UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

The Surveillance Industry and Human Rights

FIDH Submission

The International Federation for Human Rights (FIDH) welcomes the opportunity to transmit this submission to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and to contribute to the study that will be submitted to the UN General Assembly next fall. Limiting and regulating the export of dual-use products, in particular surveillance technologies, is critical in assuring the protection of freedom of opinion and expression as well as other fundamental rights.

Drawing on FIDH's experience working with member organizations and communities affected by the activities of business enterprises around the world, the following contribution stems from the concrete challenges and abuses undergone by members of civil society and affected people linked to the use of surveillance technologies.

Our contribution will address both points contained in the call for submission published by the Special Rapporteur, *i.e.* information concerning the use of such surveillance technologies (1.) and information concerning the domestic regulatory frameworks that may be applicable to the development, marketing, export, deployment, and/or facilitation of surveillance technologies by private companies (2.).

1. Overview of certain emblematic cases FIDH has followed concerning human rights violations linked to the use of surveillance technologies

- **The Egyptian repression and the use of military and surveillance equipment**

In July 2018, in a context of worsening oppression in Egypt, FIDH, the Cairo Institute for Human Rights Studies (CIHRS), the French Human Rights League (LDH) and the Armaments Observatory (OBSARM) issued a report revealing how the French State and several French companies had been supplying Abdel Fattah al-Sissi's regime with military and surveillance equipment for five years. By supplying Egyptian security services and law enforcement agencies with powerful digital tools, they helped establish an Orwellian surveillance and control architecture that has been used to repress all forms of dissent and citizen action. The report advocated for the establishment of a parliamentary inquiry and an immediate end to these exports.[1]

- **Criminal investigations into the export of surveillance technologies by French companies to Libya, Egypt and Syria**

[1]Find the report at: https://www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france

i. In October 2011, following media reports that French company Amesys had supplied "Eagle" surveillance equipment to the Muammar Gadhafi regime in 2007, FIDH and LDH filed a criminal complaint in France for complicity to torture. A judicial investigation was opened on 23 May 2012 by the specialized unit for war crimes, crimes against humanity, genocide and torture of the Paris Criminal Court (French specialized unit). The investigation is ongoing. FIDH supported seven Libyan victims to testify in the case as to how they were detained and tortured after being identified and tracked, they allege, through electronic surveillance. Six of them have joined the case as civil parties, along with FIDH and LDH. In 2017, Amesys was assigned the status of "assisted witness" in relation to allegations of complicity to torture committed between 2007 and 2011.[2]

ii. In 2012, FIDH and LDH filed a formal request with prosecutors asking courts to investigate the involvement and possible criminal complicity of French companies, including Qosmos, in supplying surveillance equipment to the Syrian regime.[3] A judicial investigation was opened on 11 April 2014. FIDH and LDH are civil parties in the case, along with five Syrian victims, represented by FIDH lawyers. These victims testified in July 2015 about acts of torture they claim are connected to Syrian regime surveillance of their electronic communications. In 2014, the prosecutor widened the scope of the investigation to include complicity to crimes against humanity. In 2015, Qosmos was assigned the status of assisted witness based on the allegations of complicity in acts to torture and crimes against humanity committed between 2010 and 2012 in France and in Syria.[4] The investigation is ongoing. Efforts to initiate criminal investigations into other European companies alleged to have been part of the supply chain (in Germany and Italy) did not succeed for legal/procedural and political reasons.

iii. Lastly, in November 2017, FIDH and LDH filed a formal request with prosecutors to investigate French company Nexa Technologies (formerly Amesys, the company involved in the Libya investigation) for alleged complicity to acts of torture and enforced disappearances in Egypt. This request was filed following revelations in the magazine Télérama about the supply of "Cerebro" surveillance technology to the Egyptian government in 2014. According to the Télérama report, the French dual-use-goods department (SBDU) responsible for granting export licenses had refrained from issuing any decision on these exports.This decision violates provisions of the Wassenaar Arrangement that have been introduced into the French system of export control. A judicial investigation by the French specialized unit was opened shortly afterwards, in December 2017.[5] FIDH and LDH are civil parties in the case. The investigation is ongoing.

- **The Italtel case: a telecom company facilitating surveillance in Iran**

In 2017, FIDH, Justice for Iran (JFI) and Redress filed a complaint with the Italian OECD National Contact Point against telecom company Italtel Group S.p.A., alleging that it breached multiple principles of the OECD Guidelines in relation to its business activities in Iran, including through a Memorandum of Understanding ("MoU") signed by Italtel and the Telecommunications Company of Iran ("TCI") in 2016. The complaint argued that the advanced technologies and services offered by Italtel to TCI risked contributing to Internet censorship and to the suppression of a wide range of fundamental freedoms and human rights in Iran. The MoU also empowered and equipped Iranian

[2] https://www.fidh.org/en/region/north-africa-middle-east/libya/16959-the-amesys-case-the-victims-anxious-to-see-tangible-progress
[3] Qosmos is suspected of having sold such equipment through a German and an Italian company
[4] https://www.fidh.org/en/region/europe-central-asia/france/designation-of-qosmos-as-assisted-witness-constitutes-an-important
[5] https://www.fidh.org/en/region/north-africa-middle-east/egypt/sale-of-surveillance-equipment-to-egypt-paris-prosecutor-opens-a

authorities including the Islamic Revolutionary Guard Corps ("IRGC") in further crushing political dissent and civil liberties throughout the country and in cyberspace. The organizations asked the Italian NCP for assistance in more thoroughly documenting the facts and called for a moratorium negotiations and business engagements between Italtel and TCI.[6]

- **Political surveillance in Colombia under A. Uribe Vélez**

Together with Colombian lawyers' collective CCAJAR, FIDH worked to bring to account those responsible for acts of espionage against human rights activists, journalists, politicians of the opposition and judges in Colombia during Álvaro Uribe Vélez's mandate. In 2015, María del Pilar Hurtado, former director of DAS (the Administrative Department of Security) was extradited and convicted of intercepting phone calls and abusing public office. Mr Uribe's former chief of staff, Bernardo Moreno, received an eight-year sentence for his involvement. The Supreme Court called for Mr Uribe to be investigated for his role in the scandal as well.[7]

On 11 September 2017, the Criminal Cassation Division of Colombia's Supreme Court of Justice sentenced another ex-director of DAS, Jorge Noguera Cotes, to 94 months in prison for his part in the wire-tapping and illegal monitoring activities. The court noted that evidence of the case revealed that Noguera, under the guise of strategic intelligence gathering, acted to unlawfully intercept private communications and carry out illegal surveillance.[8]

- **Vale and Belo Monte: corporate surveillance of human rights defenders**

In 2014, FIDH and OMCT conducted an investigation and presented the press with evidence alleging that Vale and the Belo Monte Consortium had been spying on civil society. The testimony and documents obtained during the investigation appear to substantiate claims that the companies engaged in acts of corruption, that they illegally obtained confidential information and access to databases, made illegal recordings, were involved in identity theft, and conducted unfounded employee dismissals. These offences seem to have been perpetrated with the complicity of State agents. Documents gathered seem to substantiate both the bribing of State agents and possible assistance provided by the Brazilian Intelligence Agency (*Agência Brasileira de Inteligência* - ABIN) to Belo Monte, and that Vale worked with retired ABIN agents. The alleged targets of the companies were persons and NGOs believed to be potential barriers to the companies' activities.[9]

2. Recommendations concerning regulatory frameworks applying to the surveillance industry

2.1. Reinforce the Wassenaar and EU export of dual use technology regulatory system

Some of the abovementioned cases illustrate well the gaps of the European Union system regulating the export of dual-use technologies. Moreover, to ensure that the trade of ICT technologies such as surveillance technologies do not lead to human rights violations, and to further ensure access to justice for victims, FIDH believes that there is an urgent need to strengthen the European and

[6] A summary of the case is available here: http://oecd00.fe.rzob.gocept.net:8080/oecdwatch/cases/Case_496
[7] https://www.bbc.com/news/world-latin-america-32544248
[8] https://www.fidh.org/en/impacts/colombia-the-conviction-of-das-s-jorge-noguera-is-a-triumph-of
[9] https://www.fidh.org/en/region/americas/brazil/14695-brazil-vale-and-belo-monte-suspected-of-spying-the-justice-system-must

international regulatory and policy frameworks that control the trade of these technologies through a coordinated and concerted approach.

With particular reference to the EU regulatory framework, FIDH reiterates the analysis and recommendations put forward in a dedicated policy paper of 2014.[10] On the sale and export of surveillance technologies, it especially recommends to:

- ensure the development of an effective international and European regulation of dual-use surveillance technologies in close co-operation with all relevant stakeholders, including civil society organizations, within and beyond the Wassenaar Arrangement. This includes strengthening the content of human rights considerations in the EU framework and achieving greater transparency and civil society inclusion regarding export licenses granted or denied.

- Consider ways to improve the EU Dual-Use Regulation by tackling the fragmented national export-control legislation in EU Member States and by ensuring appropriate monitoring and oversight mechanisms are in place;[11]

- Ensure the inclusion of new categories of surveillance technologies to EU and international export control lists to ensure that all relevant dual-use technology is covered by regulation and subject to licensing;

- Establish an EU-wide ad-hoc licensing requirement;[12]

- For IP Network Communication Surveillance Systems and Intrusion Software, introduce controls including case-by-case screening for all destinations with a provisional presumption of denial;[13]

- Concerning high-risk countries, deny exports that pose a substantial risk to human rights and take into account potential human rights abuses linked with the sale and export of surveillance technologies in bilateral dialogues and human rights country strategies;

- Include surveillance technologies in EU embargoes on equipment that might be used for internal repression;

- Ensure relevant regulatory authorities possess the necessary resources and technological expertise to enforce these export controls

2.2. Reinforce the international framework on Business and Human Rights and its application to surveillance technologies

Suggestions to reinforce State's obligations to protect human rights :

[10] https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf

[11] Centralizing oversight and enforcement of the Regulation would improve the level-playing field and could be a way to improve accountability. Furthermore, conflicts of interests between certain ICT companies and States exist in many countries. EU member states are indeed responsible for the licenses that businesses need to export certain technologies, but have also an interest in the commercial success of these companies. This could be avoided by placing the licensing authority at the European level;

[12] "Catch-all" controls should be made more efficient and effective by extending their application to all Member States.

[13] The license consideration process for Intrusion Software and IP Network Communications Surveillance Systems must include examination of the human rights and privacy concerns that prompted their control, and exporters should have to prove that the goods or products in question do not pose a significant risk to human rights and national security";

- Integrate specific recommendations regarding the trade of ICT technologies in the UN tools, guidelines and strategies regarding the implementation of the UN Guiding Principles on Business and Human Rights (UNGPs); include regulatory measures regarding the trade of surveillance technologies in national action plans on the implementation of the UNGPs;

- Implement conditions, triggers, benchmarks and reporting procedures to ensure the financial and technical support to the development of new technologies are not used in a way that infringe human rights;

- Include human rights clauses in public procurement processes;

- Require States to conduct human rights impact assessments (HRIA) of these technologies, including by introducing HRIA in the R&D phase of technological development

- Ensure greater scrutiny from democratic bodies to ensure trade regulations are effectively implemented;

- Implement import licenses for private companies that wish to use these technologies;

- Ensure judicial supervision of the use of surveillance technologies by the police, military and intelligence services; require ICT companies to disclose information on surveillance activities undertaken, including the time period and location;

- Request States to introduce mandatory human rights due diligence for companies in their national legislation;

- Support the development of a binding legal framework at the international level to address the sale and trade of surveillance export technologies contributing to human rights violations;

- Support the work of human rights defenders by ensuring the establishment and adequate functioning of prevention mechanisms;

2.3. Reinforce business obligations and responsibilities to respect human rights

While most of the binding obligations laid down in international law are directed at States, individuals and companies are also subject to certain obligations and responsibilities concerning respect for human rights. The United Nations Guiding Principles on Business and Human Rights (UNGPs) and the OECD Guiding Principles for Multinational Companies, revised in 2011, represent major developments in this regard. These documents reiterate the responsibility of companies to respect human rights no matter where they operate, and respect international human rights law in conflict situations. These responsibilities concern all of the human rights recognized by international law.

FIDH recommends to businesses that are involved with the surveillance industry to diligently follow the guidance found in the two documents, and to go further to insure they don't contribute to human rights violations. FIDH especially recommends to:

- Adopt a human rights policy targeted at the human rights risks associated with this sector of business activities, and include references to uphold human rights in case where the company receives governmental requests for activities such as illegal surveillance and requests for censorship;

- Exercise due diligence to identify potential human rights risks linked with their business activities and relationships, including by conducting human rights impact assessments prior to concluding any contract. In particular, ICT companies should pay specific attention to potential risks of violations of the rights to privacy, freedom of expression and freedom of association. Such due diligence processes should aim at ensuring that companies refrain from selling technologies or selling and/or providing maintenance, updates and/or any other types of services that could cause or contribute to human rights violations;

- When negotiating a contract, identify clearly the end use and end users of the products or services being provided. Avoid selling such technology if there is no clear legal framework controlling its use or if there is a documented record of human rights abuses within the country of destination;

- To avoid complicity in any misuse of products or services, stipulate clear end-use assurances in contractual agreements with customers encompassing strong human rights safeguards and protecting against their arbitrary and unlawful use; adopt policies and procedures to stop or address misuse of products and services, including contractual provisions that would allow the company to withdraw services or cease technical support or upgrades in cases of misuse;[14]

2.4. Reinforce access to justice for victims of human rights abuse linked to the use of surveillance technologies

The judicial (and especially extra-judicial) cases mentioned above demonstrate that the difficulty in granting access to justice and redress to victims of abuses linked to the use of surveillance technologies persists and constitutes a serious gap that should be addressed at the international level.

A series of challenges face NGOs, victims and other actors engaged in litigation relating to this issue. Evidentiary challenges, that is to say obtaining incriminating evidence for use in prosecutions, are significantly higher than in other contexts. This is due in part to the information asymmetry that can be common in business and human rights litigation, as well as to the inherently secret nature of the surveillance industry based on its links with (sometimes legitimate) intelligence activities. Linkage, which is a key challenge in all extra-territorial litigation, is also difficult to establish in this context. In addition, FIDH has observed a weak political willingness to investigate and prosecute companies alleged to have supplied surveillance technology to repressive governments for complicity to human rights abuses. This may be the result of valuing economic interests over competing considerations, and/or the fact that the companies in question tend to have links to their home States and in some cases, the home State's authorization to supply surveillance technologies abroad.

The following recommendations, while common to all victims of corporate abuses, are particularly urgent in cases of abuses committed ICT companies:

- Proceed with legal reforms to enable victims of abuses committed abroad to bring cases in companies' home States;

- Address barriers in access to justice posed by the principles of limited liability and the separation of legal personality by ensuring that parent companies can be held liable for human rights violations caused by their subsidiaries;

[14] The recommendations reiterate those made by the CAUSE coalition and contained in the position paper https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf p. 37

- Adopt the necessary legal and policy measures to lift financial and practical barriers that can discourage or prevent victims from bringing a case;

- Ensure, at the national level, including in NCP cases, the prompt and impartial investigation of cases alleging human rights violations by surveillance companies.