

Digital rights in the Mediterranean: What role for the European Union?

June 2021



"The opinions expressed in this document are the sole responsibility of the author and should not be considered as an official position of the MAJALAT Consortium or of the European Commission."

MAJALAT is an EU-funded initiative implemented by a consortium led by EuroMed Rights and including the following organisations: Forum des Alternatives Maroc (FMAS), REF - Réseau Euromed France, SOLIDAR, Arab Trade Union Confederation (ATUC) and Arab NGO Network for Development (ANND)



This project is co-funded by the European union and



EuroMed Rights
 EuroMed Droits
 الأورو-متوسطية لحقوق



annd
 Arab NGO Network for Development
 شبكة المنظمات العربية غير الحكومية للتعمية

This report is a MAJALAT publication and was written by Nabila Habbida, peacebuilding and human rights policy analyst. The author would like to thank the Majalat and Euromed Rights team members for their support and the following people, entities and organisations for their insights: Access Now, Association des Femmes Tunisiennes pour la Recherche sur le Développement (AFTURD), LDA Northern Morocco, Nuon Organisation for Peacebuilding, Association Ribat Al Fath pour le Développement Durable, Solidarité Laïque Tunisie, Elena Zacharenko, the Strategic Communication Task Force South and the Human Rights Division (GLOBAL.1) of the European External Action Service, and the Crisis response, Conflict Prevention and Peace Building unit of the Service for Foreign Policy Instruments (FPI.2) of the European Commission.

ON THE COVER

A young woman holding identity cards looks at her smartphone (Photo by Anete Lusina via Pexels).

Table of contents

EXECUTIVE SUMMARY.....	3
CONTEXT AND OBJECTIVES.....	6
METHODOLOGY.....	6
ABREVIATIONS.....	7
1. HUMAN RIGHTS IN THE SOUTHERN MEDITERRANEAN: SQUEEZED BETWEEN A DIGITAL REVOLUTION AND A PANDEMIC.....	8
1- Human rights and privacy in the digital age.....	8
2- Recent developments in the region.....	9
3- A closer look at data protection in the region.....	13
4- Trends and concerns.....	18
2. DIGITAL RIGHTS IN THE EU’S NEIGHBOURHOOD POLICY.....	23
1- EU priorities in its Southern Neighbourhood.....	23
2- The EU’s new Agenda for the Mediterranean.....	26
CONCLUSION AND RECOMMENDATIONS.....	31
BIBLIOGRAPHY.....	33

Figures

Figure 1. A visualisation of digital rights.....	8
Figure 2. Personal Data Protection in the Southern Mediterranean region.....	14
Figure 3. Exemples of surveillance technology used in the MENA region Source: TIMEP.....	18

Figure 4 Palestinian American figure Omar Suleiman's screenshot of the notice of his Instagram post's removal, June 2021 21

Figure 5 Participants Live Poll Results at the 2020 EU-NGO Human rights Forum (Dec 2020) 25

Executive Summary

The digital revolution is affecting all areas of life and changing the way people organise, trade and communicate at an unprecedented speed. In rapidly growing, data-hungry digital economies, personal data protection architecture is key to safeguard privacy, a cornerstone of fundamental freedoms. Legal frameworks for digital data protection are still nascent globally, and the EU's General Data Protection Regulation (GDPR) is widely seen as an international standard.

In the Southern Mediterranean region, countries with stronger institutions and legal corpus have pioneered digital privacy laws. Overall regulations are still weak because they do not define specifically enough the nature of violations, and do not set strong safeguards and remedy against abuse. The laws and their enforcement tend to be permissive towards companies, state bodies and security forces. Data protection authorities, when they exist, are often not independent and in some cases do not have the mandate and resources to enforce the law. When they do have the mandate however, their investigative power could actually facilitate state bodies' access to citizens personal data and reinforce dynamics of territorial and population control. In setting up data protection structures that do not include strict safeguards, a majority of governments in the region appear to be primarily concerned with keeping control over political activity, developing opportunities for e-commerce and tech industry, and/or control information available to the public. There seems to be a disregard for privacy as a human right; data being seen as a resource that should be taken advantage of, and protection primarily as that of assets and state control. Cybersurveillance, internet shutdowns and online censorship are widespread threats to human rights in the region. Unrolling digital transformation with weak data protection laws and without strong cybersecurity strategies and capabilities could leave citizens and institutions vulnerable to malign attacks or data mining by private companies.

In its new Agenda for the Mediterranean published in February 2021, the EU identified disinformation, cyberthreats, and accompanying the digital transition in the region among its priorities. The new policy presents digital transformation in the Southern Mediterranean as a matter of modernising trade and investment relations and creating a digital economy hub that is competitive and contributes to EU post-COVID-19 pandemic recovery. In order to "tap into the region's economic potential", networks need to be secure, regulations enable free-flow of non-personal data, a digitally-skilled workforce is connected to neighbouring markets and stronger telecommunications infrastructures help create routes with Africa and Asia that are of interest to EU economies. In this new policy framework, commitments to human rights and protection of privacy are mentioned first but their enforcement seem secondary to economic growth.

The EU makes a clear commitment towards supporting data protection regulations and governance, which responds to a key concern of human rights organisations, and could influence positively privacy debates, digital skills-building and safety of citizens in the region. However it cannot be expected to have substantial impact considering that the tech industry and telecom companies in the MENA region and globally are poorly regulated and rank very low in terms of fundamental rights. It will be difficult to evaluate both policy and practice of data protection in the region since the tech and cybersurveillance sectors continue to enjoy a disproportionate level of opacity thanks to secrecy laws. Public-private partnerships could contribute to increase opacity in favour of big tech and telecom companies, who have an incentive to break down barriers to data circulation.

Ensuring data protection and privacy means that people should have control over what private information is collected or shared about them. Supporting local understandings and innovation on privacy and data protection and regulation could have a positive impact on human rights and increase space for civil society. While the GDPR is considered as a golden standard, it is only as good as its implementation and impact. Duplicating the GDPR without taking into account the local and global economic, political and conflict dynamics could further entrench rights violations, not improve them. The EU should exercise maximum due diligence, conflict-sensitivity and gender-sensitivity in future tech-focused cooperation with the region, with a view to uphold digital rights, foster the social welfare of local innovators and workers in the digital economy and enable virtual safe spaces for rights defenders, technologists, peacebuilders and journalists.

Recommendations

The European Commission and the European External Action Service (EEAS) should:

- Use their leverage to **pressure partner countries and tech companies complicit in human rights violations to respect international law standards online and offline.**
- **Support and fund investigation, analysis, technical and legal capacity of locally-driven independent media and organisations** in order to monitor, document and influence policy-making and practices on data protection and digital rights. In particular, support **strategic litigation training and processes** against misuse of data, digital rights violations and monopoly by platforms, companies and governmental bodies; and **contribute to the creation of secure online platforms** for collaboration and documentation of legal developments and human rights violations
- **Assist the creation of an independent regional network of social justice and human rights** dedicated to build collective knowledge and coordinate strategies on technology-related issues (in the model of the Europe-wide [Justice, Equity and](#)

[Technology Table](#) led by London School of Economics).

- **Convene a regional digital multi-stakeholder dialogue** that bridges gaps between civil society expert, technologists, authorities and companies in order to better apprehend the regional socio-economic and political challenges of digital transformation;
- **Define strict evidence-based vetting and due diligence mechanisms on Public-Private Partnerships** designed to assess and incentivise compliance of companies with human rights standards and the GDPR and **ensure that technical frameworks used by companies are publicly available** when sensitive personal data is being handled.
- Ensure that DG NEAR, DG INTPA and EEAS staff in charge of policies and programmes with rights or digital components are able to **monitor GDPR application developments at EU level** and **design and implement context- and gender-sensitive intervention in close cooperation with local and international digital/human rights experts in the region** in order to avoid adverse impact of programmes supporting GDPR-inspired regulations.
- **Increase the level of expertise in digital technology among political, policy and programming staff** in DG NEAR, Foreign Policy Instruments (FPI) and the EEAS in order to improve internal practice and appropriate programme design, by:
 - recruiting experts from various backgrounds (technical, legal, human rights, private sector) in order to strengthen the understanding of technology development,
 - providing mandatory digital safety, rights and skills training to manage data appropriately and work with human rights defenders in a safe manner.
- **Improve transparency, accuracy and accessibility of up-to-date data on EU development cooperation funding** by harmonising online communications standards of the Neighbourhood, Development and International Cooperation Instrument (NDICI) and other instruments – based on models such as the [IcSP map](#) (Instrument contributing to Stability and Peace) and the EU Trust Fund for Africa’s [webpage](#) – except when data publication risks putting stakeholders in repressive environments at risk.

EU Member states should:

- **Thoroughly enforce the new EU regulation on dual-use technology export and its coordinated mechanism and adopt a wide interpretation of cyber-technology** based on the recommendations of the [human and digital rights organisations’ response statement of March 2021](#) to ensure that EU policies and activities do not support state-sponsored surveillance that violate EU’s human rights commitments.

Context and objectives

Initiated by six civil society networks from the Euro-Mediterranean region, the project MAJALAT aims at creating a space of encounter and constructive dialogue between the civil society of the South of the Mediterranean and the institutions of the European Union (EU). Each year, participants gather to exchange on six themes that are central to the relations between the EU and countries in the region: Governance and the Rule of Law, Economic Development and Social Dialogue, Migration and Mobility, Security and Countering Violence, Climate Justice, and the cross-cutting thematic of Youth. In the backdrop of the global COVID-19 pandemic in 2020, MAJALAT adapted its activity plan to continue to hold the EU-neighbourhood dialogue in spite of movement restrictions, using online communication tools.

In 2020, five webinars were held under the new thematic pillar of 'Security' – involving the participation of civil society experts, project staff and EU representatives to share ideas, examples and questions. In particular, discussions reflected on the impact of the COVID-19 crisis in the Euro-Mediterranean region and followed up on the recommendations made during the 2019 MAJALAT activity cycle. A series of recommendations were made on the three subthemes of interest to the EU: preventing and countering violent extremism, digital security and the gender dimension of security, and violence against women.

This report commissioned in May 2021 builds on these recommendations and aims to examine further the deployment of digital technology in the Mediterranean region and its impact on citizens and organised civil society.

Methodology

Based on the Terms of Reference and the areas of interest of the consortium, a methodology was developed to provide the requisite data to answer the guiding question: **How can the EU support digital rights in Southern Mediterranean countries?**

To address the questions as posed, this study embraced a mixed methods approach, drawing on primary and secondary sources including existing data stemming from media reports, digital experts' analysis, policy documents, academic literature and open-ended interviews with selected human rights defenders and researchers, as well as EU representatives working on human rights, development and peacebuilding. The research covers primarily Morocco, Algeria, Tunisia, Egypt, Jordan, Palestine and Lebanon; and to a lesser extent Israel, Libya and Syria; and focuses on developments occurring in the past two to three years.

Primary sources included 11 interviews with participants selected based on their profiles as human rights defenders, digital rights experts or EU representatives active in countries of the Southern Neighbourhood and/or on issues related to digital technology. Considering the timeframe and circumstances related to the pandemic, all interviews took place by phone or online. This work also included a brief country case study on Tunisia.

In order to respond to the question, this study examined in detail the commitments made in the EU's Joint Communication on a Renewed partnership with the Southern Neighbourhood (February 2021)

Limitations

This research was conducted online, from Belgium. It did not aim to be comprehensive or representative of the region, rather to provide a sense of the context and challenges related to digital security and human rights in the region. The limitations included the availability of potential interviewees in the data collection period and the difficulty to access information in Syria and Libya. Because of the sensitive nature of the topic, it is to be assumed that the interviews could have been influenced by the lack of security online - although precautions such as speaking on Jitsi were taken when necessary.

Abbreviations

Data protection authorities (DPAs)
Asymmetric digital subscriber line (ADSL)
European Commission (EC)
European External Action Service (EEAS)
European Union (EU)
Deep Packet Inspection (DPI)
Internet Service Providers (ISP)
United Nations (UN)
General Data Protection Regulation (GDPR)

1. Human rights in the Southern Mediterranean: squeezed between a digital revolution and a pandemic

1- Human rights and privacy in the digital age

Digital technology is being deployed at an industrial and global scale in all aspects of our lives faster than legislation can keep up with. It is literally revolutionizing how we interact, move and think as human beings, with tremendous possibilities for communication and analysis. However, the digital technology sector (hereafter referred to as 'tech') remains highly unregulated and has been designed and used with no particular regard for human rights. Societies struggle to produce regulations that keep up with the pace of innovation and mainstreaming of new digital technology. While this is a challenge even for the most "robust" democracies, prominent experts and the United Nations have asserted repeatedly that human rights law applies to instances where digital technology is used, online and offline.

Trends related to the right to privacy will be the main focus of this report. The right to privacy is about having a reasonable amount of control over information about oneself and about how it is used by others - online and offline. It is a fundamental principle that is related to dignity and agency of human beings, referenced in Article 12 of the [Universal Declaration of Human Rights](#) and Article 17 of the [International Covenant on Civil and Political Rights](#) which provide that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation. Privacy International adds that "interference with our privacy often provides the gateway to the violation of the rest of our rights" and enables "arbitrary and unjustified use of power, by controlling what can be known about us and done to us"¹.

Figure 1. A visualisation of digital rights



¹ 'Privacy Matters | Privacy International', accessed 18 May 2021, <https://www.privacyinternational.org/learning-resources/privacy-matters>.

2-Recent developments in the region

Digital transformation accelerated by the COVID-19 pandemic

The pandemic of COVID-19 and measures to contain it have tremendously accelerated the digitisation of communication and economies. The total number of Internet users raised to 60% of world population in 2020. Mobile connexion makes up the most of global Internet use, which is even more true for the Global South. While around 90% of Europeans have access to the Internet, 73% have such access in Western Asia and 55% in Northern Africa². This section will explore ways in which the digital revolution has impacted civil society organisations and citizens in the region in the past year.

Economy & market access

With the increasing digitalisation in the manufacturing, services and agriculture sectors, 24.3% of the global economy is expected to be digitally based by 2025³. The World Bank⁴ and consulted civil society organisations⁵ report that small formal or informal businesses, across the MENA region, especially those led by women, have benefitted from the rapidly growing connected platforms, thanks to the flexibility and autonomy it provides. According to the OECD, access to the Internet and the digital economy tends to improve the lives of women and girls. In Morocco, women cooperatives in isolated rural areas have had access to the technology and are able to find additional outlets for their products. This is meaningful knowing that the regional female labour force participation rate is among the lowest in the world (21%) and that unemployment is of about 35% for young graduates of both genders in MENA. The issue of lack of job security and social protection associated with the “gig economy” (or “platform economy”) is raised by the aforementioned studies but there is a lack of in-depth analysis of the underlying factors or possible solutions in the long run. While more private sector initiatives have stepped up to provide training and job opportunities in the digital sector⁶, in particular directed at youth and women, none of them seem to raise concerns related to data protection, human rights or well-being.

Digital skills

Studies and consulted civil society organisations report a variety of trends. Digital literacy is increasing rapidly, in particular among those with least access

² ‘60% of the World’s Population Is Now Online’, DataReportal – Global Digital Insights, accessed 1 June 2021, <https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet>.

³ ‘The Middle East and North Africa: From Transition to Transformation’, World Bank, accessed 16 May 2021, <https://www.worldbank.org/en/region/mena/publication/the-middle-east-and-north-africa-from-transition-to-transformation>.

⁴ ‘The Middle East and North Africa’.

⁵ Organisations consulted for this report were located in Tunisia, Morocco, Lebanon and Syria and work on sustainable development, participatory democracy, youth, gender equality, education and gender-based violence.

⁶ ‘How the Private Sector in MENA Is Leading Workers to Better Digital Skills’, accessed 16 May 2021, <https://blogs.worldbank.org/arabvoices/how-private-sector-mena-leading-workers-better-digital-skills>.

among the elderly, rural communities and isolated areas, including people who cannot read text. However, there is still a large sense of inadequacy with the digital space, especially in spaces of intergenerational exchange. On the other hand, some organisations did find tools for creative and collaborative thinking online such as jamboards. Organisations with more financial means are able to build knowledge and capacity among staff and members through internal toolkits, digital systems such as paid videoconferencing, cloud services and use intermediaries to set up their digital tools (e.g. Wasla in Morocco). Access and practicality are often more of a concern than security. Some interviewees have warned that widespread digitisation without proper infrastructure and safeguarding may entrench the digital divide which upholds two worlds: one where people are equipped with tools and skills to navigate it, and another which is not given the same access. In the words of an educator interviewed for this study, “we should take what is beneficial and preserve time and spaces without any digital intermediary”.

Education

Digital deployment seems less effective in the education sector overall, where it entrenched some of the inequalities. Platforms are sometimes archaic and often do not take into account students and families with no Internet access or equipment. More advantaged segments have protested the low quality of online education, as the parents of students in private schools in Casablanca, Morocco, who refused to pay recent fees for online classes. Digitising education appears to be a sensitive initiative which should involve all stakeholders and rely primarily on human, in-person interaction, as a Tunisian teacher interviewed for this report affirmed: “I do not want to school to be reduced to ‘giving information’”.

Civil society organisations and civic engagement

In many ways, digital tools enabled most civic engagement and rights organisations to continue some activities after the start of the pandemic. However usage is far from homogenous. Two interviewees reported that it was more economical and ecological: the LDA Northern Morocco chose to reallocate budget to communication, visibility and digitisation of its activities. Common challenges include maintaining quality of activities, maintaining members and citizens engagement over time, lack of Internet connection and digital fatigue. A sustainable development specialist in Morocco interviewed for this report said that their local outreach was less effective due to lack of in-person meetings, while international advocacy was more efficient as they received more invitations to webinars and discussions with international organisations, the EU and the UN to discuss their post-COVID-19 programmes. In other cases, the pandemic measures have seriously hampered civil society reach as they are not compatible with remote work and digital technology, in particular with work directly related to sustainable development, land, crafts and health. Other organisations remain purposefully not active on social media due to security reasons.

Local authorities and fundamental rights

Local authorities in Tunisia, Jordan and Lebanon Morocco are reported to have modernised their online platforms, which makes it easier to engage in online streamed city council meetings, request official documents and access policy-related information. In Morocco, the pandemic opened opportunities to set up a more effective social security system and to simplify and digitise public administration. In Tunisia and Morocco in particular, digitisation seems to increase the level of transparency and trust in the institutions. There is a revolution in terms of mindset: citizens are now turning to the Internet to seek information from public institutions, even if they cannot read or use it themselves (e.g. COVID measures, requirements to renew ID, etc).

Civil society networks were enlarged across social and border divides. While new actors “entered the chat” of webinars and policy discussions that were limited to “usual suspects” guests (Tunisia, Morocco), some expressed concerns regarding digitisation of debates in terms of democratic engagement since webinars allow moderators to filter questions and comments. Ahead of future elections, candidates and campaign teams should have direct contact with people, which governments could prevent by preventing assembly in the name of pandemic measures. There is also fear and sadness that creativity is lost without human contact.

Digital technology can break down barriers but also reinforce divides: How to ensure marginalised people are not further marginalised? What is like for people with disabilities? How to create a balance that does not further exclude, nor centralise excessively, and enables human contact? How to keep digital tech as a tool and not as the new structure of society? These questions must be taken into account by institutions and civil society organisations in the way they include, train and work with their members and constituents.

Digital infrastructure and connectivity

Overall, Internet speed remains slow, while prices remain high, although it is more affordable in Northern Africa than in Western Asia. A minority of users have high-speed Internet. Except for Lebanon, MENA countries have mobile broadband speeds below the global average⁷ although there has been undeniable development in the past two years. Many Internet markets in MENA countries have monopolies or other entry barriers.⁸

Network congestion was one of the main technical issues face by most countries of the region, ill-equipped for peak-time service, due to increasing demand for video and other high-bandwidth entertainment services, videoconferencing and cloud services, distance learning for students and teachers and lack of capacity through international Internet gateways. Governments and telecommunication companies in the region have enabled

⁷ ‘Mashreq 2.0: Digital Transformation for Inclusive Growth and Jobs (Vol. 2)’, Text/HTML, World Bank, 0, accessed 16 May 2021, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/246561561495359944/Mashreq-2-0-Digital-Transformation-for-Inclusive-Growth-and-Jobs>.

⁸ ‘The Middle East and North Africa’.

extended and flexible measures to cope with the bottleneck. In the field of education, operators in Jordan, Tunisia and Morocco have provided free access to existing or new online education platforms.

Connectivity vs Digital Rights

Partnership with private telecommunications and digital companies is necessary to improve bandwidth and link up isolated and poorer communities – a request that many stakeholders in the region have made. Unique, targeted cooperation has taken place in the global ICT4Dev community, bringing together technologists and development actors, by pooling skills and resources to address a local or regional issue. But when it comes to developing connectivity and the digital economy, companies have more leeway to propose “solutions”. Tech corporations such as Google, Facebook, Apple and Amazon have increased their investment in network infrastructures and cooperation with civil society organisations and development actors⁹. Activists have warned that Internet access should not come at the expense of net neutrality¹⁰ and human rights. The VENRO Tech for Good report of 2019 notes that “a number of companies that are struggling in the saturated markets of Europe and North America see their future in Asia and Africa, with their large population of young people”¹¹. Multinational companies have taken advantage of such partnerships to engage in unfair competition with local companies by appropriating market share and skilled labor force. Evidence of massive privacy breaches, opacity, gendered and racial discrimination, cognitive manipulation, censorship, exploitative labour practices and monopolistic concentration of tech giants have been brought to the fore by countless scholars and journalists. Bigger players sometimes hide behind companies which offer free support and impose self-serving norms; a support that some governments have accepted under pressure to place their countries on the global digital economy map

A striking symbol of this trend is Facebook’s Internet.org, launched as a philanthropic initiative to provide free Internet access to isolated and poor areas in the Global South. It has been present in Algeria (live), Morocco (now discontinued) and Egypt (now banned)¹². Under tremendous pressure from Net Neutrality defenders during its rollout in India, exposing network discrimination and privacy breaches, Internet.org changed its name to Free Basics and increased privacy, security and access on its platform. However, it still has major discretionary power over user traffic, which it can monitor, increase or

⁹ Toussaint Nothias, ‘Access Granted: Facebook’s Free Basics in Africa’, *Media, Culture & Society* 42, no. 3 (1 April 2020): 329–48, <https://doi.org/10.1177/0163443719890530>.

¹⁰ According to the Electronic Frontier Foundation (EFF), Net Neutrality is “the idea that Internet service providers (ISPs) should treat all data that travels over their networks fairly, without improper discrimination in favor of particular apps, sites or services” and is a principle that must be upheld to protect the future of an open Internet. ‘Net Neutrality’, Electronic Frontier Foundation, accessed 2 June 2021, <https://www.eff.org/issues/net-neutrality>.

¹¹ The report provides a number of examples of these trends. VENRO, ‘Tech for Good. Chances and Limits of Digital Instruments in the Development Cooperation of Non-Governmental Organisations’, 2019, https://venro.org/fileadmin/user_upload/Dateien/Daten/Publikationen/Dokumentationen/NRO-Report_TechForGood_EN.pdf.

¹² Facebook does not offer an overview of countries where the service is available online. Nothias.

stop at its convenience. This “walled garden”¹³ offered as development assistance to poorer communities could contribute to damage net neutrality and come at the expense of privacy, data protection and local innovation of local population¹⁴. In other words, big tech companies have been described by digital activists as gatekeepers of the Internet who can curate content available on their “free” platforms with no obligation of transparency, and consequently damage the work of local services and start-ups¹⁵.

These observations generalise the recognition that Facebook and big tech companies are political institutions¹⁶ and raise parallels with a history of (neo-)colonialism among scholars and observers¹⁷, which created exploitative dependency and impose norms that extract value and wealth from people. In particular, they have been described as practicing mass “surveillance capitalism” and “data colonialism”¹⁸, i.e. that their business model is predicated on the appropriation and exploitation of disproportionate amounts of commodified personal data - like oil or labour

3- A closer look at data protection in the region

In the context laid out in previous sections, the impact of these developments on privacy has several layers and consequences. The recommendations made during the MAJALAT fora under the “Security” pillar focus on data protection and surveillance. This section will provide a brief overview of trends on data protection standards and ways in which privacy is affected in the region.

According to OHCHR, “in the digital environment, informational privacy, covering information that exists or can be derived about a person and her or his life and the decisions based on that information, is of particular importance”.¹⁹ And because it is increasingly possible to centralise and circulate information - turned into “data” with digital technology, control over privacy requires additional safeguards to prevent unwarranted interference. Although data protection and privacy are not interchangeable, data protection is necessary to protect privacy. While the right to privacy is referenced in the constitutions of more than 160 countries in one form or the other, data protection is not systematically considered a right or even referenced as such.²⁰ It is increasingly recognised through binding frameworks at the

¹³ Jeremy Gillula, ‘Facebook’s Free Basics: More Open, Better Security, but Still a Walled Garden’, Electronic Frontier Foundation, 30 September 2015, <https://www.eff.org/deeplinks/2015/09/facebooks-free-basics-more-open-better-security-still-walled-garden>.

¹⁴ ‘How Our Personal Data Is Exploited in Unexpected Ways’, BBC Reel, accessed 30 May 2021, <https://www.bbc.com/reel/video/p09blhfw/how-our-personal-data-is-exploited-in-unexpected-ways>.

¹⁵ Nothias, ‘Access Granted’.

¹⁶ Nothias.

¹⁷ ‘How Our Personal Data Is Exploited in Unexpected Ways’.

¹⁸ Nick Couldry and Ulises Meijas, ‘The Cost of Connection’ cited in ‘How Our Personal Data Is Exploited in Unexpected Ways’.

¹⁹ ‘OHCHR | The Right to Privacy in the Digital Age: Report’, accessed 18 May 2021, <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx>.

national, regional, and international levels, and as this section will highlight, processes of codification are underway where it was not.

The GDPR, the golden standard

EU regulations have established some of the most progressive digital and data protection regulations in the world. Its centrepiece regulation, the [General Data Protection Regulation \(GDPR\)](#) boasts to be the toughest privacy and security law in the world²¹. Its key policies applying to business and activities in Europe or involving European organisations and companies forced governments, the tech industry and businesses to reckon with the organisational implications of privacy and reflect on data management.

Updating 1995's European Data Protection Directive, the GDPR entered into force in 2016 and was designed to address asymmetries between individuals and organisations in processing data, and to increase individuals' control over their data. It imposes obligations onto organisations across the world, so long as they target or collect data related to people in the EU, and has the potential to levy harsh fines against violations of its privacy and security standards (up to tens of millions of euros). Among the successes of the GDPR are its robustness, human rights safeguards during crises, its influencing role in advancing and protecting rights inside and outside the EU, and its capacity as a reference point globally. Concerns of digital rights experts include lack of enforcement, resources and cooperation among data protection authorities (DPAs) and misuse of its provisions to silence journalists and NGOs.

Sources: EU, EDRi, Access Now

Figure 2. Personal Data Protection in the Southern Mediterranean region

Country	Flagship personal data protection arsenal ²²	Observations
Algeria	<p>Constitution (1996, amended in 2020)</p> <p>Law on the Protection of Personal Data No. 18-07 (2018) (LPDP)</p> <p>DPA: Autorité nationale de protection des données à caractère personnel (AN)</p>	<p>Weak. Article 56 of the Constitution covers privacy of citizens and the new law, impelled by the GDPR adoption seeks to reflect some of its basic principles²³. The new Data Protection Agency, which is empowered to process complaints and authorize, control, advise and fine entities processing personal data – is said to be financially and administratively independent yet is placed under the authority of the Presidency. Provisions are waived if processing data is necessary to uphold “vital interests” of citizens, a notion which is not defined in the law. While they introduce important principles in the law and public debate, these developments risk, without a genuine response to popular demands of the Hirak and the continuation of state repression²⁴, to ensure, if not reinforce, control of the state and security authorities over citizens.</p>
Egypt	<p>Constitution (2014)</p> <p>Law on the Protection of Personal Data No. 151 (2020)</p> <p>DPA : Data Protection Centre (DPC)</p>	<p>Weak. Article 75 of the Constitution stipulates that private life, including e-correspondance, is inviolable, but that communications “may only be confiscated, examined or monitored by virtue of a judicial order for a limited period of time in the circumstances stipulated by law”²⁵. Impelled by the GDPR’s adoption, the Data Protection Law authorizes personal data processing when necessary for contractual or legal obligations. It exempts data processed in application of the law in Egypt. The Data Protection Centre’s can issue regulations, receive complaints related to violations as well as monitor and inspect any individual and entity dealing with personal data. Heavy fines are provisioned in case of violations starting 2022. In the context of a highly repressive socio-political environment, state-sponsored violence and corruption²⁶, this law could reinforce state reach and violence onto individuals, journalists and organisations.</p>
Israel	<p>Protection of Privacy Law (PPL) (1981)</p> <p>Protection of Privacy Regulations 5777-2017; 5761-2001; 1986 and 1981.</p> <p>DPA: Israel Privacy Protection Authority (PPA)</p>	<p>Elaborate. Israeli corpus of law on privacy is extensive. The Protection of Privacy Agency (PPA), established in 2006, is part of the Ministry of Justice and “is responsible for the protection of all personal information held in digital databases, including through the use of administrative and criminal enforcement”²⁷. It publishes guidelines interpreting the law, has investigative and administrative powers to conduct audits and impose fines in certain cases. It does not consider this corpus of law applicable to Palestinians in the West Bank and Gaza.</p>
Jordan	<p>Draft Data Protection law (in progress)</p> <p>Constitution</p>	<p>Weak. Right to privacy guaranteed by Constitution (Art. 18) but the arsenal is insufficient. Concerns include risk of conflict of interest, lack of independent oversight and safeguards on executive branch, security forces and tech industry and smartphone and personal computer mass surveillance. It allows surveillance of private communications if the judicial</p>

²⁰ ‘Creating a Data Protection Framework: A Do’s and Don’ts Guide for Lawmakers’ (Access Now, November 2018), <https://www.accessnow.org/data-protection-handbook>.

²¹ ‘What Is GDPR, the EU’s New Data Protection Law?’, GDPR.eu, 7 November 2018, <https://gdpr.eu/what-is-gdpr/>.

²² The overview does not cover the entire corpus of laws and provisions related to personal data protection. It only lists flagship elements of the personal data protection arsenal.

²³ Massyle Ait Ali, ‘La Loi sur le traitement des données personnelles publiée au Journal officiel’, N’TIC WEB, accessed 31 May 2021, <https://www.nticweb.com/news/2-non-categorise/9401-la-loi-sur-le-traitement-des-donn%C3%A9es-personnelles-publi%C3%A9e-au-journal-officiel.html>.

²⁴ ‘A Breakdown of Algeria’s New Constitution’, Middle East Eye, accessed 31 May 2021, <http://www.middleeasteye.net/news/algeria-new-constitution-breakdown>.

²⁵ ‘Egypt - Data Protection Overview’, DataGuidance, 21 August 2020, <https://www.dataguidance.com/notes/egypt-data-protection-overview>.

²⁶ ‘Egypt: Freedom on the Net 2020 Country Report’, Freedom House, accessed 31 May 2021, <https://freedomhouse.org/country/egypt/freedom-net/2020>.

²⁷ ‘Israel - Data Protection Overview’, DataGuidance, 8 October 2020, <https://www.dataguidance.com/notes/israel-data-protection-overview>.

	Cybercrime draft law (withdrawn) Telecommunications Law no 13/1995	branch approves. While fines and jail time are prescribed for unauthorized surveillance, security forces are exempt. Surveillance is permitted based on vague definitions of "terrorist activity" and "reliable information". The setting up of a Data Protection Agency is requested by the draft data protection law.
Lebanon	Data protection law - Law No. 81 relating to Electronic Transactions and Personal Data (E-Transactions Law) (2018)	Growing but still weak. It does not sufficiently restrict collection and usage of citizens' personal data by public or private entities, potentially enables data theft and trafficking by public offices and companies, favors security apparatus and businesses and electoral manipulation.
Libya	Constitution	Articles 12 and 13 of the Constitution 2011 guarantee the right to a private life for citizens and the confidentiality of correspondence and other forms of communications except where required by a judicial warrant ²⁸ . There is no dedicated data protection law in Libya, which suffers an environment of lawlessness as leadership is being intensely fought for since the fall of General Muammar Qaddafi.
Morocco	Constitution Data Protection Law 1-09-15 (2009) DPA: Commission nationale de contrôle de la protection des données à caractère personnel (CNDP)	Growing but serious concerns remain. The law recognizes the right to be informed about data collection, the "right of correction" of inaccurate data and the right to oppose processing. Exceptions include disclosure to third parties in case of "public interest" (art. 44) ²⁹ and exemptions in legitimate interest of national defense, internal or external security and crime prevention. The Data Protection Authority (CNDP) is placed under the Prime Minister's office and has investigative and law enforcement powers, i.e. can send mandate staff or Police officers to investigate violations. It can also issue orders to rectify, block, remove or destroy data, and summon people to a hearing, seize equipment and inform the public prosecutor ³⁰ . Rights defenders have reported privacy violations in numerous alleged cases of advanced surveillance against citizens which have led to arrests and prosecutions. While its data protection arsenal is seeking compliance with international standards, it appears to be in the grip of Morocco's state (security) apparatus which can manoeuvre through it to keep control.
Palestine	Palestine Basic Law (Constitutional framework) Cybercrime law (16/2017) Amended Cybercrime law (10/2018) There is no DPA but it is likely to be ineffective as Palestinian ICT infrastructure is controlled by Israel ³¹ .	Weak. The occupying power, Israel, does not apply its Protection of Privacy Law (PPL) (1981) and guidelines of its Privacy Authority (2006) to Palestinians in the West Bank and the Gaza Strip. While Palestine's basic law criminalises violation of personal freedom, private life, rights and liberties, little efforts are invested in enforcing this provision. Cybercrime law is controversial as it was enacted in full secrecy and contains vague and ambiguous clauses that restrict freedom of expression, political dissent and independent media. Article 4 of the cybercrime law (2018) penalizes unlawful access to information systems, sharing intercepted records or data and arbitrary or interference with privacy with prison sentence and heavy fines. However, the law forces Internet Service Providers (ISPs) to keep users' data for at least 3 years and grants the public prosecutor the right to collect unrestricted data, including private communications, traffic data, and metadata.
Tunisia	Constitution (2014) Data Protection Law (2004-63) DPA: Instance nationale de la protection des	Passed in 2004 before any of country of North Africa, the data protection law is now outdated (no references to online data) and its provisions have not led to court decisions or enforcement. The national Data Protection Agency (DPA) does not have oversight or regulatory power. The Revised Data Protection Bill introduced in 2018 proposes significant improvements. A case study on Tunisia provides further details on the current situation.

²⁸ 'Libya', DataGuidance, accessed 31 May 2021, <https://www.dataguidance.com/jurisdiction/libya>.

²⁹ 'State of Privacy Morocco', Privacy International, accessed 6 May 2021, <http://privacyinternational.org/state-privacy/1007/state-privacy-morocco>.

³⁰ 'State of Privacy Morocco'.

³¹ 'Exposed and Exploited: Data Protection in the Middle East and North Africa', Access Now (blog), 28 January 2021, <https://www.accessnow.org/exposed-and-exploited-data-protection-mena/>.

données personnelles (INPDP)

Sources: UNCTAD, Access Now, Freedom House, Privacy International. For more details on privacy laws and debates in Jordan, Lebanon, Morocco, Palestine and Tunisia, see section 4.



CASE STUDY: TUNISIA

In spite of the controlling nature of Ben Ali's regime, or perhaps because of it, Tunisia has pioneered data protection legislation and culture in the region, with a data protection law dating back to 2004 and a Data Protection Authority. With infrastructure steadily growing, the digital transformation agenda is promoted by the executive and the economic and urban elite³² and supported by society at large in order to support economic and human development - data protection regulation being a key asset to attract investors. At the same time, Tunisia's dynamic and organised civil society ecosystem has consistently monitored trends and engaged institutions to demand safeguards and implementation of human rights law.

65% of people in Tunisia are Internet users, increasing by 5% since 2020. Tunisian participants in this research and recent reports³³ are aware that Tunisia's data protection regulation sets high standards and know key privacy principles and potential fines in case of violations, possibly due to the reactions of veteran rights activists and public outreach by the Data Protection Agency (DPA). Nevertheless, the digital divide between urban educated Tunisians and everyone else shows that awareness is limited to an influential minority. In addition, digital rights do not seem to be a priority for the executive branch or enforced by the judicial branch.³⁴



Infrastructure

Internet access is affordable compared with other countries of the region³⁵. Mobile connections are more widespread and faster than fixed connections, which remain slow at 10Mbps. In March 2021, Tunisia was the first Maghreb country to launch a satellite³⁶, developed locally and set up to connect

³² "ces technologies sont la locomotive du développement économique du pays » said a Director at Tunisie Telecom.

'Avis d'un spécialiste | La 5G en Tunisie, une pression forte des USA et de la Chine', *La Presse de Tunisie* (blog), 2 January 2021, <https://lapresse.tn/83168/avis-dun-specialiste-la-5g-en-tunisie-une-pression-forte-des-usa-et-de-la-chine/>.

³³ Innovation for Change MENA Hub and 7amleh, "Mapping Digital Rights in the Middle East and North Africa", accessed 27 May 2021, <https://7amleh.org/2021/03/10/launch-of-mapping-digital-rights-in-the-middle-east-and-north-africa-through-a-collaboration-between-innovation-for-change-mena-hub-and-7amleh-in-pursuit-of-a-baseline-for-advocacy-for-digital-rights-in-the-region>.

³⁴ "Mapping Digital Rights in the Middle East and North Africa"

³⁵ Nadsoft,

³⁶ 'La Tunisie, premier pays du Maghreb à lancer un satellite fabriqué 100% localement', *Sciences et Avenir*, accessed 31 May 2021, https://www.sciencesetavenir.fr/sciences/la-tunisie-1er-pays-du-maghreb-a-lancer-un-satellite-fabrique-100-localement_152748.

devices and extend coverage. The government launched a five-year plan to link up the country's rural areas to the Internet. Tunisie Telecom (TT) announced plans to set up 5G and increase international bandwidth from below 300 Gbps to 350 Gbps.

Data protection

Constitution (2014) explicitly refers to the protection of the right to privacy³⁷.

Data Protection Law (2004-63)

Passed in 2004 before any of country of North Africa, it defines personal data as “any information whatever its origin or its means relating to an individual who can be identified, directly or indirectly, with the exception of any information related to public life or considered public life by law.” It is outdated (no references to online data) and its provisions have not led to court decisions or enforcement. The national Data Protection Agency (DPA) does not have oversight or regulatory power.

Draft Revised Data Protection Law (introduced in 2018)

The bill proposes significant improvements: modelled on the EU's GDPR, the bill includes principles of transparency, fairness, and respect for human dignity set to apply to any entity processing personal data in Tunisia and covers digital information such as computer and device Internet Protocol (IP) address, GPS coordinates, email address and biometric data. However it does not distinguish enough between personal and public data, which could hamper the right to access to information, and a significant contingent of rights defenders are arguing for more precise provisions related to access to justice and safeguards against state violations.

Tunisia is a signatory of the Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data³⁸.

Data Protection Agency : [Instance nationale de la protection des données personnelles \(INPDP\)](#)

COVID-19 related developments

E7mi - إحصي, Tunisia's COVID-19 contact tracing application, collects data that is anonymised, has encryption-secured storage and includes privacy policy and user consent. However, the technology used is closed source and centralised, and data not automatically erased for exposed or infected users³⁹. In May 2020, a decree to push for a National Unique Identifier Decree issued priorities for dealing with the COVID-19 crisis; however it does not specify whether the government will use a centralised database to collect and store personal data on citizens. On 14 June 2020, the government announced the launch of “Operations Hall” using cell site location tracking, which raised backlash from activists. In September 2020, the INPDP issued a strong statement denouncing publication of COVID-19 test results on social media by health professionals, mentioning fines in the provision of Tunisian privacy law⁴⁰.

Biometrics

³⁷ ‘State of Surveillance Tunisia’, Privacy International, accessed 6 May 2021, <http://privacyinternational.org/state-privacy/1012/state-surveillance-tunisia>.

³⁸ ‘Convention 108 and Protocols’, Data Protection, accessed 31 May 2021, <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.

³⁹ ‘Exposed and Exploited’.

⁴⁰ Mayara, ‘Coronavirus: l'Instance Nationale de Protection des Données Personnelles met en garde contre la divulgation de données liées à l'état de santé d'une personne contaminée’, Tunisie, 21 September 2020, <https://www.tunisienumerique.com/coronavirus-linstance-nationale-de-protection-des-donnees-personnelles-met-en-garde-contre-la-divulgation-de-donnees-liees-a-letat-de-sante-dune-personne-contaminee/>.

Draft law n°83 amending law 93-27 of 1993 on national identification planning to make biometric ID mandatory is set to be discussed in the Parliament. A statement by 30 civil society organisations opposes the bill on process grounds and demands that transparent and comprehensive consultations take place before such sensitive data protection matter is set to be submitted to Parliament⁴¹. The bill was already withdrawn in 2018 due to privacy concerns raised by civil society experts, which could allow for privacy violations and abuses of personal data as well as increased surveillance, tracking, and storage of citizens' health and banking data.⁴² The draft law did not reference safeguards or limitations on data collection and use by official authorities.

Concerns of privacy defenders on data protection and biometrics are all the more sensible as evidence of lack of proper enforcement of privacy laws led to major scandals, including incidents during the presidential and legislative elections of 2019 when candidates used personal data of Tunisian citizens (ID card numbers, names, and signatures) without explicit consent to obtain endorsements⁴³. In addition, private companies rarely report to the INPDP how their data processing is compliant with the law, according to its annual report.

Sources: Access Now, Tamleh, Privacy International, Data Reportal

For more resources on privacy debates and legislative proceedings in Tunisia, please see section 4

Countries with stronger institutions and legal corpus have pioneered digital privacy laws. Overall regulations are still weak because they do not set strong safeguards and remedy against abuse. The laws and their enforcement tend to be permissive towards companies, state bodies and security forces. Data protection authorities, when they exist, are often not independent and in some cases do not have the mandate and resources to enforce the law. When they do have the mandate however, their investigative power could actually facilitate state bodies' access to citizens personal data and reinforce dynamics of territorial and population control. In setting up data protection structures that do not include strict safeguards, a majority of governments in the region appear to be primarily concerned with keeping control over political activity and/or control information available to the public, the desire to benefit from digital economy prospects and maintain and further open business opportunities with European countries.

It appears that the GDPR is having a considerable influence in setting up data protection standards in the South Mediterranean. However, data protection laws and principles are only so good as their implementation, which has much to do with how conducive the legal, political and institutional environment is. Their enforcement is a major challenge for the entire region; worse, they can be weaponised against individuals, media and movements by repressive states in order to break political opposition and neutralise movements, as the next section will describe.

4- Trends and concerns





⁴¹ 'Le projet de loi sur la carte d'identité biométrique désapprouvé par la société civile - TN24.TN', accessed 31 May 2021, <https://tn24.tn/fr/article/le-projet-de-loi-sur-la-carte-d-identite-biometrique-desapprouve-par-la-societe-civile-349248>.

⁴² 'Exposed and Exploited'.

⁴³ 'Exposed and Exploited'.

Many trends of privacy violations and abuse have rocked the two subregions of the Middle East and North Africa in recent years, from bandwidth throttling to online harassment and censorship. This section will briefly illustrate some of the most significant trends.

Cyber-surveillance

 <p>Spyware</p>	<p>Malicious software that can infect a device and allow the collection and exfiltration of data. Text, audio, video, and keystrokes are compromised. For example, Saudi Arabia has used Israeli spyware to spy on dissidents.</p>
 <p>DPI</p>	<p>Deep Packet Inspection is used to monitor and redirect internet flow at a large scale. Governments can use this to block websites or to force users to access sites that are infected with spyware.</p>
 <p>Social engineering</p>	<p>A technique through which users are led to perform certain actions such as clicking on a link. A government can hide spyware in an email promising information about human rights violations, for example, knowing that activists may be likely to click on them.</p>
 <p>Phishing</p>	<p>A strategy in which users are fooled into revealing their passwords, allowing governments to access their private accounts. Attackers may pretend they are sharing a report on torture, for instance, and ask for the user to enter their account and password in order to read it.</p>

While online corporate surveillance is growing, politically- and security-motivated state surveillance against citizens, journalists and human rights defenders is one of most widespread in the region, practiced with technology that involves spyware, Deep Packet Inspections (DPI), phishing, social engineering and telecommunication metadata. It often relies on Europe-, US- and Israeli-made technology and has demonstrated better

effectiveness than traditional equipment in preventing undesired action or movements.

Figure 3. Examples of surveillance technology used in the MENA region
Source: TIMEP

Morocco, Algeria and Tunisia authorities (under Ben Ali in 2011) have used *Evident*, a technology sold by BAE Systems (UK) / ETI (Denmark) that enables mass surveillance of emails and mobile phone calls as well as targeted surveillance of individuals by name, email address or specific IP addresses⁴⁴. Morocco is famously known to have used the Pegasus virus, a spyware produced by NSO Group, an Israeli company which has allegedly contributed to serious human rights violations across the world,⁴⁵ to spy on journalists and activists (the cases of Maati Monjib, Abdessadak El Bouchattaoui and Omar Radi, who has been imprisoned since July 2020, have been thoroughly investigated by Amnesty International in 2019 and 2020⁴⁶). NSO Group is officially headquartered in Luxembourg and claims on its homepage that its products and services are bought “*exclusively by government intelligence and law enforcement agencies to fight crime and terror*”.

⁴⁴ ‘BAE “Secretly Sold Mass Surveillance Technology to Repressive Regimes”’, the Guardian, 14 June 2017, <http://www.theguardian.com/business/2017/jun/15/bae-mass-surveillance-technology-repressive-regimes>.

⁴⁵ ‘HIDE AND SEEK: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries’, The Citizen Lab, 18 September 2018, <https://citizenlab.ca/2018/09/hidden-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.

⁴⁶ ‘Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group’s Tools’, accessed 2 June 2021, <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/>.

In spite of EU Council Conclusions adopted in August 2013 that explicitly commit to "suspend export licenses to Egypt for any equipment that could be used for domestic repression", at least eight French companies continued to sell surveillance equipment in subsequent years, enabling individual surveillance, mass telecommunication interception, personal data collection (IDEMIA) and crowd control (drones, satellite and light armoured vehicles), with the encouragement of the French government⁴⁷. The Egyptian government has reportedly acquired other technologies from Italy, Germany, the UK, Canada and UAE⁴⁸. French and Italian companies have also been involved in selling equipment to the Assad regime in Syria⁴⁹.

Under military occupation by Israel, a cyberwarfare world leader, and governed by increasingly authoritarian factions, Palestinians have had their privacy constantly violated by a multi-layered high-tech surveillance architecture relying on increasingly intrusive measures such as social engineering, social media monitoring, arbitrary searches, drone patrols and surveillance cameras. Israel's thriving billion dollars cyber-surveillance and military industry is often marketed based on its ability to test equipment in the Occupied Palestinian Territory. Social media have become the terrain for tracking contacts and intimate details such as sexual orientation, in order to blackmail, slander and detain⁵⁰. In 2019, Israel was accused of secretly using testing facial recognition on Palestinians in Ramallah, West Bank.⁵¹ In 2021, Facebook identified the emergence of hacking and social engineering operations tied to the Palestinian Authority in the West Bank, following a sustaining trend of online repression against Palestinian whistle-blowers and political opposition⁵².

An international spyware campaign operating from the Lebanese General Security Directorate offices was exposed in 2018, targeting activists, journalists, lawyers, and educational institutions in Lebanon and over 20 countries⁵³. This new development shows how states may now be able to hire spyware instead of buying them⁵⁴.

⁴⁷ 'Egypt: A Repression Made in France', International Federation for Human Rights, accessed 31 May 2021, <https://www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france>.

⁴⁸ 'TIMEP Brief: Export of Surveillance to MENA Countries', TIMEP, accessed 2 June 2021, <https://timep.org/reports-briefings/timep-brief-export-of-surveillance-to-mena-countries/>.

⁴⁹ 'TIMEP Brief: Use of Surveillance Technology in MENA', TIMEP, accessed 6 May 2021, <https://timep.org/reports-briefings/timep-brief-use-of-surveillance-technology-in-mena/>; 'Cybersurveillance en Syrie: non-lieu pour Qosmos, société accusée de complicité de crimes contre l'humanité', JusticeInfo.net, 8 February 2021, <https://www.justiceinfo.net/fr/73468-cybersurveillance-en-syrie-non-lieu-pour-qosmos-societe-accusee-de-complicite-de-crimes-contre-lhumanite.html>.

⁵⁰ +972 Magazine July 15 and 2015, 'Exclusive: The IDF Is Monitoring What Israeli Citizens Say on Facebook', +972 Magazine, 15 July 2015, <https://www.972mag.com/the-idf-is-monitoring-what-israeli-citizens-say-on-facebook/>.

⁵¹ 'Inside Israel's Lucrative — and Secretive — Cybersurveillance Industry', Rest of World, 9 March 2021, <https://restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline/>.

⁵² Marwa Fatafta April 29 and 2021, 'Elections or Not, the PA Is Intensifying Its Authoritarian Rule Online', +972 Magazine, 29 April 2021, <https://www.972mag.com/palestinian-elections-authoritarianism-online/>.

⁵³ 'Human Rights Organizations Call for Investigation Into Arbitrary Surveillance Program in Lebanon', SMEX (blog), 24 January 2018, <https://smex.org/human-rights-organizations-call-for-investigation-into-arbitrary-surveillance-program-in-lebanon/>.

⁵⁴ Russell Brandom, 'Researchers Have Discovered a New Kind of Government Spyware for Hire', The Verge, 18 January 2018, <https://www.theverge.com/2018/1/18/16905464/spyware-lebanon-government-research-dark-caracal-gdgs>.

Digital identity

Digital ID programmes are spreading. To some extent, digital identity contributes to the Sustainable Development Goal (SDG) 16.9, which calls for legal identity for all⁵⁵. However, biometrics are extremely sensitive personal data which have to be handled under strict criteria. The [Why ID Campaign](#), a group of civil society organisations, technologists, and experts who work on digital identity advise that governments and international funders “consider the impact that ill-considered, badly designed, and poorly implemented digital identity programmes can have on human lives”. Among the key issues in the region are mandatory use, lack of transparency on storage security and incomplete safeguards against violations in an already weak data protection environment.

The Tunisian and Jordanian states have biometric ID projects and laws that are hotly debated and even opposed due to the lack of safeguards and proper consultation processes⁵⁶. Jordan in particular is considering a Smart National ID that would integrate iris scan, fingerprint and blood type. Morocco has already had a biometric ID regime since 2008 for national ID cards issued by the National Police and e-Passports. So does Lebanon with biometric passports, driving licenses and residence permits since 2016. Other concerns about attacks on fundamental freedoms are raised with regards to linking SIM cards and other communication and travel with ID, which can enable surveillance. It is mandatory in Morocco and proposed in Lebanon. It is worth noting that international organisations such as the United Nations High Commissioner for Refugees (UNHCR) are already allowed to collect and use biometrics of people who live in the refugee camps of Al Zaatari and Azraq Camps, based on technology provided within a private-public partnership that raises serious questions regarding privacy and safety among rights defenders⁵⁷.

Internet shutdowns

Repressive governments have resorted to limit, block, slow down or filter Internet access in order to break uprisings, hide human rights violations or influence elections. Shutdowns have increased during the COVID-19 pandemic globally. With centralised Internet infrastructure and fiber-optic cables under their control, the Egyptian authorities can create choke points. They famously shut down Internet and mobile services during the 2011 revolution for five days. Algeria shut down the Internet in September 2020 officially to prevent cheating during secondary school exams⁵⁸. During their eleven day-long raid in

⁵⁵ ‘Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group’s Tools’.

⁵⁶ ‘Exposed and Exploited’; Nadsoft, ‘Launch of “Mapping Digital Rights in the Middle East and North Africa” through a Collaboration between Innovation for Change MENA Hub and 7amleh, in Pursuit of a Baseline for Advocacy for Digital Rights in the Region.’; ‘State of Privacy Jordan’, Privacy International, accessed 6 May 2021, <http://privacyinternational.org/state-privacy/1004/state-privacy-jordan>; ‘State of Privacy Lebanon’, Privacy International, accessed 6 May 2021, <http://privacyinternational.org/state-privacy/1081/state-privacy-lebanon>; ‘State of Surveillance Tunisia’.

⁵⁷ ‘Exposed and Exploited’.

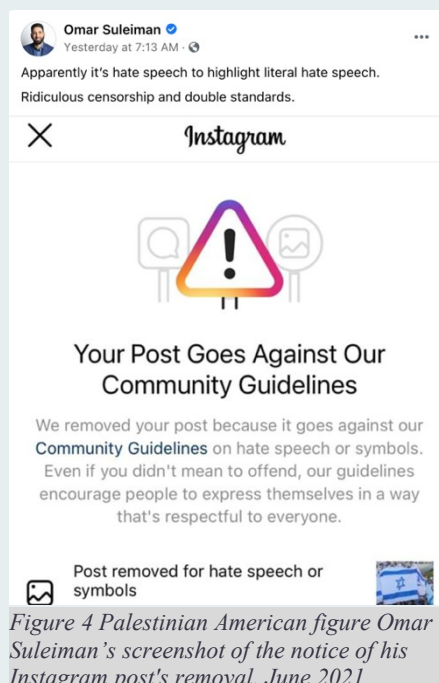
⁵⁸ ‘Internet perturbé en Algérie pour les épreuves du baccalauréat’, RFI, 14 September 2020, <https://www.rfi.fr/fr/afrique/20200914-internet-perturb%C3%A9-en-alg%C3%A9rie-les-%C3%A9preuves-baccalaur%C3%A9at>.

May 2021⁵⁹, the Israeli forces are reported to have deliberately bombed vital ICT infrastructure, whose shutdown affected Internet supply across 12 local Internet Service Providers (ISPs) within the Gaza Strip. Companies like Sandvine (US) and Allot (Israel) have provided such service in numerous Arab countries⁶⁰. With elections coming up in Libya, Algeria, Palestine and Morocco in 2021, digital activists have called for caution and scrutiny.

IN FOCUS: ONLINE CENSORSHIP AGAINST PALESTINIANS IN MAY 2021

Since 2015, Facebook, Instagram, Youtube and Twitter have increasingly censored Palestinian content, based on tailored content moderation policies informed by an Israeli state security perspective. Israel's Cyber Unit uses an "alternative enforcement" method to get content to be considered as incitement or praising terrorism (e.g. *shaheed*, meaning "martyr" in Arabic) in order to generate a violation of the platforms' community standards, flag the targeted content and request its removal. This method has imposed severe limitations on freedom of expression and opinion on Palestinian narratives and likely to continue if words like "zionism" enter the fold of hate speech⁶¹. The page of the Palestinian Ministry of Health in Gaza was taken down three times, including during the COVID-19 pandemic. Instances of censored posts and suspensions of accounts, including large accounts of social media influencers, have spectacularly increased in the aftermath of May 2021's upsurge of violence⁶², which suggests that the number of flagging has increased. Emi Palmor, former head of the Israel's Cyber Unit, is a member of Facebook's Oversight Board. According to the Israeli Ministry of Justice, Facebook complies with 95% of Israeli requests to remove content⁶³. However when confronted by digital rights activists, platforms tend to blame technical errors⁶⁴.

Such patterns are documented in other parts of the world: tech corporations' cooperation with repressive states leads to shutting down the last vital online space for people, journalists and human rights defenders, social media, where



⁵⁹ 'Israeli Airstrikes Destroyed Internet Infrastructure in Gaza', *SMEX* (blog), 28 May 2021, <https://smex.org/israeli-airstrikes-destroyed-internet-infrastructure-in-gaza-report/>.

⁶⁰ 'Sandvine ... the Surveillance Octopus in the Arab Region', *Massar* (blog), 24 October 2020, <https://masaar.net/en/sandvine-the-surveillance-octopus-in-the-arab-region/>.

⁶¹ 'Analysis: Facebook Zionism Hate Speech Policy Proposal', *Access Now* (blog), 2 March 2021, <https://www.accessnow.org/facebook-hate-speech-policy-zionism/>.

⁶² 'Israel-Palestine: How Social Media Was Used and Abused', *Middle East Eye*, accessed 3 June 2021, <http://www.middleeasteye.net/news/israel-palestine-social-media-used-abused-disinformation-manipulation-censorship>.

⁶³ 'Facebook Complying with 95% of Israeli Requests to Remove Inciting Content, Minister Says', *Haaretz.com*, accessed 3 June 2021, <https://www.haaretz.com/israel-news/business/facebook-removes-inciting-content-at-israel-s-request-minister-says-1.5432959>.

⁶⁴ Maya Gebeily, 'Instagram, Twitter Blame Glitches for Deleting Palestinian Posts', *Reuters*, 10 May 2021, <https://www.reuters.com/article/israel-palestinians-socialmedia-idUSL8N2MU624>.

they cannot enjoy their fundamental freedoms of expression and assembly in addition to being the target of surveillance. It seems naive to rely on tech and ICT companies to enforce digital rights, in particular as enforcement is implemented via automated decision-making that notoriously delivers erroneous results.

Personal digital security practices reported by civil society interviewees vary greatly. As an interviewee targeted by a repressive regime pointed out, abuse does not come from technology but technology is part of it. It is just a tool that can be used in different ways. In conflict-affected and marginalised areas, “people want food, medicine, no one cares about COVID-19” or digital rights. Suspicion towards digital technologies stem from tech-savvy activists but also from older generations, whose experience with state repression informs a certain fear that ICT could be an entry point for oppressive measures. Others expressed fear of hacking and screen grabs from external parties or beneficiaries, with or without malicious intent. Screen grabs of political positions or chats that reveal certain sexual orientations that are considered reprehensible by authorities have led to arrests, detention and torture.

The privacy-related best practices reported by interviewees include using applications that are deemed safer (the most tech-savvy declared opting for Jitsi for video conferencing and Signal for messages and calls, instead of Zoom and Whatsapp respectively), requesting consent in internal proceedings such as recording meetings, informing partners and beneficiaries of what is going to be done with their information, monitor repressive developments in other countries of the region in order to analyse the situation locally, providing digital safety training to colleagues and beneficiaries.

Expertise in the region

Technologists and rights activists in the region have increasingly organised in recent years; some in locally grown and regional organisations, others in international organisations. All of them regularly produce high quality and timely analysis of key developments on data protection and digital rights in the region. Below are some of the national and international organizations whose analysis contributed to this report.



Research on digital rights in the MENA region

The reports below cover in detail data protection and privacy debates in the MENA region.

[Exposed and exploited: Data protection in the Middle East and North Africa](#) - Access Now, January 2021

[Mapping Digital Rights in the Middle East and North Africa](#) – 7amleh and Innovation for Change, March 2021

[State of Privacy](#) – Privacy International, 2019

[Country reports](#) of the Freedom on the Net monitoring tool – Freedom House

2. Digital rights in the EU's Neighbourhood Policy

1- EU priorities in its Southern Neighbourhood

The EU's main cooperation policy for engaging the Southern Mediterranean is the European Neighbourhood Policy, which traditionally covers good governance and rule of law, socio-economic development, migration and support to refugees, climate change, environment, energy and security.

Dis/Misinformation and Cybersecurity

Digital technology in EU foreign policy discourse has longest been featured within its security policy, as a threat. Among the areas of interest are the spread of disinformation/misinformation, cybersecurity and cybercrime enabled by the rapid evolution of new technology, the absence of regulation and intense global competition among state and non-state actors. Coinciding with intensification of polarisation with Russia, China and other regional powers, and the rise to power of authoritarian regimes across the world, strategic communications and countering disinformation outside its borders have become a strategic objective for the EU as reflected in umbrella policies such as the EU Global Strategy⁶⁵.

In the aftermath of the conflict in Syria and the rise of the so-called Islamic State of Iraq and the Levant (ISIL), the EEAS set up a Strategic Communication Task Force South, in short (StratCom) Task Force South, aiming to contribute to fact-based communication, countering disinformation and narrative-positioning in the region in 19 countries from Morocco to Iran. Unlike its Eastern counterpart created years earlier to counter false information and Russian state-sponsored discourse⁶⁶, the Task Force South has a flexible mandate that tends to focus on a larger set of negative consequences of the unregulated control of telecommunications and digital technology on the circulation of information in the region. In practice, it is composed of a small team of Arabic-speaking political and media analysts, who, with no programmatic budget, relies on journalists, media and digital rights experts to monitor issues such as cyber attacks and suppression of content, tailor country-specific structural and tactical responses in collaboration with the EU Delegations. The team also

⁶⁵ 'A Global Strategy for the European Union's Foreign and Security Policy', Text, EEAS - European External Action Service - European Commission, accessed 3 June 2021, https://eeas.europa.eu/topics/eu-global-strategy/17304/global-strategy-european-unions-foreign-and-security-policy_en.

⁶⁶ 'Questions and Answers about the East StratCom Task Force', Text, EEAS - European External Action Service - European Commission, accessed 3 June 2021, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/questions-and-answers-about-east-stratcom-task-force_en.

works to support space for independent media and relies on the European Endowment for Democracy (EED) and DG NEAR-funded projects on media.

The Instrument contributing to Stability and Peace (IcSP), the EU's peacebuilding fund, has started to integrate this dimension in programmes with media organisations, civil society organisations and initiated a dialogue with big tech companies. European Neighbourhood Instrument (ENI) funded programmes, such as El-Hiwar, have also offered such [trainings](#) to officials and civil society experts from the region⁶⁷.

Cybersecurity (civil) and cyberdefence (military) focus on malware attacks and include cybercrime such as “ransomwares”, illegal use of crypto-currency and phishing; hybrid tactics (including disinformation) and cyberattacks targeting critical infrastructure such as hospitals, ministries, oil refineries or nuclear plants⁶⁸. While this is a rapidly evolving area, China and Africa are among the main areas of attention. In this framework, the EU has developed a cyberdiplomacy toolbox (including sanctions), cyberdialogues and structural cooperation (10 partners: Brazil, Canada, China, India, Japan, Mexico, Russia, South Africa, South Korea, and the United States), cooperation with NATO and engagement with the African Union (UA), ASEAN and EU Neighbourhood countries; normative initiatives such as Microsoft's proposal for a digital Geneva convention⁶⁹ and a global commission on cyberspace stability. In this framework, support to Public Private Partnerships will amount to €450 million, including via Horizon2020⁷⁰.

Development cooperation

For years, the main component related to digital space in external relations and development cooperation programming was connectivity. NGOs and other non-state actors have been the most innovative by finding uses for technology that improve transparency, operations, with a view to supporting people and programmes. As digitisation is inevitably changing the way we interact at a global level, EU external action is slowly catching up the pace. The Directorate-General for International Partnerships of the European Commission (DG INTPA) is leading on issues related to development programmes and digital transition, although according to INTPA and DG NEAR officials, very few programmes or policies have included a strong component on digital rights to this day. Clear and comprehensive Information about past and current programmes in the region remains difficult to collect, each instrument and programme having different communication practices (European Neighbourhood Instrument (ENI),

⁶⁷ ‘EU-Funded Project El-Hiwar II – Sectorial Training Course on Fake News, Misinformation, Fact-Checking Techniques and Reliable Sources of Information on the EU | College of Europe’, accessed 26 May 2021, <https://www.coleurope.eu/news/eu-funded-project-el-hiwar-ii-sectorial-training-course-fake-news-misinformation-fact-checking>.

⁶⁸ Cybersecurity priorities are reflected in the following EU policy documents : *Façonner l'avenir numérique de l'Europe* (2020) ; *Règlement sur la cybersécurité* (2019) – volet action extérieure ; *Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide* (2017)

⁶⁹ ‘A Digital Geneva Convention to Protect Cyberspace | Microsoft Cybersecurity’, accessed 3 June 2021, <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace>.

⁷⁰ ‘Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-Threats’, Text, European Commission - European Commission, accessed 3 June 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2321.

EU Emergency Trust Fund for Africa (EUTF Africa), EU Trust Fund for Syria (EUTF Syria), Instrument contributing to Stability and Peace (IcSP), European Instrument for Democracy and Human Rights (EIDHR)). According to Brussels-based officials, consultations are being held with civil society regarding the upcoming programming of the new Neighbourhood, Development and International Cooperation Instrument (NDICI). An internal handbook on digitalisation directed at European Commission programme staff is currently being drafted.

In the last two years, the digital revolution has been more prominently reflected in some of the key foreign and regional policy documents related to the Southern and Eastern Mediterranean region, and accelerated by the human and economic impact of the COVID-19 pandemic. As part of the development paradigm and in the framework of support to SDGs, digital transformation has become in a short period of time one of the main priorities of EU intervention, with the goal of leveraging the benefits of digital technology while minimising risks.

Human rights

Moreover, as digital surveillance has increasingly affected human rights defenders in the region, protection of digital rights and prevention of harm has taken a prominent space in EU policy. Section 4 of the [EU Action Plan on Human Rights and Democracy](#) (2020-2024) is entirely dedicated to protection of rights online and includes commitments to develop tools to detect and respond to closing civic space, misinformation and democratic backsliding, “including the use of digital technologies and counter-terrorism measures as well as disproportionate measures imposed under state of emergency”. It also commits EU institutions to support online media literacy and digital skills, and strengthen civil society organisations’ and independent media’s capacity to counter disinformation and information manipulation. Legal aid and digital innovation features among the priorities in relation to “rights-based and gender responsive justice”; addressing the “digital gender divide” is mentioned as a structural inequality, although it is unclear whether it refers to skills, online space and/or other aspect of digital rights and space.

The annual EU-NGO human rights Forum of December 2020 was dedicated to the impact of new technologies on human rights.

29



Figure 5 Participants Live Poll Results at the 2020 EU-NGO Human rights Forum (Dec 2020)

Discussions involved EU high level representatives and parliamentarians in charge of the issue, as well as key privacy and digital rights actors at international and regional levels, such as David Kay, (now former) UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and European Digital Rights network (EDRi), who have not regularly been part of the traditional human rights dialogues and external relations in Brussels. The final report⁷¹ lists a number of key recommendations that should guide future policy and programming exercises, and be refined and adapted to specific actions and contexts.

At the time of writing, EU human rights and democracy country strategies, which guide EU's action in the fields of cooperation and human rights in a given country - in particular that of EU Delegations, are currently being drafted and should reflect some of these recommendations. In practice, the European Union Human Rights Defenders mechanism launched in 2015 and funded by EIDHR - ProtectDefenders.eu - has come through to provide support to human rights defenders targeted by digital surveillance and hate speech online, and training on digital security to organisations.

Overall digital rights issues are reflected in the EU's neighbourhood policy and practice through the lens of economic development, security and human rights. Digital rights experts are increasingly perceived as human rights defenders by EU staff and representatives. In terms of transparency, this research process stumbled across the difficulty of obtaining information on EU funding and projects invested in this field, in part due to lack of internal communication and instruments having unequal practices of external communications. This highlights that, in spite of tremendous progress in inter-institutional processes in recent years, collaboration in policy-making and implementation between regional and thematic units of the European Commission and the EEAS remains a significant challenge due to geographic silo-ing and lack of staff. This also shows that standards of transparent, accessible e-government practices have yet to be improved in the EU institutions themselves. In this regard, the EUTF Africa website stands out as one of the most comprehensive, readable and transparent online database of projects.

5- The EU's new Agenda for the Mediterranean

The EU Joint Communication "Renewed partnership with the Southern Neighbourhood", hereafter referred to by its tag line "A new Agenda for the Mediterranean", was launched on 9 February 2021. It sets out the EU's priorities for its Southern Neighbourhood under the European Neighbourhood Policy (ENP) as reviewed in 2015, which was itself a revision of the 2011 ENP launched in the aftermath of the uprisings in the Middle East and North Africa. An [online consultation](#) to inform the new policy was conducted by IEMed in January 2021 and closed just over two weeks before the new Agenda was

⁷¹ 'Report of the 22nd EU NGO Human Rights Forum - The Impact of New Technologies on Human Rights', 2020, <https://prod5.assets-cdn.io/event/5773/assets/8386445075-51a909d2e0.pdf>.

published, a window of participation and partnership deemed too short by civil society representatives⁷².

This Agenda conveniently narrows the focus on the EU's Southern Neighbourhood, whose relationship and cooperation with the EU are remarkably distinct from that of the Eastern neighbourhood. This makes future EU action to be more agile and tailored to context. While the 2015 review brought a strong security and counter-migration dimension, the new Agenda brings a strong focus on economic recovery post-COVID-19, in which the green and digital transition agendas are to take a large part.

The EU's top priority: digital transformation at the service of post-COVID-19 economic recovery

Beyond the need to stabilise the pandemic and relaunch cooperation, the document is clear about prioritising the EU's economic growth and the protection of its financial interests in the region. In order to do so, the EU will seek to "tap into the region's economic potential", which involves supporting and accelerating digital transformation in the region in order to open more outlets in the digital economy that are of interest to the EU⁷³. Strengthening the region's governments' ability to handle these transitions and to enforce decisions, including via a strong judiciary and regulations such as data protection, would presumably create a conducive environment to that end.

EU support to digital transition in the region is to be structured around four pillars: data protection regulation and governance; infrastructure and access to networks; digital literacy and skills, and entrepreneurship and digital services. Supporting digital rights and skills are also mentioned as a driver of human development and respect for fundamental rights. Attention is emphasised on providing access and skills to marginalised communities and rural areas. The NDICI and the European Fund for Sustainable Development plus (EFSD+) will be the main instruments for EU cooperation with partner countries of the region (up to 7 billion Euros under the NDICI).

Among the key commitments related to this theme:

Data protection	As a matter of governance and rule of law, the EU makes here a clear and detailed commitment to support data protection and privacy legislation and architecture, to promote "human and user-centric approach to the digitalisation of systems and services (which) will increase state efficiency and build trust in institutions. (...) The EU will continue to engage with partner countries to ensure a high level of protection of the fundamental
-----------------	---

⁷² 'EU Agenda for the Mediterranean: More than Speed Dating?', EuroMed Rights, accessed 3 June 2021, <https://euromedrights.org/publication/eu-agenda-for-the-mediterranean-more-than-speed-dating/>.

⁷³ European Commission, 'Joint Communication: Renewed Partnership with the Southern Neighbourhood - A New Agenda for the Mediterranean', 9 February 2021, https://ec.europa.eu/neighbourhood-enlargement/news_corner/news/southern-neighbourhood-eu-proposes-new-agenda-mediterranean_en.

⁷⁴ In other words, "as a location for the restructuring of EU firms' global value chains in the wake of the pandemic, and how this might be supported by EU programmes" - 'How New Is the EU's New Agenda for the Mediterranean?', CEPS (blog), 3 March 2021, <https://www.ceps.eu/how-new-is-the-eus-new-agenda-for-the-mediterranean/>.

	rights to privacy and data protection and promote further convergence with EU and international data protection standards, facilitating commercial exchanges and law enforcement cooperation.” Such frameworks are also explicitly aiming to ensure the “free flow of non-personal data”. Action points include providing capacity building for civil society organisations (CSOs) and supporting the development of data protection frameworks “enforced by strong and independent supervisory authorities”, along with promoting the ratification and implementation of relevant international conventions.
Infrastructure and connectivity convergence	As part of creating conducive environment for business “economic integration”, EU programmes will aim to increase connectivity across the Mediterranean, through regulatory convergence in telecommunications, trust services, investments in high bandwidth telecommunication infrastructure, and ensuring deployment of the EU’s 5G toolbox principles to ensure network security.
Rights	On principle, the EC and the EEAS commit to work with partner governments of the region to “bring about more robust and enabling frameworks for freedom of expression, and support healthy information environments”, and to “ensur(ing) a user-centric and the ethical use of technologies in line with the EU Charter of Fundamental Rights”.
Cybersecurity and disinformation	Interestingly, disinformation along with climate change is treated as a security and defence matters. In relation to terrorism, hybrid threats and cybercrime, continued cooperation is anticipated on law enforcement, online recruitment and dissemination of terrorist content online. On vulnerability of critical infrastructure (e.g. energy, transport, banking and health) and disinformation, the EU wants to “share best practices, train cyber security experts and explore possibilities offered by innovative tools for law enforcement purposes, in full respect of human rights and civil liberties” and make full use of existing international frameworks, such as the Council of Europe Budapest Convention.
Tech innovation and	The EU promises association to its lead research fund Horizon Europe ⁷⁵ in particular in the human dimension of

⁷⁵ ‘Horizon Europe’, European Commission, accessed 21 May 2021, https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

research	connectivity, innovation and creating a knowledge society and economy.
E-government and education	The EU aims to encourage the deployment of platforms for eHealth, e-commerce, culture and cultural heritage, and cooperate on digital education under the 2021-2027 digital education action plan. In particular, it aims at fostering convergence on electronic identification.
Digital skills and technical assistance	Providing technical assistance and supporting digital skills training is the cross-cutting action point through all thematic priorities of Euro-Mediterranean cooperation, from education, to SMEs providing technical support to promote financial inclusion, especially on digital payments and digital literacy for SMEs,

Strong points

To some extent, the structure for the EU's proposed partnership on digital transformation responds to some of the demands of governments, rights organisations and experts of the region interviewed for this report. It sets a horizon of high level of protection of rights to privacy and personal data in the region. Referencing the GDPR, whose provisions aim to provide human rights safeguards in particular during crises, would be very much appreciated locally. Technology should be user-centric, designed by and for people, and support to local companies on innovation will empower SMEs and generate context- and needs-based tools. Although the amount dedicated to it is unknown, digital skills building will certainly be in high demand by non-specialised CSOs. Initiatives seeking to connect Mediterranean countries with their continents (Asia and Africa) can only help re-anchor and offer choices to societies and economies in the region. Gender equality, women's empowerment and gender peace and security are referenced throughout the document, although it is unclear what exactly it aims to tackle and how it translates into the action points listed.

Gaps and concerns

While the Agenda seems to intend to be pro-active on data protection and regulation, many listed action points appear to be driven by economic and security concerns. Interventions on management and regulation of online activity are raised mainly to address violent extremism, terrorism and corruption. Issues of online gender-based violence, racism and disability are not mentioned. It is worth noting that the document pairs digital and green transitions together and links climate change agenda with energy security and defence: protecting assets and infrastructure appear to be paramount.

While it aims to help set strong standards to protect personal data, privacy and human rights, the document does not refer to the EU documents or international standards that provide guidance and inform principled EU

cooperation and uphold digital rights. In order to design projects involving digital technology, EU policy and programme staff should rely on internal or external good practices such as the [Principles for digital development](#)⁷⁶.

Concerns regarding implementation and impact could legitimately be raised if the main goal of the Agenda is economic growth rather than human development aligned with human and environmental needs. Considering that EU discourse and international organisations reflect certain techno-optimistic narratives that tend to accept the norms set by the tech industry, the EU could inadvertently, in its support to digital transformation, contribute to entrench oppressive structures and foster instability instead of resilience - no matter how many data and privacy regulations are passed. For this reason, it is crucial to save space for autonomous innovation and independent research by academia, expert organisations, as well people and groups on the front lines, which could foster a healthy ecosystem of ideas and exchange in spite of a challenging political environments.

The document also refers to the Middle East Peace Process by committing to "build upon the recent establishment of diplomatic relations between Israel and a number of Arab countries, with a view to enhancing the prospects for a negotiated two-state solution based on the internationally agreed parameters as well as regional peace and security." Access Now in an earlier report⁷⁷ recalls that the European Commission determined in a 2011 Decision on personal data protection that "Israel provides adequate protection with regard to the automated processing of personal data" and that the Decision applies "without prejudice to the status of the Golan Heights, the Gaza Strip and the West Bank, including East Jerusalem, under the terms of international law".⁷⁸ The state of Israel has an extensively documented practice of digitally-enabled human rights violations from hate speech, incitement, censorship and apartheid to extra-judicial killings and accusations of war crimes and crimes against humanity. Israeli surveillance technology is used in other countries of the region to stifle freedom of expression and target human rights defenders. Cooperation with Israel under such terms could be a threat to digital rights regionally: it is likely to further enable human rights violations and apartheid against Palestinians and entrench oppressive behaviours in the region.

The question of exports of dual-use technology

Digital surveillance is considered a dual-use technology, i.e. having both civilian and military applications, including the Internet as the most common

⁷⁶ These Principles elaborated by international development institutions and non-governmental organisations include are nine living guidelines that are designed to help integrate best practices into technology-enabled programs and are intended to be updated and refined over time. They include guidance for every phase of the project life cycle, and they are part of an ongoing effort among development practitioners to share knowledge and support continuous learning.

⁷⁷ 'Exposed and Exploited'.

⁷⁸ The Official Journal of the European Union. (2011, January 31). Retrieved January 10, 2021, from <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2011%3A027%3A0039%3A0042%3AEN%3APDF>

one⁷⁹. The control of EU dual-use exports is a key component of global non-proliferation efforts and is governed by the newly revised “Regulation of the European Parliament and the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items” approved in March 2021⁸⁰, based on the [Wassenaar Arrangement](#) - the only existing, non-binding international standard to date. The new EU Regulation widens the previous EU control list to cyber-surveillance items and emerging technology, and creates a new EU coordination mechanism to facilitate intra-EU communication, due diligence and transparency on sales. This regulation has the potential of setting a mode for other regional and multilateral bodies, and civil society organisations have hailed the increased progress in restrictions of these arms exports. Nonetheless, the regulation will be tested by enforcement. Furthermore, it does not tackle the economic and political drivers that limit its impact. Defence ministries are closely linked to equipment exports and the sensitive, yet highly lucrative, market of cyber-weaponry increases incentives to sell: relying on the sole willingness of executive branches of states to prevent sales is unlikely to be effective. Stronger accountability and due diligence mechanisms should be enforced by states by implementing the recommendations made by leading rights organisations in March 2021⁸¹.

The former UN Special Rapporteur on freedom of opinion and expression, David Kaye, called for a moratorium on exports of surveillance technology⁸² until an international regulatory mechanism is in place. This statement was supported by digital rights organisations, such as Privacy International and Access Now, which added that the proliferation of cybersurveillance systems is a systemic and global problem that requires the strengthening of international norms and harmonised standards globally in order to address the systemic deficiencies in regulating the trade of technologies that facilitate surveillance. A ban could only be a step in a more comprehensive approach to dual-use tools⁸³.

⁷⁹ ‘Dual-Use Technologies for Conflict Prevention and Peacebuilding’, *EU-CIVCAP* (blog), 7 February 2018, <https://eu-civcap.net/2018/02/07/dual-use-technologies-for-conflict-prevention-and-peacebuilding/>.

⁸⁰ Expected to come into force in August 2021. ‘Trade of Dual-Use Items: New EU Rules Adopted’, accessed 29 May 2021, <https://www.consilium.europa.eu/en/press/press-releases/2021/05/10/trade-of-dual-use-items-new-eu-rules-adopted/>.

⁸¹ ‘New EU Dual Use Regulation Agreement “a Missed Opportunity”’, accessed 2 June 2021, <https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/>.

⁸² ‘Moratorium Call on Surveillance Technology to End “Free-for-All” Abuses: UN Expert’, UN News, 25 June 2019, <https://news.un.org/en/story/2019/06/1041231>.

⁸³ Access Now Team, ‘Export Bans Alone Won’t Stop Surveillance — We Need a New Global Approach’, *Access Now* (blog), 18 November 2019, <https://www.accessnow.org/export-bans-wont-stop-surveillance-we-need-a-new-global-approach/>.

Conclusion and Recommendations

In the backdrop of a fast-paced digital revolution, the launch of new EU development funding instrument and pressure to incentivize a post-COVID-19 economic recovery, the EU and partner countries in the Mediterranean are set to renew their cooperation priorities. While human rights and data protection are high on the EU's new Agenda for the Mediterranean, their implementation seem secondary to economic growth. The EU's industry interests are at odds with the need to reign in exports to repressive regimes. The EU and Member States will have to continue to walk a fine line between championing human rights and enabling harmful digitally-enabled practices in the region.

While supporting GDPR-like regulations may offer welcomed opportunities for litigation against companies and institutions who abuse data subjects' rights, it is not the end game of privacy and digital rights in a world where the tech industry remains highly unregulated and exploitative. Many companies' privacy practices continue to violate the regulation's basic principles, knowingly or not, and it is questionable whether digital rights can be enforced in the long run when tech corporations are able to pay record fines with no harm to their profits. Online privacy may exist in law but is still largely absent in practice.

The EU should exercise maximum due diligence, conflict-sensitivity and gender-sensitivity in future tech-focused cooperation with the region, with a view to uphold digital rights, foster the social welfare of local innovators and workers in the digital economy and enable virtual safe spaces for rights defenders, technologists, peacebuilders and journalists.

Recommendations

The European Commission and the European External Action Service (EEAS) should:

- **Use their leverage to pressure partner countries and tech companies complicit in human rights violations** to respect international law standards online and offline.
- **Support and fund investigation, analysis, technical and legal capacity of locally-driven independent media and organisations** in order to monitor, document and influence policy-making and practices on data protection and digital rights. In particular, support **strategic litigation training and processes** against misuse of data, digital rights violations and monopoly by platforms, companies and governmental bodies; and **contribute to the creation of secure online platforms** for collaboration and documentation of legal developments and human rights violations
- **Assist the creation of an independent regional network of social justice and human rights** dedicated to build collective knowledge and coordinate strategies on technology-related issues (e.g. in the model of the Europe-wide [Justice, Equity and Technology Table](#) led by London School of Economics).

- **Convene a regional digital multi-stakeholder dialogue** that bridges gaps between civil society expert, technologists, authorities and companies in order to better apprehend the regional socio-economic and political challenges of digital transformation;
- **Define strict evidence-based vetting and due diligence mechanisms on Public-Private Partnerships** designed to assess and incentivise compliance of companies with human rights standards and the GDPR and **ensure that technical frameworks used by companies are publicly available** when sensitive personal data is being handled.
- Ensure that DG NEAR, DG INTPA and EEAS staff in charge of policies and programmes with rights or digital components are able to **monitor GDPR application developments at EU level** and **design and implement context- and gender-sensitive intervention in close cooperation with local and international digital/human rights experts in the region** in order to avoid adverse impact of programmes supporting GDPR-inspired regulations.
- **Increase the level of expertise in digital technology among political, policy and programming staff** in DG NEAR, Foreign Policy Instruments (FPI) and the EEAS in order to improve internal practice and appropriate programme design, by:
 - recruiting experts from various backgrounds (technical, legal, human rights, private sector) in order to strengthen the understanding of technology development,
 - providing mandatory digital safety, rights and skills training to manage data appropriately and work with human rights defenders in a safe manner.
- **Improve transparency, accuracy and accessibility of up-to-date data on EU development cooperation funding** by harmonising online communications standards of the Neighbourhood, Development and International Cooperation Instrument (NDICI) and other instruments – based on models such as the [IcSP map](#) (Instrument contributing to Stability and Peace) and the EU Trust Fund for Africa's [webpage](#) – except when data publication risks putting stakeholders in repressive environments at risk.

EU Member states should:

- **Thoroughly enforce the new EU regulation on dual-use technology export and its coordinated mechanism and adopt a wide interpretation of cyber-technology** based on the recommendations of the [human and digital rights organisations' response statement of March 2021](#) to ensure that EU policies and activities do not support state-sponsored surveillance that violate EU's human rights commitments.

Bibliography

- DataReportal – Global Digital Insights. ‘60% of the World’s Population Is Now Online’. Accessed 1 June 2021. <https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet>.
- Middle East Eye. ‘A Breakdown of Algeria’s New Constitution’. Accessed 31 May 2021. <http://www.middleeasteye.net/news/algeria-new-constitution-breakdown>.
- ‘A Digital Geneva Convention to Protect Cyberspace | Microsoft Cybersecurity’. Accessed 3 June 2021. <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace>.
- EEAS - European External Action Service - European Commission. ‘A Global Strategy for the European Union’s Foreign and Security Policy’. Text. Accessed 3 June 2021. https://eeas.europa.eu/topics/eu-global-strategy/17304/global-strategy-european-unions-foreign-and-security-policy_en.
- Access Now. ‘Access Now Releases “Expanding Connectivity to Fight COVID-19: Recommendations for Governments and Telcos”’, 30 April 2020. <https://www.accessnow.org/expanding-connectivity-to-fight-covid-19/>.
- ‘Algeria - Loi N° 18-07 Du 10 Juin 2018 Relative à La Protection Des Personnes Physiques Dans Le Traitement Des Données à Caractère Personnel.’ Accessed 31 May 2021. https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=107253.
- Ali, Massyle Ait. ‘La Loi sur le traitement des données personnelles publiée au Journal officiel’. N°TIC WEB. Accessed 31 May 2021. <https://www.nticweb.com/news/2-non-categorise/9401-la-loi-sur-le-traitement-des-donn%C3%A9es-personnelles-publi%C3%A9e-au-journal-officiel.html>.
- Access Now. ‘Analysis: Facebook Zionism Hate Speech Policy Proposal’, 2 March 2021. <https://www.accessnow.org/facebook-hate-speech-policy-zionism/>.
- April 29, Marwa Fatafta and 2021. ‘Elections or Not, the PA Is Intensifying Its Authoritarian Rule Online’. +972 Magazine, 29 April 2021. <https://www.972mag.com/palestinian-elections-authoritarianism-online/>.
- La Presse de Tunisie. ‘Avis d’un spécialiste | La 5G en Tunisie, une pression forte des USA et de la Chine’, 2 January 2021. <https://lapresse.tn/83168/avis-dun-specialiste-la-5g-en-tunisie-une-pression-forte-des-usa-et-de-la-chine/>.
- the Guardian. ‘BAE “Secretly Sold Mass Surveillance Technology to Repressive Regimes”’, 14 June 2017. <http://www.theguardian.com/business/2017/jun/15/bae-mass-surveillance-technology-repressive-regimes>.
- Brandom, Russell. ‘Researchers Have Discovered a New Kind of Government Spyware for Hire’. The Verge, 18 January 2018. <https://www.theverge.com/2018/1/18/16905464/spyware-lebanon-government-research-dark-caracal-gdgs>.
- European Commission - European Commission. ‘Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-Threats’. Text. Accessed 3 June 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2321.
- Data Protection. ‘Convention 108 and Protocols’. Accessed 31 May 2021. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.
- ‘Creating a Data Protection Framework: A Do’s and Don’ts Guide for Lawmakers’. Access Now, November 2018. <https://www.accessnow.org/data-protection-handbook>.
- JusticeInfo.net. ‘Cybersurveillance en Syrie: non-lieu pour Qosmos, société accusée de complicité de crimes contre l’humanité’, 8 February 2021. <https://www.justiceinfo.net/fr/73468-cybersurveillance-en-syrie-non-lieu-pour-qosmos-societe-accusee-de-complicite-de-crimes-contre-lhumanite.html>.

- DataReportal – Global Digital Insights. ‘Digital in Tunisia: All the Statistics You Need in 2021’. Accessed 31 May 2021. <https://datareportal.com/reports/digital-2021-tunisia>.
- EU-CIVCAP. ‘Dual-Use Technologies for Conflict Prevention and Peacebuilding’, 7 February 2018. <https://eu-civcap.net/2018/02/07/dual-use-technologies-for-conflict-prevention-and-peacebuilding/>.
- ‘E7mi - إحمي’. Accessed 31 May 2021. https://e7mi.tn/faq_fr.html.
- DataGuidance. ‘Egypt - Data Protection Overview’, 21 August 2020. <https://www.dataguidance.com/notes/egypt-data-protection-overview>.
- International Federation for Human Rights. ‘Egypt: A Repression Made in France’. Accessed 31 May 2021. <https://www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france>.
- Freedom House. ‘Egypt: Freedom on the Net 2020 Country Report’. Accessed 31 May 2021. <https://freedomhouse.org/country/egypt/freedom-net/2020>.
- EuroMed Rights. ‘EU Agenda for the Mediterranean: More than Speed Dating?’ Accessed 3 June 2021. <https://euromedrights.org/publication/eu-agenda-for-the-mediterranean-more-than-speed-dating/>.
- ‘EU-Funded Project El-Hiwar II – Sectorial Training Course on Fake News, Misinformation, Fact-Checking Techniques and Reliable Sources of Information on the EU | College of Europe’. Accessed 26 May 2021. <https://www.coleurope.eu/news/eu-funded-project-el-hiwar-ii-sectorial-training-course-fake-news-misinformation-fact-checking>.
- European Commission. ‘Joint Communication: Renewed Partnership with the Southern Neighbourhood - A New Agenda for the Mediterranean’, 9 February 2021. https://ec.europa.eu/neighbourhood-enlargement/news_corner/news/southern-neighbourhood-eu-proposes-new-agenda-mediterranean_en.
- Access Now. ‘Exposed and Exploited: Data Protection in the Middle East and North Africa’, 28 January 2021. <https://www.accessnow.org/exposed-and-exploited-data-protection-mena/>.
- Haaretz.com. ‘Facebook Complying with 95% of Israeli Requests to Remove Inciting Content, Minister Says’. Accessed 3 June 2021. <https://www.haaretz.com/israel-news/business/facebook-removes-inciting-content-at-israel-s-request-minister-says-1.5432959>.
- Gebeily, Maya. ‘Instagram, Twitter Blame Glitches for Deleting Palestinian Posts’. *Reuters*, 10 May 2021. <https://www.reuters.com/article/israel-palestinians-socialmedia-idUSL8N2MU624>.
- Gillula, Jeremy. ‘Facebook’s Free Basics: More Open, Better Security, but Still a Walled Garden’. Electronic Frontier Foundation, 30 September 2015. <https://www.eff.org/deeplinks/2015/09/facebooks-free-basics-more-open-better-security-still-walled-garden>.
- The Citizen Lab. ‘HIDE AND SEEK: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries’, 18 September 2018. <https://citizenlab.ca/2018/09/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
- European Commission - European Commission. ‘Horizon Europe’. Text. Accessed 27 May 2021. https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
- CEPS. ‘How New Is the EU’s New Agenda for the Mediterranean?’, 3 March 2021. <https://www.ceps.eu/how-new-is-the-eus-new-agenda-for-the-mediterranean/>.
- BBC Reel. ‘How Our Personal Data Is Exploited in Unexpected Ways’. Accessed 30 May 2021. <https://www.bbc.com/reel/video/p09blhfw/how-our-personal-data-is-exploited-in-unexpected-ways>.
- ‘How the Private Sector in MENA Is Leading Workers to Better Digital Skills’. Accessed 16 May 2021. <https://blogs.worldbank.org/arabvoices/how-private-sector-mena-leading-workers-better-digital-skills>.

- SMEX. ‘Human Rights Organizations Call for Investigation Into Arbitrary Surveillance Program in Lebanon’, 24 January 2018. <https://smex.org/human-rights-organizations-call-for-investigation-into-arbitrary-surveillance-program-in-lebanon/>.
- Rest of World. ‘Inside Israel’s Lucrative — and Secretive — Cybersurveillance Industry’, 9 March 2021. <https://restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline/>.
- RFI. ‘Internet perturbé en Algérie pour les épreuves du baccalauréat’, 14 September 2020. <https://www.rfi.fr/fr/afrique/20200914-internet-perturb%C3%A9-en-alg%C3%A9rie-les-%C3%A9preuves-baccalaur%C3%A9at>.
- DataGuidance. ‘Israel - Data Protection Overview’, 8 October 2020. <https://www.dataguidance.com/notes/israel-data-protection-overview>.
- SMEX. ‘Israeli Airstrikes Destroyed Internet Infrastructure in Gaza’, 28 May 2021. <https://smex.org/israeli-airstrikes-destroyed-internet-infrastructure-in-gaza-report/>.
- Middle East Eye. ‘Israel-Palestine: How Social Media Was Used and Abused’. Accessed 3 June 2021. <http://www.middleeasteye.net/news/israel-palestine-social-media-used-abused-disinformation-manipulation-censorship>.
- July 15, +972 Magazine and 2015. ‘Exclusive: The IDF Is Monitoring What Israeli Citizens Say on Facebook’. +972 Magazine, 15 July 2015. <https://www.972mag.com/the-idf-is-monitoring-what-israeli-citizens-say-on-facebook/>.
- Sciences et Avenir. ‘La Tunisie, premier pays du Maghreb à lancer un satellite fabriqué 100% localement’. Accessed 31 May 2021. https://www.sciencesetavenir.fr/sciences/la-tunisie-1er-pays-du-maghreb-a-lancer-un-satellite-fabrique-100-localement_152748.
- ‘Law on the Protection of Personal Data No. 151 (2020) (English Translation)’, n.d. <https://www.privacylaws.com/media/3263/egypt-data-protection-law-151-of-2020.pdf>.
- ‘Le projet de loi sur la carte d’identité biométrique désapprouvé par la société civile - TN24.TN’. Accessed 31 May 2021. <https://tn24.tn/fr/article/le-projet-de-loi-sur-la-carte-d-identite-biometrique-desapprouve-par-la-societe-civile-349248>.
- DataGuidance. ‘Libya’. Accessed 31 May 2021. <https://www.dataguidance.com/jurisdiction/libya>.
- ‘Libya - Constitution of Libya, 2012.’ Accessed 31 May 2021. https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=93473&p_country=LBY&p_count=148&p_classification=01.01&p_classcount=12.
- ‘Loi 09-08 Relative à La Protection Des Personnes Physiques à l’égard Du Traitement Des Données à Caractère Personnel | DGSSI’. Accessed 31 May 2021. <https://www.dgssi.gov.ma/fr/content/loi-09-08-relative-la-protection-des-personnes-physiques-l-egard-du-traitement-des-donnees-caractere-personnel.html>.
- World Bank. ‘Mashreq 2.0: Digital Transformation for Inclusive Growth and Jobs (Vol. 2)’. Text/HTML. Accessed 16 May 2021. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/246561561495359944/Mashreq-2-0-Digital-Transformation-for-Inclusive-Growth-and-Jobs>.
- Mayara. ‘Coronavirus: l’Instance Nationale de Protection des Données Personnelles met en garde contre la divulgation de données liées à l’état de santé d’une personne contaminée’. Tunisie, 21 September 2020. <https://www.tunisienumerique.com/coronavirus-linstance-nationale-de-protection-des-donnees-personnelles-met-en-garde-contre-la-divulgation-de-donnees-liees-a-letat-de-sante-dune-personne-contaminee/>.
- UN News. ‘Moratorium Call on Surveillance Technology to End “Free-for-All” Abuses: UN Expert’, 25 June 2019. <https://news.un.org/en/story/2019/06/1041231>.
- ‘Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group’s Tools’. Accessed 2 June 2021. <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/>.

- Nadsoft. 'Launch of "Mapping Digital Rights in the Middle East and North Africa" through a Collaboration between Innovation for Change MENA Hub and 7amleh, in Pursuit of a Baseline for Advocacy for Digital Rights in the Region.' Accessed 27 May 2021. <https://7amleh.org/2021/03/10/launch-of-mapping-digital-rights-in-the-middle-east-and-north-africa-through-a-collaboration-between-innovation-for-change-mena-hub-and-7amleh-in-pursuit-of-a-baseline-for-advocacy-for-digital-rights-in-the-region>.
- Electronic Frontier Foundation. 'Net Neutrality'. Accessed 2 June 2021. <https://www.eff.org/issues/net-neutrality>.
- 'New EU Dual Use Regulation Agreement "a Missed Opportunity"'. Accessed 2 June 2021. <https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/>.
- Nothias, Toussaint. 'Access Granted: Facebook's Free Basics in Africa'. *Media, Culture & Society* 42, no. 3 (1 April 2020): 329–48. <https://doi.org/10.1177/0163443719890530>.
- 'OHCHR | The Right to Privacy in the Digital Age: Report'. Accessed 18 May 2021. <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx>.
- 'Privacy Matters | Privacy International'. Accessed 18 May 2021. <https://www.privacyinternational.org/learning-resources/privacy-matters>.
- EEAS - European External Action Service - European Commission. 'Questions and Answers about the East StratCom Task Force'. Text. Accessed 3 June 2021. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/questions-and-answers-about-east-stratcom-task-force_en.
- 'Report of the 22nd EU NGO Human Rights Forum - The Impact of New Technologies on Human Rights', 2020. <https://prod5.assets-cdn.io/event/5773/assets/8386445075-51a909d2e0.pdf>.
- Massar. 'Sandvine ... the Surveillance Octopus in the Arab Region', 24 October 2020. <https://masaar.net/en/sandvine-the-surveillance-octopus-in-the-arab-region/>.
- Privacy International. 'State of Privacy Jordan'. Accessed 6 May 2021. <http://privacyinternational.org/state-privacy/1004/state-privacy-jordan>.
- Privacy International. 'State of Privacy Lebanon'. Accessed 6 May 2021. <http://privacyinternational.org/state-privacy/1081/state-privacy-lebanon>.
- Privacy International. 'State of Privacy Morocco'. Accessed 6 May 2021. <http://privacyinternational.org/state-privacy/1007/state-privacy-morocco>.
- Privacy International. 'State of Surveillance Tunisia'. Accessed 6 May 2021. <http://privacyinternational.org/state-privacy/1012/state-surveillance-tunisia>.
- Team, Access Now. 'Export Bans Alone Won't Stop Surveillance — We Need a New Global Approach'. *Access Now* (blog), 18 November 2019. <https://www.accessnow.org/export-bans-wont-stop-surveillance-we-need-a-new-global-approach/>.
- World Bank. 'The Middle East and North Africa: From Transition to Transformation'. Accessed 16 May 2021. <https://www.worldbank.org/en/region/mena/publication/the-middle-east-and-north-africa-from-transition-to-transformation>.
- TIMEP. 'TIMEP Brief: Export of Surveillance to MENA Countries'. Accessed 2 June 2021. <https://timep.org/reports-briefings/timep-brief-export-of-surveillance-to-mena-countries/>.
- TIMEP. 'TIMEP Brief: Use of Surveillance Technology in MENA'. Accessed 6 May 2021. <https://timep.org/reports-briefings/timep-brief-use-of-surveillance-technology-in-mena/>.
- 'Trade of Dual-Use Items: New EU Rules Adopted'. Accessed 29 May 2021. <https://www.consilium.europa.eu/en/press/press-releases/2021/05/10/trade-of-dual-use-items-new-eu-rules-adopted/>.
- VENRO. 'Tech for Good. Chances and Limits of Digital Instruments in the Development Cooperation of Non-Governmental Organisations', 2019. https://venro.org/fileadmin/user_upload/Dateien/Daten/Publikationen/Dokumentationen/NRO-Report_TechForGood_EN.pdf.

webmanagercenter.com, and Talel. 'La Loi Sur La Protection Des Données Personnelles Ouvrira à La Tunisie de Grandes Perspectives d'investissement'. *Webmanagercenter* (blog), 20 April 2018. <https://www.webmanagercenter.com/2018/04/20/418851/la-loi-sur-la-protection-des-donnees-personnelles-ouvrira-a-la-tunisie-de-grandes-perspectives-dinvestisment/>.
GDPR.eu. 'What Is GDPR, the EU's New Data Protection Law?', 7 November 2018. <https://gdpr.eu/what-is-gdpr/>.

Annexes

Table 1. A non-comprehensive overview of UN standards on digital rights

<p>Universal Declaration of Human Rights (1948)</p>	<p>In particular Article 19: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”</p>
<p>International Covenant on Civil and Political Rights (1966)</p>	<p>In particular Article 19: “1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. “</p>
<p>UN Human Rights Council resolution on “The role of freedom of opinion and expression in women’s empowerment” (A/HRC/23/L.5) (2013)</p>	<p>“3. Calls upon all States: (d) To facilitate equal participation in, access to and use of information and communications technology, such as the Internet, applying a gender perspective, and to encourage international cooperation aimed at the development of media and information and communication facilities in all countries”</p>
<p>UN Human Rights Council resolution on “The promotion, protection and enjoyment of human rights on the Internet” (A/HRC/32/L.20) (2016)</p>	<p>The resolution affirms a human rights-based approach on technology deployment and access to Internet and requests all States to make efforts to bridge the many forms of digital divides; including gender and disability-related gaps.</p>
<p>U.N. Sustainable Development Goals (SDGs) – Goal 9</p>	<p>9.C : “...strive to provide universal and affordable access to the Internet in least developed countries by 2020”</p>
<p>Special Procedures of the Human Rights Council</p> <ul style="list-style-type: none"> ● Special Rapporteur on the right to peaceful assembly and association; ● Special Rapporteur on contemporary forms of racism; ● Special Rapporteur on extrajudicial, summary or arbitrary executions; ● Special Rapporteur on the promotion and protection of the right to freedom of expression; ● Special Rapporteur on the situation of human rights defenders; ● Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism 	<p>Reports by Special Rapporteurs increasingly seek to document the intersection of technology and human rights. Recent reports published covered:</p> <ul style="list-style-type: none"> - content regulation in the digital age - emerging digital technologies and racial inequality - the freedom of expression during disease pandemics; - consequences on online violence against women and girls from a human rights perspective - targeted killings through armed drones; - the right to freedom of peaceful assembly and of association in the digital era
<p>The UN Secretary-General’s Roadmap for Digital Cooperation</p>	<p>UN’s plan to connect all people by 2030; respect human rights online; and protect the most vulnerable from the potential risks of digital technology deployment. Its implementation is coordinated by the Office of the Secretary-General’s Envoy on Technology</p>