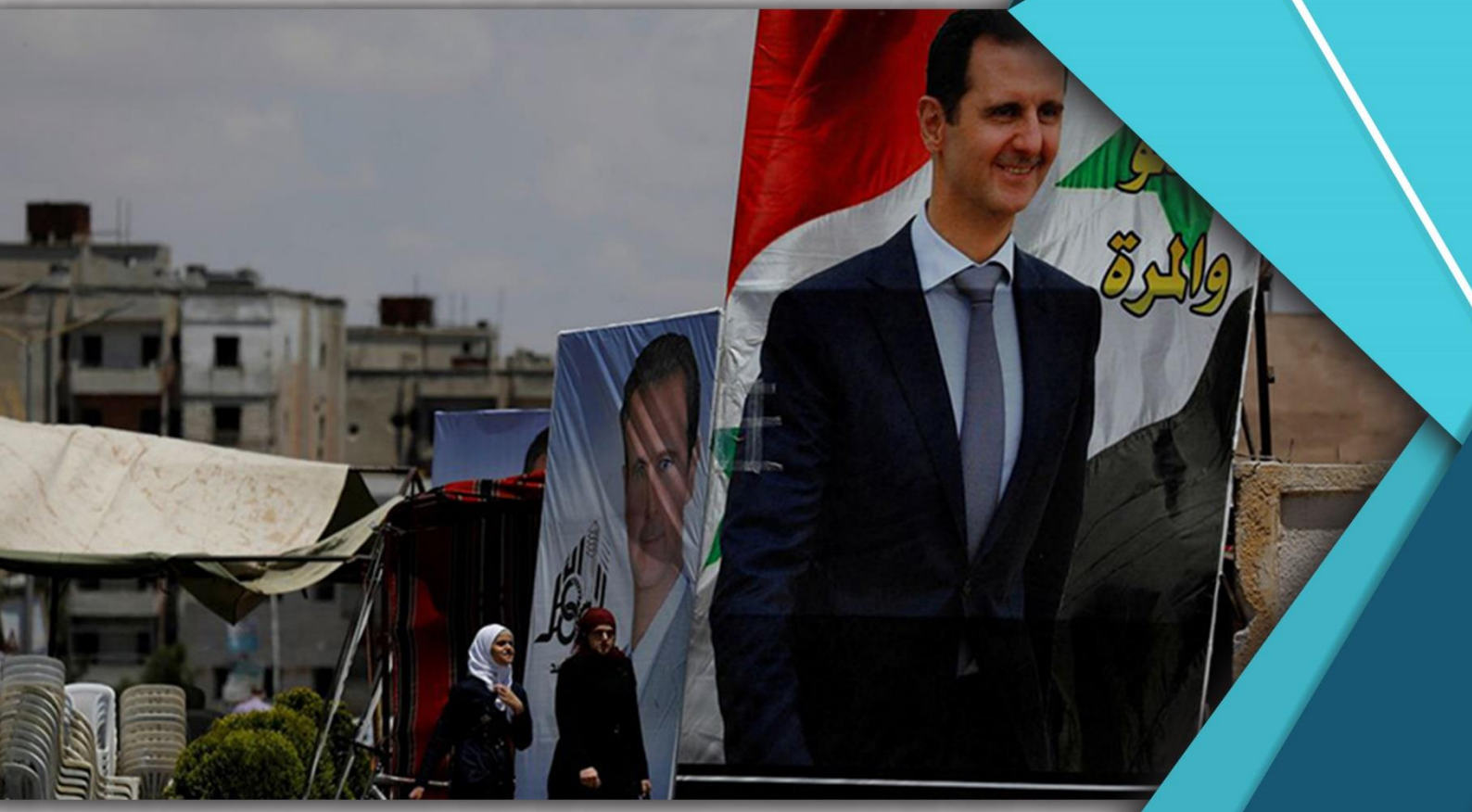
Syria: Cybercrime Law is an Additional Tool for Suppressing Freedom of Expression



سوريون من أجل الحقيقة والعدالة

Syrians For Truth & Justice

14 June 2022

Syria: Cybercrime Law is an Additional Tool for Suppressing Freedom of Expression

The new 2022 Cybercrime Law overlaps with other laws, notably Syrian Penal Code amendments, increasing the ambiguity of already vague laws

On 18 April 2022, Syrian President Bashar al-Assad issued Law No. 20 of 2022, relative to cybercrime. The law provides for reorganizing criminal legal rules governing digital crime included in Legislative Decree No. 17 of 2012. The target degree frames the enforcement of the provisions of the Law of Network Communication against Cybercrime.

The Syrian legislative authority commented on the law's timing, saying the law responds to peaking rates of cybercrime within the Syrian community due to technical and technological progress. Therefore, the law was issued to protect legal interests, regulate freedoms in cyberspace, and limit "misuse of technology."

Additionally, the legislative authority claimed that Law No. 20 reframes the legal concept of cybercrime, stretching its scope to include various forms of criminal behavior related to information and information systems.

Groundwork for Law No. 20

Four months before Law No. 20 went official, *al-Watan* newspaper, close to the Syrian government (SG), published leaks on draft amendments to the Cybercrime Law No. 17 of 2012, now repealed.

The leaked information includes potential tightening of penalties against crimes committed online, including those perpetrated on social media platforms, and an increase in corresponding fines up to 10 million Syrian pounds (SYP). These stricter punitive measures were effectually established in law No. 20.

Ahead of the *al-Watan* leaks, Colonel Louay Shalish, head of the Cybercrime Combating Branch within the Ministry of Interior, on 24 October 2021 told state-run *Syrian Arab News Agency* (SANA) that the ministry had organized over 1,200 cybercrime reports since early January 2021, and arrested 160 people. Most of the persons arrested committed crimes of online fraud, extortion, slander, and defamation.

Shalish highlighted that cybercrimes verging on "undermining the prestige of the State," insulting national symbols, public administrations, the judiciary, or an employee exercising public authority amount to crimes punishable by law. He added that the judicial police will address crimes of this character with the knowledge of the public attorney in the concerned province

Legal experts with Syrians for Truth and Justice (STJ) believe that one of the key reasons that prompted the SG to issue Law No. 20 is the intense wave of criticism and cynicism that had recently swept social media, lashing against all levels of government administration, including the prime minister, ministers, employees, etc. This crushing wave of ridicule corresponds to acute deterioration in living standards, amidst the SG's failure to meet citizens' basic needs in their areas of areas. In addition to a low supply of vital commodities such as bread, there has been a shortage of a wide range of services, including electricity, water, healthcare, and public transportation.

What is Cybercrime Law No. 20?

Article 1 of Law No. 20 broadened the scope of cybercrime definition, bringing under its mantel all forms and patterns of shared digital content, including posts and footage uploaded onto social media. The law comprises 50 articles which aim to re-establish new criminal legal

principles for the concept of cybercrime, previously encompassed by Law No. 17 of 2012, known as the Law of Network Communication against Cybercrime.

In addition to the new definitive and updated criminal scopes, Law No. 20 levels unsparing fines against crimes in cyberspace, which complement the penalties and the growing threat they pose to individual freedoms. The law's fines are harsher than those established in the Penal Code. Law No. 20 pushed incarceration periods to sentences ranging from one month to 15 years, and fines ranging from 200,000 SYP to 15 million SYP.

Law No. 20 of 2022 entered into force on 18 May 2022, working by its 50th Article, which stipulates that: **"This law shall be published in the Official Gazette, and shall be effective one month after its issuance."**

Based on the wider criminal scopes the law propagates, legal experts with STJ believe that "digital content" in Article 1, will probably be used to cover posts on social networking sites, comments on a user's personal posts, comments on other users' posts, or re-publishing the shared contents, posted by individuals or pages.

The new law equates publishing and re-publishing in terms of criminalization and punishment, in keeping with Article 35. The article states that: **"Online republishing amounts to [first-hand] publishing in terms of criminalization and punishment."**

Therefore, Law No. 20 stretched the powers of the executive authority over additional target segments of Syrian citizens, robbing them of freedom of expression in all modes of writing. This is a violation of Article 42(2) of the operative 2012 Syrian constitution, which guarantees the following: **"Every citizen shall have the right to freely and openly express his views whether in writing or orally or by all other means of expression."**

Notably, the definitive aspects highlighted in Article 1 of Law No. 20 expanded the scope of target crimes in an overbroad manner because it functions against all Syrian citizens using social media, without pinpointing the bases of criminalization.

Manipulating Definitions

As an update to the repealed Law No. 17 of 2012, the definition of cybercrime in Law No. 20 of 2022 provides a looser frame, which the SG can bend in various ways to prosecute Syrian netizens for any content they share on social media, regardless of the content's nature.

Article 1 of Law No. 17 defined cybercrime as any crime committed using a computer or the internet, or that occurs against information systems or the network.

In Law No. 20, however, Article 1 defines cybercrime as criminal behavior in accordance with the provisions of this law, committed by means of information technology, targeting information or information systems, and including the act of sharing content online.

Expanding the definition to the act of content sharing demonstrates that the SG intends to further diminish already narrow spaces of expression, including online ones, such as Facebook, which citizens use to voice their anger at the underperformance of the current government.

Criminalized by this definition, digital activity opens new doors for repression. With the inclusion of "social media shared content", the SG expands the practices of policing to online environments, using the definition to legally prosecute a larger number of critics of government administrations, including executive authorities.

Types of Crime under Law No. 20

Law No. 20 of 2022 aggregates cybercrimes into two categories: A. traditional cybercrimes and B. cybercrimes against the State internal security.

A. Traditional cybercrimes target people. Articles 30 and 31 list these crimes as legal fraud, violation of privacy, digital defamation, publishing illegal audio or video recordings without the consent of the owner, data theft and crimes related to the smart card.

The smart card is a system through which Syrian citizens use cards to purchase rationed SG subsidized goods, such as bread. Cards are used by individuals and families, determining their monthly shares of goods available through the system.

B. Cybercrimes against the State internal security, also labeled as nontraditional, are listed in articles 27, 28, and 29. They cover acts that target the constitution, undermine the prestige of the State, or its financial standing, and insult religions, or religious sanctities and rituals.

Notably, the nontraditional crimes, or those targeting internal security, are novel in the online context, because they did not exist in the repealed Law No. 17 of 2012.

However, these crimes, particularly undermining the constitution, the state prestige and its status, are established in the Syrian Penal Code No. 148 of 1940, as well as its amendments, stipulated by Law No. 15 of 2022, issued on 28 March 2022.

In that sense, committing these crimes online amounts to aggravating circumstances.

Shortcomings of Law No. 20

One of the law's major defects lies in the deep convergence between its provisions and the crimes it addresses and those subject to other laws, particularly amendments to the Penal Code. The amendments are established in Law No. 15 of 2022, across articles 9 to 14. Notably, the conflation of these two legal frames adds an extra layer of ambiguity to the ambivalence dominating the structures of Syrian laws, which are inseparable in various ways, and are conflicted at times.

The Syrian legislator, when drafting the law, should have limited the scope to combating crimes involving information, online infiltration, hacking or sabotaging information systems, breaching, stealing, or publishing personal data and information without permission, and electronic fraud, such as e-document forgery.

The legal experts believe that crimes such as undermining the prestige or financial status of the State, or insulting religions, or religious sanctities and rituals, should not have been integrated into the law on the pretext that they are perpetrated using technology. This mesh will render the applications of these laws more complex because the same criminal behavior falls under the mantle of various legal frames, each with different sets of penalties and fines. This multiplicity of punitive frames will pose challenges for both judges and defense lawyers, who will suffer under the weight of legal interpretation of available texts. Interpretation difficulties will affect disharmony with the spirit of justice and equity, as well as lead to incompatibilities in the application of the law.

Therefore, crimes against the constitution, or ones related to State prestige, religions, and drugs which are committed in cyberspace naturally fall under the Penal Code, which indeed

addresses them. The Penal Code is the applicable law regardless of the fact that these crimes were perpetrated using information technology or high-tech products.

Along these lines, STJ's legal experts pose the following question, why did the SG opt for tightening its legal grip by citing the same crime in two legal frames, as well as doubling the sentences and fines leveled against citizens taking to social media to express their minds?

Relating to the legal dimension, the experts also ask, what purpose underlies issuing new definitions that only serve to inflate the vagueness and unintelligibility of existing laws, not to mention their conflicting stances?

Laws No. 20 and No. 15: Similarities and Differences

A. Crimes Against the Constitution

Syrian General Penal Code No. 148 of 1949, and its recent amendments in Law No. 15 of 2022	**Cybercrime Law No. 20 of 2022**
Crimes against the constitution—Article 291 targets those who perpetrate: An assault aimed at changing the State constitution by illegal means shall be punished.	Crimes against the constitution—Article 27 targets: Anyone who establishes or manages a website or a web page or publishes digital content online with the intent of provoking acts aiming at or calling for changing the Constitution by illegal means or excluding part of the Syrian land from the sovereignty of the State or provoking armed rebellion against the existing authorities under the Constitution or preventing them from exercising their functions derived from the constitution, shall be punished.
Penalty	
Temporary imprisonment for no less than five years. The penalty shall be life imprisonment if the perpetrator resorts to violence.	Temporary imprisonment from seven to fifteen years.
Fine	
500,000 SYP. The maximum fine was amended to one million SYP.	Between 10 to 15 million SYP.

B. Undermining the Prestige of the State

Syrian Penal Code No. 148 of 1949, and its recent amendments in Law No. 15 of 2022. **Amendments to Article 287**	**Cybercrime Law No. 20 of 2022**
Undermining the prestige of the State and compromising national and [Arab] identity—Article 10 targets: (Every Syrian, who is informed of the act's repercussions, and still disseminates false or exaggerated news that undermines the prestige or status of the State . . .). Syrians are liable to punishment regardless of their location.	Article 28: Undermining the prestige of the State—Article 28 targets: Anyone who publishes false news online using information technology means that undermines the prestige of the State or prejudices national unity. Syrians and non-Syrians are liable to punishment
Penalty	
Imprisonment for no less than six months.	Temporary imprisonment from three to five years
Fine	
Amending minimum criminal fines in the General Penal Code and all other legislation to 500,000 SYP and amending the maximum fine limit to one million SYP (Article 5).	Between five to 10 million SYP.

C. Prejudicing/Undermining the (Financial) Standing of the State

Amendments—Article 12 of Law No. 15 of 2022, amending Article 287 of the Syrian Penal Code No. 148 of 1949	**Cybercrime Law No. 20 of 2022**
Undermining the standing of the state—Article 12 targets: Any Syrian who spreads news that enhances the image of a hostile State to undermine the status of the Syrian State shall be liable for the same penalty.	Undermining the financial standing of the State—Article 29 targets: Whoever establishes or manages a website or a web page or publishes digital content with the intent of causing decline, instability, or undermining confidence in national banknotes or their exchange rates specified in official publications.
Penalty	
Imprisonment for no less than six months.	Temporary imprisonment from four to fifteen years
Fine	
Amending minimum criminal fines in the General Penal Code and all other legislation to 500,000	Between five to 10 million SYP.

SYP and amending the maximum fine to one million SYP (Article 5).	

D. Awakening Racial and Sectarian Strife/ Insulting Sanctities

Article 10 of Law No. 15 of 2022, amending Article 287 of the Syrian Penal Code No. 148 of 1949	**Cybercrime Law No. 20 of 2022**
Awakening racial and sectarian strife—Article 10 targets: Whoever in Syria during wartime or anticipation of its outbreak made calls aimed at compromising national or [Arab] identity or awakening racist or sectarian strife	Offending a religion, religious sanctities, or rituals—Article 31 targets: Whoever establishes or manages a website or a web page or publishes digital content online with the intent of offending a religion, religious sanctities or rituals, inciting hatred or inciting violence.
Penalty	
Imprisonment for no less than six months	Temporary imprisonment from three to five years
Fine	
500 ,00 and amending the maximum fine to one million SYP (Article 5).	From three to 10 million SYP

Figures on Cybercrime

Damascus Province

In cooperation with an organization operating in SG-held areas, anonymized for security reasons, STJ carried out a field study documenting the number of cybercrimes recorded between January 2018 and December 2019, in Damascus province.

Notably, Law 17 of 2012 was still in force during the interval covered by the study.

During the study's time scope, nearly a year, approximately 800 cybercrimes were pending before the specialized cybercrimes court (it falls under the jurisdiction of a special court in Damascus). The number includes cases that were in progress from previous years, and those re-coded for 2019.

A final verdict was issued in half of these cases, namely 400 cases. Most of these cases fall under traditional online crimes, which registered the following rough percentages:

Traditional crimes:

1. Online defamation or slander, insulting a public official, or violating public morals, amounted to nearly **25%, making 200 cases**.
2. Online intimidation, threat to inflict undue harm, threat to disclose secrets or information that undermines a person's dignity and honor, and impersonation amounted to nearly **27%, making 216 cases**.
3. Miscellaneous crimes (online incitement to debauchery, sending indecent images, publishing information that weakens the nation's resolve, advertising pornographic content/committing and inciting debauchery, amounted to nearly **7%, making 56 cases.**
4. Insulting the President of the Republic or the Prime Minister amounted to **1%, making 8 cases.**

Rif Dimashq (Damascus Countryside) province

Since early 2019, the specialized cybercrimes court in Rif Dimashq (Damascus Countryside) province presided over nearly 235 cases, including both cases in progress from previous years, and those recently brought before the court. Most of these cases fall under traditional online crimes, which registered the following rough percentages:

1. Defamation, slander, smear, cursing and swearing amounted to nearly **23.3%, making 55 cases.**
2. Intimidation and threats amounted to nearly **18.5%, making 43 cases.**
3. Breaching public ethics and morals amounted to nearly **21.6%, making 51 cases.**
4. Provoking sectarian strife amounted to nearly **1.3%, making 3 cases.**
5. Insulting a public official, a judicial authority, or a public administration amounted to nearly **4%, making 9 cases.**
6. Blackmail amounted to nearly **11%, making 26 cases.**

Services Presiding over Cybercrime

In theory, the Judicial Police—criminal security branches and police departments affiliated with the Ministry of Interior—have general jurisdiction over cybercrimes. The Judicial Police has a set of competencies, including functions and controls exercised depending on the nature of circumstances, whether normal or exceptional. In normal circumstances, they carry out criminal investigations, collect evidence, receive notifications and complaints, and organize records and reports, among other tasks.

However, the Judicial Police often stretch their powers, performing the functions of an "investigating judge", carrying out actions such as arresting perpetrators, conducting searches, and seizing objects found during these searches. With this, the police infringe on the powers of the judicial authority.

The duties, jurisdiction and powers of the Judicial Police are established in Law No. 20 of 2022 in Article 38, which states:

A. A Judicial Police, within the Ministry of Interior, shall be established to substitute the Judicial Police established under Legislative Decree No. 17 of 2012. The Judicial Police specializes with:

1. Investigating cybercrimes.
2. Collecting digital evidence.
3. Arresting perpetrators of these crimes, after obtaining a permit from the Public Prosecutor, and referring perpetrators to the competent judiciary.
4. Seizing technological means, used in committing one of the crimes established in this law, or one of their components, after obtaining a permit from the Public Prosecutor.
5. Inspecting information technology means and software, wherever they are, after obtaining a permit from the Public Prosecutor and seizing them in accordance with the rules stipulated in the Code of Criminal Procedure.

B. The judicial police shall seek the assistance of permanent or temporary experts to carry out the tasks assigned.

In practice, SG-affiliated security services will most likely play a major role in investigations, home raids, and arrest of "suspects", and probably extracting confessions from detainees under torture, especially in cases of crimes related to internal security or "terrorism".

Crimes related to internal security, or those labeled as "terrorist" are classified as "above the law". Under such classification, the judicial authorities, the investigative or referral judges, cannot reach out to defendants, which denies the defendants the chance to challenge security services decisions or appeal them.

Another factor that plays into repression is that security services are immune to prosecution for crimes committed by their members while carrying out their duties, according to Decree No. 14 of 1969 establishing the General Intelligence Directorate, also known as the General Security Directorate.

Security services retained their role in combating cybercrime even when the Syrian interior minister had issued Decision No. 564/s on 22 March 2012, which provided for establishing the Anti-Cybercrime Department, under the Directorate of Criminal Security.

Additionally, the department, now dismantled by virtue of Article 38 (a) of Law No. 20, was also assigned a judge to preside over its activities. On 29 March 2012, the Minister of Justice issued Resolution No. 5413,[1] which named a judge as a representative of the Ministry of Justice.

However, even in the presence of the judge, evidence was lacking as to the judiciary's ability to monitor potential violations by the department.

Controversies of Cybercrime Reporting and Investigation Mechanisms

In the case that someone needs to report a cybercrime, they can choose to refer to either the nearest police station or the Public Prosecution to file a complaint or report an online offense, or submit information through phone, email, or a form available online.

[1] Tariq al-Khin. *Cybercrimes*. Damascus, Syrian Virtual University, 2018. Page 123. https://pedia.svuonline.org/

While any person can report cybercrime through phone, email, or the available online form, a complainant (the victim) can also choose to refer to either the nearest police station or to the Public Prosecution to file a complaint or report an online offence.

Investigations are then handled by the Judicial Police, who search and inquire into perpetrators, based on a complaint or report, collect evidence, identify the perpetrators, and arrest them, as entailed by Article 38 of Law No. 20.

The process of investigation, however, remains dangerously controversial. The controversy is of two-fold and pertains to the law itself.

First, the law established definite measures neither for investigation nor for evidence collection. This warrants the members of the Judicial Police to use all methods to investigate a crime.

Without an order from their superiors, police members can camouflage, impersonate, and hire informers. Informers would enable police/security services to espionage on people, through joining chat rooms, using fake handles, and then reporting information to concerned authorities.

The second is that the law entitles the Judicial Police to carry out "electronic investigation" or exercise "electronic surveillance" against suspects, monitoring all their online activities, including emails.

Even though paragraph 4 of Article 38 obliges the Judicial Police to obtain permission from the judicial authority—public prosecution and investigative judges— investigations are mostly carried out outside the wake of the law and without informing prosecutors, especially in cases that supposedly jeopardize state security. This allows the Judicial Police or security services to spy on people's accounts under the pretext of suspected cybercrimes.

Spaying is a violation of the law, deriving this status through comparability to breaching the sanctity of home and disclosure of secrets, established in Articles 557, 5558, 565, and 567 of the Syrian Penal Code. In addition to investigative controversies, Article 38 of the law offers the Judicial Police no fewer problematic powers when it comes to search measures. Searching is originally within the jurisdiction of the primary investigation authority (the judicial authority), as established by Articles 90 to 95 of the Code of Criminal Procedure. However, Article 38 exceptionally brings those measures under the jurisdiction of the Judicial Police (executive authorities), who are permitted to search computers, their attached components and applications, regardless of their location, whether inside or outside Syria.

Conclusion

On 7 April 2022, STJ published a report analyzing Circular No. 3 of 2022, issued by the Minister of Justice and relative to pre-trial detention in the specific context of cybercrime. Based on the analysis, STJ predicated Cybercrime Law No. 20 of 2022 and deduced the following:

1. The authorities will use overly broad sentences to prosecute SG detractors for crossing the line between freedom of expression and violation of rights. The line lacks a clear and all-encompassing definition in the to-be-issued law.
2. The authorities will use terms that lend themselves to various interpretations and have no root determinants, or clear definitions. The authorities could easily use terms related

to "public interest" to frame social criticism as violating this interest. These terms thus become new repression tools to crack down on SG critics.

3. Leaks about the amendments to the cybercrime law are an alarming reminder of the hundreds, and maybe thousands, of arbitrary arrests witnessed in Syria before 2011, which were perpetrated by the verdicts of the exceptional Supreme State Security Court (SSSC) and similar sweeping arrests warranted later by the Counter-Terrorism Court (CTC). Residents of government-held areas see in the impending amendments on the cybercrime law an equal danger, threatening to consider any divergence from the government's perspectives and any non-compliant opinion posted online fake news that amounts to the felony of "undermining the prestige of the State and national unity."

4. Legal experts with (STJ) believe that the SG intends to pass a new and tighter version of the Cybercrime Law, which explains the leaks and media discussion. The leaks are a buffer to mitigate the expected acute reactions the law would give rise to among an already inflamed Syrian public. Additionally, the experts stressed that the draft law, should it be ratified, would pose a threat to the almost non-existent freedom of expression in Syria.

With the law, the government is sending a direct and clear message to citizens that courts shall prosecute any person who would dare to express a non-standard opinion whether writing it online, exchanging it as a message, or telling it as a mere joke. The threat of the law gains more momentum when viewed within the recently rising popular criticism of the government's performance and failure to provide basic necessities, curb extreme price increases, or address wide-spreading poverty among people in its areas, who are facing multiple living challenges and difficulties to secure heating fuel amidst continued power blackouts.

سوريون من أجل الحقيقة والعدالة
Syrians For Truth & Justice

About Us:

Syrians for Truth and Justice (STJ) is a nonprofit, nongovernmental organization monitoring human rights violations in Syria. Founded in 2015, STJ has been based in France since 2019.

STJ is an impartial and independent Syrian human rights organization operating across Syria. Our network of field researchers monitor and report human rights violations occurring on the ground in Syria, while our international team of human rights experts, lawyers, and journalists gather evidence, examine emerging patterns of violations, and analyze how violations break domestic Syrian and international law.

We are committed to documenting violations of human rights committed by all parties in the Syrian conflict and elevating the voices of all Syrians victimized by human rights violations, regardless of their ethnicity, religion, political affiliation, class, and/or gender. Our commitment to human rights monitoring is founded on the idea that professional human rights documentation meeting international standards is the first step to uncovering the truth and achieving justice in Syria.

WWW.STJ-SY.ORG

STJ_SYRIA_ENG

EDITOR@STJ-SY.ORG