S260608

SNHR
الشبكة السورية لحقوق الإنسان
SYRIAN NETWORK FOR HUMAN RIGHTS

Statement

The Syrian Network for Human Rights Calls for Reviewing the Cybercrime Law and Ensuring it is Not Used to Restrict Freedom of Expression

Monday 22 June 2026

The Syrian Network for Human Rights (SNHR), founded in June 2011, is a non-governmental, independent group that is considered a primary source for the OHCHR on all death toll-related analyzes in Syria.

Damascus - The Syrian Network for Human Rights (SNHR) calls for a review of the Cybercrime Law No. 20 of 2022 and of its enforcement mechanisms, particularly in cases related to digital content and to freedom of opinion, expression, and public debate, in a way that ensures its harmonization with the Constitutional Declaration issued on 13 March 2025, with the international human rights standards, and with the principles of legality, necessity, proportionality, and effective judicial oversight.

SNHR affirms that combating cybercrime and protecting digital security are two legitimate aims that don't conflict with protecting freedom of expression, the right to privacy, and fair-trial guarantees, so long as the legal provisions are precise and clear, and are applied within a narrow and proportionate scope, in a way that prevents the use of penal criminalization to restrict peaceful expression or to limit legitimate civic participation in public affairs.

On the evening of Wednesday, 17 June 2026, the Internal Security Forces affiliated with the Ministry of Interior in the Syrian government arrested the content creator Hassan Akkad in the city of Damascus. According to information obtained by SNHR, and based on the press statement issued by the Public Prosecutor in Damascus on 18 June 2026, the arrest came against the background of a legal complaint relating to charges of defamation, slander, and libel via the electronic network, after the claim was studied by the Public Prosecution specialized in cybercrime, and was referred to the competent authorities to complete the investigations in accordance with legal procedures. On Sunday, June 21, 2026, SNHR have documented the release of Hassan after the withdrawal of the complaint against him.

While adjudicating individual incidents and determining legal responsibilities remains within the jurisdiction of the competent judicial authorities, SNHR affirms that this incident, and the context of applying the Cybercrime Law in cases related to digital content, raise serious concerns about the dividing lines between cybercrimes that affect systems, data, and digital security on the one hand, and acts associated with freedom of opinion and expression, peaceful criticism, and the circulation of information across the digital space on the other hand.

Without asserting at this stage the nature of the content subject to the complaint, or the extent to which the penal provisions apply to it, SNHR believes that the case highlights the need for a legislative and procedural review that ensures the scope of the Cybercrime Law isn't expanded to cover patterns of peaceful expression or public debate, and that custodial measures aren't resorted to except where there are specific, necessary, and proportionate legal justifications, subject to effective judicial oversight.

SNHR had previously issued a legal study on Law No. 20 of 2022, in which it concluded that a number of its articles contain broad terms that aren't precisely defined, which raises problems related to the principle of criminal legality, a principle that requires offenses and penalties to be clearly defined and foreseeable. The importance of this principle increases in cases related to freedom of expression, because legislative vagueness may in practice lead to expanding the scope of criminalization and to creating a chilling effect that drives individuals to refrain from expressing their opinions for fear of legal prosecution.

The problem isn't limited to the legal provisions themselves, but rather extends to their enforcement mechanisms. The international standards related to the right to liberty, the presumption of innocence, and fair-trial guarantees require that pretrial detention remain an exceptional and reasoned measure, built on a specific individual necessity, and subject to effective and prompt judicial review. They also require guaranteeing the right of the person subject to prosecution to know the reasons for the arrest, to seek the assistance of a lawyer from the earliest stages of the investigation, to review the evidence submitted against him in accordance with the law, and to challenge the procedures and decisions issued against him.

The proper application of the law also requires clearly distinguishing between cybercrimes that target systems, networks, and data, or the digital privacy of individuals, or that involve fraud, extortion, or electronic hacking, and cases related to expressing an opinion, publishing information, or directing criticism at public figures or public institutions. International human rights law recognizes the possibility of imposing specific restrictions on freedom of expression, however it requires that these restrictions be clearly provided for in law, that they pursue a legitimate aim, and that they be necessary and proportionate to that aim. As for the expansion in the use of penal provisions to address public discussions or disputes related to published content, outside the narrow limits permitted by international law, it raises serious concerns about the widening scope of criminalization at the expense of fundamental freedoms.

Within the context of the transitional phase, the Cybercrime Law and its enforcement mechanisms must be reviewed, since they are part of reforming the legal system inherited from the Assad era, and they contribute to strengthening confidence in justice. This requires a transition to a legal approach grounded in legality, the protection of rights, and judicial oversight, and to guaranteeing that penal legislation isn't used as a tool to restrict the public sphere or to limit peaceful debate.

SNHR affirms that protecting society from cybercrime and strengthening digital security must be achieved through a precise and clear legal framework, not through loose provisions or disproportionate procedures. It also affirms that any future review of the law, or of its enforcement mechanisms, should be grounded in the principles of legality, necessity, proportionality, independent judicial oversight, fair-trial guarantees, and the protection of the right to freedom of expression and the right to privacy.

RECOMMENDATIONS

SNHR believes that guaranteeing a balance between combating cybercrime and protecting fundamental rights and freedoms requires the adoption of clear legislative, institutional, and procedural measures during the transitional phase, foremost among them:

1. Conducting a comprehensive review of the Cybercrime Law No. 20 of 2022 by an independent legal committee comprising judges, lawyers, experts in constitutional law and in international human rights law, experts in digital technologies, and representatives of the relevant civil society, with the aim of assessing the extent to which the law's provisions conform to the international standards on freedom of opinion and expression, the right to privacy, and fair-trial guarantees, and of identifying the articles that contain loose or undefined terms that may permit broad interpretations leading to the restriction of fundamental rights.
2. Amending the provisions that criminalize forms of expression or publication over the internet through general and imprecise wording, and ensuring the clear definition of the criminalized acts, their legal elements, and the penalties prescribed for them, in a way that is consistent with the principle of criminal legality and prevents expansion in interpretation or criminalization.
3. Confining the application of the provisions related to content and expression to the narrowest limits until they are reviewed and amended, and not resorting to penal provisions to address disputes related to published content except in cases that meet the standards of legality, legitimate aim, necessity, and proportionality.
4. Guaranteeing the full procedural rights of Hassan Akkad, and of every person subject to investigation or prosecution under the Cybercrime Law, including informing him of the reasons for the arrest, enabling him to contact a lawyer and his family, bringing him without delay before a competent judicial authority, and enabling him to challenge the legality of the procedures taken against him.
5. Ensuring that pretrial detention in cases related to publication and expression remains an exceptional measure, not resorted to except where there are clear, specific, necessary, and proportionate legal grounds, while giving priority to measures that are less restrictive of personal liberty, in harmony with the presumption of innocence and the right to personal liberty and security.
6. Strengthening judicial oversight over the procedures of seizure and investigation in cybercrime cases, and ensuring that no procedures affecting individuals' liberty or their digital privacy are taken, including searching devices, accessing personal data, or monitoring electronic accounts, except on the basis of reasoned judicial orders subject to legal oversight.

7. Issuing clear guidelines for the public prosecution offices, the judicial police, and the authorities competent to investigate cybercrime, including standards that protect freedom of expression and prevent expansion in the use of the legal provisions related to content published on the internet, in a way that contributes to unifying legal practices and reducing divergent interpretations.
8. Harmonizing the national legislation related to freedom of expression, the media, and the digital space with the provisions of the International Covenant on Civil and Political Rights, particularly the articles related to freedom of expression, the right to personal liberty and security, fair-trial guarantees, and the right to privacy, and with the international principles and practices related to protecting freedom of expression in the digital environment.
9. Publishing periodic data and statistics related to the application of the Cybercrime Law, including the numbers of cases referred to the judiciary, the nature of the acts subject to prosecution, and their judicial outcomes, in a way that enhances transparency and societal oversight, and helps in assessing the impact of the law and the extent to which its application conforms to the principles of the rule of law.
10. Opening a structured institutional dialogue between the public authorities, civil society organizations, human rights bodies, professional syndicates, and legal and technical experts, about the future of the legal regulation of the digital space in Syria, in a way that ensures the development of modern legislation capable of confronting emerging cybercrime without prejudice to the fundamental rights of all persons.
11. Training judges, members of the public prosecution, and judicial police officers on the international standards related to freedom of expression, digital rights, fair-trial guarantees, and the protection of privacy, in a way that contributes to developing judicial and procedural practices that take into account the special nature of the electronic space, and preserve the balance between protecting society and safeguarding fundamental rights and freedoms.

SNHR stresses that reforming the legal framework governing the digital space represents part of a broader process to rebuild trust between society and the institutions of the state during the transitional phase, and that protecting fundamental rights doesn't obstruct the combating of cybercrime, but rather makes it more legitimate, more effective, and more consistent with the rule of law.

SNHR

SYRIAN NETWORK
FOR HUMAN RIGHTS

info@snhr.org
www.snhr.org

No justice without accountability