Analyzing Cybercrimes Law No. 10 of 2018

Study by:

Lawyers for justice

محامون من أجل العدالة

November 2024

EXECUTIVE SUMMARY

*This study, supported by the Swiss Representative Office as part of the project **"Promoting Digital Rights: Safeguarding Freedom of Expression in Palestine,"** explores the implications and applications of Cybercrimes Law No. 10 of 2018. The project is implemented by **Lawyers for Justice (L4J)**, an independent Palestinian legal advocacy organization dedicated to defending human rights and supporting justice and accountability mechanisms. The project addresses concerns raised by the 2018 Cybercrimes Law, which has been criticized for vague provisions and severe sanctions that risk stifling public discourse and digital freedoms.*

Through a comprehensive approach, this study examines how the law impacts fundamental rights, documents its application in specific cases, and provides legal and expert opinion on the alignments of the law with international human rights standards and the Palestinian constitutional framework.

*This endeavor aims to foster a rights-based approach to digital governance by engaging with civil society, legal experts, and governmental authorities. It seeks to contribute to the Palestinian government's ongoing review of the law by offering independent legal and policy analyses through an **Advisory Committee**, promoting a balanced framework that addresses cybersecurity challenges while protecting freedoms.*

Examining impact of Cybercrimes Law No. 10 (2018) on digital freedoms

The study, funded by the Swiss Representative Office, examines the implications of ***Cybercrimes Law No. 10 of 2018*** *in Palestine.*

It reveals significant overreach and vague provisions, particularly in Articles 20 and 22, which enable suppression of free expression under broad interpretations.

Case studies highlight the law's use against journalists, activists, and citizens for criticizing government actions online. Criminal penalties, lack of judicial oversight, and misuse of surveillance powers undermine privacy and fair trial rights. Gender-specific violations also emerge, disproportionately impacting women.

The study emphasizes the need for reform, including revising vague provisions, enhancing judicial safeguards, and decriminalizing free speech to align with international human rights standards.

Towards Balanced Governance of Digital Rights

This study calls *for urgent reform of Cybercrimes Law No. 10 (2018) to protect fundamental rights, ensure transparency, and align Palestinian digital policies with international human rights standards.*

Table of Contents

1.0 Introduction

The Cybercrimes Law No. 10 of 2018, issued by the President of the Executive Authority on April 29, 2018, and published in the Palestinian Official Gazette on May 3, 2018, is one of the most controversial laws in Palestinian legal discourse. Concerns have escalated about the potential exploitation of this law to infringe on the constitutional rights enshrined in the Palestinian Basic Law. Although the published version of this law came after a series of amendments to its previous version in 2017, following some recommendations made by civil society organizations, the rapid issuance and publication of the law in the Official Gazette closed the door for civil society to provide further review and recommendations. Such input could have better aligned the provisions of the law with the constitutional rights and public freedoms outlined in the Palestinian Basic Law and the international human rights conventions to which the State of Palestine has acceded.

With the proliferation of social media and its increasing impact on shaping public opinion—now forming an alternative means of communication and influence in the context of digital progress—there has also been a growing need to balance a law to combat cybercrimes on one hand and the preservation of fundamental constitutional public rights and freedoms on the other. This is particularly critical as certain provisions of the law pose a threat to the right to freedom of expression, privacy, and personal life.

Since the issuance of the aforementioned law by decree, the Lawyers for Justice group has followed a large number of cases referred to the judiciary under the Cybercrimes Law. The group has also monitored the extent to which the law, in its enforced form, has impacted public rights and freedoms, particularly as it has directly affected such rights, including freedom of expression, restrictions on journalistic freedoms, and other constitutional rights. The decision issued by the Ramallah Magistrate's Court on October 17, 2019, stands out as a significant example of such restrictions, as it ordered the blocking of dozens of media websites based on the Cybercrimes Law No. 10 of 2018, without any objective standards justifying the court's decision. This decision was preceded by another in 2017, which also included the restriction of dozens of websites. Moreover, the issuance and publication of this law in the Official Gazette disregarded the principle of legal legitimacy in alignment with Article 15 of the Palestinian Basic Law.

The issuance of Cybercrimes Law No. 10 of 2018 is part of a long series of laws issued by decree from the President of the Executive Authority under what is known as the state of necessity, owing to the continued absence of the Legislative Council for over 17 years. This situation has deepened the role of the Executive Authority in managing and issuing legislation to serve its general policies without oversight, sidelining the role of civil society from effectively influencing these laws before their adoption. Consequently, this has directly contributed to creating an oppressive environment and the misuse of authority by those responsible for enforcing the law against the exercise of public rights and freedoms, amidst the Executive Authority's dominance over the judiciary.

The most significant aspects of this problem are twofold: first, the absence of the Legislative Council has opened the door for the Executive Authority to approve the provisions of this law without any legislative review based on the Palestinian Basic Law and international human rights conventions to serve the public interest. Second, the misuse of the law's provisions contradicts constitutional rights, including freedom of expression, privacy, and personal life.

Citizens, activists, and human rights defenders—particularly those relying on digital communication technologies in practicing their public and constitutional rights—face a significant challenge to their rights-based activities. This challenge arises in the context of a weak judiciary that now provides legal cover for prosecuting individuals without any safeguards ensuring an environment that respects the law and constitution. This situation constitutes an obstacle to developing and protecting these rights in a manner consistent with the Palestinian Basic Law and international human rights conventions, given the digital advancements the world is experiencing.

The adoption by the State of Palestine of the two international covenants on human rights and their incorporation into the national legal system in 2023 provides an additional justification for a comprehensive review of the Cybercrimes Law No. 10 of 2018. The inclusion of these covenants as national laws makes the standards they outline supreme over others and necessitates their consideration in any future legislative process. It also mandates the rectification of previous laws to the extent that they do not conflict with these covenants.

Through this report, the Lawyers for Justice group seeks to highlight some provisions of the Cybercrimes Law that contain serious violations affecting public rights and freedoms. This is particularly important in light of the absence of clear standards to guide the interpretation of the law's provisions during implementation, ensuring that the interpretation and application of the law's provisions are not arbitrary or deviant, nor do they exceed the Palestinian Basic Law and international conventions. This is based on the group's practical experience in cases related to this law since its issuance and enforcement, leading to recommendations to ensure the protection of individuals' and groups' rights and freedoms against abuse and the misuse of authority and to mitigate such abuse.

Lawyers for Justice, in partnership with an advisory committee established to review the Cybercrimes Law, comprising various civil society organizations, the Legal Clinic at Birzeit University, activists, and individuals, aims through this report to shed light on specific provisions of the Cybercrimes Law that contain serious violations of public rights and freedoms. This is particularly critical in the absence of clear standards for interpreting the law's provisions during application, which has led to instances of misuse and deviation in interpreting and implementing the law. The report draws upon practical experiences from numerous cases brought before Palestinian courts under this law since its enactment. It concludes with recommendations to safeguard the rights and freedoms of individuals and groups against abuse of authority while addressing the law's impact on journalists, union members, opinion activists, and influencers in Palestinian society.

The report is based on the Lawyers for Justice group's extensive work over several years since the issuance of the Cybercrimes Law No. 10 of 2018 by decree. It reflects the stages of investigation, litigation, and legal representation provided to individuals and groups affected by the law, as well as legal consultations offered throughout this period. The report also highlights documented violations observed through monitoring complaints and incidents under this law, carefully comparing its provisions with the Palestinian Basic Law and international human rights conventions. This process has culminated in clear conclusions and actionable recommendations aimed at addressing the law's shortcomings. Furthermore, the report underscores the importance of ongoing consultations with the Minister of Justice and various justice institutions, which have sparked a renewed awareness about the limitations of the law and the critical need to balance cybersecurity measures with the protection of constitutional freedoms, including freedom of expression and privacy. The following case is a very recent one and a testament to the attention of justice institutions to the cybercrimes law and its limitations:

> On November 10, 2024, the Qalqilya Magistrate's Court issued a decision acquitting R.R., a female activist, of the charge of defamation against the authorities. The court ruled that the act attributed to her did not constitute a crime and did not warrant punishment. This followed a complaint filed by the Ministry of Education in April 2024 against R.R. for a Facebook post in which she criticized the ministry's policies concerning applicants for its annual employment exam. In August 2024, the Public Prosecution in Qalqilya initiated legal action against R.R., during which she was pressured into admitting to the Facebook post in exchange for avoiding detention. Despite this coerced admission, Lawyers for Justice provided legal defense for R.R., arguing that her expression on social media fell within the protected scope of freedom of expression. The court ultimately concluded that her actions did not constitute a criminal offense under Article 45 of Cybercrimes Law No. 10 of 2018 and subsequently acquitted her.

2.0 Legal Commentary

The Lawyers for Justice Group followed the consultations that preceded the approval of the Cybercrimes Law No. 10 of 2018, as well as earlier consultations that led to the approval of Cybercrimes Law No. 16 of 2017, which was repealed under Article 55 of the current law. Despite repealing the earlier decree-law, which underwent limited consultations, and replacing it with the new Law No. 10 of 2018—where the latter received more opportunities for community feedback and recommendations—most of the recommendations from civil society organizations were not adequately incorporated to ensure that the law aligned with public rights and freedoms. As such, involving civil society in these consultations appeared to be a mere formal process to grant superficial legitimacy to the law before its approval, resulting in numerous practical issues during its application.

The Executive Authority ensured the approval of Law No. 10 of 2018 on April 29, 2018, and its rapid publication in the Palestinian Official Gazette on May 3, 2018, to guarantee its enactment and enforceability. However, this was done without considering Article 15 of the Palestinian Basic Law, which requires sufficient time for those affected by new laws to comprehend and adapt their behavior accordingly.

Before examining the cases, instances, and judicial applications of this law to highlight violations, arbitrariness, and challenges in its implementation, the report will analyze the primary legal provisions of Cybercrimes Law No. 10 of 2018. These provisions have faced significant issues in practical application, particularly regarding conflicts with public rights and freedoms. Issues arise due to the absence of clear standards to interpret and apply the law, resulting in an overly broad understanding of the terminology and concepts within the law. This has created practical challenges in implementing its provisions, exposing constitutional public rights and freedoms to infringement and curtailment.

Below are the key observations on the provisions of Decree-Law No. 10 of 2018 compared to the Palestinian Basic Law and international human rights standards:

Observation 1: Article 3 of the Cybercrimes Law states:

- 1. A specialized unit shall be established within the police and security forces, composed of judicial officers, called the Cybercrimes Unit, under the judicial supervision of the Public Prosecution, each within its jurisdiction.
- 2. The regular courts and the Public Prosecution shall examine cybercrime cases within their competencies.

This article expands the powers of all security apparatuses to manage the Cybercrimes Unit without restricting it to judicial officers, contrary to Article 21 of the Code of Criminal Procedure. This unjustified expansion undermines the principle of protecting civilians' private lives. It grants unchecked power to other security agencies, conflicting with their legal mandates and opening the door to arbitrary interference in individuals' privacy and private lives, violating the inviolability of private life guaranteed under Article 32 of the Palestinian Basic Law. Additionally, the Public Prosecution's role in supervising these units remains weak.

Observation 2: Article 21 of the Basic Law guarantees:

- The right to express opinions by speech, writing, photography, or other means, in accordance with the law.
- The protection of artistic and literary freedom, subject to judicial orders for works considered harmful.
- Freedom of the press and media, prohibiting restrictions except as outlined by judicial rulings.

While this article enshrines constitutional rights and freedoms, the phrase "in accordance with the law" leaves room for interpretations that could restrict these freedoms, undermining the guarantees of the Basic Law and international human rights conventions. This ambiguity risks legitimizing the prosecution of digital content, violating the principle that no crime or punishment exists without explicit legal provision (Article 15, Basic Law).

Observation 3: Article 29 imposes penalties on legal persons for crimes committed on their behalf, with fines and potential suspension of activity or dissolution for offenses punishable by imprisonment. However, this broad application includes minor offenses, contrary to international standards requiring necessity and proportionality.

Observation 4: Article 31 obligates service providers to:

- Share subscriber information with competent authorities upon request from the Public Prosecution or a court.
- Block links or content based on judicial orders.

This provision infringes on privacy by allowing judicial orders rather than judicial rulings to justify blocking content.

Observation 5: Article 32 grants broad powers to judicial officers and the Public Prosecution to search persons, places, and technological devices, seizing related tools without clear limits on search durations. This unrestricted authority risks abuse and privacy violations.

Observation 6: Article 37 accepts evidence from information systems and electronic networks, even if obtained unlawfully, compromising fair trial guarantees.

Observation 7: Article 39 allows security authorities to block websites that threaten national security or public order. This vague criterion risks misuse and imposes restrictions on freedom of expression without adequate safeguards.

Observation 8: Article 45 broadly criminalizes acts committed using electronic means, referencing expansive terms like "undermining national security," enabling the prosecution of activists, journalists, and human rights defenders for vague offenses.

Observation 9: The law lacks transparency mechanisms for monitoring data access and electronic surveillance, violating international standards.

Observation 10: The law omits provisions criminalizing unauthorized surveillance by public or private entities, leaving privacy violations unchecked.

Observation 11: The law does not include provisions for dismissing prolonged prosecution cases or ensuring fair trial procedures.

It is worth noting that many civil society organizations previously participated in extensive consultations with representatives of the Palestinian government following the issuance of Cybercrime Law No. 16 of 2017, which was later repealed. These consultations succeeded in contributing to the cancellation of that law. However, Cybercrime Law No. 10 of 2018 was subsequently issued without incorporating the majority of the proposals and observations submitted during these discussions.

Following the formation of the 19th Palestinian government and the decision taken on April 23, 2024, to establish a committee headed by the Minister of Justice to review the provisions of Cybercrime Law No. 10 of 2018, representatives from civil society were included in this committee. Several institutions, most notably the Independent Commission for Human Rights (ICHR), presented their perspectives and recommendations for amendments to the law. While the outcomes, conclusions, and recommendations of the committee's work have not been officially announced to date, the committee's mandate is a unique opportunity to revisit the law and ensure it strikes the balance between addressing the cybersecurity challenges with protecting freedoms.

The advisory committee believes that fostering new and collaborative approaches with civil society organizations, integrating all proposals and observations, and collectively adopting them for presentation to the ministerial committee can provide a significant contribution to the reform process. Such cooperation would help ensure alignment with principles that safeguard public rights and freedoms in both theory and practice.

3.0 Violations of International Human Rights Standards

An examination of the provisions of the Cybercrimes Law reveals significant inconsistencies with international human rights standards. Without delving into the law's practical application, its misinterpretation, or the unjustified expansion of its provisions to align with the interests of the Executive Authority, the discussion of the law's provisions against international human rights standards is paramount. The Cybercrimes Law conflicts with the human rights standards outlined in international agreements, as well as the Palestinian Basic Law, which guarantees constitutional rights and freedoms. Furthermore, the law contravenes various provisions governing procedural fairness in national legislation, particularly regarding preliminary investigation regulations. This reflects the intent of those who approved the law to expand the powers of judicial officers, extending these to the General Intelligence and Preventive Security Services, which frequently use the law to monitor and prosecute individuals while suppressing public freedoms without judicial oversight. This approach severely restricts freedom of opinion and expression.

The Cybercrimes Law violates numerous international standards designed to protect public rights and freedoms, particularly in the realm of digital rights. Key violations include:

1. Infringement of Privacy Rights (Article 17 of the ICCPR)

Certain provisions of the Cybercrimes Law contravene Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which ensures respect for privacy and the need to protect it from arbitrary interference. The Cybercrimes Law fails to align with international standards regarding surveillance and privacy, often exceeding exceptional circumstances concerning monitoring practices.

In a 2013 report to the Human Rights Council, the Special Rapporteur on Freedom of Opinion and Expression emphasized that state surveillance of communications and information technology constitutes a highly intrusive act that may conflict with freedom of expression and privacy, potentially undermining democratic foundations. The report recommended that:

- Surveillance should be conducted only in highly exceptional circumstances.
- It must be strictly overseen by an independent judicial authority.
- Laws should include clear safeguards regarding the nature, scope, and duration of surveillance measures, as well as the necessary grounds for their authorization and available remedies.

The Cybercrimes Law, however, lacks these safeguards, granting broad monitoring powers that conflict with privacy protections.

2. Restrictions on Freedom of Expression (Article 19 of the ICCPR)

The Cybercrimes Law imposes extensive restrictions on public rights and freedoms, particularly freedom of opinion and expression and the exercise of constitutional rights. Several of its provisions, as discussed in this report, violate Article 19 of the ICCPR. This article safeguards the right to hold opinions without interference and to seek, receive, and impart information and ideas through any medium.

Additionally, the law contradicts the provisions of Decree-Law No. 18 of 2023, which incorporates the ICCPR into Palestinian national law and mandates that its provisions take precedence over other laws. The Cybercrimes Law should have been amended to comply with the ICCPR, but it was not, thus undermining constitutional and international guarantees.

3. Contradiction with the European Convention on Human Rights **(Article 10)**

The Cybercrimes Law also conflicts with Article 10 of the European Convention on Human Rights, which states:

"Everyone has the right to freedom of expression. This right includes freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This article shall not prevent states from requiring the licensing of broadcasting, television, or cinema enterprises."

By imposing severe restrictions on freedom of expression and the exchange of information, the Cybercrimes Law breaches the protections outlined in this article. It enables public authorities to interfere with digital content and communication without clear justification or due process, violating the foundational principles of free expression and access to information.

The Cybercrimes Law No. 10 of 2018 fails to adhere to the international human rights standards set forth in instruments like the ICCPR and the European Convention on Human Rights, as well as its own national obligations under the Palestinian Basic Law. The law's provisions must be amended to:

- Uphold the principles of privacy and limit state surveillance to exceptional, clearly defined circumstances.
- Ensure freedom of expression is protected without arbitrary or overly broad restrictions.
- Align all national laws with the ICCPR and other international conventions to which Palestine is a party.

4.0 Advisory Opinion of International Senior Lawyers Project (ISLP)

Below is the advisory opinion issued by the International Senior Lawyers Project (ISLP), an independent, non-governmental, and non-profit organization comprising approximately 2,000 experienced volunteer lawyers who provide pro bono legal services to promote the rule of law, human rights, and fair, responsible, and inclusive development. This opinion, prepared in collaboration with the American Bar Association, was provided at the request of the Lawyers for Justice Group to comment on the provisions of Cybercrimes Law No. 10 of 2018.

Key Points from the ISLP Advisory Opinion Presented to the Lawyers for Justice Group:

1. **Palestine's Commitment to the ICCPR**

In 2014, the Palestinian Authority committed to implementing the International Covenant on Civil and Political Rights (ICCPR), which protects the right of all individuals to enjoy freedom of opinion and expression. The primary purpose of Article 19 of the ICCPR is to respect, protect, and promote freedom of opinion and expression, including political expression, as an essential condition for democracy.

2. **Parity with the European Convention on Human Rights (ECHR)**

Article 10 of the European Convention on Human Rights (ECHR) provides the same protection for freedom of expression as Article 19 of the ICCPR. Article 10(1) ensures:

"Everyone has the right to freedom of expression..."

Additionally, Article 10(2) mirrors Article 19(3) of the ICCPR by allowing:

"The exercise of these freedoms to be subject to such restrictions as are prescribed by law and are necessary in a democratic society for the prevention of disorder or the protection of the rights of others."

3. **Limitations and Interpretations of Restrictions**

The protection offered under Article 10(1) sets forth principles, while the restrictions under Article 10(2) are exceptions that must be narrowly and precisely interpreted. The requirement that restrictions be "prescribed by law" mandates that they must be clear, precise, and accessible, enabling citizens to regulate their conduct and foresee the consequences of specific actions. Vague or imprecise laws tend to deter legitimate expression and violate Article 10. A restriction is "necessary" only when it is:

- (a) Responding to a pressing social need that is convincingly demonstrated,
- (b) Proportionate, and
- (c) The least restrictive means available.

4. **Necessity in a Democratic Society**

Both Article 19 of the ICCPR and Article 10 of the ECHR require any restriction on freedom of expression to be "necessary in a democratic society." For this condition to be met, the European Court of Human Rights has held that the restriction—such as a penalty—must be proportionate. Any interference should be as minimal as possible.

5. Case Law: Stern Taulats and Roura Capellera v. Spain

In this case, anti-monarchy activists burned a large photograph of the royal couple and were convicted of insulting the monarchy. If the defendants failed to pay the fine, they faced imprisonment. The European Court of Human Rights (ECtHR) ruled that burning the photograph was part of political criticism of the monarchy and did not incite hatred or violence. The ECtHR determined that the criminal penalty imposed—especially imprisonment in case of non-payment—constituted a disproportionate interference with freedom of expression, violating the standards necessary in a democratic society.

6. Case Law: Cumpănă and Mazăre v. Romania

In this case, the ECtHR ruled that imprisoning journalists for defamation of public officials was disproportionate and unnecessary in a democratic society, violating Article 10. The court noted the chilling effect criminal penalties have on journalism and emphasized that courts must exercise "utmost caution when national authorities impose measures or sanctions that discourage the press from participating in public-interest discussions."

7. Criminal Penalties for Non-Violent Speech

The ECtHR consistently holds that imposing criminal penalties, including imprisonment or fines, for non-violent speech—especially political speech—violates freedom of expression under Article 10 of the ECHR. In contrast, the Cybercrimes Law mandates imprisonment or fines for Palestinian defendants publishing similar types of speech online.

8. Specific Articles in the Cybercrimes Law

The Cybercrimes Law prescribes imprisonment or fines for the following types of online speech:

A. Article 20: Violations of intellectual, literary, or industrial property rights.
B. Article 22: Publishing information online that involves unlawful interference in the private or family life of individuals, even if the information is true.

5. Comments by the International Senior Lawyers Project (ISLP) on the Palestinian Cybercrimes Law

1. Absence of Sovereignty Provisions in the Palestinian Basic Law

The Palestinian Basic Law lacks a specific sovereignty clause that would provide superior legal protection for freedoms such as freedom of expression. This omission allows courts to apply laws, such as Articles 20 and 22 of the Cybercrimes Law, which contradict the Basic Law. This gap weakens the constitutional safeguards for fundamental rights and freedoms.

2. Impact of Article 19 of the Basic Law

Article 19 of the Basic Law states:

"There shall be no restriction on freedom of opinion, and every person shall have the right to express their opinion and disseminate it by speech, writing, or other means of expression or art, provided it is in accordance with the law."

The stipulation "provided it is in accordance with the law" effectively subjects the guarantee of freedom of expression to the constraints of other laws, such as Articles 20 and 22 of the Cybercrimes Law. This undermines the intent of Article 19, as it prioritizes restrictive laws over constitutional protections.

3. Intersection with Media Freedom (Article 27 of the Basic Law)

While Article 19 provides general protection for freedom of expression, Article 27 specifically safeguards media freedom:

- **Article 27(1)**: Recognizes the right to establish newspapers and all media outlets as a universal right but subjects their financing to "legal scrutiny."
- **Article 27(2)**: Ensures freedom of the press, including broadcasting, publishing, and distribution, and emphasizes the protection of media professionals.
- **Article 27(3)**: Prohibits media censorship and bans their suspension, confiscation, or cancellation except by law or judicial order.

However, as with Article 19, the exceptions introduced in Article 27(3) weaken media protections, allowing restrictive laws like Articles 20 and 22 of the Cybercrimes Law to prevail. These exceptions have already been used to target journalists and media activists, who have faced charges under the Cybercrimes Law and even the **Jordanian Penal Code of 1960**, for offenses such as "stirring strife" and "insulting high authorities."

4. Article 21 of the Cybercrimes Law

Article 21 ostensibly aims to protect freedom of expression and creative works but imposes two exceptions:

1. Expression must be "in accordance with the law."
2. Legal action against creators of artistic, literary, or intellectual works can only occur "by judicial order."

These exceptions fail to shield individuals from prosecution under Articles 20 and 22 of the Cybercrimes Law, thereby undermining freedom of expression and creative liberties.

Articles 20 and 22 of the current Cybercrime Law No. 10 of 2018 impose restrictions on the exercise of freedom of opinion and expression. These provisions can be widely exploited during the practical enforcement of the law, particularly concerning the prosecution of satirical or critical content, as well as individuals with artistic backgrounds who share creative content through digital platforms. These articles have also been used to target journalists actively engaged in producing social programs, whether their content is shared through personal blogs, printed and periodical magazines and newspapers, or online platforms.

5. Conflict with International Standards

Palestine's reliance on imprisonment or fines under Articles 20 and 22 of the Cybercrimes Law significantly conflicts with international human rights standards, particularly **Article 10 of the European Convention on Human Rights (ECHR)**. These penalties are inconsistent with principles of proportionality, necessity, and the least restrictive means of safeguarding public interests.

6. Vagueness of Article 20

Article 20 of the Cybercrimes Law is excessively vague, imprecise, and unpredictable. As such, prosecutions under this article violate international human rights standards, as laws governing expression must be clear, precise, and accessible to prevent arbitrary enforcement and protect legitimate speech.

6. Judicial Applications

The Lawyers for Justice Group has monitored and followed numerous cases related to the enforcement of Cybercrimes Law No. 10 of 2018 and its practical applications in Palestinian courts. Since the law came into effect in 2018, the Palestinian Public Prosecution has referred hundreds of cases under its provisions. Many of these cases have relied on contentious articles of the law and predominantly targeted citizens, human rights activists, journalists, and civil society bloggers who criticized the policies of the Palestinian Authority (PA) and the behavior of its executive agencies.

The observed criminal prosecutions often extended beyond restricting freedom of opinion and expression. They included actions criminalizing any behavior encouraging the exercise of such rights, such as calls for peaceful assemblies or general advocacy for respecting public rights and freedoms. Additionally, some provisions of the law have been used to target individuals based on their political affiliations or critical views of PA policies and institutions.

Below is a summary of key cases prosecuted under Cybercrimes Law No. 10 of 2018:

1. Case of Citizen A.A.

- **Case No.:** 292/2019
- **Court:** Hebron Magistrate's Court
- **Details:**
  In 2017, A.A. was summoned by the Preventive Security Directorate in Hebron for expressing political opinions critical of the political system and public institutions on social media. He was detained without legal justification.
  In 2019, the Public Prosecution charged him with:
  - Incitement of racial strife (Article 150, Penal Code No. 16 of 1960).
  - Insulting high authorities (Article 195/1, Penal Code).
  - Creating a website to publish information endangering state security and public order (Article 20/3, Cybercrimes Law No. 16 of 2017, which was repealed).
    A.A. was held in custody until released on bail. Despite the repeal of Law No. 16 of 2017, its provisions were used in this case. On April 7, 2021, he was acquitted.

2. Case of Journalist A.D.

- **Case No.:** 2411/2020
- **Court:** Nablus Magistrate's Court
- **Details:**
  In August 2020, A.D. was arrested in Nablus, and all his electronic devices were confiscated. Charges included:
  - Publishing information inciting racial strife (Article 24, Cybercrimes Law No. 10 of 2018).

Disseminating false news to incite fear (Article 91(a), Telecommunications Law No. 3 of 1996).
A.D. was detained without justification, undermining the presumption of innocence. He was released on bail in September 2020 and acquitted in October 2022.

3. Case of Citizen Y.K.

- **Case No.:** 415/2020
- **Court:** Nablus Magistrate's Court
- **Details:**
  In November 2019, Y.K. was summoned by the Civil Police following a complaint by a local authority for defamation. He faced charges under:
  - Articles 188 and 358, Penal Code No. 16 of 1960.
  - Article 45, Cybercrimes Law No. 10 of 2018.
    Y.K. criticized the performance of the Beit Furik Municipality. After 10 sessions, the court dismissed the case based on the complainant's request.

4. Case of Citizen A.R.

- **Case No.:** 2548/2020
- **Court:** Ramallah Magistrate's Court
- **Details:**
  In July 2020, A.R. was arrested by police officers in a demeaning manner. He was charged with defamation against the authorities via electronic platforms (Article 45, Cybercrimes Law No. 10 of 2018). The court released him on bail in July 2020, and he was acquitted in January 2023.

5. Blocking of Websites

- **Request No.:** 12/2019
- **Court:** Ramallah Magistrate's Court
- **Details:**
  In October 2019, the court ordered the blocking of 59 websites at the request of the Attorney General, citing Article 39 of Cybercrimes Law No. 10 of 2018. This marked the first major application of Article 39, which allows for website blocking by judicial request within 24 hours.

6. Case of Citizen F.J.

- **Case No.:** 2975/2021
- **Court:** Ramallah Magistrate's Court
- **Details:**
  In July 2021, F.J. was arrested in Jenin and later transferred to Ramallah. He was charged with defamation against public authorities (Article 45, Cybercrimes Law No. 10 of 2018). F.J. remains on trial as of this writing.

7. Case of Citizen M.S.

- **Case No.:** 4536/2024
- **Court:** Ramallah Magistrate's Court
- **Details:**
  In October 2024, M.S. was arrested after speaking on **Al Jazeera** about threats he faced from security services due to his political opinions. He was charged with:
  - Defamation via electronic platforms (Article 45, Cybercrimes Law No. 10 of 2018).
  - Insulting public authorities (Article 196/2, Penal Code No. 16 of 1960).
    Proceedings are ongoing

Gendered Implications in Judicial Applications of the Cybercrime Law

The Cybercrime Law has been widely applied, affecting not only men but also women activists, including female journalists, social media bloggers, and influential figures who play significant roles in leading local communities and unions. The practical enforcement of this law has notably impacted women, as documented by the group since the enactment of Cybercrime Law No. 10 of 2018. Numerous cases of harassment, prosecution, and intimidation against women due to their activism have been recorded. These cases have taken multiple forms, including the prosecution of female journalists, unionists, and social bloggers under the pretext of violating the Cybercrime Law. Some women have been threatened with legal action, while others have faced privacy breaches and unjustified searches of their belongings due to their journalistic activities.

This law, with its numerous flaws, fails to provide a safe legal environment for women activists and professionals in Palestinian society. Women are often threatened by the ambiguous provisions of the law, and human rights organizations, lawyers, and advisors, including Lawyers for Justice, receive frequent requests for legal consultations from women activists and journalists seeking to ensure compliance with the Cybercrime Law before engaging in any activities.

This trend has been particularly noticeable since 2021, following incidents in which several women had their personal phones confiscated by security personnel, either in civilian or military attire, while documenting peaceful protests in Ramallah. Some women were subjected to blackmail, threats, or prosecution when attempting to retrieve their phones. These experiences have led many women to withdraw from legitimate activism out of fear of persecution under the Cybercrime Law.

7. Conclusion

This report, prepared by Lawyers for Justice in coordination and consultation with the advisory committee for reviewing Cybercrimes Law No. 10 of 2018, critically examines the law's provisions and highlights the challenges it poses. The committee, recently established to identify the law's problematic areas, has worked to provide a critical analysis of the articles that conflict with the Palestinian Basic Law and international human rights standards, particularly the International Covenant on Civil and Political Rights (ICCPR), which Palestine joined in 2014 and incorporated into its legal framework through Law No. 18 of 2023, as well as other agreements such as the European Convention on Human Rights.

The report delves into the significant concerns regarding the law's impact on public rights and freedoms, particularly its adverse effects on freedom of expression. Many provisions of the law have directly targeted this fundamental right, leading to prosecutions against activists, human rights defenders, journalists, union members, civil society bloggers, and ordinary citizens for exercising their constitutional rights guaranteed by the Palestinian Basic Law. Furthermore, the report emphasizes the law's lack of alignment with international human rights standards, including its failure to adhere to the principle of legality in criminal justice and its reliance on overly broad terms and concepts. The absence of clear regulations governing the law's application exacerbates its misuse, leaving it as a tool to undermine constitutional rights, especially freedom of expression and press freedom, without clear and defined standards to balance combating cybercrimes with safeguarding public freedoms.

Additionally, the report includes numerous cases and incidents followed up in Palestinian courts, representing only a fraction of the total cases referred over the past six years. These cases illustrate the challenges encountered in interpreting and applying the law's provisions and the frequent reliance on arbitrary measures to suppress public rights and freedoms, resulting in the erosion of these rights. This occurs amidst the law's failure to establish mechanisms that prevent the abuse of authority under the guise of enforcing the Cybercrimes Law.

Finally, the advisory committee reviewing the Cybercrimes Law has, through this report, adopted a legal stance along with a series of substantive and technical recommendations. These outcomes will be detailed in two separate papers: the first will address the legal position on the Cybercrimes Law and its effects on opinion activists and human rights defenders, while the second will outline a set of practical and technical recommendations aimed at ensuring the protection of public rights and freedoms during the law's implementation and enforcement.

8. Recommendations

The enactment of Cybercrime Law No. 10 of 2018 has sparked significant debate regarding its compliance with constitutional safeguards and international human rights standards. Despite initial revisions from its predecessor, Cybercrime Law No. 16 of 2017, the law remains mired in controversies, with stakeholders raising concerns over its ambiguous language, broad criminalization, and potential misuse to curtail fundamental rights. These concerns necessitate an urgent review to ensure the law aligns with the principles of justice, freedom, and accountability.

This section builds on consultations with members of the advisory committee, civil society representatives, legal experts, and human rights defenders. It presents a set of practical recommendations aimed at revising the Cybercrime Law to safeguard freedoms, particularly digital rights, privacy, and freedom of expression, while ensuring robust mechanisms for addressing genuine cybersecurity challenges.

The proposed recommendations emphasize the need for legislative clarity, proportional sanctions, and procedural safeguards. The goal is to establish a legal framework that fosters trust, accountability, and transparency, aligning with both the Palestinian Basic Law and the international conventions ratified by Palestine, such as the International Covenant on Civil and Political Rights (ICCPR).

Building upon the guiding principles and insights gathered through consultations with civil society, legal experts, and the advisory committee, the following practical recommendations are proposed to enhance the Cybercrime Law and ensure its alignment with constitutional and international standards:

- **Clarify Key Definitions:** Provide precise definitions for terms such as "cybercrime," "public order," and "national security" to prevent overly broad interpretations that could lead to rights violations.
- **Ensure Proportionality in Sanctions:** Revise penalties to ensure they are proportionate to the severity of the offense. Eliminate excessively punitive measures for nonviolent acts, such as posting opinions online.
- **Strengthen Privacy Protections:** Include robust safeguards against unauthorized surveillance and ensure that any monitoring is subject to judicial oversight and permitted only in exceptional cases.
- **Restrict Overreach in Enforcement:** Introduce clear guidelines and accountability mechanisms for law enforcement to prevent abuses during investigations and arrests, particularly in cases involving freedom of expression.
- **Harmonize with Existing Laws:** Ensure that the Cybercrime Law does not conflict with other legislation, such as the 1995 Press and Publications Law, which protects journalistic freedoms.
- **Introduce Oversight Mechanisms:** Establish an independent body to oversee the application of the law, investigate complaints, and provide recourse for individuals who believe their rights have been infringed.
- **Limit Vague Phrases:** Remove ambiguous phrases like "in accordance with the law" that undermine constitutional protections by allowing for subjective enforcement.
- **Freedom of Expression:** Prohibit the use of the law to prosecute individuals for expressing opinions or engaging in peaceful activism, and repeal provisions that criminalize such activities.

- **Clear Legal Standards for Freedom of Expression:** Define precise legal standards to restrict freedom of expression, ensuring restrictions are specific, necessary, and proportionate to prevent misuse and ensure accountability.
- **Protect Human Rights Defenders:** Codify protections for journalists, activists, and human rights defenders to ensure they can operate without fear of harassment or prosecution.
- **Promote Judicial Independence:** Safeguard judicial independence to ensure impartiality in interpreting and applying the law, including through training on human rights standards for judges and prosecutors.
- **Mandate Periodic Reviews:** Require regular evaluations of the law's implementation and its impact on rights, with reports submitted to the public and relevant oversight bodies.
- **Develop Public Awareness Programs:** Launch initiatives to educate the public on their digital rights and responsibilities, fostering a more informed and rights-conscious society.
- **Create a National Observatory:** Establish a digital rights observatory to monitor violations, track enforcement trends, and provide recommendations for ongoing legal reforms.
- **Introduce a Safeguard Clause:** Include a provision explicitly stating that no action under the law may contravene constitutional rights or international human rights commitments.
- **Enhance Consultation Processes:** Institutionalize civil society engagement in legislative amendments, ensuring diverse perspectives are represented in future legal revisions.
- **Ensure Transparency in Surveillance Requests:** Mandate the publication of anonymized, periodic reports detailing the number of surveillance requests, their justifications, and outcomes to uphold accountability.
- **Independent Judicial Oversight:** Establish an independent body to review complaints related to the law’s enforcement, ensuring alignment with constitutional and international human rights standards.
- **Annual Transparency Reports:** Require annual reports detailing cases filed under the law, types of violations, and outcomes to ensure transparency, accountability, and responsible enforcement.

THIS REPORT WAS MADE POSSIBLE WITH THE GENEROUS SUPPORT OF THE SWISS REPRESENTATIVE OFFICE AND THE COLLABORATIVE EFFORTS OF THE ADVISORY COMMITTEE FOR THE REVIEW OF CYBERCRIMES LAW.

CONTACT

Lawyers for Justice Ramallah, Palestine
Phone: +970-22422510
Email: info@lawyers4justice.ps
Website: www.lawyers4justice.ps