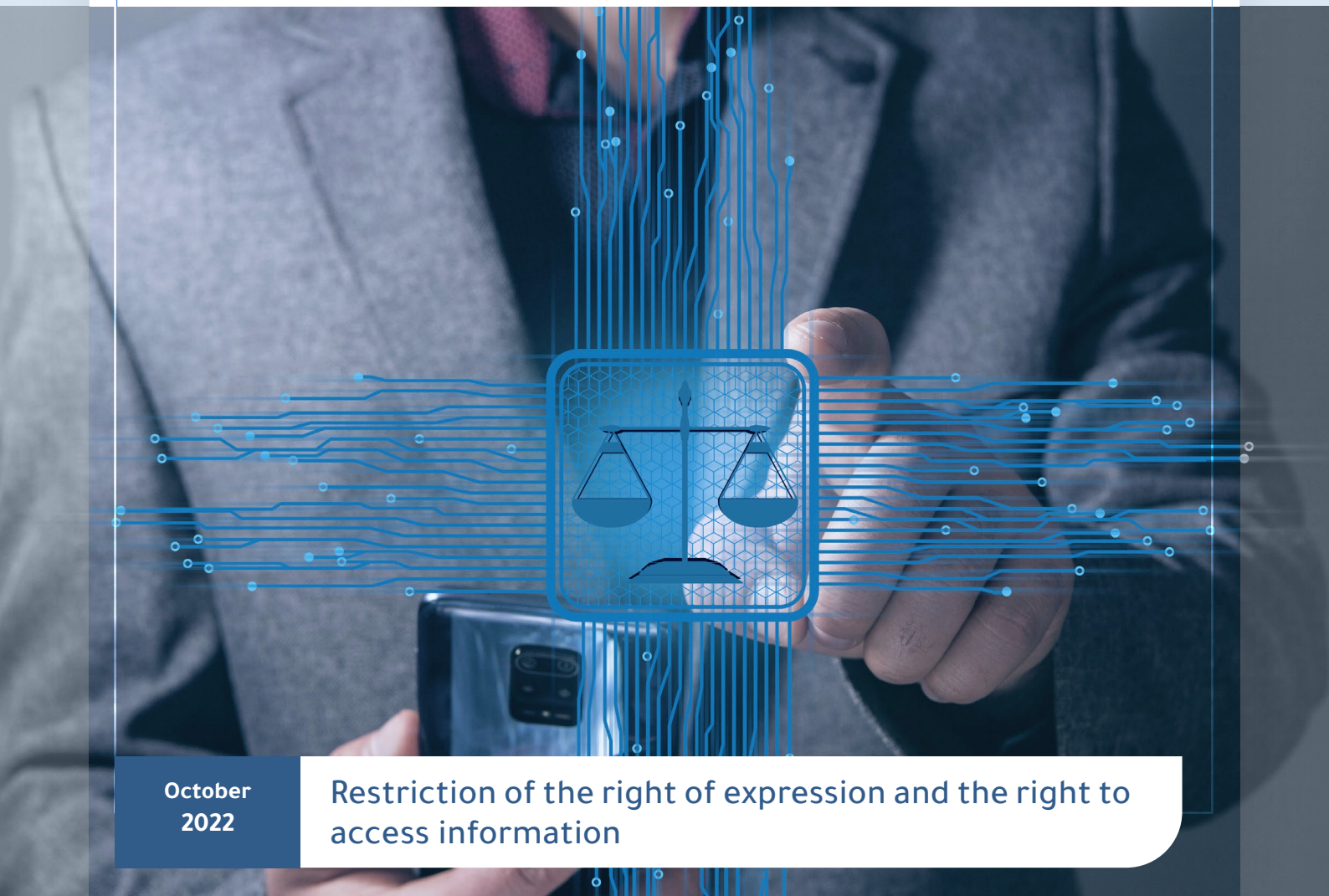
المركز السوري للإعلام وحرية التعبير
Navenda Sûriyayî ya Ragihandinê û Azadîya Derbirînê
Syrian Center for Media and Freedom of Expression

# Legal Review of the Cybercrime Law No. 20 of 2022



October 2022

Restriction of the right of expression and the right to access information

# Legal Review of the Cybercrime Law No. 20 of 2022

## Restriction of the right of expression and the right to access information

**General supervision:** Mazen DARWISH, founder and director of the Syrian Center for Media and Freedom of Expression.

**Prepared by:** Dr. Ayman MENEM, Director of the Legal Office at SCM.

**Reviewed by:** Yara BADER, Media and Freedoms Program Manager at SCM.

**Technical Consultation:** Ayman ALMANI, Director of the Technical Department at SCM.

# Contents:

# Introduction

It is an established fact that freedom of expression is a great human value, which includes freedom of thought, creativity, and freedom of writing, in addition to freedom of the media and the press of all forms: paper, electronic or audio-visual. It is also no secret that the right to freedom of expression and media freedoms are not only individual rights, but a great privilege of the larger societies. The violation of these freedoms would have society-wide repercussions, as they are the foundation for building societies and democracies by allowing the free flow of information, raising awareness and informing citizens of their rights and duties.

In international law, access to information and freedom of expression are one and the same. Both have had a huge boost with the advent of World Wide Web and social media. Some governments have used every possible means from the outset to close this space down or subjugate it, through laws issued under the pretext of violation prevention, blurring the space between regulation and restriction, and twisting the relationship between freedom and constraint, between the rule and the exception. Therefore, limiting the individuals' rights to freedom of expressions has become the rule, with absence of a freedom of expression philosophy and a standard essence thereof, whether in legislation, policies, or practices.

Since 1963, the policies of the successive governments in Syria have been hostile towards freedom of expression. Syria has tumbled to the bottom of global press freedom indices, along with such countries as North Korea and Iran. In an extensive study conducted in 2005 on internet censorship in the MENA region, Human Rights Watch concluded that "the Syrian Government relies on a combination of repressive laws and illegal measures to suppress the right of Syrians to free access to and dissemination of information online.[1]" In 2007, the Organization called upon the Syrian Government to "immediately release writers and activists it detains solely on charges of expression or for posting information online«.

Not only has the Syrian Government silenced and banned any form of free media, but it has also systematically restricted and blocked access to the cyber space. In a 2008, first-of-its-kind study titled "Taming the Internet", the Syrian Center for Media and Freedom of Expression documented "161 blocked websites until 28 April 2008, which [was] just an estimate figure of the total number of blocked websites verified by the SCM team"[2]. YouTube was among the victims!

Within the authorities' ongoing efforts towards complete dominance over the digital space and marginalization of all forms of freedom of expression and opinion online, the Syrian President issued Law No. 20 of 2022[3] on 18 April, which reconfigures the criminal legal rules of cybercrime stipulated in Decree No. 17 of 2012, after the People's Assembly approved the draft law submitted in December 2021 by the Ministry of Communications and Technology. Taking effect on 17 May 2022, a month after it was issued, the Law reflects a close-minded

1 Syria: Stop arrests for posting comments online. Human Rights Watch, 8/10/2007

2 Taming the Internet, Syrian Center for Media and Freedom of Expression

3 Full text of the Cybercrime Law No. 20 of 2022, Syrian Ministry of Communications and Technology.

and repressive state orientation, contrary to all international standards of freedoms and freedom of expression in particular.

## Law No. 20 of 2022

The new Law includes 50 articles listing the obligations and duties of internet access and internet service providers (ISPs), and articles additional to those contained in Decree 17,[4] part of which relate to the crimes of personal accounts identity thefts, privacy violations, defamation and libel, electronic disdain, and violations of the decency and modesty norms. The articles utilized most as grounds to detain journalists and writers in Syria are titled: "Undermining the prestige of the state", "Undermining the financial prestige of the state", and constitution-related crimes. Violating these articles is punishable for up to 15 years in prison by the law, in addition to fines of up to 15 million Syrian pounds. Financial fines are not subject to amnesty decrees that cover detention penalties. The fines are unaffordable by the majority of Syrians, as the minimum monthly salary in government-controlled areas is 37,600[5] Syrian pounds.

Given the limited reliance on banking and use of electronic cards in financial transactions in Syria, and the already limited internet connectivity[6] and unaffordability due to high costs in relation to the average per capital income[7] and lack of proper infrastructure to enable citizens to rely on it in their transactions, which are already subject to the Electronics Transactions Law No. 3 of 2014, the current Law's main goal is to reassert the government control on society. A new cybercrime law is the last thing the society needs. Crimes related to publication are covered in already effective laws[8], regardless of the medium: visual, auditory, or print. Moreover, electronic blackmail and invasion of privacy are also covered by other laws[9]. Therefore, the new law is only an added restriction of freedoms and reinforcement of impunity.

What the country badly needs is laws that protect citizens from state invasion of their privacy and enable them to prosecute state agencies illegal privacy violations through any electronic means. There is also a need for laws to counter hate speech. According to a 2017 study by the Syrian Center for Media and Freedom of Expression[10], hate speech constituted more than 27% of the overall media content of official and semi-official media platforms, which incite violence based on political grounds. The society also needs laws to incriminate cyber armies and organized fake social media accounts[11], used or supported by the government[12] as a tool to ambush its political opponents and human rights activists, and to overflow the digital space with disinformation.

4 Enforcement of the provisions of the Law on Online Communication and Cybercrime.

5 Salary scale in Syria, 2022, the Complete Guide.

6 link

7 link

8 General Penal Code and Military Penal Code.

9 Violation of Privacy: Media Law No. 108 of 2012, General Penal Code, Articles 557, 565, 566, 576

Electronic Blackmail: Cybercrime Law, Legislative Decree No. 17 of 2012

10 The Syrian Center for Media and Freedom of Expression launches a study on hate speech and incitement of violence in Syrian media.

11 The Syrian Electronic Army, a Cyberspace War?

12 President Bashar Al-Assad praises the Syrian Electronic Army.

Law 20 of 2022 includes severe punishments that far exceed their equivalents in other laws for the same criminal acts using the same means as stipulated in the General Penal Code and Military Penal Code, among others[13]. The law also uses vague language that incriminates a wide range of freedom of expression acts, in an apparent contradiction to international laws, particularly the International Covenant on Civil and Political Rights, which requires strict conditions for the limitation of basic rights, incompliance with which could render a limitation illegitimate. It also contradicts the Syrian constitution, which guarantees the rights of free public expression, be it verbal, written, or in any other form.

Law 20 is an advanced stage of a path the government has taken to quell the public uprising and reclaim control over the public space, eliminate any opposing opinions, and restore the pre-2011 status quo. The government added to the many already effective freedom-restricting legislations another set of laws, starting with the Law on Peaceful Demonstrations No. 54 of 21 April 2011, Law No. 22 of 2012 that established the Anti-Terrorism Court, Anti-Terrorism Law No. 19 of 2012, Media Law No. 108 of 2012, Law No. 17 of 2012, and finally the current Law, which was also proceeded by a number of decrees, decisions and measures:

### Establishment of Cybercrime Combating Branch in the Ministry of Interior

On 22 February 2012, the Syrian Minister of Interior issued Decision No. 465 establishing a unit under the Criminal Security Department dedicated to counter, investigate, discover, and analyze information crimes, collect digital criminal evidence and arrest perpetrators of such acts and bring them to justice. The unit was called "Cybercrime Combating Branch". It replaced the Department of Combating Digital Crimes established by Decision No. 1130/U of 2009. The new branch includes the following departments:

* Department of Investigation and Surveillance: responsible for investigating, evidence-collection and arrest of cybercrime suspects, particularly the crimes listed in the Electronic Signature and Network Services Law in force, and Decree No. 17 of 2012.
* Informatics Evidence Department.
* Register Office.

### Training of Judges specialized in cybercrime trials, July 2017

The Ministries of Interior, Communications and Technology, and Justice cooperated with the Arab Academy for E-Business to train judges in charge at on handling cybercrime cases. The training focused on monitoring electronic content, especially on social media, collection of information stored on user devices, and screening of information systems and information storage and transfer tools. Judge Hadi Al-Sha'ar[14], Minister of Justice, announced then that his ministry would collaborate with the Ministry of Communications and Technology and the Ministry of Interior to train a group of judges of various ranks to investigate and counter cybercrimes and to verify the admissibility of digital evidence. Syria, thus, became the second

13 Pursuant to the provision of article 180 of the General Penal Code, which states that "if a general provision and a special provision both apply to a certain act, the special provision shall be enforced".

14 Syria: A New "Cybercrime" Law, The Syrian Center for Media and Freedom of Expression.

country in the region after the UAE to establish cybercrime courts and introduce related training and procedures to the judiciary.

### Establishment of courts for information and communications crimes (25 March, 2018)

Legislative Decree No. 17 of 2012 on the Regulation of Online Communication and Countering Cybercrime did not specify the competent courts to hear public right cases filed under its provisions, so these cases would be distributed among criminal justice courts based on geographical jurisdiction or the nature of the crime. For example, individuals charged with undermining the prestige of the state would be referred to counter-terrorism courts. This had been the case until Law No. 9 of 2018 was issued to establish courts specialized in informatics and communication crimes on 25 March, 2018.

Article 1 of Law 9 provides for the establishment of a public prosecutor's office, an investigation department, and criminal courts of first instance and courts of appeal to deal with information and communications crimes. Article 4 stipulated that "special rooms would be dedicated in the Court of Cassation to consider information and communications crime and misdemeanor appeals". Article 2 stipulated that the jurisdiction of the courts of first instance shall cover all misdemeanors, regardless of whether public rules consider them to fall under the jurisdiction of the courts of first instance and magistrate courts or not, in a manner that does not contradict the provisions of Article 5(B) of this law". Article 5(B) states: "Cybercrimes related to provisioning, financial, terrorism or state security crimes shall remain under the jurisdiction of the courts dealing with their subject matter."

In April 2018, the information courts commenced their work handling hundreds of cases and issuing judgements in presence or by default against defendants. Damascus Information Court of First Instance alone handled 450-500 cybercrime cases in the first six months of its work, according to its president, Judge Salem Daqmaq[15].

### Changes in security branches monitoring internet and communications (July, 2019)

At the end of July, 2019, the Russian military command in Syria issued directives to make high-level structural changes in security branches specialized in communications and signal systems. These included merging the work of Branch 225 (Communications Branch specialized in surveillance of local and international communications), Branch 211 (Computer Branch, specialized directly in internet services), and Branch 237 (Wireless Branch, specialized in tapping and jamming radio calls inside Syria).

The Russians also modified the technical devices in those branches, introduced other modern devices and changed the operating system. At the same time, they appointed a group of new officers who had received special trainings in Syria and Russia. They also introduced new, faster and more accurate methods of information sharing and exchange, linked information access points, and restricted information flow directly to the National Security Bureau. The leaderships of those three branches were requested to issue directives to ease surveillance on certain matters, such as internet websites and local calls and assign this task to the Criminal Cybercrime Security Branch at the Ministry of Interior. These three branches were

15 Imposing Large Financial Fines on Violators. The Assad Regime Intends to Introduce Amendments to the Media Law. Alsouria.net

also requested to dedicate full time to the new structure and prepare for an advanced phase of "information security[16].

### Ministry of Interior warns social media users of suspicious websites (February 2021)

In February 2021, the Ministry of interior[17] warned social media users in Syria of the consequences of using websites with foreign ties. Just hours after the warning, the Ministry announced the arrest of eight people accused of communicating with suspicious websites, based on the Cybercrime Law. However, the Ministry did not name or specify any "suspicious pages" but threatened with imprisonment any person who communicates or interacts with such pages. The Ministry's Facebook page also published an interview[18] with the Head of the Cybercrime Branch of the Criminal Security Department explaining the legal liability of leaking or disseminating rumors or interacting with foreign websites or providing them with any information or data, pursuant to the provisions of the Penal Code and the Cybercrime Law.

### Amnesty for all detainees under the Cybercrime Law (May 2021)

The number of detainees of cybercrimes covered by Decree 13 of 2021, which included a general amnesty for perpetrators of a number of misdemeanors, offenses, and felonies committed before 2 May 2021, clearly showed how large the extent of criminalization under Decree 17 was despite its limited provisions, and the reality of freedom of expression after the entry into force of Law No. 20 which covers more than 15 crimes not stipulated by Decree 17.

Among those covered by the amnesty, issued only weeks before the presidential elections, were more than 400 public sector employees who had been arrested for cybercrimes, in addition to several judges, lawyers, journalists, police officers, customs inspectors, university students, businesspeople and human rights activists who had expressed opinions contrary to the mainstream or official narrative of the Syrian Government. According to a report by Middle East Affairs[19], none of the released detainees had criticized the President or showed any opposition to the authority. Most of them had been arrested by security forces for minor activities on social media ranging from likes and comments on Facebook, condemning the increasingly difficult living conditions, and criticizing the government, to statements condemning corruption.

### Head of the Cybercrime Branch declares use of emojis can constitute a cybercrime.

In a statement to Al-Baath Newspaper[20], on 14 September, 2021, the mouthpiece of the ruling

16 The State of Media in Syria, 2019. Syrian Center for Media and Freedom of Expression.

17 Damascus Begins the Presidential Elections Campaign by Activating the "Cybercrime" Law | Middle East

18 Syrian Ministry of Interior Facebook Page: https://www.facebook.com/page/264301457287719/search/?q=%202021%20%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9

19 Syria releases hundreds of social media critics ahead of election - Middle East Affairs

20 http://newspaper.albaathmedia.sy/2021/09/14/%d8%aa%d8%b9%d8%aa%d9%85%d8%af-%d9%83%d8%af%d9%84%d9%8a%d9%84-%d8%b9%d9%84%d9%89-%d8%ac%d8%b1%d8%a7%d8%a6%d9%85-%d9%85%d9%86-%d8%a8%d9%8a%d9%86%d9%87%d8%a7-%d8%a7%d9%84%d8%aa%d9%87%d8%af%d9%8a%d8%af/

Baath party[21], the Head of the Anti-Cybercrime Branch, Colonel Louay Shalish stated that emojis can constitute a cybercrime if their use is confirmed to be serious. He added that all offenses could be classified as cybercrimes if they take place online, regardless of the used media, or method of communicating the message or threat, be it a photo, a text or voice message, or emoji, if the intent of the sender was clear. These statements caused a wide public uproar, even in international media. The French weekly Courier International[22] published an article about this statement, causing the official to retract his words, assuring that his security Branch was only dedicated to the protection of Syrians, not their repression. He added that the emoji matter had been cited out of context.

These statements, even if retracted, clearly portray the security mentality supposed to implement freedom-related laws. Some saw them as warning messages or threats that any use of the internet could entail prosecution and incrimination.

### Completion of Russia's expansion in the internet sector in Syria (17 November 2021)

There have been several visits by Russian delegations since 2015 from the Ministry of Digital Development, Communication and Mass Media, and by Russian ICT companies to Syria, to promote cooperation in communications and digital transformation projects in Syria, the last of which[23] was in November 2021. As a result, 12 digital transformation projects were launched in several Syrian ministries. In addition, agreements were concluded to launch other projects in digital learning and communications.

Russian officials have repeatedly stated that Russian companies are ready to cooperate with Syrian companies and the Syrian Ministry of Communications and Technology in supporting the development of telecommunication services, provision of better services, and improving internet services to reach most populations in different areas at affordable costs and good 2G and 3G connection quality, in addition to enhancing Russian satellite coverage of Syrian territories for commercial purposes[24], which was approved by the Syrian government.

Russia's expansion in the Syrian internet sector means Russia gets access to Syrian users' information and data, which it can later use in data analysis, monitoring of social trends and designing political and economic projects in its interest. By dominating the ISPs, Russian companies would enable the Syrian government to closely monitor social media. They would also try to force subscribers to use certain platforms and applications that would enable them to collect user data and information and share it with security agencies, with criminal charges ready under the Cybercrime Law.

### Ministry of Justice Circular on the pretrial detention of cybercrime suspects

The Syrian Minister of Justice issued a circular on 23 January 2022 to Prosecutors General of the Tribunal and judges of penal courts regarding the pre-trial detention of cybercrime suspects,

21 Despite the 2012 constitutional amendment, the Arab Socialist Baath Party retained its status as the ruling party in theory and practice, being the party of the absolute majority in the People's Assembly.

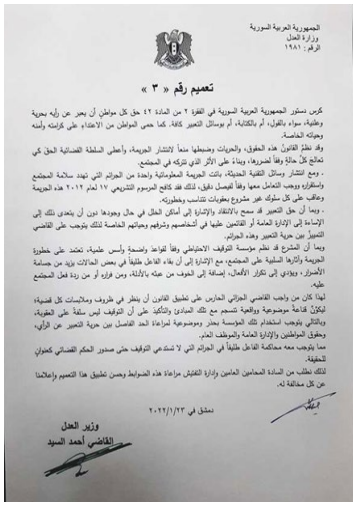
22 En Syrie, on criminalise les émojis.

23 Cooperation in Communications and Digital Transformation between Syria and Russia, SANA

24 Syrian-Russian Meeting in the Ministry of Communications and Technology to Discuss Potential Cooperation in Cybersecurity and Digital Transformation.

stressing that pre-trial "must be used with caution and objectivity, taking into account the boundary between freedom of expression, freedom of citizens, public administration, and public officials"[25].

The circular stated: "As freedom of expression means[26] a person can criticize and point at any shortcomings, if any, without crossing the line to offend the public administration or insult its officials as persons, or their honor or private lives, a judge must, therefore, make a distinction between freedom of expression and these crimes, which threaten social integrity and stability".



الجمهورية العربية السورية
وزارة العدل
الرقم : ١٩٨١

تعميم رقم « ٣ »

كرس دستور الجمهورية العربية السورية في الفقرة ٢ من المادة ٤٢ حق كل مواطن أن يعبر عن رأيه بحرية وعلنية، سواء بالقول، أم بالكتابة، أم بوسائل التعبير كافة. كما حمى المواطن من الاعتداء على كرامته وأمنه وحياته الخاصة.

وقد نظم القانون هذه الحقوق، والحريات وضبطها منعاً لإنتشار الجريمة، وأعطى السلطة القضائية الحق كي تعالج كل حالة وفقاً لخطورتها، وبناءً على الأثر الذي تتركه في المجتمع.

. ومع انتشار وسائل التقنية الحديثة، باتت الجريمة المعلوماتية واحدة من الجرائم التي تهدد سلامة المجتمع واستقراره ووجب التعامل معها وفقاً لفيصل دقيق، لذلك فقد كافح المرسوم التشريعي ١٧ لعام ٢٠١٢ هذه الجريمة وعاقب على كل سلوك غير مشروع بعقوبات تتناسب وخطورته.

. وبما أن حق التعبير قد سمح بالانتقاد والإشارة إلى أماكن الخلل في حال وجودها؛ دون أن يتعدى ذلك إلى الإساءة إلى الإدارة العامة أو القائمين عليها في أشخاصهم وشرفهم وحياتهم الخاصة لذلك يتوجب على القاضي التمييز بين حرية التعبير وهتك الجرائم.

وبما أن المشرع قد نظم مؤسسة التوقيف الاحتياطي وفقاً لقواعد واضحة وأسس علمية، تعتمد على خطورة الجريمة وتأثيرها السلبية على المجتمع، مع الإشارة إلى أن بقاء الفاعل طليقاً في بعض الحالات يزيد من حساسة الأضرار، ويؤدي إلى تكرار الأفعال، إضافة إلى الخوف من عليه بالأذى، ومن فراره أو من ردة فعل المجتمع عليه.

لهذا كان من واجب القاضي الجزائي الحارس على تطبيق القانون أن ينظر في ظروف وملابسات كل قضية؛ ليكوّن قناعة موضوعية وواقعية تتسم مع تلك المبادئ والتأكيد على أن التوقيف ليس سلفاً على العقوبة؛ وبالتالي يتوجب استخدام تلك المؤسسة بحذر وموضوعية لمراعاة الحد الفاصل بين حرية التعبير عن الرأي، وحقوق المواطنين والإدارة العامة والموظف العام.

مما يتوجب معه معاكسة الفاعل طليقاً في الجرائم التي لا تستدعي التوقيف حتى صدور الحكم القضائي كعنوان للحقيقة.

لذلك نطلب من السادة المحامين العامين وإدارة التفتيش مراعاة هذه الضوابط وحسن تطبيق هذا التعميم وإعلامنا عن كل مخالفة له.

دمشق في ٢٠٢٢/١/٢٣

وزير العدل
القاضي أحمد السيد

This is not the first circular of its kind. The ministry had issued decrees, circulars and communiqués to regulate pre-trial detentions. Pre-trial detention includes restricting the freedom of a suspect for the sake of public interest and to protect the society's right to punish perpetrators. The legislator called it 'pre-trial detention' not 'pre-trial imprisonment' to stress that it is a preventive exceptional measure that affects personal freedoms.

One of these circulars is Circular No. 50 issued on 18 December 1953, which obliges investigation judges to expedite their decisions in detainees' cases, and Circular No. 13 issued on 7 February 1955, which insists on giving this topic the utmost attention. The repeated jurisprudence of the Syrian Court of Cassation[27] listed the following goals for pre-trial detention:

* Protect the accused him/herself from public opinion reactions.
* Appease public outrage.
* Prevent the accused from contacting witnesses and influence them.
* Fear of destroying a crime scene.
* Gravity of the crime.

While seemingly emphasizing that freedoms are not to be compromised arbitrarily, the circular acknowledges pre-trial detention in cybercrimes. Moreover, it makes judges lean more towards detention as they are the only persons with the discretion to make decisions thereof, although the objectives of pre-trial detention according to the aforementioned Syrian Court of Cassation jurisprudence only apply to rare cases of cybercrime. If pre-trial detention is enforced without justification, it becomes an unlawful restriction of liberty, and an arbitrary use of the authority's own rights. Therefore, the Minister of Justice resolution of the legal controversy, which could have ended up in favor of persons accused of cybercrime, supported by judicial jurisprudence, raises fears that the executive power, represented by the Minister of Justice, pre-empted Law No. 20 by sending a clear message to Syrians that

25 Minister of Justice on Cybercrime: Prosecuting Perpetrators at Liberty in Crimes that do not Require Detention.

26 As stated in the circular of the Ministry of Justice, taking into account that international conventions and provisions - the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights use the right to freedom of expression.

27 Decision 2/1963, Basis 4435, Courts of Cassation, Syria; Rule 295, Compendium of Criminal Jurisprudence Part 1 to Part 6, Darkazalli; Decision 653/1979, Basis 617, Courts of Cassation, Syria; Rule 1715, Due Processes of Criminal Trials Part 1 and Part 2 - Istanbul: 19370.

any persons involved in criticizing the authority could be subject to immediate detention and prosecution.

### Law No. 15 of 2022 amending a number of articles of the General Penal Code (28 March 2022)

The critical living conditions all over the country and the government failure to address the situation or limit its deterioration and to provide basic services to citizens, led to more Syrians criticizing the government performance on social media. As a response, the authority amended some articles in the General Penal Code doubling the fines and expanding the circle of incrimination of other articles, including those related to the freedom of expression. This was a clear message to Syrians that criticizing the government or any of its officials would be criminalized and prosecuted. The amendments included:

* Increasing the minimum and maximum limits for infraction, misdemeanor, and criminal fines. The minimum misdemeanor fine stipulated in the General Penal Code, and all other legislations that include this penalty became 100,000 SYP, and the maximum fine became 500,000 SYP.

* Increasing the minimum criminal fine stipulated in the Penal Code and all other legislations that include this penalty to 500,000 SYP, and the maximum to one million SYP, unless the legislation states a higher amount.

The law also amended:

* The title of articles 285-288 of the General Penal Code from "crimes of undermining the prestige of the state and national sentiment" to "crimes of undermining the prestige of the state and compromising the civic and national identity".

* Article 285 from "Whoever in Syria during war or when war is anticipated makes claims aimed at 'weakening national sentiment'" to "undermines the civic or national identity, triggers racial or sectarian strife shall be punishable by provisional detention." The remarkable thing is the replacement of the verb 'weaken' by 'undermine', whose meaning may be so flexible as to include a greater number of acts and opens the door to broader interpretations by the authority.

* Article 286 from "Anyone in Syria, under the same conditions, who disseminates news known to be false or exaggerated and that would "weaken national sentiment" shall be subject to the same penalty" to "disseminates despair or weakness among the members of the society."

### Article 287: The first paragraph:

1. "Any Syrian citizen who knowingly disseminates false or exaggerated news abroad in a way that would undermine the prestige of the state, or its financial status shall be punished by imprisonment for at least six months (and a fine between 50-500 SYP)" was amended to:

1. "Any Syrian citizen who knowingly disseminates false or exaggerated news abroad in a way that would undermine the prestige of the State, or its financial status shall be punished by imprisonment for at least six months.

And a second paragraph was added:

2. Any Syrian who disseminates news that would polish up the image of an enemy state with the aim of undermining the status of the Syrian State shall be subject to the same punishment.

Here, too, the legislator expanded the scope of these articles to include a greater number of acts and perpetrators. Whereas article 287 stipulates that the news must be disseminated from abroad and that the perpetrator should be aware that such news is false or untrue in order for the crime to be complete, the new amendment was silent about the perpetrator's place and awareness.

* Article 292: A third paragraph was added:

1. Whoever attempts to strip a part of Syrian territory away from the State sovereignty shall be punished with provisional detention.
2. The punishment shall be life imprisonment if the perpetrator, in doing so, resorts to violence.
3. Any Syrian who calls, verbally or in writing, for a part of Syrian territory to be separated or ceded.

The amendments did not affect punishments, which remained the same. However, under the same social and political conditions, and within the same period, Law No. 20 added more fines and increased the minimum punishment for the same criminal acts, providing for severe punishments and heavy fines for undermining the prestige of the State or its financial status. This confirms that such strict responses are part of a general policy that aims to eventually allow the government to impose its full control over all spaces of expressions, similar to the isolation policy it had imposed on the Syrian society in the 1980s.

### Law No. 20 Re-Regulates the Penal Rules for Cybercrimes

Crimes provided for in Legislative Decree No. 17 of 2012 are:

* Illegal access to an information system.
* Use a website domain name.
* Obstruction of access to service
* Interception of information
* Designing and using malware

* Sending spam emails[28]
* Online scamming
* Illegitimate use of payment cards
* Violating the privacy of others
* Any crime punishable by the law and is committed online

The crimes added by Law 20 of 2022 to those mentioned in Decree 17 are:

* Electronic defamation
* Electronic libel or disdain
* Infringement of decency or modesty
* Offenses against the constitution
* Undermining the state prestige
* Undermining the financial status of the state
* Crimes related to narcotic drugs and psychotropic substances
* Insulting religions, sanctities, and religious rites.

First, the law obliges ISPs, in articles 3-5, to ensure the privacy and protection of action data of all subscribers for a period of time determined by the regulatory authority. It also obliges ISPs to save a copy of the action and content data hosted by them. This applies to ISPs who are obliged to save a copy of the digital content exchanged with the action data that identifies the content creator. This is subject to the punishment provided for in Article 6 (1-6 months imprisonment and a fine of 2-4 million SYP), if they fail to perform their obligation or neglect it. Pursuant to Article 4 of the executive directives of the Law issued by Decision No. 207 of the Minister of Communications and Technology on May 10, 2022:

"The action and content data shall be hosted for at least six months, and the duration shall be determined in the ISPs license, provided that saving such data shall be carried out in accordance with specific conditions set by the regulatory authority or the network services authority, each according to its competence."

Periodic storage of data constitutes a violation of privacy and of Article 36 of the Constitution "Private life is inviolable and protected by law", and Article 37 "The confidentiality of postal correspondence, telecommunications, radio communications, and all other types of communications shall be guaranteed by the law". It cannot be assumed that Article 7 of the

28 Spam email: any form of messages, whatever the content thereof, sent online to other persons without the recipient's will to receive it. Executive Instructions of Decree No. 17 of 2012.

new Law[29], which punishes perpetrators who disclose of data or digital content, provides protection from privacy infringement, which occurs[30] once data is stored, regardless of whether it is later disclosed or not.

Moreover, the nature of the security agencies in Syria and their dominance over state facilities confirm their periodic access to stored data and to the identities of online content creators, which include accounts of individuals on social media, and all forms of their messages: audio, visual, and written. In addition, the legislator allows the authorities to obtain and confiscate any offline data stored on mobile phones, computers or other devices, as being digital evidence, which the judicial police may search, just by obtaining permission from the investigating judge.

This clear disregard for the right to privacy allows for the incrimination of the freedom of expression and enables government to censor criticism. Moreover, it fosters a culture of self-censorship and fear among average individuals and media professionals alike, knowing all online data is being recorded. This further erodes the fundamental right of upholding and expressing opinions without external influence, fosters censorship, restricts criticism and dissent, and establishes the closure of the digital space, ending its effectiveness as a space of free expression.

In addition to violating international conventions, including Article 19 of the Universal Declaration of Human Rights, storing user data is in violation of the global direction towards the universalization of freedom of communication and information media. According to the Special Rapporteur on Freedom of Opinion and Expression[31], "[States should regard] Communications [and information technology] surveillance [...] as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance [...] must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, [...] and the kind of remedy provided by the national law."

According to the Special Rapporteur on Freedom of Opinion and Expression too[32]: "Governments may not force communications service providers, or hardware or software suppliers, to incorporate surveillance tools in the systems they operate, produce, or provide for the use of public, private or state bodies, and may not force them to collect or store

29 Article 7: imprisonment of 6 months to two years for the disclosure of data or digital content, and 3-5 years if the data relates to a public entity.

30 Some believe that service providers (internet, applications, programs) store data by the mentioned categories. There is a new category in circulation, which is user behavioral data (activities, interactions, interests, and desires) which is not yet covered by international or national privacy laws. Storing such data is not regarded as breach of privacy, but accessing it for non-operational purposes may constitute a breach, such as for monitoring, surveillance, influence, or denial of freedom of expression.

However, the privacy clause in the new Law did not include any clear categories or specific types of data. It did not specify which data requires a court warrant to access, "if any".

Moreover, obliging service providers to store all user, traffic, and content data and share it with the authorities when requested was absolute, without any references to data encryption by the service providers or any level of protection. This means that all data sent to/from any service provider on the Syrian network can be accessed.

31 Special Rapporteur on Freedom of Opinion and Expression, report submitted to the Human Rights Council in 2013, document no. (HRC/A/23/40), "Outcomes and Recommendations", Item 81.

32 Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue, 16 May 2011, Paragraph 84, document no. (HRC/A/17/27

specific information for the purposes of governmental surveillance. Governments should not request service providers to collect or pre-store any data. Individuals shall have the right to express their opinions anonymously, and governments must refrain from forcing individuals to provide their identity as a prerequisite to receive services".

The CJEU in Tele2Sverige and Watson and Others (C-203/15 and C-698/15, hereafter 'Tele2') held that Member States may not impose on the providers of electronic communication services an obligation of general and indiscriminate retention of data. The Court found that such obligation not only interfered with the protection of privacy and personal data but was also incompatible with the freedom of expression principle. The Court, however, laid down that where such a retention is warranted in cases where there is a serious threat to national or public security, the nature of the measure must be 'strictly' proportionated to its intended purpose. More importantly, the Court specified that a decision imposing such an order must be subject to effective review either by the Court or by an independent administrative body with binding authority. The Court also called for a clear and precise national-level rules governing the scope and application of retention of data to safeguard against risk of abuse.[33]

Technical explanation of digital data/evidence categories:

There are three classic categories of electronic evidence[34]:

While criminal justice standards for accessing electronic evidence vary by jurisdiction, regional instruments and bilateral agreements often refer to three categories of electronic evidence that correspond to three levels of procedural protection, based on the level of intruding the privacy of the target individual:

* User information: the data in this category relates to information that can be mainly used to identify the user of a certain service. Such information may be provided by the user during sign-up or collected while providing the mentioned service. This category often includes such information as: name, address, e-mail address, phone numbers, etc.

* Traffic/access and transaction data: this often includes information that can be used to verify the origin, duration or date of connection and means of access to a certain service, in addition to links to and communications with other users, including contacts. Depending on jurisdiction, this could include information related to when using a service started and ended.

* Content data: relates to the content of communications and traditionally includes such information as the collection of e-mails, text messages, or photos.

While these categories may seem clear, they may have significant overlapping. For example, some types of access data (such as IP addresses) are considered to have the same protection

33 The Cases of Privacy International la Quadrature Du Net and Others, Global Freedom of Expression

34 https://www.internetjurisdiction.net/news/new-ij-framing-brief-discusses-categories-of-electronic-evidence-in-the-context-of-new-types-of-data

as user information. Likewise, there is an ongoing debate about location data and whether they fall within the transaction data or content data. The content of each category may also vary depending on jurisdiction.

These three categories directly correspond to three specific levels of procedural and substantive protection to protect the privacy of individuals and ensure due legal processes. Concretely, user information may be directly requested from law enforcement authorities, which is usually the starting point of investigations. Access to this information is traditionally considered less intrusive than other categories.

Similarly, regarding traffic/access data and transactions, the judicial authorities often set the minimum limit. Orders must be issued or at least verified by the prosecution authority. While content data often requires authentication by the court.

**Technical opinion:**

Most service providers (internet, applications, programs) store data by the aforementioned categories. There is a new category in circulation now, which is user behavior data (activities, interactions, interests, and desires) which is not yet covered by international or national privacy laws. Storing such data is not regarded as breach of privacy, but accessing it for non-operational purposes may constitute a breach, such as for monitoring, surveillance, influence, or denial of freedom of expression.

However, the privacy clause in Law 20 did not include any clear categorization of data to specific types. It did not specify which data requires a court warrant to access, "if any".

Moreover, obliging service providers to store all user, traffic, and content data and share it with the authorities when requested was absolute, without any references to data encryption by the service providers or any level of protection. This means that all data sent to/from any service provider on the Syrian network can be accessed.

Article 21 - Violation of Privacy:

"Whoever disseminates private information online using any IT means without consent of the information owner, and even if such information is true, shall be punished by imprisonment from 1-6 months and a fine of 500,000-1,000,000 SYP."

The Law does not provide a definition of privacy or of 'undermining the State prestige' or any other contentious terms, while it elaborates in providing definitions for decisive technical terms. However, Decision No. 207, issued by the Minister of Communications and Technology on 10 May 2022 providing explanatory and executive instructions of the Law, included the following definition: "Individuals have the right to protect their personal, private or family secrets, correspondence, reputation, and activities online".

The problem in Article 21 is the same as Decree 17 which is that the right to privacy is an absolute right that has no exceptions, even in order to achieve other interests, such as when the information is true and there is a public interest justifying its publication, or if there is a professional obligation to publish it. Rather, publishing any information without consent from its owner is considered a crime, even if it is true.

Article 23 - Unlawful recording:

* "Whoever uses IT means to obtain video or audio recordings or take pictures of another person without their consent shall be punished by 1-6 months imprisonment and a fine of 500,000-1,000,000 SYP.

* The penalty provided for in Paragraph A of this Article shall be increased to 6-12 months of imprisonment and a fine of 1,000,000 - 2,000,000 SYP if the offense is committed against a public servant, either while performing their duties or as a result of such performance".

While Paragraph 'A' is not problematic since it requires the person's consent and approval to obtain audio or video recordings of them or taking their pictures, Paragraph 'B', which includes the same actions may provide protection for corrupt individuals, and restrict media work and investigative journalism, which rely on recordings and documents to expose corruption acts. The legislator decided that if the acts are committed against a public servant, either while performing their duties or as a result of such performance, they are subject to more severe punishment. This is while global legislations tend to consider privacy margin to be inversely proportional to the government function, i.e. the value of transparency outweighs the privacy of officials performing public duty, their margins of privacy are, therefore, narrow, especially when it comes to financial liabilities, income disclosure and accounting for any changes thereof.

Article 24 - Electronic defamation:

Article 24 tightens the punishments stipulated in Article 568 of the General Penal Code for the same offenses. It increased the minimum imprisonment period and repealed the authority granted to judges to choose one of the two punishments, i.e. imprisonment or fine, if the defamation is committed in public, according to the following:

* Whoever uses IT means to defame other people publicly online shall be punished by 1-3 months of imprisonment and a fine of 300,000-500,000 SYP.

* The punishment shall be increased to 3-12 months of imprisonment and a fine of 500,000-1,000,000 SYP if the defamation offense is committed against a public servant, either while performing their duties or as a result of such performance.

Article 24 of the Law imposed the punishment without distinguishing between types of employees. It used the term "public servant", which means any employee who works for a public legal person. While Article 376 of the General Penal Code stipulates one of the means specified in Article /208/[35] as punishment for defamation, which are: a maximum of one

35 The public means specified in Article 208 thereof are:

1. Acts and actions that happen in a public place or a location that is accessible to the public or exposed to public eye, or witnessed, due to the fault of the perpetrator, by a person who has nothing to do with the act.

2. Speech or screaming, either vocally or through an automatic tool, so that, in both cases, they are heard by those who has nothing to do with the act.

3. Writing, drawing, paintings, photographs, videos, icons, and symbols of all types if displayed in a public space, a location accessible to the public or exposed to public eyes, sold or displayed for sale, or distributed to one or more persons.

year of imprisonment if defamation targets courts, regulatory bodies, the military, public administrations, or a public servant for their role or capacity, and a maximum of three months of imprisonment and a fine of 100 SYP if defamation targets another employee for their role or capacity.

The legislator, therefore, has distinguished between two types of employees.

* An employee who exercises public authority, i.e. someone with the authority to issue orders and demand citizens to follow them, such as a mayor.

* An employee whose job is limited to following orders they receive. They cannot exercise public authority or issue enforceable orders, such as police officers, administrative officers, and registrars[36].

In addition, Article 377 of the General Penal Code stipulates that: "Except for the defamation of the President of the state, suspects[37] are to be discharged if the subject of the defamation is related to their duty and proved to be true", considering that public interest requires the exposure of any bad behavior exhibited by an employee in public administrations or institutions. In contrast, Article 24 of Law 20 did not consider the validity of the subject matter.

Article 25: Electronic libel or disdain

The Law treats libel and disdain as one offense despite their differences in terms of the criminal elements, punishment and the increase in minimum punishment. Overall, imposing severe punishments on defamation i.e., electronic libel and disdain raise questions about how much the legislator had considered the unique individual characteristics including age, experience, etc.

Article 27 - Offenses against the constitution:

According to Article 27: "Whoever creates or manages a website or a webpage, or publishes digital content, with the intention of triggering actions that aim to or call for unlawful change of the constitution, or the separation of a part of Syrian territory from the sovereignty of the State, or incitement of armed insurrection against the authorities appointed by the constitution, or preventing them from practicing their constitutional duties, or change or overturn the ruling regime, shall be punished by provisional detention from 7-15 years and a fine of 10-15 million SYP"

The Law here is severe in both the criminal elements and the punishments. The offense, according to the new Law, is considered committed once a website is created or managed, or digital content is created with the aim of changing the constitution or calling for doing so. While Article 291 of the General Penal Code stipulates that for a punishment of 5-year detention to be executed, an infringement must at least be committed with the aim of changing the constitution unlawfully. This cannot happen without conclusive evidence that the perpetrator has committed a concrete action towards committing the offense, and

36 Ministry of Higher Education, Syrian Virtual University, Mohammad Al-Omar PhD., Educational Legislations, Damascus, Syria.

37 A suspect: is a person whom the investigation judge is convinced to have committed a misdemeanor.

The accused: is a person whom the investigation judge is convinced to have committed a crime.

that this action aims to achieve the purpose specified in Article (291/1) of the General Penal Code, i.e. changing the constitution. A person who initiates this action is then subject to the punishment of the infringement in full, as if they have committed the crime fully. They are then punished only for the preliminary or initial actions that call for, or lead to, changing the constitution.

Law 20 also increases the punishment for the same criminal act. While it imposes provisional detention of 7-15 years for any person who creates or manages a website or webpage or creates online digital content with the intention of inciting actions that aim to separate a part of Syrian territory from the sovereignty of the State, Article 13 of Law 15 of 2022, amending Article 292 of the General Penal Code stipulates that: 3- Any Syrian who writes or sends correspondence calling for the separation or ceding of a part of the Syrian territory shall be punished by at least five years of imprisonment.

Article 28 - Undermining the state prestige

* Whoever uses IT means to disseminate false news online that could undermine the prestige of the state or compromise national unity shall be punished by provisional imprisonment of 3-5 years and a fine of 5-10 million SYP.

While Article 12 of Law 15 of 2022, amending Article 287 of the General Penal Code stipulates that:

* Any Syrian who knowingly disseminates false or exaggerated news that could undermine the prestige or status of the State shall be punished by at least six months of imprisonment.

With the absence of any clear definition of 'prestige' and 'undermining', the term remains ambiguous and subject to the discretion of judges, in clear contradiction to the principle of legality which is founded on the knowledge of the rules of criminalization and the acts that constitute an offense under the law. In addition, the criminal description of the act itself was changed; from 'demeanor' in the General Penal Code to 'crime' in Law 20. Moreover, Article 28 does not mention knowledge that the news being disseminated is false or exaggerated, rather, disseminating false news is considered a crime even if the suspect believes it to be true.

Article 29 - Undermining the financial status of the state:

* Whoever creates or manages a website or a webpage or creates online digital content with the intention of undermining, destabilizing or damaging trust in the national currency, or exchange rates as stated in official bulletins, shall be punished by provisional imprisonment of 4-15 years and a fine of 5-10 million SYP.

While Article 309 of the General Penal Code stipulates that:

* Whoever disseminates, using one of the means mentioned in Paragraphs 2 and 3 of Article 208, fabricated facts, or false allegations in order to undermine the national currency or damage trust in the State currency, bonds or any securities related to public financial confidence shall be punished by imprisonment of 6 months to three

years and a fine of (…).

In addition to changing the criminal description from 'demeanor' prescriptible within three years in the General Penal Code to 'crime' prescriptible within 10 years and increasing the maximum limit of the fine, Law 20 imposes a punishment merely for dissemination with no regard to the veracity of the news in question, while the General Penal Code which stipulates the news and allegation must be false and fabricated for the crime elements to be complete.

Article 32- Attempt

Attempts to commit the misdemeanors stipulated in this Law are punishable according to the provisions of the Penal Code.

In principle, attempts to commit misdemeanor should not be punishable without a specific legal provision. Punishment for attempt shall be the case only in crimes, and punishable misdemeanor attempts, and the punishments thereof must be specified. Since attempt is the initiation of an action with the intention to commit a crime or a misdemeanor that is terminated or rendered ineffective, attempt in information technology crimes with mere abstract behavior is inconceivable. The same is true for unintentional, passive, or accidental crimes. Therefore, the intention of the legislator for listing attempt for cybercrimes is not clear. This raises fears that attempt could be considered an additional pretext to violate freedom of expressions, and all freedoms in general.

Article 33 - Strengthening of punishment

**Punishment shall be increased pursuant to Article 247[38] of the Penal Code in the following cases:**

* If the perpetrator exploits their position or job to commit any of the crimes stipulated in the Law.
* If the victim in the crimes stipulated in this Law is a minor.
* If any of the crimes stipulated in other effective laws are committed using IT means.

The legislator transcends the exclusive aggravating reasons stipulated in Article 30 of Decree 17 of 2012[39] and increased the punishments for any criminal act if it is committed using technological means. This confirms that the Law closes the virtual space almost completely and criminalizes any forms of expression of opinion if it contradicts the narratives of the authority. The use of the internet or technology, therefore, is enough to increase the punishment by the third or half for dissemination crimes listed in Law 19 of 2012 on

38 Article 247 of the Penal Code: "The Law does not specify the effect of an aggravating reason; the said reason obliges the punishment to be increased as follows: the death penalty shall replace life hard labor. Each provisional punishment shall be increased by one third to a half, and a fine should be doubled».

39 Article 30: Punishments are increased pursuant to the provisions of Article 247 of the Penal Code in one of the following cases:

- If the crime subject undermines the state or public safety.

- If the crime was committed by an armed gang.

- If the crime targets a minor or a person in a similar capacity.

- If the perpetrator exploits their position to commit the crime.

counterterrorism, for example, or those listed in the Revolution Protection Law issued under Decree No. 6 of 1965, or Article 123 of the Military Penal Code, among others.

Article 35 - Online re-sharing shall be treated as own posts in terms of criminalization and punishment

The legislator gave no regard to the possibility of absence of criminal intent when content re-sharing is done unintentionally, or without scrutiny for example. The damage resulting from resharing is treated as equal to that of original posting, despite the difference in the strength and severity in their respective impact. The legislator also states that if a person reacts by resharing an online post whose content is considered a crime under this Law, they shall be treated the same way as the original creator of the post in terms of criminalization and punishment.

Article 40 - Initiation of public proceedings: The Public Prosecutor's Office has the discretion to institute proceedings against the public right unless such initiation is essentially restricted by established legislations.

In addition to problems posed by considering the Public Prosecution a judiciary body, even though Article 10 of the Code of Criminal Procedure provides that Public Prosecution should be subordinate to the Minister of Justice (executive authority), its competence to initiate a public right case is also problematic. The Public Prosecution is competent to file a public right case to the criminal court, and it shall initiate it and follow it through until its conclusion, according to Article 1 of the Code of Criminal Procedure. The Public Prosecution has no ownership of the case once filed with the competent courts. Rather, it shall only be a custodian thereof according to Article 1(3).

Therefore, after filing a public right case, the Public Prosecution may not waive, renounce or reconcile with the defendant whatever the reasons or conditions, as this is in contradiction with the Guidelines on the Role of Prosecutors adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990. Article 18 of these Guidelines stipulates that diversion schemes should be explored instead of legal proceedings and that "prosecutors shall give due consideration to waiving prosecution, discontinuing proceedings..."[40]

It should be noted that, in addition to the discretionary power granted to the Public Prosecution to initiate public proceedings, it is compelled to initiate it if the victim appoints himself/herself as a personal plaintiff in accordance with the provisions of the Law (Article 1/2 of the Code of Criminal Procedure). Under the Law, every affected citizen may submit a petition to the Public Prosecution in his/her area of residence explaining what they have been subjected to, attached with a screenshot of the libel, slander, or extortion, which the Public Prosecutor's Office will in turn divert to the Criminal Security Department, Cybercrime Branch. The Branch in turn engages experts from the Ministry of Defense, Ministry of Justice and Ministry of Communications and Technology to carry out investigations. After identifying the wanted person, a warrant is issued against them, and it is referred back to the Public Prosecutor's Office which received the case in the first place, and then to court.

40 the Guidelines on the Role of Prosecutors adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990

## No Immunity for Media Professionals

The Law has been arbitrarily used to target media professionals, internet activists, citizens and any critical voice. Many basic cyber rights of citizens were denied, especially the right to freedom of expression and digital privacy. This has been compounded by dominance of the executive authority and the Minister of Justice on the judiciary, which is supposed to be the guarantor of freedoms, regardless of the nature of the legal text since the constitution has entrusted the judge's conscience with the proper implementation of the law. Charges against journalists or activists varied, including insulting the judiciary, undermining the prestige of the State, communicating with suspicious pages, or even individual complaints by influential people affected by the publication, or whose roles were criticized. Publication here refers to anything published on media platforms or posted on social media.

For example, during last year:

* Journalist Hala Al-Jurf was arrested in late January 2021 under the Cybercrime Law for violating the rules of publishing on social media and was later released by the presidential pardon of May 2021.

* Journalist Wadah Mohieddin was arrested in mid-January 2021 by the Cybercrime Division of the Criminal Security Branch in Aleppo and transferred to Damascus, due to Facebook posts. He was also released by the presidential pardon of May.

* Journalist Kenan Waqqaf was arrested on 7 March 2021 from "Al-Wahda" newspaper offices in Tartus governorate for writing a Facebook post in which he talked about a kidnapping for ransom carried out by the son of the governor of Al-Hasakah, Major General Ghassan Khalil. He remained in detention until the presidential pardon of May was issued. This was Waqqaf's second arrest. He was previously arrested in September 2020 for resharing[41] on his Facebook page an investigative journalistic report he had carried out and was published on Al-Wahda state newspaper.

As a result of the overlap between the work of the different agencies, the non-compliance with the Code of Criminal Procedure in terms of arrests and investigations, and the response by the information Branch to cases that are not related to cybercrime, especially involving media professionals and publication offenses, all have made it more challenging to monitor and document arrests, detentions, or abuse cases against media professionals and activists that are carried out pursuant to Law 20, and also makes it challenging to distinguish these crimes from other crimes such as those listed in the Media Law No. 18 of 2012, under an almost complete absence of the right to access information. Although the Cybercrime Law holds media professionals accountable, as citizens, when they post on social media, and leaves the matter of holding them accountable for issues related to their media outlets to the Media Law, all cases or allegations related to publication, whether on media platforms or digital media, were reverted to the Information Branch.

41 Kenan Waqqaf, the Journalist who Criticized Al-Assad's Negligence and was Abandoned by Colleagues. Enab Baladi

Media Law No. 108 of 2012 included the following cybercrimes:

1. Publication prohibition crimes: Article 12 prohibits media platforms from publishing any content that could provoke sectarian strife or incite crime. It also prohibits publishing any content related to the military and armed forces, unless already issued or allowed by the armed forces themselves, and anything that undermines any national symbols. The Media Law also imposes the punishments stipulated in the applicable laws, in addition to suspending the outlet work for at least three months and revoking its license if the violation is repeated.
2. Abuse of personal privacy: Article 13 of the Media Law prohibits media professionals from attacking the private lives of individuals or violating their privacy. Article 80 of the Media Law punishes whoever violates the aforementioned Article 13 by the applicable punishments. Therefore, Article 21 of Law 20, which is concerned with violating private life, is the applicable law, and the punishment is 1-6 months of imprisonment and a fine of 500,000-1,000,000 SYP.
3. Electronic libel and defamation:

Since the scope of Law 20 expands to cover crimes committed online regardless of the means, it is, therefore, the general law governing cybercrimes. The Media Law issued by Decree 108 of 2011, however, is the special law applicable for cybercrimes related to the media, pursuant to Article 180 of the General Penal Code, which stipulates:

"If a general and a special text both apply to a certain action, the special text shall be applied". However, Law 108 does not provide any immunities to media professionals from prosecution and legal action under Law 20, and it disregards the safeguards listed in Article 101 thereof: "A media professional may only be arrested or interrogated in the presence of a representative of the Journalists Union in all acts that constitute crimes that the media professional commits during the performance of their duties, except in cases of flagrante delicto," because for it to be active, it requires that the media website be an actual professional one (with administrative license), and be run by a legitimate media professional. Social media pages and personal accounts of media professionals are subject to the Cybercrime Law. This way, the legislator deprives media workers from their professional status when they are not on duty. In practice, media professionals were prosecuted without any immunity using Decree No. 17.

The following cases have been documented on violations related to cybercrime law or handled by the Cybercrime Branch, whether against journalists (whose cases are supposed to be addressed under the Media Law), or social media activists (the Cybercrime Law):

* Five security summons cases were documented: one by an unknown security branch, and four by the Cybercrime Branch.
* Five arrests were recorded: one by an unknown security branch, and the rest by the Cybercrime Branch.
* Considering the type of violation, arrests were the largest category: 16 journalists and Facebook activists were arrested. Some of the cases reached courts. Two journalists

were trialed:

* Ammar Al-Azzo, head of the Press Bureau in Aleppo governorate and SANA reporter. He was charged with corresponding with an unknown page that publishes corruption cases related to several officials.

* Journalist Amer Drao, a journalist in Al-Madina Radio in Aleppo, Hashtag Syria website, Al-Nour Radio, and Al-Manar Channel. He was arrested due to a claim by Hilal Hilal, Assistant Secretary General of Al-Baath Party that the journalist was "weakening the resolve of the nation and national sentiment".

## Recommendations

The Syrian Government must respect its international commitments, especially in regard to:

* Respect Article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression"; and commitment to Article 19 of the International Covenant of Civil and Political Rights when passing any legislation or regulation that contains restrictions on freedom of expression.

* Fulfill its obligations to provide open, secure, and affordable and steady internet connection as one of the basic human rights, which include, in addition to the right to freedom of expression and media rights and freedoms, the rights to peaceful assembly, establishment of associations, access to information, and exchange of ideas, especially when no other alternatives are available.

* Suspend Law 20 of 2022 and end any criminal prosecutions related to exercising the right to freedom of expression.

* Form a committee of experts to draft a new law on online communication that adheres to international standards, including removing restrictions off the Criminal Code on freedom of expression and limit punishments to in financial fines, in addition to reviewing the penal laws governing publishing and expression in Syria.

* Remove the offences of libel, defamation and disdain from the Penal Code, classify them as civil offences, and clearly specify what constitutes prohibited conduct.

* Acknowledge the right to access and use the internet as a human right and a prerequisite for exercising the right to freedom of expression. Refrain from imposing internet disruptions and shutdown. Work to provide complete affordable access to the internet.

* Take immediate and targeted action to protect the safety of journalists and any persons who are attacked for exercising their right to freedom of expression, address any attacks on them, and put an end to impunity for such attacks.

* Immediate and comprehensive release of all those arrested or sentenced for exercising their right to freedom of expression, whether online or otherwise, and ensure that their sentences are removed from their judicial records.

* Take immediate and long-term steps to prohibit illegal or arbitrary surveillance, provide strict legal safeguards to guarantee the privacy of electronic communications, and prohibit surveillance of e-mails or other forms of electronic communication, except on an individual scale with the permission of an independent court based on compelling evidence that suggests actual criminal activity.

* Adopt a legislation that provides protection for data privacy, is consistent with the relevant articles of the Constitution, and absolutely prohibits individuals, companies or security services from viewing or analysing packages of data unless warranted by a competent court.

* Provide due protection for and guarantee the right of citizens to peacefully advocate for change, criticize the government or its policies, and any of the three authorities and their symbols, or officials; and completely refrain from attaching liability on the dissemination of information, especially that related to alleged human rights violations.

* Allocate budgets and invest internet revenues in expanding information technology and communications reach. These funds should not be used to improve surveillance and monitoring systems.

* Develop and strengthen Syria's relationships with foreign law enforcement agencies, and international anti-cybercrime institutions and organizations, and adhere to international laws in this field.

* Counter hate speech through legal and regulatory provisions that ensure everyone has safe and secure access to social media and the ability to express themselves with no risk of discrimination, racism, violence, or hostility.

* Civil society organizations and independent experts should conduct a comprehensive study on digital freedoms in Syria that covers risks to online freedom of expression and helps to expand the scope of internet beneficiaries. The study should develop a comprehensive vision of the independence of digital broadcasting bodies and protect them against the control of the executive authority.