

PROTEST SURVEILLANCE INTO COURTS

PI's report on the legal implications of unrestrained protest surveillance for the fair trial rights of activists, human rights defenders and protesters

December 2024

privacyinternational.org



ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.



Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission.This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

KEY FINDINGS

1. Information gathered through the surveillance of protests is being used as evidence in criminal proceedings against activists, protesters, and human rights defenders in jurisdictions across Europe, Asia, Africa, and the Americas.

2. The evidence gathering, which often takes place contrary to the right to privacy, happens in secret and without transparency as to how information has been collected, with whom it has been shared, and who has accessed it.

3. Such evidence is being widely used during the trial phase of criminal proceedings, but also ancillary processes such as bail hearings.

4. As a consequence of deploying protest surveillance without reasonable suspicion and other safeguards required under the right to privacy, the evidence collected is often presented in misleading ways and is prone to deletion (including exculpatory information) and fabrication.

5. Unlawful or unregulated evidence gathering by law enforcement and judicial systems is preventing defendants from being able to adequately comment on and challenge information used against them in criminal proceedings. This is incompatible with the right to be able to participate effectively in the proceedings, which is central to the right to fair trial.

CONTENTS

Acknowledgments **5**

Executive Summary **6**

Abbreviations **8**

Introduction **9**
Why it matters? 13

1. Unlawful and unregulated collection of evidence **17**

2. Impact of unlawful protest surveillance onthe right to a fair trial **23**
An explanation of the equality of arms and the right to adversarial proceedings: 24
2.a. Lack of transparency impeding effective participation in proceedings 25
2.b. Misleading inferences drawn from unscrutinised evidence 31
2.c. Necessary protections to ensure effective participation in proceedings and scrutiny of evidence 38

3. Fair trial rights and ancillary proceedings **42**
A case study on Uganda 44

4. The privatization of evidence gathering **47**

Conclusion **53**

Recommendations **55**

ACKNOWLEDGMENTS

Privacy International thanks the following individuals and organisations for their vital support and assistance in documenting harms arising from the use of evidence obtained from the surveillance of activists, protesters and human rights defenders in court:

American Bar Association Centre for Human Rights

Thai Lawyers for Human Rights

Unwanted Witness

The Centre for Internet and Society

Dorothy Mukasa

Ginna Anderson

Lana Baydas

Janjira Sombatpoonsiri

We also acknowledge the vital importance of other individuals who cannot be named.

EXECUTIVE SUMMARY

This report seeks to shed light on the due process implications of the blanket and indiscriminate surveillance of protesters, activists, and human rights defenders participating in protests. Our report demonstrates that information gathered through the surveillance of protests is being used in criminal proceedings against activists, protesters, and human rights defenders. It also shows that when this information is being admitted as evidence in criminal proceedings it undermines the right to fair trial. In particular, information obtained in breach of the right to privacy of activists, protesters, and human rights defenders is processed opaquely without clear transparency as to how it has been collected, with whom it has been shared, and who as accessed it. This information is both being widely used during the trial phase, but also ancillary processes such as bail hearings.

As a consequence of deploying protest surveillance without reasonable suspicion and other safeguards under the right to privacy, the evidence collected is often presented in misleading ways and is prone to deletion (including exculpatory information) and fabrication. These harms are exacerbated by the role of other actors, such as companies, in the management and presentation of evidence obtained through surveillance; their role further blurs chain of custody and obfuscates what happens to the information once collected.

The result is that the accuracy, integrity, and credibility of the evidence cannot be adequately assessed by the defence. This in



turn undermines the ability to participate effectively in the proceedings, which is central to the right to a fair trial. We found evidence that the fair trial rights of activists, protesters and human rights defenders were breached in this way in jurisdictions across Europe, Asia Africa and the Americas. Core to the widespread nature of these findings was our methodology. This involved both examining judgments and court records, as well as undertaking semi-structured interviews with activists, lawyers, and civil society organisations with direct experience of challenging surveillance evidence used in proceedings across a number of the jurisdictions we examined.

The widely divergent contexts we looked at range from rule of law democracies to authoritarian polities. Notwithstanding the differing governing contexts and legal frameworks authorising surveillance and its onward uses in criminal proceedings, the harmful practices we have identified are criminalising the right to protest and freedom of expression and dissent more broadly. The report therefore proposes a number of urgent fair trial safeguards. These safeguards seek to prevent the use of unlawful evidence in criminal proceedings against activists, protesters and human rights defenders. If implemented they would provide defendants with mechanisms to ensure transparency of evidence gathering without which protesters, activists and human rights defenders are unable to adequately challenge and comment on evidence used against them.

ABBREVIATIONS

ibid.	in the same source
ACHPR	African Convention on Human and Peoples' Rights
ACHR	American Convention on Human Rights
App No(s)	Application Number/Applications Numbers
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
FRT	Facial Recognition Technology
HRDs	Human Rights Defenders
ICCPR	International Covenant on Civil and Political Rights
OHCHR	Office of the United Nations High Commissioner for Human Rights
SOCMINT	Social Media Intelligence
THLR	Thai Lawyers for Human Rights
UN	United Nations
UN Doc	United Nations Document

INTRODUCTION

The widespread and increasing use of various new technologies to track activists and human rights defenders (HRDs) involved in protests has been widely documented.[1] Through the use by law enforcement of technologies, such as IMSI catchers, social media monitoring (SOCMINT)[2], bodycams, drones, and facial recognition technology (FRT), demonstrations have become sites of blanket and indiscriminate surveillance.[3] Activists are also frequently tracked prior to and after specific protests have taken place. These surveillance measures have a serious impact on the enjoyment of human rights, starting with the rights to privacy and freedoms of assembly and expression.[4]

In their 2020 report the UN Office of the High Commissioner for Human Rights (OHCHR) noted that digital surveillance technologies, including those that interfere with communications, "often lead to harassment and intimidation" and "have a chilling effect on demonstrations as people fear subsequent reprisals for

---

1 See for example, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association on the protection of human rights in the context of peaceful protests during crisis situations, UN Doc A/HRC/50/4 (16 May 2022) §58:
States have employed various new technologies during protests in the context of crises, including surveillance technologies such as CCTV cameras, body cameras and aerial surveillance vehicles, and face recognition technology. Surveillance technologies have frequently been deployed without transparency and accountability, and have been used to crack down on peaceful protests. The use of surveillance technology has expanded dramatically during the COVID-19 pandemic, in a manner that has serious implications for State monitoring and suppressing of protests and dissent.

2 For more information, see: PI, 'How social media monitoring can be used at a protest' (6 May 2021) https://privacyinternational.org/explainer/4509/how-social-media-monitoring-can-be-used-protest *All links in this report were last accessed on 7 November 2024.*

3 PI, 'Tracking protest surveillance', https://privacyinternational.org/examples/tracking-protest-surveillance

4 See for example a Joint Declaration which states that surveillance deployed at protests "creates a climate of fear and has a chilling effect on the right to freedom of peaceful assembly". 'Joint Declaration on Protecting the right to freedom of assembly in times of emergencies' by The United Nations Special Rapporteur on the rights of Freedom of 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 Chairman of the African Commission on Human and Peoples' Rights (ACHPR), and the OSCE Office for Democratic Institutions and Human Rights (ODIHR) (15 September 2022) https://www.ohchr.org/sites/default/files/documents/issues/fassociation/2022-09-15/JointDeclarationProtectingRightFreedominTimesEmergencies15Sept2022.pdf

planning or participating in protests".[5] General Comment No. 37 on the Right of Peaceful Assembly adopted by the UN Human Rights Committee also notes the central role of communications technologies in organising and participating in protests and the risk that surveillance can therefore impede assemblies and the right to privacy.[6]

In countries with increasingly politically repressive and authoritarian regimes, certain forms of protest have been restricted to the point that they are in effect prohibited. For example, in Russia – peaceful expressions of opposition to the war in the Ukraine, including through protests, have been criminalised through broadly framed war censorship laws.[7] Not only have activists been prosecuted through these laws but infringing them also opens one up to being categorised as "foreign agents" under a 2012 law that has been made harsher since the outbreak of war with the Ukraine.[8] The foreign agents law includes sanctions ranging from fines, imprisonment, to loss of citizenship.[9] In these authoritarian contexts, the purpose of the growing surveillance of individuals involved in protests is explicitly to enforce repressive laws and thereby to limit dissent to the extent that any form of protest becomes unlawful.

In parallel, in democratic contexts - state authorities have regularly been invoking their positive obligation to protect freedom of assembly, as well as their prerogative to limit protests in the name of public order and national security, as justifications to impose general and indiscriminate surveillance and interfere with internet communications.[10] Yet it has been reasserted many times that these prerogatives are not unlimited. For example, the UN Human Right Committee's General Comment 37 emphasises the requirement on state authorities that

---

5 Report of the Office of the United Nations High Commissioner for Human Rights on the impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, UN Doc A/HRC/44/24 (24 June 2020) https://www.ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights §29.

6 UN Human Rights Committee: General Comment No 37 (2020) on the Right of Peaceful Assembly, UN Doc CCPR/C/GC/37 (17 September 2020) https://documents.un.org/doc/undoc/gen/g20/232/15/pdf/g2023215.pdf?token=mCCMuYSCpcOuJGGkKR&fe=true §10.

7 Human Rights Watch, 'Russia's Legislative Minefield, Tripwires for Civil Society since 2020' (7 August 2024) https://www.hrw.org/report/2024/08/07/russias-legislative-minefield/tripwires-civil-society-2020

8 *ibid.*

9 *ibid.*

10 Article 21 ICCPR and others.

derogations can only be on grounds of national security and public safety, which must be construed strictly.[11]

While the starting point for the treatment of protests by law enforcement and judicial administrations must be that the authorities should be facilitating peaceful assemblies,[12] instead, the trend has been for the increasing blanket deployment of invasive surveillance technologies at peaceful protests without due transparency and accountability.[13] This trend spans across diverse political contexts, from authoritarian regimes to well established democracies, as we address below.

We have previously argued that surveillance of activists and HRDs involved in protests needs to be subject to a set of human-rights based safeguards to prohibit blanket and indiscriminate surveillance and to introduce measures to ensure that the surveillance measures have a legitimate basis, to be proportionate, and to be independently authorised.[14] There should also be safeguards in place in relation to access to and retention of data generated through the surveillance of protests.[15] However, as the focus has been on the surveillance measures and their impact during protests, little to no attention has been given to what is happening with the personal information of protesters once it is gathered. **The present report seeks to underline a further set of discrete harms arising from protest surveillance, with a specific accent on the subsequent use of this information in criminal proceedings against protesters.**

Our research has covered countries with varying levels of human rights safeguards and room for civil society activity and protest, encompassing authoritarian regimes

---

11 In accordance with the UN Human Right Committee's General Comment 37, national security ground can only be relied upon where "restrictions are necessary to preserve the State's capacity to protect the existence of the nation" (cited above, §42). Also, General Comment 37 states that public safety restrictions can only be justified where the assembly creates a real risk to the life and/or security of persons (§42). It goes on to state that these derogations and positive obligations should not be deployed to "unduly disrupt peaceful assemblies", including those that have a disruptive element (§44).

12 General Comment No. 37, cited above, §72.

13 Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association on the Protection of human rights in the context of peaceful protests during crisis situations.

14 PI, 'Restraining Protest Surveillance: when should surveillance of protesters become unlawful?' (November 2022) https://privacyinternational.org/sites/default/files/2023-01/PI-RPS-sp-v7-RGB_no_blank.pdf. See also Siatitsa Ilia, 'Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications", 913 International Review of the Red Cross (2021) https://international-review.icrc.org/articles/freedom-assembly-under-attack-surveillance-interference-internet-communications-913

15 PI, 'Restraining Protest Surveillance: …', cited above.

to more rule of law contexts. Among others, we have looked at Serbia, Russia, India, Thailand, Uganda, Colombia, the United Kingdom, and France. We have observed similar patterns in all of them notwithstanding the varying levels of rule of law protections for activists and HRDs involved in protests, such as the application of laws protecting freedom of expression and assembly as well as the independence of judicial and court systems.[16] The harms we have documented relate to the onward uses of surveillance data to subject activists and HRDs involved in peaceful protests to criminal proceedings and punitive sanctions under both administrative and criminal law.

In particular, we show how the blanket collection of information relating to protesters, HRDs, and activists through surveillance measures, often as not in breach of the right to privacy and freedom of expression, is increasingly leading to violations of their fair trial rights. Insufficient protections around what happens with the information once gathered and its onward uses means that the information of activists and HRDs involved in peaceful protests is regularly ending up in criminal proceedings against them. The impact that the uses of protest surveillance have for the overall fairness of these proceedings may lead to further human rights breaches, not least: the right to liberty, and the right not to be subjected to inhuman and degrading treatment. The findings of this report has been informed by research we have conducted, including through interviews with activists, HRDs, and lawyers representing protesters in different countries around the world.

With the consent of the interviewees, we recorded the interviews we carried out. Where relevant we reproduce excerpts and/or summaries of the responses we received. Any information attributed to individuals we interviewed is therefore based on recordings we made. A number of the interview responses also formed the basis for several country-specific case studies that we produced as an ancillary resource to this report. Where relevant we refer and provide links to these case studies below.

---

16 Moreover, the legal justifications for surveillance may be different across the various countries we have examined. As above, in more repressive contexts the rationale for surveillance may be to prevent protests altogether by arresting protesters and activists. By contrast, in countries with nominal rule of law protections – the purpose of surveillance may as we have seen ostensibly be to maintain public safety or to investigate criminal offending. This is notwithstanding the fact that the purported relevant legal basis may not in fact have been satisfied (for example there may not have been grounds to deploy surveillance to investigate alleged criminal wrongdoing).



WHY IT MATTERS?

The significant challenges that new data-driven technologies have for due process and fair trial rights, in particular those relating to evidence, is nothing new. Indeed, already in 2019, we documented how law enforcement in both the UK and the US had begun to exploit data generated through connected devices and the Internet of Things in criminal investigations and as evidence in criminal proceedings.[17] At the time, we noted that the volume and nature of these forms of data collection pose unique challenges to the defence's ability to examine and challenge evidence obtained from devices such as Amazon's Alexa.[18] We highlighted that these challenges have implications for the principle of equality of arms and the right to an adversarial hearing, which are inherent components of the right to a fair trial.

17 PI, 'With my fridge as my witness?!' (28 June 2019) https://privacyinternational.org/long-read/3026/my-fridge-my-witness

18 *idid.*

The deployment of data generated through the surveillance of activists and protesters in criminal proceedings raises many similar issues, however it deserves particular attention for multiple reasons including:

a. The fact that demonstrations and protests (both in physical and online spaces) have become sites of blanket and indiscriminate surveillance means that there is a heightened risk of surveillance data being used in criminal proceedings in ways that breach the defence's fair trial rights. A focus on what surveillance technologies are in use and the implications this presents for privacy rights, while of vital significance, has meant that the onward uses of the information gathered on activists/protesters is overlooked.

b. Activists and HRDs are already vulnerable to mistreatment by the authorities by engaging in protests and demonstrations, which may be seen as illegitimate dissent. In addition to this, they may also be drawn from persecuted and/or marginalised groups in the case of those advocating for indigenous and LGBTQI+ rights or racial equality (for example).

c. Freedom of assembly underpins participatory democracy by bolstering popular engagement with the body politic, for example through individuals speaking out, signing petitions, and participating in civil society activism. In recognition of this, engaging in peaceful protests has specific protection under international human rights law (under Article 21 ICCPR).

As such, any restrictions on participating in protests must be in accordance with the law, pursuant to a legitimate aim, and proportionate. Arresting, prosecuting, and detaining protesters on the basis of surveillance data may represent a disproportionate interference with freedom of assembly. This is not least because the combined use of intrusive surveillance on protesters and activists and subjecting them to punitive criminal sanctions has a chilling impact on freedom of assembly and more broadly the right to political participation (Article 25 ICCPR).

In the following pages we address four key interrelated trends highlighting how the fair trial and due process rights of activists, HRDs, and protesters are being breached through the uses of surveillance data in criminal proceedings. In particular, we have found that:

1. The unlawful collection of data of protesters, activists and HRDs is increasingly being relied on in criminal proceedings against them – from effecting their arrests to being admitted as evidence in criminal trials.[19] We consider that unlawfully collected information should not be used in this way and must in particular not be turned into evidence. Onward uses of unlawful collected data in criminal proceedings not only violates the right to privacy, which should require their deletion, they also destroy the essence of the right to a fair trial.

2. The opacity around the production and management of information gathered through unlawful protest surveillance effectively makes it impossible for protesters, activists, and HRDs to challenge. This is increasingly having a negative impact on the equality of arms and the right to adversarial proceedings – which as we address below are core elements of the fair hearing component of the right to a fair trial. Moreover, a lack of adequate oversight and clear chain of custody protocols in relation to what should happen with information gathered through blanket protest surveillance, facilitates the generation and presentation of misleading evidence. This also undermines both the fair hearing requirement and the presumption of innocence and burden of proof.

3. Information collected through the surveillance of activists, protesters, and HRDs is regularly being used in ancillary proceedings, such as a bail procedures, without appropriate due process safeguards. Fair trail rights in a number of instruments we examined do not cover ancillary proceedings. This

19 Prior to surveillance data being used in criminal proceedings (i.e. during its collection by law enforcement), we refer to it as 'information'. Once admitted into criminal proceedings, we refer to it as 'evidence'. Where we are concerned with exculpatory information (in the event that such information is omitted, deleted, or modified during the course of criminal proceedings) – we also refer to it as evidence. This is without prejudice as to whether the evidence is legitimate and lawful for the purposes of national rules of evidence, international human rights law, or any other legal provision.

position is no longer tenable in a context where more and more jurisdictions are using such proceedings in a punitive way against activists, protesters, and HRDs in lieu of full criminal proceedings in which prosecutors and law enforcement agencies would face greater accountability.

4. The increasing role of third parties, including private companies, in the collection of surveillance information creates novel risks for the integrity of the evidence being generated and admitted into proceedings, as well as the possibility for defendants to effectively challenge it.

Where we refer to fair trial and due process rights, we rely on international human rights law standards.[20]

20 We place particular reliance on provisions such as Article 14 ICCPR, Article 8 of the American Convention on Human Rights (ACHR), Article 6 of the European Convention on Human Rights (ECHR), and Article 7 of the African Charter on Human and Peoples' Rights (ACHPR), as well the accompanying jurisprudence of the associated human rights bodies and courts.

1. UNLAWFUL AND UNREGULATED COLLECTION OF EVIDENCE



One of the patterns that we have been able to document in our research is that law enforcement authorities are routinely failing to provide basic information regarding the surveillance data that is used to subject activists and HRDs to criminal sanctions. This includes information relating to the provenance of surveillance data, such as the nature and type of technology used.

The lack of transparency has often been cited through the lens of the right to privacy and the associated difficulties it causes with respect to oversight and effective remedy.[21] However, transparency failures around deployments of digital surveillance and the accompanying collection of surveillance data does not appear to be regularly addressed from the perspective of the impact that it has on fair trial rights. In this section, we show how the unlawful and/or unregulated gathering of information through the digital surveillance of protesters, activists, and HRDs is regularly being introduced into criminal proceedings.[22] The lack of transparency proceeds in tandem with the introduction of unlawful evidence into criminal trials involving activists and HRDs participating in protests given that testing and assessing its lawfulness becomes more difficult, if not impossible.

---

21 See for example §39 of General Comment No 37, cited above.

22 When we refer to unregulated information gathering, we refer to data that is collected without sufficient legal basis and safeguards, such as those relating to transparency, which by extension may also be unlawful (although this will be dependent on national legal frameworks).

During climate change protests across Serbia in 2021, unidentified plainclothes officers were seen filming protesters with unknown large hand-held devices.[23] Before the protests commenced, the government had also deployed thousands of surveillance cameras across the country equipped with FRT. In the aftermath of the protests, hundreds of individuals who had attended the demonstrations were arrested and charged with misdemeanour traffic offences (in effect for jaywalking), which attracted fines.[24] The government denied that FRT had been used to identify, arrest, and prosecute the protesters involved in the demonstrations. The Serbian Data Protection Authority (DPA) found that the arrested individuals *"were recognised based on the direct observation of police officers, in accordance with the Law on Misdemeanours"*.[25]

However, the DPA's inquiry was limited in scope and the criminal proceedings initiated against protesters and activists suggested that some form of FRT had been used. We carried out interviews with one of the lawyers who represented many of the protesters. He explained that most protesters and activists were not formally identified or arrested at the site of demonstrations themselves. Instead, too many individuals who had attended the demonstrations in Belgrade were arrested shortly thereafter in large numbers by local police in other parts of the country, which made the claims of direct observation by the police less credible. It is noteworthy that the lawyer we interviewed also explained that under Serbian law only traffic police enact affect arrests and impose fines for these offences, which was not what happened in practice. Therefore, the surveillance measures were unlawful insofar as the information obtained did not arise from the direct observation of protesters and activists by traffic police officers. The surveillance was also unregulated in the sense that there was no lawful basis for deploying FRT against protesters.

---

23 Standish, Reid, 'Serbia's Legal Tug-Of-War Over Chinese Surveillance Technology (Part 2)', *Radio Free Europe,* (23 November 2022) https://www.rferl.org/a/serbia-chinese-surveilllance-backlash-standish/32145138.html

24 *ibid.* See also, PI, 'Prosecuted for protesting: Serbia' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

25 Commissioner for Information of Public Importance and Personal Data Protection, 'Poverenik sproveo postupak nadzora u MUP, povodom sumnji na upotrebu tehnologije za prepoznavanje lica (Facial Recognition Technology)' (18 February 2022) https://www.poverenik.rs/sr-yu/saopstenja/3730-повереник-спровео-поступак-надзора-у-муп,-поводом-сумњи-на-употребу-технологије-за-препознавање-лица-facial-recognition-technology.html (in Serbian)

The issues we have documented above are not limited to Serbia; instead, we also provide similar examples in relation to France and Russia. In Russia, particularly since its invasion of the Ukraine in 2022, large numbers of protesters have been arrested and detained through the use of technologies such as live FRT. For example, a 2023 Reuters investigation found through a review of 2000 criminal cases against protesters in Moscow that video surveillance (including live automated FRT) had been used as evidence in hundreds of cases involving the arrest, fining, and in some cases imprisonment of activists participating in protests.[26]

This led to the condemnation of Russia by the European Court of Human Rights in the *Glukhin v Russia* case. In this case, it considered the lawfulness of the Russian authorities using surveillance technologies, including FRT, in criminal proceedings against an activist.[27] The applicant was arrested and charged with failing to notify the authorities of a planned solo demonstration. He asserted before the European court that he first came to the attention of the authorities through their use of SOCMINT and that the police applied FRT to social media content and surveillance footage in order to identify, arrest, and charge him. He also argued that the surveillance measures and the information they generated were unlawful as a matter of Russian administrative law.

While the use of these surveillance measures in the proceedings against him were wholly opaque[28], the European Court found through its own fact-finding that FRT had been deployed for the purposes outlined above.[29] This is significant because as a consequence of the lack of transparency regarding the use of surveillance evidence in the applicants' criminal proceedings, the Court was

---

26 Masri, Lena, 'A Reuters review of more than 2,000 court cases shows how Russia uses facial recognition to identify and sweep up the Kremlin's opponents' (28 March 2023) https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/ See also PI, 'Prosecuted for protesting: Russia' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

27 ECtHR, *Glukhin v Russia,* App no 11519/20, Judgment, 4 July 2023.

28 For example, the Russian authorities did not confirm or deny whether FRT had been used and police reports relating to the applicant's arrest did not explain what technology had been used to effect his arrest. See *Glukhin v Russia,* cited above, §70.

29 *Glukhin v Russia,* cited above, §72. The Court reached this conclusion with reference to the speed at which the applicant was identified and the publicly available information on the use of FRT to identify protesters by the Russian authorities.

forced to engage in fact-finding, which is ordinarily outside its remit in accordance with the fourth instance doctrine.[30]

The European Court found that the surveillance measures used to identify, arrest, and charge the applicant had interfered with his right to privacy and freedom of expression (as protected by Articles 8 and 10 ECHR, respectively). In relation to Article 8, it held that the technology used was particularly intrusive and its deployment did not correspond to a "pressing social need" and therefore it could not be regarded as "necessary in a democratic society".[31] While there was a legal basis for using FRT, the domestic legal framework was said to lack detailed rules governing the scope and application of measures involved the uses of FRT as well as the absence of strong safeguards against the risk of abuse and arbitrariness.[32]

Significantly, the applicant submitted that his rights under Article 6 ECHR had also been breached through the use of the surveillance evidence in his criminal proceedings. However, the Court did not substantively consider this point in accordance with its longstanding practice of only examining what it considered to be the core legal questions and therefore not assessing remaining complaints.[33]

In a further case before the same court, on this occasion involving France[34], the Court considered whether the reliance of law enforcement on intelligence reports ("notes blanches") was a sufficient ground for restricting the freedom of environmental activists through the imposition of home arrest orders.[35] The Court's judgment focused on whether the information contained in the reports could justify the imposition of such sanctions rather than the modes in which the surveillance data was gathered and handled. However, the case underlines the opacity around the information in such intelligence reports, which are then used in imposing punitive penalties on activists and protesters. According to research carried out

30 ECtHR, *García Ruiz v Spain,* App no 30544/96, Judgment, 21 January 1999, §28.
31 *Glukhin v Russia,* cited above, §89.
32 *Glukhin v Russia,* cited above, §§82-83.
33 See for example, *Centre for Legal Resources on behalf of* ECtHR, *Valentin Câmpeanu v Romania* [GC], App no 47848/08, Judgment, 17 July 2014 §156.
34 ECtHR, *Domenjoud v France,* App no 34749/16, Judgment, 16 May 2024.
35 While such orders are imposed under administrative rather than criminal law, they are highly onerous, and compliance is monitored by law enforcement. Moreover, breaching such an order is a criminal offence.

by the French organisation, Data Rights there is no publicly available information about the provenance of information included in such reports and the procedure for a claimant to obtain disclosure is an onerous one (we address this further below).[36]

Reports shared in confidence with Data Rights by the claimant involved in the litigation demonstrate that information is obtained through highly intrusive surveillance, including mobile phone metadata obtained through requests to service providers, YouTube video analysis, and footage of demonstrations potentially gathered through SOCMINT (albeit not certain). According to Data Rights, the legal basis for these measures is unclear, but is likely to be Article L 811-3(5b) of the Interior Security Code. These are general powers that permit surveillance to be rolled out to prevent "collective violence that could seriously harm the public peace". It is difficult to see how such a legal basis is sufficiently clear, foreseeable, and adequately accessible to meet the in accordance with the law requirement for the purposes of Article 8 ECHR.[37]

The Russian, Serbian, and French[38] examples relate to the gathering of unlawful and unregulated evidence in ways that interfered with the right to privacy, freedom of expression, and freedom of assembly. However, they also showcase why further attention needs to be afforded to what happens with the data gathered through unlawful and/or unregulated means including when information is collected in violation of national law and international human rights law.

The clear pipeline between blanket and disproportionate surveillance measures at protests and evidence in criminal proceedings means that any information

---

36 See also PI, 'Prosecuted for protesting: France' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

37 See for example, *Ben Faiza v France* App No 31446/12, 8 February 2018, which related to the use of GPS technology to track a suspect during a criminal investigation. In that case law enforcement relied on general powers for investigating officials to take whatever intelligence-gathering steps they deemed useful in order to establish the facts of the case. This provision was held by this Court to be insufficiently precise as it did not provide sufficient clarity in relation to the extent and manner in which officials were permitted to exercise their discretion. The intelligence reports are also being gathered pursuant to general powers with the lack of clarity around the scope of the powers underlined by the fact that the means through which pictures of demonstrations had been gathered were unclear even once a report had been disclosed.

38 We note that there are other similar examples of unlawful and/or unregulated evidence advanced in relation to other countries below.

gathered has the potential to be used in judicial proceedings. Yet human rights bodies and courts have found the retention by law enforcement agencies of information gathered through protest surveillance to be in violation of the right to privacy. For example, in *Catt v UK*, the European Court found that the ongoing retention of an activist's data despite the fact that he had never been convicted of a crime and was not assessed as a threat was incompatible with his right to privacy.[39] The Court highlighted thus that the authorities cannot surveil, investigate, and retain the data of activists on the mere basis of their having participated in protests. In its judgment, the Court held that the ongoing retention of personal information was likely to have a chilling effect, and that data must be deleted once its continued retention is disproportionate.[40]

We are concerned by the increasing number of cases where unlawful evidence is being admitted into criminal proceedings regardless of safeguards under the right to privacy. As such, it is urgent to develop due process safeguards relating to the information of protesters, activists, and HRDs. As we demonstrate below, these due process safeguards can only be developed by interrogating the gathering and retention of information obtained through surveillance at protests in terms of their impact on fair trial rights.

We have shown in this section that the opacity as regards the technologies deployed by law enforcement agencies is closely linked to the impacts on the fair trial rights of protesters, activists and HRDs. This is both insofar as the lack of transparency is inherent in surveillance that breaches the right to privacy and as a result leads to unlawful evidence gathering and in inhibiting defendants and even courts from properly scrutinising information once it is admitted into criminal proceedings.

---

39 ECtHR, *Catt v the United Kingdom,* App, no 43514/15), Judgment, 24 January 2019, §80. See also PI, 'Catt v the United Kindgom case' https://www.privacyinternational.org/legal-action/catt-v-united-kingdom

40 *Catt v the United Kingdom*, cited above, §119.



2. IMPACT OF UNLAWFUL PROTEST SURVEILLANCE ON THE RIGHT TO A FAIR TRIAL

In the previous section, we highlighted the growing use of information gathered through the unregulated and unlawful surveillance of activists and HRDs participating in protests as evidence in criminal proceedings and the accompanying lack of transparency. In this section, we examine in detail the varying impacts that the increased deployment of information obtained through the surveillance of activists, protesters, and HRDs as evidence in criminal proceedings has on their right to a fair trial. We examine the impact of protest surveillance on the right to a fair hearing – and in particular the equality of arms and the right to adversarial proceedings – as well as the presumption of innocence. For context, we provide hereinafter a brief explanation of the equality of arms and the right to adversarial proceedings and how they fit into our research below.

AN EXPLANATION OF THE EQUALITY OF ARMS AND THE RIGHT TO ADVERSARIAL PROCEEDINGS:



The right to a fair hearing incorporates both of these closely interrelated principles. The equality of arms principle refers to the requirement that both parties to the proceedings have "the same procedural rights and any distinctions must be based on law, have objective and reasonable justification and not result in disadvantage or unfairness to the defendant".[41] Its purpose is to ensure that both parties have equal opportunity to contest arguments and evidence presented by the other party. The right to an adversarial trial in comparison requires that both the prosecution and the defence "must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party".[42]

There is therefore considerable overlap between these two aspects of the right to a fair trial given that both equality of arms and the right to an adversarial trial can cover the defendant's access to information. They can be distinguished on the basis that the equality of arms necessitates ensuring that a defendant is granted equal access to information (relative to the prosecution); whereas the right to an adversarial trial requires that a defendant is able to access all relevant evidence.[43] In light of the overlapping nature of these principles – we examine them together under the umbrella of effective participation in the proceedings.

---

41 UN Human Rights Committee, General Comment No 32, UN Doc CCPR/C/GC/32 (23 August 2007) §8, §13.
42 ECtHR, *Rowe and Davis v United Kingdom,* App No 28901/95, Judgment, 16 February 2000, §60.
43 See for example, ECtHR, *Vermeulen v Belgium,* App No 19075/91, Judgment, 20 February 1996, §33.

2.a. Lack of transparency impeding effective participation in proceedings

The lack of transparency, which as set out above is closely tied to the secretive gathering of information through the surveillance of protesters, activists, and HRDs in breach of right to privacy, means that defendants cannot engage with the proceedings from a position of parity. This breaches the equality of arms and adversarial proceedings principles since protesters, activists, and HRDs cannot properly interrogate evidence that they do not know. Alternatively, if the existence of the information is known – details of how it was gathered, how it was stored, with whom it was shared, and how it was used are unlikely to be available to the defendant. The impact on an individual's right to fair trial, as we address below, are likely to be similar in either of these eventualities.

In addition to the equality of arms and the right to adversarial proceedings, the position of being unable to effectively interrogate information obtained through protest surveillance is also incompatible with a number of procedural requirements pursuant to the right to a fair hearing. One example is the obligation for a defendant to have adequate time and facilities to prepare their defence.[44] This incorporates the obligation on the part of the prosecution to disclose relevant evidence that has been collected during the investigative phase and for the defendant to have the time and facilities to be able to effectively examine it.[45]

In the Serbian example that we refer to also above, the failures of transparency regarding the source of surveillance evidence in turn had implications for both the equality of arms and the right to an adversarial trial of the individuals fined for their involvement in protests. Through our interview with the Serbian defence

---

44 See for example, UN CCPR, *Wright v Jamaica*, Communication No 349/1989, UN Doc CCPR/C/45/D/349/1989 (1992), §8.4. For a similar requirement see, Article 6(3), ECHR.

45 See for example, ECtHR, *Rowe and Davis v United Kingdom* (2000) 30 EHRR 1, §59. We note that the right of disclosure of relevant evidence is not absolute and there may be circumstances in criminal proceedings in which non-disclosure may be appropriate, for example to protect the identity of a witness. However, non-disclosure must be necessary and justified. None of the examples we document relate to 'necessary' limitations on the right of disclosure and neither do they appear to involve reasoned decisions where consideration, including the balancing of countervailing factors, was given to the question of whether non-disclosure could be justified.

lawyer, we were told that due to the lack of clarity regarding the mode by which individuals were identified it was effectively impossible to interrogate the evidence adduced by the prosecution.[46] This is because when police officers were cross-examined during court proceedings (which arose from protesters appealing their fines), they were unable or unwilling to say how the accused had been identified. This obfuscation went to considerable lengths, including police officers informing the court that an unnamed individual "from the IT department" had identified numerous defendants. Given that the individual from the IT department was not named, they could not be called to give evidence. Ultimately many of the cases were successful and the fines overturned, because the appellate courts found protesters had precisely not been recognised through direct observation of police officers as required under Serbian law.

This illustrates how secret or opaque indiscriminate surveillance at protests is incompatible with the equality of arms principle and the right to an adversarial trial. Defendants will as a matter of course be unable to access the same information as the prosecution (equality of arms) and by extension will also not be able to question and comment on the evidence (the right to an adversarial trial). This finding is supported by OHCHR's most recent report to the UN Secretary General on Human Rights in the Administration of Justice to which we submitted our preliminary findings by way of submissions. The report found that digital information secured through the surveillance of activists, protesters, and HRDs and subsequently used as evidence in criminal proceedings "can impact the right to a defence, as it is often gathered without transparency, making it difficult for the defence to challenge its accuracy, credibility and lawfulness."[47]

The findings in OHCHR's report on Human Rights in the Administration of Justice are also underlined by the French example set out above and provided to us by Data Rights. Data Rights explained to us that the confidential law enforcement

46 See also, PI, 'Prosecuted for protesting: Serbia' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting.

47 UN Secretary General report on human rights in the administration of justice, UN Doc A/79/296 (7 August 2024) §18.

reports used to justify the home arrest orders are as a rule undated.[48] As such, it is impossible to know when the surveillance information underpinning them was collected and by extension whether they were collected for the express purpose of being used to justify the home arrest order or in turn if they were part of a wider criminal investigation. Without a clear date, the possibility to even question the lawfulness and accuracy of such information is completely undermined.

The failures of the Russian authorities in *Glukhin* case to provide information as regards the source of the evidence, as well as how it had been collected (for example the nature, size, and contents of the FRT database) also highlighted the same issues. Even if the European Court did not consider the applicant's grounds regarding the right to a fair trial (Article 6), the refusal on the part of the authorities to fully disclose how they had identified him vitiates the possibility of being able to interrogate and comment on this critical evidence.

Glukhin case underlines the direct pipeline between unlawful evidence and fair trial violations described above. The European Court found that the surveillance measures breached the applicant's right to privacy and as a result they were unlawful. Without transparency as regards a surveillance measure and how it was used, including all inputs and outputs it generated (which in this case was mitigated through fact-finding by the human rights Court itself) assessing the lawfulness of prosecution evidence itself becomes more difficult or impossible. This is significant because the use of unlawful evidence may render proceedings unfair under the right to a fair trial.[49]

Human rights jurisprudence, especially the European Court's, suggests that in order for a violation to be found the proceedings as a whole must be rendered unfair due to how the evidence was obtained.[50] Where for example the defendant

48 See also, PI, 'Prosecuted for protesting: France' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

49 Article 6(1) ECHR. In this regard we note that the ECtHR has previously held that the determination of the admissibility of evidence is one for national courts to make – ECtHR, *Schenk v Switzerland,* App No 10862/84, Decision, 06 March 1986, §§45-46. However, under Article 6(1) the Court must assess the overall fairness of the proceedings, which could be compromised in the event that that a defendant is not able to effectively challenge evidence or oppose its use.

50 ECtHR, *Ayetullah Ay v Turkey,* App nos 29084/07, 1191/08, Judgment, 27 October 2020, §§ 123-130.

had the possibility to contest the authenticity and quality of the evidence and the evidence was not the sole (or main) basis on which a conviction was secured, the Court has found no breach of Article 6 ECHR.[51] In *Khan v the United Kingdom*, the European Court of Human Rights held that there was no need for other corroborating evidence where the unlawful evidence was very strong and there was no risk of it being unreliable.[52]

We believe that this approach should be revisited in light of (a) the increasing prevalence of privacy violations through the surveillance of activists participating in protests and (b) the challenges that this surveillance poses for the equality of arms and the right to an adversarial trial. For these reasons, we believe that activists and HRDs will be unable to properly challenge the authenticity and quality of evidence (including for example whether a surveillance mechanism has a propensity for bias or if the information it generates is accurate).

The policing of the anti-monarchy protests in Thailand in 2020-2021 also supports this conclusion. Research conducted by civil society organisations points to the largescale deployment of spyware on activists involved in anti-government demonstrations (notwithstanding the position of the authorities that it was not being deployed).[53] For example, an investigation conducted by the Internet Law Reform Dialogue (iLaw), DigitalReach, and Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto, has found that the phones of at least 30 individuals involved in the protests were infected by Pegasus spyware between 2020 and 2021.[54] Apple notified some of the individuals whose devices had been infected in 2021 with a further set of notifications in 2022. Following the second round of notifications, it is apparent that the total number of infections was likely substantially higher than 30 individuals.[55] The individuals who had been targeted included activists, human rights defenders, and academics.[56]

---

51 ECtHR, *J.H v the United Kingdom*, 44787/98, 25 September 2001, §§78 –79.

52 ECtHR, *Khan v the United Kingdom,* App no 35394/97, Judgment, 12 May 2000.

53 Internet Law Reform Dialogue (iLaw), DigitalReach, and the Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto, Parasite that Smiles: Pegasus Targeting Dissidents in Thailand (17 July 2022) https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/.

54 *ibid.*

55 *ibid.* See also, PI, 'Prosecuted for protesting: Thailand' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

56 *ibid.*

Considering the critical role that social media played in organising the 2020-2021 protests in Thailand, the primary function of the use of spyware was likely to obtain intelligence relating to the locations and organisation of protests. However, it may also have been used in decisions to arrest and detain protesters.[57] This can be seen from the proximity in time between spyware infections and the arrest of activists and protesters.[58] Not only was there a proximity in time between the use of spyware on protesters and their arrests, but while in detention there were examples of activists suffering further infections at the time when law enforcement had full access to their mobile devices. In this way, the exercise of powers of arrest and detention were driven by the use of surveillance technologies, but also in turn spurred further information gathering that could yield additional evidence in criminal proceedings against activists and protesters.

Information obtained through spyware cannot lawfully be admitted as evidence under the rules of evidence in Thailand.[59] However, in previous cases the authorities have been able to circumvent the inadmissibility of digital evidence that had been obtained unlawfully through state officials testifying that they had obtained evidence from "secret investigations". This in turn allowed the authorities to argue that the information should be admitted as evidence without providing explanations as regards its provenance.[60] It is unclear if this justification was used in relation to the prosecution of protesters and activists arrested in the wake of the 2020-2021 anti-monarchy protests. However, during an interview we did with Akarachai Chaimaneekarakate, the Advocacy Lead of Thai Lawyers for Human Rights (THLR)[61] – we learned that multiple cases were brought against protesters and activists on the basis of information obtained through surveillance measures such as SOCMINT.[62] Such measures are unregulated but may not be unlawful under Thai law (even if as we have argued

57 Parasite that Smiles: Pegasus Targeting Dissidents in Thailand, cited above.
58 *ibid.*
59 *ibid.*
60 Parasite that Smiles: Pegasus Targeting Dissidents in Thailand, cited above.
61 THLR offers free litigation and legal support to human rights defenders whose civil and political rights have been violated.
62 See also, PI, 'Prosecuted for protesting: Thailand' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

as above, opaque, blanket, and disproportionate surveillance of protesters is contrary to international human rights law). There is however a risk that such surveillance measures are used as a 'legal' means to confirm information originally obtained through spyware.

In all, the above examples highlight how the blanket and indiscriminate surveillance of activists participating in protests completely compromises the exercise of core due process rights including the equality of arms and the right to an adversarial trial and by extension the overall fairness of proceedings. As underlined by the 2024 OHCHR report, there must be clearer positive transparency obligations under the fair hearing rights that we have explored above, including during the investigative phase. This is the only means by which the nexus between unlawful and secretive information gathering and the downstream fair trial impacts can be addressed. We address the substance of what these safeguards could look like below.

In the case of technologies such FRT and SOCMINT, this should also include transparency as regards all input data. With regard to access to and inspection of all relevant information, as noted above, the right to a fair hearing[63] imposes positive obligations on the authorities to provide adequate time and facilities to enable a defendant to prepare their case. The OHCHR's report on Human Rights in the Administration of Justice similarly underlines that transparency rights must be further incorporated into the equality of arms including the positive obligations to provide adequate time and facilities.[64]

63 Article 6(3)(b) ECHR and Article 14(3)(b) ICCPR.

64 See for example, §17 – in which the OHCHR states the following in relation to the use of AI in criminal proceedings: In criminal trials, the accused has a right to a defence and must have adequate facilities for the preparation of that defence, which includes access to documents and other evidence and must include all materials that the prosecution plans to offer in court against the accused or that are exculpatory. These rights might be undermined in situations in which defendants are unaware that AI systems were used in making a decision that affected them, where defendants are unable to understand how AI systems reached the decision that was made, or where defendants are unable to challenge or appeal the decision-making process or the decision itself."

2.b. Misleading inferences drawn from unscrutinised evidence

The surveillance of activists and HRDs involved in protests is increasingly leading to false and/or misleading inferences being drawn in evidence presented in criminal proceedings at the detriment of the effective participation of the parties in the proceedings, as well as the presumption of innocence principle.[65] Digital information obtained through protest surveillance is particularly vulnerable to manipulation, alteration, destruction, or omission whether accidental or with intent. As such, the largescale collection of data through such surveillance (often in breach of safeguards under the right to privacy) increases the risk that exculpatory evidence is deleted, information is selectively presented to draw certain inferences about a suspect, and/or data indicative of guilt is entirely fabricated. In a context where information is regularly gathered unlawfully, secretively, and without due transparency throughout the investigation and even once proceedings have commenced, defendants are unable to interrogate and challenge misleading or even fabricated digital evidence.

This embeds an approach whereby the starting point is that the accused committed the offence in question and the burden of proof is reversed in favour of the prosecution thereby violating the presumption of innocence

The risk that surveillance evidence is omitted, selectively presented or even manipulated increases in a context where:

1. The surveillance technologies in use generate large amounts of digital evidence, which are often stored for long periods of time. This increases the risk that information is subject to further secondary uses by law enforcement, that information is accidentally or deliberately deleted, and/or that it is manipulated or overlooked. As we have seen above, unlawfully collected evidence is not being deleted or subjected to procedures designed to prevent it being admitted to criminal proceedings; and

65 Enshrined at Article 14(2) ICCPR and Article 6(2) ECHR, the presumption of innocence requires that criminal courts cannot start with the preconceived idea that the accused has committed the offence charged; the burden of proof is on the prosecution, and any doubt should benefit the accused. See for example, Council of Europe, Guide on Article ECHR, https://www.echr.coe.int/documents/d/echr/guide_art_6_criminal_eng, page 70.

2. Members of the judicial system may to have an automatic trust in technology and its use by law enforcement, despite the fact that surveillance technology is often novel and untested.[66] This risk is often coupled with a limited understanding as regards the capabilities and limitations of a particular technology being deployed.

The intersection of the above issues is highlighted by the so-called *Bhima Koregaon* case in India, which involved the arrest of 16 activists who had participated in the commemoration of an historic Dalit military victory in 2018.[67] The activists were charged with terrorism offenses after riots triggered by Hindu nationalists that appeared to be in response to speeches delivered at the commemoration.[68] The activists were subjected to surveillance over a period of two years prior to the commemoration and malware was used to plant fabricated information on their computers that purported to show them engaging in terrorist activists as members of banned groups.[69]

While the cases have not yet gone to trial, the fabricated information played a significant role as evidence in bail proceedings involving the defendants.[70] In particular, the lower courts gave deference to the information and accepted that it demonstrated the defendants' roles in terrorist activities and banned groups and thereby denied them release on bail.[71] It was not until a decision of the highest court, the Supreme Court, on the bail applications – that the credibility and probity of the evidence was examined. The Supreme Court found that an

---

66 See for example Angwin, Julia, and others, 'Machine Bias', ProPublica, 23 May 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing This study found that an algorithmic tool used in the US to produce risk assessments for sentencing purposes was followed by judges before imposing lengthy custodial sentences on defendants with little further reasoning or consideration. This was despite the fact that the tool was almost twice as likely to categorise black defendants as a higher risk compared to white defendants convicted of similar offences as well as the fact that even prosecuting authorities have accepted that the tool should not be determinative of sentences.

67 Siddhartha Deb, 'The unravelling of a conspiracy: were the 16 charged with plotting to kill India's prime minister framed?', *The Guardian*, 12 August 2021 https://www.theguardian.com/world/2021/aug/12/bhima-koregaon-case-india-conspiracy-modi

68 In particular, the activists were arrested and charged for alleged links to Maoist organisations, including purchasing bullets and firearms for the group.

69 Siddhartha Deb, 'The unravelling of a conspiracy…', cited above.

70 See also, PI, 'Prosecuted for protesting: India' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

71 See Supreme Court of India, *Vernon v The State of Maharashtra and ANR*, Crl.A No 640/2023, §16.

"element of evidence-analysis" was required in the determination of the bail applications and that when this was done, the fabricated information had *"weak probative quality or quality"*.[72]

Prior to the intervention of the Supreme Court, the Defendants were denied their right to participate effectively in the proceedings. In particular, they were unable to adequately interrogate how the information implicating them was generated, who handled it, and how it ended up on their electronic devices.[73] The lower courts gave deference to the prosecution's version of how the information had been assembled and technical evidence pointing to fabrication was dismissed outright.[74]

This example and the others we set out below also showcases that the blanket collection of information through protest surveillance and its use in criminal proceedings is also not compatible with the presumption of innocence and the burden of proof, which is always on the prosecution. This is because blanket and disproportionate protest surveillance embeds an approach whereby the starting point for law enforcement agencies and judicial administrations is that the accused was guilty of an offence and the burden of proof is reversed in favour of the prosecution.

In France, a number of cases involving environmental protesters demonstrate the propensity for intensive systematic surveillance undertaken by law enforcement to lead to the rapid attribution of guilt for alleged criminal offences to activists and protesters and for the courts to readily accept the credibility of evidence arising from surveillance.[75] The result is that potentially every-day behaviours are recast through the lens of surveillance, which already imputes suspicion onto its

72 *ibid.*, §29.
73 *ibid.*
74 Siddhartha Deb, 'The unravelling of a conspiracy…', cited above.
75 See for example, Laske, Karl &Lindgaard, Jade, 'Sur fond d'espionnite, les incroyables dérives de l'enquête contre la mouvance écologiste', Médiapart (29 September 2023) https://www.mediapart.fr/journal/france/290923/sur-fond-d-espionnite-les-incroyables-derives-de-l-enquete-contre-la-mouvance-ecologiste (in French)

subject, as indicative and even determinative of guilt.[76] As above, this directly violates the presumption of innocence principle.

According to information provided to us by Data Rights – a journalist covering a 2022 protest against a plant of Lafarge company close to Marseille (which culminated in activists breaking into the factory with the goal of destroying it) – was subjected to arrest and detention following a raid on his property. In his account as provided to Mediapart, the journalist said that during the house raid that led to his custody ten policemen broke the (unlocked) door, yelled at him that if he moved, they would beat him[77]. The policemen scattered the contents of his wardrobe, selected a dark T-shirt, a dark pair of trousers and protective glasses, and then took pictures of this assortment. They commented that the colours were monochromous thereby suggesting that he was involved in the protest. Once in custody the journalist said that police officers informed him that they had been tracking him for months and that they presented him with geolocational data that they had obtained as well as contact information of individuals he knew. In the end, no evidence was found against him, charges were dropped, and he was released.

In the UK[78], the British Broadcasting Corporation (BBC)[79] reported that two protesters involved in Black Lives Matter demonstrations and who had been prosecuted for allegedly assaulting and abusing police officers were acquitted after the court found that the prosecution had deliberately failed to disclose exculpatory bodycam footage.[80] According to their legal representatives, the bodycam footage showed the protesters being pushed and struck by officers policing the protest rather than the pair being involved in any violence against the officers.[81]

---

76 Barbier, Marie and Lindgaard, Jade, 'À Bure, la justice a bafoué les droits de la défense', Médiapart and Reporterre (1 May 2020) https://reporterre.net/A-Bure-la-justice-a-bafoue-les-droits-de-la-defense

77 Karl Laske and Jade Lindgaard, "Sur fond d'espionnite, les incroyables dérives de l'enquête contre la mouvance écologiste", Médiapart (29 September 2023), https://www.mediapart.fr/journal/france/290923/sur-fond-d-espionnite-les-incroyables-derives-de-l-enquete-contre-la-mouvance-ecologistehis

78 See also, PI, 'Prosecuted for protesting: United Kingdom' (November 2024) https://privacyinternational.org/long-read/5460/prosecuted-protesting

79 The BBC is a British public service broadcaster that provides news, entertainment and cultural content.

80 Titheradge, Noel, 'Police officers widely misusing body-worn cameras', *BBC News* (28.September 2023) https://www.bbc.co.uk/news/uk-66809642

81 Deighton, Pierce, Glynn, 'DPG clients interviewed for BBC investigation uncovering police camera misuse', *DPG,* https://dpglaw.co.uk/dpg-clients-interviewed-for-bbc-investigation-uncovering-police-camera-misuse/.

With regard to disclosure obligations, Section 3(1)(a) of the Criminal Procedure and Investigations Act 1996 provides that the disclosure duty on the part of prosecutors encompasses material that might reasonably be considered capable of undermining the case for the prosecution. As per Section 7A of the 1996 Act this is an ongoing duty. However, as set out in the Crown Prosecution Service's (CPS) Disclosure Manual:

> *"The prosecution team's duties under the CPIA are* ***not simply about compiling schedules of unused material as part of preparation for court.*** *At the heart of every investigation is the obligation, in the CPIA and Code of Practice,* ***to pursue all reasonable lines of enquiry, whether these point towards or away from the suspect.***
>
> *In the early stages of the investigation,* ***it may not be clear whether an offence has been committed, whether a prosecution is likely to follow and whether material obtained may be used in evidence or will be unused."***[82]

There is an inherent tension that is likely to be particularly relevant in the context of the policing of protests between the requirement to exhaust all levels of inquiry, which naturally entails the gathering of extensive material that may be unused by the prosecution, and the due process rights of protesters, activists and HRDs. The clear link between blanket and disproportionate surveillance measures at protests and evidence in criminal proceedings means that any information gathered during protests has the potential to be used in such proceedings. As above, the volume of data gathered combined with the opacity of how it is processed once collected makes it difficult to challenge its integrity, accuracy, and/or credibility. Together with the lack of independent oversight of the disclosure process, including over what information is found to be relevant/irrelevant and whether exculpatory material is flagged, this example demonstrates the incompatibility of blanket surveillance with the equality of arms and adversarial proceedings principles.

---

82 Crown Prosecution Service (CPS), *Disclosure Manual (*Refreshed 14 July 2022) https://www.cps.gov.uk/legal-guidance/disclosure-manual

In accordance with human rights standards and in particular the right to privacy, surveillance information captured at protests should only be retained where there is reasonable individualised suspicion that an individual committed an offence, as we have previously highlighted.[83] The European Court of Human Rights' jurisprudence has for example also found that reasonable suspicion is required in cases of targeted surveillance in the criminal context (which applies to the surveillance of activists and HRDs).[84] In the UK case set out above, the failure to comply with the safeguard meant that the authorities started with the idea that the accused were guilty, and the burden of proof was reversed so that the protesters had to prove that they were not guilty of assaulting the police officers. As such, the case also points to a failure to comply with the presumption of innocence and burden of proof.

In Russia, for example, criminal proceedings involving civil society activists demonstrate the possibility for surveillance measures to completely erode the presumption of innocence principle and right to a fair hearing. In one case an activist who participated in anti-government protest was subjected to secret surveillance in her home, including through video and audio recording devices in her bedroom.[85] The prosecution played numerous clips of the recordings made in her home during the trial. This was notwithstanding the fact that most of the recordings were inaudible and did not contain information relevant to the criminal charges.[86] The Defendant was not able to adequately challenge this evidence and nor was significant information about how it was produced, including its judicial authorisation, disclosed to her in contravention of the equality of arms.

These examples demonstrate that data protection principles as well as the right to privacy are insufficient on their own to guard against the challenges to the fair hearing rights and the presumption of innocence created by the misleading and

---

83 ül, *'Restraining Protest Surveillance:...', cited above.*

84 See for example, *Konstantin Moskalev v Russia*, App No 59589/10, 7 November 2017, §53.

85 TrialWatch, Russian Federation vs. Anastasia Shevchenko, October 2021, https://humanrightsembassy.org/attachments/article/385/Fairness%20report%20on%20the%20trial%20of%20Anastasia%20Shevchenko%20in%20Russian%20Federation.pdf

86 *ibid.*

selective presentation of (often unlawfully collected) evidence obtained through surveillance. Overly wide exemptions for national security and law enforcement, may enable authorities to view and process the personal data of activists and HRDs without due safeguards and limits. Further, as we have seen above in relation to the jurisprudence of the ECtHR concerning Article 6 ECHR, evidence collected contrary to the right to privacy may nevertheless be used in criminal proceedings without violating the right to fair trial. As such there is an urgent need for bespoke fair trial protections, including procedural safeguards, that take account of the fact that information may have been gathered contrary to the right to privacy and used for multiple onward purposes.

Such safeguards should apply in the information gathering phase, including in respect of the collection and handling of any data that may be used as evidence. This is because of the ways that the indiscriminate surveillance of protesters, activists, and HRDs by law enforcement is directly leading to violations of principles such as the equality of arms, the right to adversarial proceedings, the presumption of innocence and the burden of proof as evidenced by the examples above.[87]

87 We note that this is something that the ECtHR has previously rejected in its jurisprudence. For example, in *Schenk v Switzerland,* the Court concluded that the unlawful interception of evidence did not mean that the defendant was treated as guilty prior to a conviction in view of other corroborating evidence.

2.c. Necessary protections to ensure effective participation in proceedings and scrutiny of evidence

In all, the core fair trial violations that we have highlighted in the above two sections of the report interlink in a number of ways. Firstly, they all involve the use of unlawful and/or unregulated surveillance evidence in criminal proceedings against activists and HRDs. Secondly, the evidence is frequently being used without due transparency as regards what technology was used, the nature of any input data, what information was collected and what if anything was inferred from it, and which body approved and oversaw the collection of the evidence. In this opaque context, defendants are unable to interrogate and challenge the digital evidence used against them, which is itself vulnerable to manipulation, alteration, destruction, or omission whether accidental or with intent. This in turn compromises an accused's fair trial rights by vitiating the equality of arms and the right to an adversarial trial and/or reversing the burden of proof and the presumption of innocence.

As argued more broadly in the case of fair trial challenges posed by digital evidence collection, there is a critical need for procedures to *"verify and validate the evidence processing at all stages"*, including in *"establishing chain of custody, data integrity, attribution, and reliability of forensic methods and tools in the digital investigation"*.[88] However, the above two sections also demonstrate that such evidence gathering and processing protocols must contain specific protections relating to cases involving the prosecution of activists and HRDs participating in protests.

These should start from the premise that peaceful protest is a protected activity and incorporate safeguards under the human right to privacy. For example, the use of invasive surveillance technologies such as FRT against those peacefully participating in an assembly should be prohibited. This should entail prohibiting the use of invasive surveillance technologies such as FRT against those

88 Stoykova, Radina, 'The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations', 49 *Computer Law and Security Review* (July 2023).

peacefully participating in an assembly.[89] Generally, the authorities should not engage in the recording of participants in assemblies, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law and subject to the principles of necessity and proportionality.

Privacy protections around access to and retention of surveillance data, including deletion of information where the above safeguards are not adhered to, should also be implemented as the starting point. These must at a minimum include the deletion of information collected in breach of the principle of proportionality and the need for reasonable suspicion as well as adherence to the notification requirement. While there may be legitimate reasons for withholding information from a suspect, including the risk that significant information is destroyed, limitations on the notification requirement must be construed narrowly and cannot serve as a trump card vis a vis other fundamental rights concerns.[90] This is because the notification requirement is critical to ensuring that potentially exculpatory information is not deleted and that defendants are properly able to prepare their defence.[91]

However, we consider that there is an urgent need for additional complementary fair trial safeguards that protect the rights of activists, HRDs and protesters against downstream abuses of their information particularly in the event that deletion and notification requirements are violated. For example, we consider that all digital information gathered through the surveillance of activists involved in protests should be subject to a review as regards its lawfulness before it is admitted as evidence into proceedings.

---

89 See recommendations in OHCHR's 'Report on the Impact of new technologies … in the context of assemblies, including peaceful protests' (cited above).

90 For example, under Article 8 of the ECHR – the notification requirement is not absolute and a priori notification can be delayed, but only where it would seriously jeopardise the purpose for which the surveillance was authorised. The European Production Order Certificate (EPOC) annexed to the EU's E-evidence Regulation contains wide grounds for an issuing authority (for example a court or prosecutor's office) to delay notifying the person whose data are being requested, including where doing so would obstruct investigations or in the interests of national or public security.

91 Fair Trials, 'Policy brief: The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters' (Published: December 26, 2018 (Last updated: February 25, 2022)) https://www.fairtrials.org/articles/publications/digital-or-not-fair-trial-principles-apply-challenges-of-e-evidence-and-the-right-to-a-fair-trial/

Failure to carry out this review should necessitate a finding that an accused's fair trial rights have been breached. Such a review must at the very least:

- Incorporate the inspection and testing (including for accuracy and/or bias) of information to be admitted as evidence into proceedings, including any inferred data. Such a review of all relevant evidence should include the possibility for a review by an independent expert. Law enforcement agencies should log when certain information is obtained as well as further uses of relevant data (which should also be dated). Such logs must be provided to the defence.

- Incorporate the inspection and testing of any information not being admitted into proceedings to ascertain if the data contains exculpatory details that would otherwise not be considered as part of the proceedings.

- Allow for the deletion and exclusion of unlawfully collected information from criminal proceedings thereby preventing such information being admitted as evidence at the trial stage.

- Be subject to independent judicial oversight, including throughout the performance of all of the above.

There is also an urgent need for an ex-post remedy that systematically requires deletion and exclusion of unlawful evidence where such information has been relied upon to the detriment of a defendant's fair trial rights. This is a distinct procedural remedy to the a priori review set out above and would offer a further layer of protection. Such a remedy would act as a deterrent to the use of evidence that would violate a defendant's fair trial rights in the first instance and ensure that procedural safeguards are not ancillary and incidental to substantive ones.[92] Where information obtained through unlawful surveillance was admitted as evidence, it should automatically render the criminal proceedings unfair as it undermines the enjoyment of the right to a fair hearing.

---

92 Civil Rights Defenders, 'Draft Paper, Evidentiary standards and remedies for use of illegally or improperly obtained evidence in the case-law of the European Court of Human Rights' (1 April 2020) https://crd.org/wp-content/uploads/2020/12/Evidentiary-standards-ECHR_FT-draft-paper_1Apr2020.pdf

A number of these recommendations are in line with the ECtHR's recent findings in the case of *Yüksel Yalçınkaya v. Türkiye,*[93] which (albeit not directly relating to participation in protest) concerned a challenge, including on grounds under Article 6 ECHR, to a defendant's trial and conviction for alleged membership of a terrorist organisation.[94] The conviction largely rested on evidence demonstrating the defendant's use of the encrypted ByLock messaging app. The proceedings were consistent with domestic criminal law and a significant number of other prosecutions and convictions similarly on the sole basis that an accused used ByLock. In its Grand Chamber judgment, the ECtHR found that electronic information that was not collected pursuant to independent judicial authorisation and oversight as well as procedures to protect its integrity would raise prima facie doubts regarding its reliability and quality.[95] The Court found that there was a requirement to assess the integrity of such information prior to its communication to the judicial authorities and that this could take place through examination by an independent expert.[96]

93 ECtHR, *Yüksel Yalçınkaya v Türkiye*, App No 15669/20, Judgment, 26 September 2023.

94 Turkut, Emre & Yıldız, Ali, 'ByLock Prosecutions and the Right to Fair Trial in Turkey: The ECtHR Grand Chamber's Ruling in Yüksel Yalçınkaya v. Türkiye', *Statewatch* (March 2024) https://www.statewatch.org/media/4200/sw-echr-yalcinkaya-bylock-report.pdf

95 Turkut, Emre & Yıldız, Ali, 'ByLock Prosecutions…', cited above.

96 *ibid.*

3 FAIR TRIAL RIGHTS AND ANCILLARY PROCEEDINGS



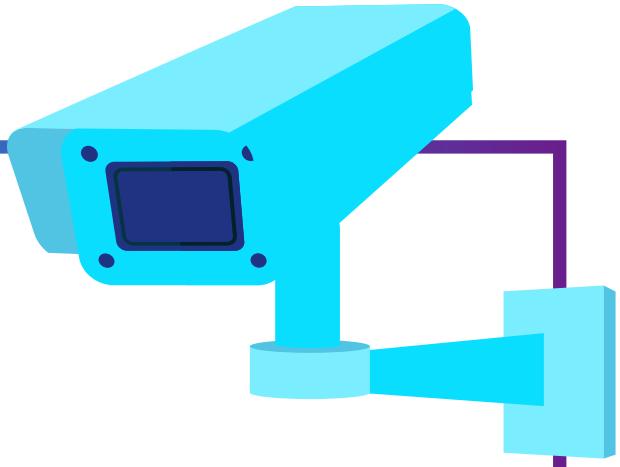
As above, we have construed criminal proceedings broadly to encompass all stages from when an individual is arrested to when they are acquitted and/or sentenced. We are concerned about the increasing number of fair trial breaches occurring in the pre-trial phase and therefore the trial phase cannot be viewed in isolation. We explained above that these breaches occurring earlier in criminal procedures are likely to render the whole proceedings, including the trial phase, unfair. The European Court of Human Rights, for example, acknowledges that fair trial rights are engaged at the time that an individual's rights are substantially affected, which is likely to be at the point of arrest.

However, the international human rights law framework underpinned by provisions protecting the right to a fair trial (such as Article 14 ICCPR and Article 6 ECHR) is largely focused on the trial itself as the site through which violations are adjudicated on and found. For example, despite the European Court recognising the importance of due process safeguards before the trial stage – it has previously found that Article 6 stricto sensu does not apply to pre-trial judicial proceedings. This includes ancillary proceedings such those relating to pre-trial detention (including bail procedures) on the basis that they are not determinative of civil rights and obligations or of a criminal charge.[97]

97 ECtHR, *Neumeister v Austria*, App no 1936/63, Judgment, 27 June 1968, §14.

In this section, **we argue that fair trial rights need to apply as widely as possible to cover all stages of criminal proceedings, including those relating to pre-trial detention and bail.** This is in light of the collapsing distinction between the investigative and trial phases arising from the role of blanket and indiscriminate surveillance of activists, HRDs, and others involved in protests in the generation of information used as evidence in such proceedings. A consequence of this collapsing distinction is that the same data may be used as evidence in both the trials of activists and HRDs and in decisions to detain them or deny them bail with significant implications for their human rights, including the right to privacy and freedom of assembly. Existing safeguards under privacy and data protection rights are similarly ineffective in cases where surveillance data is used as evidence in criminal proceedings, given that these frameworks are unlikely to be able to protect against onward uses of information that has been gathered unlawfully.

A number of the jurisdictions we have examined and some of the examples outlined above demonstrate a nexus between the generation of surveillance information used as evidence and the use of pre-trial detention to silence and intimidate activists. In the case of the Bhima Koregaon prosecutions in India, referred to also earlier on, none of the cases actually proceeded to trial. Instead, the defendants were held in pre-trial detention for a number of years. Their surveillance and the fabricated evidence placed on a number of computers belonging to the accused played a direct role in the decisions to detain and then deny them bail. The courts made assessments of their guilt on the basis of the surveillance evidence and as a result they were unable to continue their activities (and by extension others might be dissuaded from similarly engaging in acts of dissent against the government). For this reason, the finding by the Indian Supreme Court that bail hearings should include an element of evidence analysis was significant. Otherwise, pre-trial detention can be used in a way that is determinative of the rights of the accused, including the charges levelled against defendants, with less consideration of the probity of the evidence than in a trial.



A CASE STUDY ON UGANDA

In our interview with Dorothy Mukasa, the executive director of the non-governmental organisation, Unwanted Witness[98] in Uganda, she highlighted a similar set of trends to those exposed by the Bhima Koregaon case. Dorothy explained that the last few years have seen an explosion in the surveillance of activists participating in protests. She said that there had been an increase in CCTV cameras across cities in Uganda.[99] From 2019, the cameras in Kampala have been equipped with FRT and this is also being implemented in other cities across the country.[100] She explained that cameras across the country's highways were also being equipped with FRT.[101] She also said that SOCMINT is regularly being used by law enforcement in view of new powers introduced in 2021 under the Ugandan Computer Misuse Act for social media posts that "insult" the president of Uganda.[102]

Dorothy said that the deployment of surveillance during anti-government protests (including through cameras equipped with FRT) was leading to the arrests of large numbers of activists peacefully participating in protests.[103] Many of these individuals were arrested at the homes and places of work, including by plainclothes police officers in unmarked cars, after the demonstrations

98 Unwanted Witness is a civil society organisation founded to promote online freedoms and protect digital rights in Uganda, https://www.unwantedwitness.org/about/

99 https://x.com/KagutaMuseveni/status/1200120752114196481.

100 Monitor, 'CCTV cameras finally arrive' (August 02, 2018 — updated on January 11, 2021), https://www.monitor.co.ug/uganda/news/national/cctv-cameras-finally-arrive-1771740.

101 Human Rights Watch, 'Uganda: Rights Concerns Over License Plate Tracking', (14 November 2023), https://www.hrw.org/news/2023/11/14/uganda-rights-concerns-over-license-plate-tracking.

102 African Centre for Media Excellence, 'Country Report: Biometric Digital Identity Programs and Independent Journalism in Uganda' (June 2023) https://acme-ug.org/wp-content/uploads/Biometric-Digital-Identity-Programs-and-Independent-Journalism-in-Uganda.pdf.

103 See for example: Kafeero, Stephen, 'Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests', *Quartz* (27 November 2020) https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters

had concluded.[104] To her knowledge few of these cases resulted in protesters and activists being prosecuted despite the fact that formal charges were issued in a number of cases and as such she was not aware of many such cases progressing to the trial stage. Instead, individuals were detained by law enforcement in pre-trial detention.[105] Some individuals were thereafter released on bail. Dorothy further explained that she thought that the government did not want to bring the cases to trial as there was a recognition that they many of them were not meritorious. In this sense, she said that the process itself amounted to a form of punishment.

There is therefore a risk that the blanket and indiscriminate surveillance of activists, HRDs, and others involved in protests and the consequent generation of information eventually used as evidence is precipitating the use of ancillary proceedings in ways that compromises access to the courts and avoids the need for consideration of the information collected. Similar safeguards to those we outlined above, including in relation to the testing and inspection of electronic evidence, must apply to the full spectrum of criminal proceedings, including at the pre-trial stage. This is particularly the case given the lower evidentiary thresholds required to effect the arrests and pre-trial detention of activists and as above the potentially significant impacts on fundamental rights and freedoms such decisions can have.

Any evidentiary safeguards and protocols must in particular allow accused individuals to test the accuracy of surveillance evidence used in decisions against them. For example, in the case of Uganda – Dorothy noted that

104 Human Rights Watch, 'Submission to the Uganda Parliament's Committee on Human Rights Inquiry' (22 March 2022) https://www.hrw.org/news/2022/03/22/human-rights-watch-submission-uganda-parliaments-committee-human-rights-inquiry

105 *ibid.*

some individuals arrested during demonstrations were apprehended as a consequence of being mistakenly identified through surveillance measures. In some of these cases such individuals were eventually released but only after they were dropped in random locations and told to stay silent about what had happened to them. As above, the risk of misidentification is particularly high where surveillance technologies are untested and embed inaccuracies and biases and the evidentiary threshold is lower than the trial stage.

Protocols and safeguards relating to the pre-trial phase could borrow from existing jurisprudence and approaches of national courts. For example, South African courts do treat bail proceedings as dispositive of significant fundamental rights.[106] As such, bail proceedings require an intensive evaluation of any evidence introduced by the prosecution and law enforcement agencies, including with respect to principles such as the right to an adversarial trial and the presumption of innocence.[107]

106 Ntontela, Mahlubandile, 'Striking a balance in bail proceedings – how does a court determine bail in the interest of justice?', *De Rebus* (1 July 2020) https://www.derebus.org.za/striking-a-balance-in-bail-proceedings-how-does-a-court-determine-bail-in-the-interest-of-justice/

107 *ibid.*

4 THE PRIVATIZATION OF EVIDENCE GATHERING



Another concerning trend we have observed across our research is the growing roles of private companies and other private actors, in the generation and processing of surveillance information used as evidence in criminal proceedings against protesters, activists, and HRDs. Private actors include, beyond companies, in particular any organisation and group who may have varying agendas, but in the protest context they operate in support of government positions around the repression of protesters. The support and funding received by such groups is often opaque and their activities may be facilitated by national governments, but also those of other countries.

Private companies are increasingly developing the infrastructure for both surveillance measures and systems to process and manage the information collected for onward use as evidence in criminal proceedings. Information gathered by surveillance performed by private actors is increasingly being used as evidence in criminal proceedings against activists and protesters. Both the role of companies and other private actors poses significant challenges for the quality and integrity of the data collected, the effective participation of protesters and activists in criminal proceedings, and the presumption of innocence principle.

With respect to the role of corporations, the very fact that it is often the companies that themselves determine the capabilities of surveillance and evidence management infrastructure is a point of concern as they are in turn

able to shape how evidence is presented to courts and therefore the extent to which its probity and credibility can be challenged.

For example, Cellebrite's 'Guardian' interface, which is marketed at law enforcement agencies, consists of software allowing the review, categorisation (for example it could be marked as data 'pending analysis'), and 'real-time' sharing of 'evidence'.[108] Cellebrite recently announced a partnership with Amazon Web Services as part of its Pathfinder platform, which it markets as an "investigative analytics solution". The resulting Pathfinder in the Cloud product incorporates "AI capabilities" that can be used to "swiftly identify meaningful data and connections across multiple devices".[109] Cellebrite states on its website that the tool can be deployed to identify "slang and terms associated with criminal activity" and also enables "investigators to search for and categorize explicit images".[110]

As with other forms of public private partnerships, contracts between state authorities and private corporations in the provision of surveillance technologies are obscured by commercial secrecy or national security exemptions under domestic procurement and freedom of information laws.[111] Exactly how surveillance technologies could be deployed in relation to protesters and by extension how the information generated will thereafter be used and presented may remain completely opaque, even during criminal proceedings.

In the case of the Cellebrite technology, even high-level information about the training data used by the AI tool, for example, is likely to be completely opaque. It is concerning that the tool may be deployed to analyse slang as probative of criminal offending. Slang is liable to be taken out of context and misread as indicative of criminal offending particularly with respect to communities that are

---

108 Cellebrite, 'Guardian', https://cellebrite.com/en/guardian/

109 Cellebrite, 'Cellebrite Enhances Investigative Analytics Solution with Amazon Web Services (AWS)', Press release (16 September 2024) https://cellebrite.com/en/cellebrite-enhances-investigative-analytics-solution-with-amazon-web-services-aws

110 *ibid.*

111 PI, 'Safeguards 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

already racialised by law enforcement.[112] Without clarity as regards the training data, it is possible that an Artificial Intelligence (AI) tool reproduces existing racial biases and discrimination and thereby misconstrues innocent speech by activists and protesters. This could in turn influence the development of a criminal investigation and how evidence is presented at trial. It could do so in ways that undermines the presumption of innocence since it could embed an approach whereby certain speech is de facto criminal rather the prosecution having to prove criminality.

In the Serbian example above, the CCTV and hand-held cameras deployed in the policing of the environmental protests were supplied to law enforcement through a Safe City project[113] that arose out of a 2017 agreement with Huawei.[114] The capabilities of these tools, including whether they were equipped with FRT, was completely opaque. The Serbian DPA's investigation concluded that the handheld devices were EP 821 trunking terminals supplied by Huawei.[115] However, it took further journalistic investigation to establish that the devices have video and photo generation capabilities, which could facilitate the use of FRT via the backdoor.[116]

The contract between Huawei and the Serbian authorities has not been disclosed and it is therefore unclear what (if any) level of access Huawei had to the evidence generated and its role in processing, analysing, and presenting it (for example through reports) for law enforcement uses. The same is true of the CCTV cameras set up in Belgrade and other cities. If they are equipped with FRT capabilities that have not been activated, does the contract between Huawei and the Serbian authorities regulate how and when the cameras are

---

112 Ball, Jeremy & Lowbridge, Caroline, 'CPS to review guidance on using drill music as evidence, *BBC News* (24 January 2022) https://www.bbc.co.uk/news/uk-england-nottinghamshire-60070345

113 As we have previously documented, Huawei's Safe City initiative involves the company teaming with local police and law enforcement agencies to install CCTV systems, provide management systems for personal data or even carry out policing functions traditionally entrusted to the state. As of November 2021, the company has claimed to have built more than 160 so-called Smart Cities in over 100 countries and regions around the globe. PI, 'Mapping Huawei's Smart City Creep' (17 November 2021) https://privacyinternational.org/long-read/4689/mapping-huaweis-smart-cities-creep

114 Standish, Reid, 'Serbia's Legal Tug-Of-War…', cited above.

115 *ibid.* See also PI, 'Prosecuted for protesting', cited above.

116 *ibid.*

activated and the control over the ensuing information generated?[117]

This information would have been critical to ensuring that the criminal proceedings involving activists were fair under, human rights law – Article 6(1) ECHR and Article 14(1) ICPPR. This is because without the information, it becomes impossible for the accused to fully test the lawfulness and accuracy of the evidence presented to the court. Given that there was no legal basis for deploying FRT and the Serbian police forces were regularly unable to explain how they had identified the individuals they charged, lawyers for the accused were able to contest the fines in question. But what if there was a legal basis in place for using evidence generated through FRT and the authorities had set out how identification had taken place? In this case, the above information regarding the role of third parties becomes even more critical in ensuring that criminal proceedings against activists involved in protests respect the fairness requirement.

In relation to the role of other private actors, the issues raised are very similar. For example, in our interview with Akarachai – we learned that out of 307 cases against protesters filed under Thailand's lèse-majesté law during the 2020-2021 anti-monarchy protests, 161 were filed by various groups.[118] Often complaints were filed on the sole basis of information gathered through SOCMINT by members of such groups. This would consist of members of the groups going through social

---

117 With respect to the CCTV cameras in Belgrade, we note that these were first announced in 2019 by the Minister of Interior and the Director of Police, which stated that the cameras would be equipped with facial and license plate recognition software. Following the announcement, Serbian civil society organisations requested clarification from the authorities, including information relating to the public procurement of the cameras. The Ministry responded by stating that the public procurement information was entirely confidential. Meanwhile, in 2017 Huawei published more information than the Serbian government in relation to the services to be provided under the Safe City project. These were to include "smart video surveillance and intelligent transport systems, advanced 4G network, unified data centres and related command centres". The information also revealed that test cameras had been installed and had been made operational. Following a report by Share Foundation, Huawei removed this publicly available information. See Share Foundation, 'Serbian government is implementing unlawful video surveillance with face recognition in Belgrade: policy brief' (4 December 2019) https://www.sharefoundation.info/wp-content/uploads/Serbia-Video-Surveillance-Policy-brief-final.pdf

118 Thailand's lèse-majesté law criminalises 'defamatory' speech against the monarchy. Article 112 of Thailand's criminal code, external says anyone who "defames, insults or threatens the king, the queen, the heir-apparent or the regent" will be punished with a jail term between three and 15 years. Given that this is an offence against the body-politic, anyone can file a criminal complaint against another individual, Criminal Code: Royal Family (Sections 107-112), Thailand, https://library.siam-legal.com/thai-law/criminal-code-royal-family-sections-107-112/

media feeds of protesters and activists and, *inter alia,* taking screenshots of posts that criticised the Thai monarchy.[119] Akarachai explained that these actors would sometimes build a profile of each protester whose social media feed they monitor and organize relevant information (e.g., name, occupation, address, workplace address, information about social media posts, etc.) into a single document. They would then threaten certain protesters by stating that they would submit these documents to the police if they continued their activities. Akarachai advised that these screenshots sometimes only captured part of a particular post rather than its entirety. There is therefore a significant risk that surveillance data could be taken out of context, altered in some way or even fabricated altogether.

For these reasons, the role of companies and other private actors pose a direct challenge to the establishment of bespoke chain of custody protocols in relation to the management of electronic evidence generated by surveillance technologies. In many cases, in particular where third parties have active control over evidence gathered by surveillance technologies, there will be no way to properly safeguard the integrity of the information generated. This is because the role of third parties increases the likelihood that the information generated may be accessed by multiple actors for different purposes. Consequently, there is a risk that information may be altered or deleted prior to the point that it is introduced into criminal proceedings.

The lack of transparency as to how the technology can be deployed and the evidence presented also makes it much more difficult, if not impossible, to test the accuracy, authenticity and ultimately the lawfulness of the information gathered. This both has the potential to undermine the equality of arms and presumption of innocence principles. In relation to the former, the lack of transparency makes it difficult or even impossible to challenge the evidence in question – including whether its potential unlawfulness may render the proceedings as whole unfair. In relation to the latter, as above – the lack of

119 SOMBATPOONSIRI, Janjira. Intersectional Powers of Digital Repression: How Activists are Digitally Watched, Charged, and Stigmatized in Thailand. International Journal of Communication, [S.l.], v. 18, p. 23, feb. 2024. ISSN 1932-8036. Available at: https://ijoc.org/index.php/ijoc/article/view/21411/4526. Date accessed: 18 Nov. 2024.

accountability and oversight regarding the role of third parties increases the risk that evidence is framed in misleading ways to impute guilt onto a defendant.

Therefore, the development of protocols to secure the fair trial rights of activists, HRDs and others involved in protests, including at the pre-trial phase, must incorporate safeguards in relation to the role of third parties. With respect to private companies, these must at a minimum involve the documentation and disclosure of when third parties accessed surveillance evidence, the nature of the information accessed, the purposes for which it was accessed, and any secondary uses of the information. To the extent that this information is protected by national security or commercial secrecy laws, we note that information could be provided to lawyers for the accused on a confidential basis or could even be examined by an independent third party. However, we are concerned that any omission of such information (to the extent that it is included in contracts or other procurement documents) must be strictly necessary, proportionate, and justified before its omission. Overly broad exemptions or commercial confidentiality provisions are likely to compromise not only privacy and data protection standards, but also fair trial rights.

Defendants should also be informed of the role of any private actors, including how they processed and stored relevant evidence.

CONCLUSION

This report has highlighted a number of due process and fair trial issues arising from the increasing use of information generated and collected by new and untested surveillance technologies in criminal proceedings involving activists, HRDs and others participating in protests.

The blanket and indiscriminate nature of protest surveillance, which starts from the premise that anyone engaging in protest is in effect a suspect, increases the risk that evidence will be altered, destroyed, fabricated, or omitted (in the case of exculpatory information). This risk is heightened in light of the volume of information gathered through the surveillance of protests. As a consequence, the generation of surveillance evidence in the investigative phase and its inclusion in subsequent criminal proceedings undermines the presumption of innocence principle.

Opaque evidence gathering techniques are incompatible with the equality of arms principle and the right to an adversarial trial as the inability of the accused to access relevant evidence will mean that it cannot be contested, commented on, or questioned. The inability to properly assess and test the lawfulness and accuracy of the evidence generated is likely as a matter of course to render proceedings unfair.

The increasing role of digital surveillance evidence in ancillary proceedings means that many of the same fair trial issues are likely to arise in these procedures. This is particularly significant, because pre-trial detention is often being used to sanction activists and HRDs who may have been subjected to wrongful arrest and prosecution.

Finally, the growing privatisation of evidence gathering further erodes the possibility for the accused to engage with the lawfulness, accuracy, and credibility of surveillance evidence. It is often private corporations that

determine the nature and capabilities of surveillance technologies used by law enforcement and security authorities. The capabilities of the measures deployed as well as the degree of control companies have over the information generated and how it is presented are often hidden behind national security exemptions and/or commercial confidentiality. The increasing role of private actors in the surveillance of activists, protesters, and HRDs and therefore in the preparation and management of evidence similarly undermines the defence's effective participation in criminal proceedings and the presumption of innocence.

It is therefore critical that appropriate safeguards ensuring the protection of both the rights to privacy and fair trial should be embedded throughout the investigative phase and across all criminal procedures. The starting point in relation to evidence gathering must be that peaceful protest is a protected activity under international human rights law. This should entail prohibiting the use of invasive surveillance technologies such as FRT against those peacefully participating in an assembly. Generally, the authorities should not engage in the recording of participants in assemblies, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law and subject to the principles of necessity and proportionality. Where surveillance takes place in contravention of these requirements, data relating to protesters should be immediately deleted.

However, given the blanket and indiscriminate nature of protest surveillance, there is a high risk that gathering of information to be used as evidence is conducted unlawfully and in breach of the above requirements.

RECOMMENDATIONS

In light of the unacceptable risks to fairness as a consequence of downstream uses of surveillance data as evidence in criminal proceedings and without prejudice to any of the above privacy-focused protections, we consider that:

1. There is an urgent need for comprehensive bespoke procedures and protocols for digital information collection that embeds both privacy and due process safeguards. The protocols should include chain of custody requirements in order to preserve the integrity of information gathered, which should be implemented before the trial stage commences and which must be subject to independent judicial oversight. At a minimum these must incorporate:

    a. The possibility for the defence to test and assess the lawfulness and accuracy of all surveillance evidence. The assessments must include the possibility for the appointment of independent experts to examine relevant technical evidence.

    b. The assessment should include a review of whether relevant information gathered by law enforcement contains exculpatory evidence that may otherwise be deleted.

    c. Law enforcement must log when information is gathered (and the date of any further uses of the data) during the investigative phase and such logs should be provided to the defence at the same time as information is provided for this assessment.

    d. Where preliminary assessment indicates that surveillance information has been gathered unlawfully, in particular in breach of the human right to privacy, it must be excluded and not introduced into criminal proceedings. Defendants should also have recourse to a distinct

procedural remedy enabling the exclusion of digital surveillance evidence admitted in breach of fair trial requirements as well as its deletion thereafter.

2. Information should be provided to the defence regarding the role of private companies in the preparation of surveillance information for use as evidence, including all processing operations relating to the raw data. This must in particular include disclosure regarding the role and function of any AI technology supplied by relevant companies. Any omissions on grounds of national security or commercial secrecy, must be strictly necessary, proportionate, and justified before the omission of the information in question.

3. There must also be an obligation to disclose the role of any private actors where they have gathered relevant evidence used in criminal proceedings relating to activists, HRDs and protesters. This should include the source of the information as well as how it was processed (including storage arrangements) by the private actor in question. The defence must be given the opportunity to authenticate information gathered and prepared by private actors.

4. Fair trial rights already impose positive obligations on states to provide defendants with appropriate tools and procedures to be able to uphold their due process rights. These obligations must include sufficient technical access and equipment as well as time to be able to interrogate digital surveillance evidence in accordance with principles of equality of arms and adversarial proceedings.

5. National judges, prosecutors, and law enforcement must be appropriately trained and equipped to interrogate evidence generated through the surveillance of activists and HRDs participating in protests to minimise the risk of breaches of the presumption of innocence and wrongful convictions. In the context of law enforcement, any training must emphasise the relevant lawful grounds on which surveillance can lawfully take place in the context of the policing of assemblies – in particular the prevention of crime, public order, and national security.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).