. [↑](#footnote-ref-50)
51. Brief of amici curiae submitted in John Doe a.k.a. Kidane v. Federal Democratic Republic of Ethiopia before the United States Court of Appeals for the District of Columbia Circuit. [↑](#footnote-ref-51)
52. A/HRC/26/36, para. 56 [↑](#footnote-ref-52)
53. See, for example, Amnesty International, *Use of Force: Guidelines for Implementation of the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials* (2015), p. 46. [↑](#footnote-ref-53)
54. Principle 20 of the Basic Principles, and OSCE/ODIHR, *Guidelines*, para. 147. [↑](#footnote-ref-54)
55. Principle 19 of the Basic Principles. [↑](#footnote-ref-55)
56. Principle 2 of the Basic Principles. Less-lethal weapons may still have lethal consequences or affect bystanders (see principle 3 of the Basic Principles). [↑](#footnote-ref-56)
57. See Amnesty International, *Use of Force Guidelines*, chap. 6. [↑](#footnote-ref-57)
58. Ibid. [↑](#footnote-ref-58)
59. OHCHR, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (United Nations Human Rights Office of the High Commissioner 2011).

Principle 11 and 13 (a). [↑](#footnote-ref-59)
60. A/HRC/31/66, paras. 83, 84 [↑](#footnote-ref-60)
61. A/69/265, paras. 77-87; A/HRC/31/66, para. 56 [↑](#footnote-ref-61)