

**Mandate of the Special Rapporteur on the rights to freedom of peaceful assembly and of association**

# Human rights compliant uses of digital technologies by law enforcement for the facilitation of peaceful protests

by the UN Special Rapporteur on the rights to peaceful assembly and of association,  
Clément Nyaletsossi Voule

**Summary:** This document supplements the Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests,<sup>1</sup> and is one of the key components of a technical and practical toolkit developed by the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, in collaboration with the United Nations Office on Drugs and Crime and the Office of the United Nations High Commissioner for Human Rights, pursuant to Human Rights Council Resolution 50/21.<sup>2</sup>



<sup>1</sup> See A/HRC/55/60.

<sup>2</sup> As mandated by the HRC Resolution 50/21, the toolkit was developed in collaboration with UNODC and OHCHR. The Special Rapporteur is responsible for the produced text. See A/HRC/RES/50/21.

## Introduction

1. This document supplements the Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests,<sup>3</sup> and is one of the key components of a technical and practical toolkit developed by the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, in collaboration with the United Nations Office on Drugs and Crime and the Office of the United Nations High Commissioner for Human Rights, pursuant to Human Rights Council Resolution 50/21.<sup>4</sup>
2. It aims to strengthen human rights compliance regarding the use of digital technologies by setting out principled guidance, based on international human rights standards and good practices, to assist law enforcement officials in the fulfilment of their obligation to promote and protect human rights while facilitating peaceful protests. This document should be read in line with the Model Protocol, its associated checklists, and the handbook for law enforcement officials.
3. This document supplementing the Model Protocol is produced in light of UN Human Rights Council Resolution 50/21 which expressed concern about the use of digital technologies in the context of peaceful protests and the harmful impact these often have on those exercising their right to freedom of peaceful assembly and of expression. Specific concern was raised regarding ‘the arbitrary and unlawful surveillance, both in physical spaces and online, of individuals engaged in peaceful protests, including through the use of closed-circuit television and aerial surveillance vehicles, as well as through the use of new and emerging digital tracking tools, such as biometric technologies, including facial and emotional recognition and international mobile subscriber identity-catchers (“stingrays”)’. This echoes consistent concerns raised by the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association.<sup>5</sup>
4. This document is drafted to address the human rights concerns posed by the use of existing and emerging technologies in the context of peaceful protests. In light of the pace of technological change, the scope of this document is relevant to existing and future digital technologies. The document details a human rights-based approach that includes guidance on effective human rights due diligence, and ensuring accountability through the life cycle of the use of the technologies in the context of peaceful protests.

---

<sup>3</sup> See A/HRC/55/60.

<sup>4</sup> As mandated by the HRC Resolution 50/21, the toolkit was developed in collaboration with UNODC and OHCHR. The Special Rapporteur is responsible for the produced text. See A/HRC/RES/50/21.

<sup>5</sup> See Joint Declaration by UN Special Rapporteur on the rights of freedom of peaceful assembly and of association, the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights (IACHR), the Special Rapporteur on Human Rights Defenders and focal point for reprisals in Africa and Chairperson of the African Commission on Human and Peoples' Rights (ACHPR), the Representative of Indonesia to the ASEAN Intergovernmental Commission on Human Rights (AICHR), and the OSCE Office for Democratic Institutions and Human Rights (ODIHR) (2023) [Joint Declaration on Freedom of Peaceful Assembly and of Association and Misuse of Digital Technologies](#); UN Special Rapporteur on the rights of freedom of peaceful assembly and of association, Report to the UN HRC (2019) [Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association](#), A/HRC/41/41.

## General Principles:

5. The obligation to facilitate the right to peaceful assembly is enshrined in Article 21 of the International Covenant on Civil and Political Rights.
6. Peaceful protests are fundamental to the health of functioning democracies. Protests should not be seen as opportunities for surveillance or the pursuit of separate law enforcement objectives, such as counter terrorism measures or the development of intelligence profiles.
7. Peaceful protests may occur in physical places, digital spaces, or in a combination of the two.<sup>6</sup>
8. Human rights protections apply equally to offline and digital spaces,<sup>7</sup> and to any use of digital services made by protest participants.
9. Any use of digital technologies by law enforcement within the context of peaceful protests should be for the express purpose of facilitating the right to freedom of peaceful assembly and enabling and protecting other associated rights, such as the right to privacy and freedom of expression.<sup>8</sup> The use of such technologies should be in accordance with a limiting principle to circumscribe their use, rather than an authorising principle that permits expansive use.
10. There should be no blanket authorisation for the use of digital technologies in the context of peaceful protests. As discussed below, any decisions to use such technologies should be made on a case-by-case basis and in line with a human rights-based approach, which necessarily ensures accountability. This includes compliance with international human rights law, and international standards and best practices.
11. A robust and clear domestic legal framework governing the use of digital technologies by law enforcement that conforms to international human rights law must be established. This framework must address the full range of human rights implications, including with regards to civic freedoms,<sup>9</sup> and cannot be reduced to matters of data protection law. Domestic law should be supported by appropriate practical guidance and policies, such as standard operating procedures, codes of practice and/or assessment matrices.
12. The facilitation of peaceful protests may occur within a broader law enforcement context in which the use of certain digital technologies may be permissible, providing that this aligns with

---

<sup>6</sup> Human Rights Committee, general comment No. 37 (2020) on the right of peaceful assembly (article 21) (17 September 2020) CCPR/C/GC/37, paras 6, 13, 34. See also UN Special Rapporteur on the rights of freedom of peaceful assembly and of association, ‘Protection of human rights in the context of peaceful protests during crisis situations.’ (16 May 2022) A/HRC/50/42 §56.

<sup>7</sup> UNHRC Res 26/13 (2014) A/HRC/RES/26/13 para 1. See also UNHRC Res 24/5 (2012) A/HRC/RES/21/16 para 1.

<sup>8</sup> Human Rights Committee, general comment No. 37 (2020), para 74. See also Human Rights Committee, Communication No 1948/2010 *Turchenyak et al v Belarus* (10 September 2013) CCPR/C/108/D/1948/2010 paras 7.4, Inter-American Court of Human Rights, *Women Victims of Sexual Torture in Atenco v Mexico* (ser C) No 371 (28 November 2018) paras 171-172, African Commission on Human and Peoples’ Rights, ‘Guidelines on Freedom of Association and Assembly in Africa’ (21 September 2017) para 66.

<sup>9</sup> For examples of some broader rights implications, see Report of the Office of the United Nations High Commissioner for Human Rights, ‘The right to privacy in the digital age.’ (4 August 2022) A/HRC/51/17 paras 48-52. Also see Report of the United Nations High Commissioner for Human Rights, ‘Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests.’ (25 June 2020) A/HRC/44/24, paras 35-36. See also African Commission on Human and Peoples’ Rights, ‘Guidelines for the Policing of Assemblies by Law Enforcement Officials in Africa’ (4 March 2017) para 15.

international human rights law.<sup>10</sup> If digital technologies are used in law enforcement activities adjacent to, and separate from, peaceful protests, law enforcement officials must consider any potential impacts on the peaceful protest and protest participants, especially those in position of vulnerability, such as children, and ensure that the use of digital technologies remains consistent with their obligation to protect human rights and facilitate peaceful assemblies.

13. Children enjoy specific protections under international human rights law.<sup>11</sup> Additional specific efforts – both enabling and protective – must be undertaken to ensure that their human rights are protected and their right to peaceful assembly is facilitated when law enforcement officials use digital technologies in the context of protests, including in digital spaces.<sup>12</sup> A normative framework and guidelines should be developed providing strong human rights safeguards concerning the use of digital technologies in facilitating children’s participation in peaceful protests. This should incorporate UNICEF guidance, ensuring that any interference with a child’s privacy is provided for by law, intended to serve a legitimate purpose, upholds the principle of data minimization and is proportionate.<sup>13</sup> Such guidelines should ensure the best interests of the child and fully comply with the UN Convention on the Rights of the Child.
14. Authorities should strictly refrain from deploying in the context of peaceful protests the army or any military-type units, tactics or equipment or other units outside the official law enforcement chain of command. The facilitation of peaceful assemblies, including peaceful protests should be the responsibility of civilian law enforcement. Any unit involved, including corporate actors, must fall under the command of law enforcement authorities or agencies and follow the laws and regulations applying to law enforcement. All uses of digital technologies in this context should comply with the laws and regulations applicable to law enforcement and be in line with the international human rights law framework.
15. Some technological measures are incompatible with the obligation to facilitate the right to peaceful assembly and must not be used in a protest context. These include but are not limited to hindering or limiting Internet access or imposing Internet shutdowns,<sup>14</sup> indiscriminate and/or untargeted surveillance,<sup>15</sup> surveillance on the basis of group affiliation, and the use of spyware or other forms of equipment interference targeting the digital devices of participants.<sup>16</sup>

---

<sup>10</sup> Prior to any potential use digital policing technologies must be rigorously tested, paying particular attention to issues of bias and potential human rights impact.

<sup>11</sup> UN Convention on the Rights of the Child, Article 15.

<sup>12</sup> UN Special Rapporteur on the right to privacy, Joseph A. Cannataci, ‘Artificial intelligence and privacy, and children’s privacy’, (25 January 2021) A/HRC/46/37, para 127(p),(v). See also, UNICEF, ‘Free and Safe to Protest: Policing Assemblies Involving Children’, August 2023.

<sup>13</sup> See UNICEF (2023) ‘[Free and Safe to Protest: Policing Assemblies Involving Children](#)’, page 29.

<sup>14</sup> UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule ‘Protection of human rights in the context of peaceful protests during crisis situations’ (16 May 2022) A/HRC/50/42, para 57.

<sup>15</sup> UN Special Rapporteur on the rights to freedom of peaceful assembly and of association’ (17 May 2019) A/HRC/41/41, paras 57; United Nations High Commissioner for Human Rights ‘Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests’, (25 June 2020) A/HRC/44/24, para 53(f).

<sup>16</sup> Office of the United Nations High Commissioner for Human Rights, ‘The right to privacy in the digital age’ (4 August 2022) A/HRC/51/17, para 19. General comment No. 37 (2020) CCPR/C/GC/37, para 11.

16. Digital technologies should not be used to categorize, profile or remotely identify individuals, including by biometric means, before, during, or after protests. The use of such technologies at protests is inconsistent with the obligation to facilitate the right to peaceful assembly.<sup>17</sup>
17. Law enforcement should take all feasible steps and ensure all possible alternatives are considered to prevent and avoid the use of force in the context of peaceful protests.<sup>18</sup> Any decision to use force must meet the requirements of legality, necessity and proportionality, precaution, non-discrimination and accountability, and be in strict compliance with the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. Autonomous weapons systems must never be used in the context of a protest.<sup>19</sup>
18. Effective training of law enforcement officials involved in decision-making and the use of digital technologies is key to facilitating peaceful protests. This training should provide clear guidance on the use of technologies in a manner that aligns with human rights law and standards and information relating to how different types of digital technologies work, including information on their capabilities, limitations and inherent or other forms of bias, as well as potential human rights and civic freedoms implications, including for children. Training should also cover accountable decision-making concerning the use of technologies in the context of peaceful protests. Law enforcement officials should be provided with robust and clear protocols on the use of digital technologies, including in protest settings, that translate international human rights standards into practice.<sup>20</sup>

## A human rights-based approach

19. To foster overall human rights compliance, a human rights-based approach should underpin any decisions by law enforcement or any other authorities over the acquisition, use and management of digital technologies and any associated data.<sup>21</sup> Any use of digital technologies should be subject to a rigorous authorisation process. The underlying request for authorisation should be evidence based and fully justified, clearly setting out the specific objective pursued by the use of digital technologies, evidencing utility, and providing sufficient information to evaluate the potential harm to human rights.
20. The acquisition and use of any digital technologies in the context of protests must meet the requirements of legality, necessity and proportionality. This must be demonstrated effectively, and supported by appropriate evidence.
21. Any decision to use digital technologies must be justified on a case-by-case basis. Additionally, all protests are different and often evolve over the course of their lifecycle. This underscores

---

<sup>17</sup> A/HRC/44/24, para. 53 (f); European Commission for Democracy through Law and OSCE/ODIHR, *Guidelines on Freedom of Peaceful Assembly* (3rd ed, Warsaw/Strasbourg, 2019), para163.

<sup>18</sup> See the Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, by the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, A/HRC/55/60.

<sup>19</sup> Human Rights Committee, general comment No. 37 (2020), CCPR/C/GC/37, para 95:

<sup>20</sup> See <https://www.ohchr.org/sites/default/files/documents/issues/trafficking/statements/20230915-jd-foaa-digital-technologies.pdf> para 23.

<sup>21</sup> For discussion on a human rights-based approach to AI generally, see Lorna McGregor, Daragh Murray, Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68 *International & Comparative Law Quarterly*. For uses of digital surveillance tools, see Murray, D., Fussey, P., McGregor, L. and Sunkin, M. (2021) 'Effective Oversight of Large-scale Surveillance Activities: A human rights perspective', *Journal of National Security Law and Policy*. 11(3): 743-770.

the need for any decisions regarding uses of digital technologies to be dependent on and adapted to the specific circumstances at hand. Such decisions must be justified, documented and available for scrutiny. For instance, decisions made prior to a protest may need to be reconsidered as an assembly evolves, or new decisions may need to be made in light of changing circumstances. Consistent with the requirement that law enforcement should comply with the principles of precaution and use the least intrusive means possible in facilitating the right to peaceful assembly, it is important to note that prior authorisation for the use of digital technologies does not make the use of such technologies mandatory. If the evolving circumstances of the protest do not warrant the use of digital technologies, then the commanding officer should order the reduction or discontinuation of their use.

22. Law enforcement officials should be transparent about any digital technologies to be used in the context of a protest, and their manner of use. This is consistent with the requirement that any interference with rights be foreseeable. Transparency is also essential for building trust and legitimacy. Such transparency should extend to any involvement/relationships with third parties, including corporate providers and users of relevant digital technology, and any associated data handling.<sup>22</sup>
23. Transparency does not automatically confer accountability. To enable accountability and to facilitate the right to an effective remedy, appropriate mechanisms should be developed to ensure law enforcement decisions and justifications covering the use of digital technologies are clearly articulated and are auditable.<sup>23</sup>
24. The acquisition of digital technologies for use in the context of protests should be done in a transparent manner, and subject to human rights due diligence in line with the United Nations Guiding Principles on Business and Human Rights. This should include a genuine and effective evaluation of the potential utility of the technology to accomplish any legitimate law enforcement objectives, as well as the potential human rights harm associated with that technology. Analysis of potential harm should not be restricted to the right to privacy, but should include the full range of potentially affected human rights and civic freedoms. This analysis should specifically assess the human rights impact of such technology on individuals or groups in situations of vulnerability, which may in some cases include women, children, minoritised persons and those facing historic discrimination and marginalisation.
25. Meaningful and inclusive community consultation and engagement should occur well in advance of any use of digital technologies by law enforcement. This should involve meaningful consultation across social groups and, particularly, with those in situations of vulnerability, such as children, to ensure an intersectional analysis of the potential and actual impacts of the technology. Consultations should include opportunities to provide feedback that can directly inform decision-making. As good practice, the outcomes of this consultation should be made public.<sup>24</sup>

---

<sup>22</sup> See Privacy International, 'Safeguards for Public-Private Surveillance Partnerships' (December 2021).

<sup>23</sup> UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Surveillance and human rights' (28 May 2019) A/HRC/41/35, para 50. See also Council of Europe, *Guidelines on facial recognition* (Council of Europe 2021) p 10; *Szabo and Vissy v. Hungary*, Judgment, ECtHR, App. No. 37138/14, 12 January 2016, para 71.

<sup>24</sup> See UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 'Surveillance and human rights:' (28 May 2019) A/HRC/41/35, paras 52-53.

26. The above are general principles relevant to law enforcement use of digital technologies to fulfil their obligation to promote and protect human rights in the context of peaceful protests. They apply across all stages and types of protests. It is important that a holistic approach is adopted, taking into account the full lifecycle of a protest, and that decision-making is promptly and adequately adapted, in line with the legality, necessity and proportionality requirements as events evolve, in order to ensure continued compliance with the obligation to facilitate the right to peaceful assembly.

## The use of digital technologies prior to a protest

27. In certain situations it may be appropriate for law enforcement to use digital technologies to give effect to their obligation to facilitate the right to peaceful assembly. This may assist with law enforcement preparedness and may include obtaining or analysing de-identified logistical information such as: estimates as to the number of attendees, crowd densities and/or the likely route of the protest.<sup>25</sup>

28. However, law enforcement uses of digital technologies prior to a protest can interfere with the right to peaceful assembly and other human rights. This particularly applies to the creation of chilling effects that may unduly restrict, or otherwise impact, the free participation and exercise of fundamental freedoms in digital and offline spaces.<sup>26</sup>

29. In deciding whether to use digital technologies for the sole purpose of accumulating situational awareness for the facilitation of peaceful protests, law enforcement officials must take into account the wider range of rights and freedoms implications including less visible impacts such as the potential for stigmatisation and chilling effects.<sup>27</sup> The threshold for initiating situational awareness through the use of digital technologies should be high and any decision in this regard should prioritise available less intrusive mechanisms, in line with the necessity and proportionality requirement. As good practice, law enforcement should at all times prioritise constructive dialogue with organisers.

30. Appropriate processes and practices should be developed to effectively distinguish the collection of information for the purposes of situational awareness or for ensuring the safety and rights of participants from intelligence gathering for other investigative processes.<sup>28</sup>

---

<sup>25</sup> European Commission for Democracy through Law and OSCE/ODIHR, *Guidelines on Freedom of Peaceful Assembly* (3rd ed, Warsaw/Strasbourg, 2019), para 163.

<sup>26</sup> Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', A/HRC/51/17, para 43. For more detailed discussion on the chilling effects of surveillance see, Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki & Amy Stevens, 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Zimbabwe and Uganda' (2023) *Journal of Human Rights Practice*; Amy Stevens, Pete Fussey, Daragh Murray, Kuda Hove & Otto Saki, "'I Started Seeing Shadows Everywhere': The Diverse Chilling Effects of Surveillance in Zimbabwe' (2023) *Big Data & Society*.

<sup>27</sup> UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, 'Rights to freedom of peaceful assembly and of association' (17 May 2019) A/HRC/41/41, para 56-57. See also Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Protest and Human Rights. Standards on the rights involved in social protest and the obligations to guide the response of the State' (September 2019) OEA/SER.L/V/II, para 236.

<sup>28</sup> See paragraph 9 above.

31. To minimise risks to human rights, including privacy, freedom of expression, and peaceful assembly, any data generated for the purposes of establishing situational awareness should not be retained unless it is necessary for accountability purposes.<sup>29</sup>
32. Any use of digital technologies to categorise a protest (e.g. as violent/non-violent or high risk/low risk) should be treated with extreme caution. There are recognised biases associated with digital tools, and such digitally-generated designations can significantly impact the right to freedom of peaceful assembly, including by influencing how law enforcement officials approach the protest and select equipment. The use of such tools may also have an impact on accountability due to the inscrutability of decision-making. The use of such tools is not recommended.

## During a protest

33. In certain circumstances, digital technologies may assist the facilitation of peaceful protest. For example, law enforcement may use digital technologies to ensure protesters' safety, protect public order, respond to emerging security threats, and enable the separation of specific participants directly engaged in or threatening violence, in an otherwise peaceful protest.<sup>30</sup> Any use of technologies in this manner must be consistent with international human rights law standards.
34. A bright line distinction must be made between monitoring or observing a protest for the reasons set out above,<sup>31</sup> and recording or surveillance of protest participants. Any recording, processing, or retention of data fundamentally changes the nature of the law enforcement action. It gives rise to a higher degree of intrusiveness vis-a-vis the rights to privacy, freedom of expression and freedom of peaceful assembly. Such recording also heightens the risk of chilling effects and consequent erosion of democratic participation.<sup>32</sup> This means that any decision to record, process or retain information, should be exceptional, subject to a high level of justification, stringent authorisation, and based exclusively on the obligation to ensure accountability.<sup>33</sup> This includes retaining information concerning use of force, detention or arrest, human rights violations, including sexual and gender based violence, or dispersal, or where it relates to the subject of a complaint; or where oversight authorities, complainants or other relevant actors have a suspicion of law enforcement misconduct in the context of the protest.<sup>34</sup> To minimise the rights impact, any retained data should only be used for the purposes that justified its collection. Appropriate processes that prioritise human rights safeguards,

---

<sup>29</sup> See paragraph 34 below.

<sup>30</sup> United Nations High Commissioner for Human Rights, 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (25 June 2020), A/HRC/44/24, paras 9, 12, 24.

<sup>31</sup> As stated in paragraph 33.

<sup>32</sup> See Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', (4 August 2022) A/HRC/51/17, para 43. See also 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests Report of the United Nations High Commissioner for Human Rights', (25 June 2020) A/HRC/44/24, paras 24, 34.

<sup>33</sup> See UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, 'Rights to freedom of peaceful assembly and of association' (17 May 2019) A/HRC/41/41, para 55. In light of the obligation to facilitate peaceful assembly, consideration should be given as to the severity of potentially criminal activity by protest participants for which accountability will be pursued.

<sup>34</sup> See also UN Special Rapporteur on the rights of Freedom of Assembly and of Association '10 Principles for the Proper Management of Assemblies: Implementation Checklist' (A/HRC/31/66); Special Rapporteur on the rights to Freedom of Peaceful Assembly and of Association (2023) 'Advancing accountability for serious human rights violations related to the exercise of the rights to freedom of peaceful assembly and of association', A/HRC/53/38



including protecting children's rights, should govern such exceptional cases. There should be a presumption of non-retention for any other digital data gathered in the context of a protest.

35. Given that a certain level of disruption may be a legitimate feature of peaceful protests,<sup>35</sup> and in light of potential chilling effects linked to any recording of protests, consideration should be given to the seriousness of the crime for which any recording may be initiated.<sup>36</sup> This threshold should be kept under regular review and adjusted with a view to optimising the facilitation of peaceful protests and ensuring the protection of human rights.
36. Individuals have a legitimate expectation of a degree of anonymity during protests, across both digitally-mediated and offline environments. Participants' tactics intended to preserve their anonymity, such as measures for encryption or wearing masks can be important to ensure the enjoyment of the right to peaceful assembly and should not be regarded as inherently suspicious or as a justification for the use of surveillance tactics.<sup>37</sup>
37. Facial recognition technologies and other biometric identification technologies must not be utilised to identify or track individuals peacefully participating in a protest.<sup>38</sup>
38. Data gathering and management processes should distinguish between collection, retention and processing and be consistent with human rights and data protection law.

## Post-Protest

39. Access to and the use of any information obtained during the course of a peaceful protest should be limited to the lawful and legitimate law enforcement purposes for which it was initially collected.<sup>39</sup> This is essential in order to limit any chilling effects, and to facilitate the right to peaceful assembly over the long term.
40. In exceptional circumstances access to retained information may be required for the purposes of facilitating accountability.<sup>40</sup> In such circumstances, access should be regulated by domestic law, in line with applicable international human rights law standards, including legality, necessity, and proportionality.<sup>41</sup> An independent authorisation process to handle such exceptional requests should be established as good practice.

---

<sup>35</sup> See European Court of Human Rights, *Laurijsen and Others v The Netherlands* App No 56896/17, 56910/17, 56914/17, 56917/17, 57307/17, 21 November 2023, para 54.

<sup>36</sup> See European Court of Human Rights, *Glukhin v Russia* App No 11519/20, Judgment, 4 July 2023 §87-89. See also *Catt v the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para 123.

<sup>37</sup> Human Rights Committee, general comment No. 37 (2020) CCPR/C/GC/37, para 60.

<sup>38</sup> United Nations High Commissioner for Human Rights, 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', (25 June 2020) A/HRC/44/24 para. 53(h); UN Special Rapporteur on freedom of peaceful assembly and of associations and regional mechanisms, [Joint Declaration on Freedom of Peaceful Assembly and of Association and Misuse of Digital Technologies](#) para 54, and A/HRC/44/24.

<sup>39</sup> OSCE/ODIHR, *Guidelines on Freedom of Peaceful Assembly* (3rd ed, Warsaw/Strasbourg, 2019) paras 163, 172. See also African Commission on Human and Peoples' Rights, 'Guidelines for the Policing of Assemblies by Law Enforcement Officials in Africa' (4 March 2017) para 15.5.

<sup>40</sup> See paragraph 34 above.

<sup>41</sup> Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies, A/HRC/31/66, para 78.

## Oversight and accountability

41. Oversight should consist of both internal and external mechanisms. External mechanisms should be independent and impartial, and have the power to hold law enforcement to account, including concerning uses of digital technologies and associated forms of data.
42. Data-focused oversight should develop specific and transparent mechanisms for individuals, including for children, to ascertain and challenge information held about them. These mechanisms should ensure the right to an effective remedy and incorporate provision for an effective complain process, which is accessible also to children, and that includes clear protocols for data deletion. These mechanisms should ensure individuals, including children, can challenge State and non-State practices which disregard their rights in the collection, analysis, storage and sharing of their data, such as collected by law enforcement in the contest of protests. To the extent possible alignment between these internal and external mechanisms should be optimised.
43. To facilitate effective oversight and accountability, a transparent and auditable record of decision-making concerning uses of digital technologies should be maintained.<sup>42</sup> This should include: a clear articulation of the intelligence-base underpinning any measure (including assessment of the quality or reliability of the intelligence, and the severity and imminence of the threat); and considerations of potential harm; and any decision taken to prevent or mitigate potential human rights violations. The examination of potential harms should be broad, taking into account all rights and civic freedoms affected.<sup>43</sup>
44. Effective oversight should apply before, during and after a protest and across the full lifecycle of a technological deployment. Accountability for breaches of law and organisational procedure should be administered via a system that is robust, victim-oriented, and that guarantees due process rights.

### *Acknowledgement:*

*The Special Rapporteur sincerely thanks all who have contributed. With thanks to OHCHR, UNODC, Prof. Pete Fussey, University of Essex, Dr. Daragh Murray, Queen Mary University of London, and all who have contributed by providing written submissions and/or participating in regional and global consultations which his mandate held in preparation of the toolkit.*

---

<sup>42</sup> Human Rights Committee, general comment No. 37 (2020), CCPR/C/GC/37, para 62. See also United Nations High Commissioner for Human Rights, 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (25 June 2020) A/HRC/44/24, para 37, Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age' (4 August 2022) A/HRC/51/17, para 52; *Szabo and Vissy v. Hungary*, Judgment, ECtHR, App. No. 37138/14, 12 January 2016, para 71.

<sup>43</sup> Fussey, P., and Murray, D. (2019) *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Human Rights, Big Data and Technology Project