Unveiling the Legal Landscape:

A Comprehensive Analysis of the Legal Framework Addressing Cybercrime and Cyberviolence in Albania

Prepared by: Anisia Mandro

June 2024

**The original language of the document is English.*

What is illegal offline, it is illegal online.

Acknowledgements

The **Analysis of the Legal Framework Addressing Cybercrime and Cyberviolence in Albania** was realized by the Albanian Women Empowerment Network (AWEN), in the framework of the programme "Protection and Promotion of Women Rights in Albania", with the financial support of the Swedish Government.

This publication is fully funded by the Swedish Government. The Swedish Government does not necessarily share the opinions expressed herein.

ABBREVIATIONS

AKCESK	The National Authority for Electronic Certification and Cyber Security
CM/Rec	Committee of Ministers Recommendation
CoE	Council of Europe
CPC	Criminal Procedure Code
CSIRT	National Computer Security Incident Response Team
DCM	Decision of the Council of Ministers
DVC	Domestic Violence Coordinator
ECRI	European Commission against Racism and Intolerance
ECtHR	European Court of Human Rights
EU	European Union
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
HRC	Human Rights Council
ILO	International Labour Organisation
LGBTI	Lesbian, gay, bisexual, transgender, intersex
NCGE	The National Council on Gender Equality
PACE	Parliamentary Assembly of the Council of Europe
CEDAW	The Convention on the Elimination of All Forms of Violence against Women
SDG	Sustainable Development Goals
T-CY	Cybercrime Convention Committee

I. Introduction

In the dynamic landscape of the international arena, concerted efforts have been mobilized to combat the scourge of cyberviolence and crime. Through a multifaceted approach encompassing legal frameworks and policy initiatives, the overarching goal remains steadfast: to safeguard online spaces, protect user rights, and mitigate the proliferation of harmful content detrimental to individual's emotional, psychological, social and physical well-being.

At the heart of this global endeavour lies the recognition that cyberviolence disproportionately affects women and girls, with its roots deeply entrenched in gender inequality – manifesting through discrimination, stereotypes, and sexism. This inequality is further compounded for women facing intersecting forms of discrimination, such as those belonging to minority groups, women with disabilities or those identifying as LGBTI.

While the origins of sexism predate the digital age, the internet has emerged as a potent amplifier, providing a new platform for the dissemination of sexist hate speech and violence to a vast audience. Consequently, new forms of gender-based violence have emerged which exacerbate existing gender inequalities and the spill-over effects are manifold: they influence women's visibility, public (political and democratic) participation, and freedom of expression.[1] Notably, offline domestic violence has also acquired a new dimension through online channels, worsening the severity of the abuse.

Statistics speak for themselves.

A recent regional study conducted by UN Women sounded alarm bells, revealing that a staggering 41% of women in Albania have endured some form of technology-facilitated violence.[2] The perpetrators, often individuals in social proximity, including partners, family members, or colleagues continue to contribute to a pervasive culture of intimidation and harassment.

The situation requires attention.

With 83.1% of the population having access to internet,[3] recent years have witnessed the escalating prevalence of online violence[4] against women and girls in Albania– with instances impacting their mental health,[5] and culminating in tragic outcomes such as suicide resulting from cyber bullying or stalking.[6] Cases of cyberviolence on platforms like TikTok and

[1] Human Rights Council. (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. para 14, 19 and 26. Available here. "Acts of online violence often compel women to withdraw from online spaces, with research indicating that 28% of women who experience ICT-based violence intentionally reduce their online presence."
[2] UN Women – Albania. (2023). The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia. Available here. According to Study, the majority of cyber violence against women is perpetrated by unknown persons (50.3%) or persons known only virtually (17.5%), and one third of cases is perpetrated by persons in social proximity, among others partners, family members or colleagues (32.1%).
[3] INSTAT. (2023). Statistics on the use of information technology. Available here.
[4] Facilitated by the use of information and communication technology.
[5] See: Together for Life. (2023) Women and Mental Health in Albania – public health policies and their gender approach towards mental health. Available here.
[6] See for more information: Sukth Case. (2024). Available here.; Berat Case. (2019). Available here.

Telegram demonstrate urgent need to address the dissemination of derogatory content, including deep fake manipulating targeting women and girls, often even for financial gain.[7]

As the terminology surrounding cyberviolence and cybercrime continues to evolve, it remains clear that urgent and concerted action is indispensable to safeguard the digital realm for all individuals, irrespective of gender, race, or identity. In essence, this pervasive and evolving threat of cyberviolence and crime necessitate comprehensive strategies to address the myriad manifestations and safeguard the well-being and dignity of individuals in online spaces. Action thus calls for a holistic approach, rather than fragmented initiatives.

This study will focus on cyber violence and crime against women, analysing both the readiness of the Albanian legal framework to tackle new forms of gender-based violence, as well as the preparedness of institutions to react timely, efficiently and professionally in protecting the victims and survivors or technology-facilitated gender-based violence. The analysis is conducted against international standards in place, and puts forwards a number of legislative, policy, and institutional recommendations.

II. Understanding cybercrime and cyberviolence

Cybercrime, covering offenses committed both against and by means of computer technology, is inherently intertwined with the concept of cyberviolence (*and vice-versa*). This multifaceted phenomenon manifests in various forms,[8] spanning from cyber harassment and privacy violations to hate crimes and direct threats of physical harm. Information and communication technology tools are also used for trafficking in women and girls, or as a threat to compel them into trafficking situations.

At its core, **cyber harassment** encompasses unwelcomed sexually explicit communications, offensive interactions across social media platforms, and menacing threats of physical or sexual violence. Additionally, it extends to cyberbullying, revenge porn dissemination, defamation, and incitement to self-harm or suicide. Within the realm of cyber harassment, distinct dimensions emerge: private interactions involving direct communication channels like email or private messaging; and public manifestations through threatening or defamatory content disseminated across internet platforms. Public harassment may also involve inciting third parties to target the victim, amplifying the harm inflicted.

Cyberviolence extends to direct threats or acts of physical violence facilitated through computer systems, including instances of murder, kidnapping, rape, and extortion, etc. These grave offenses highlight the intersection of technology with real-world violence, posing significant challenges to law enforcement and societal safety. Motivated by biases rooted in perceived personal characteristics or group affiliations, cyberviolence further encompasses hate speech targeting individuals based on attributes such as gender, race, ethnicity, religion, sexual orientation, or disability. Such discriminatory acts not only inflict psychological distress but also perpetuate systemic oppression and social marginalization.

[7] See for more information the Telegram Case (2024). Available here.
[8] See for more information: Cybercrime Convention Committee (T-CY) – Working Group on cyberbullying and other forms of online violence, especially against women and children. (2018). Mapping Study on Cyberviolence (with Recommendations adopted by T-CY). Available here.

Violation of privacy represents another facet of cyberviolence, encompassing intrusions into personal data, doxing, cyber stalking, sextortion, and impersonation. These infringements often result in the manipulation, theft, or exposure of intimate information, perpetrating harm against individuals in both online and offline realms.

Cyberstalking, often intertwined with other criminal activities, encompasses the collection of personal information for purposes of psychological manipulation, intimidation, or coercion. This behaviour, sometimes paralleling offline stalking, underscores the evolving nature of deviant conduct in the digital age, posing complex challenges for legal frameworks and social norms alike.

As technology continuous to evolve, new forms of violence emerge, which, without proper legislation and legislative oversight, pose heightened risk to fundamental human rights and freedoms.
The readiness of Albanian legislation to address these emerging forms of violence remains in question. Following this, are the authorities and mechanisms in place adequately equipped to safeguard the lives and ensure the well-being of victims, and prevent such incidents? These questions will be analysed in the following Sections.

III. An analysis of the Albanian legal and policy framework

The standards set forth by the Council of Europe regarding violence against women and cybercrime, along with their intersection, as well as the case law of the European Court of Human Rights (ECtHR), serve as foundational pillars guiding both the Albanian legal framework and judicial reasoning. As a candidate country, Albania is also influenced by EU standards. In line with the sustainable agenda, Sustainable Development Goal 16 (SDG) also acts as a guiding beacon, emphasizing the urgent need to foster peaceful and inclusive societies, free from all forms of violence.

This section will delve into the Albanian legal and policy framework concerning cybercrime and violence against women, while also examining relevant international instruments that shape domestic legislation and policy. The legal analysis aims to inform stakeholders, including policy makers and civil society actors, about existing gaps in both legal and policy domains. It will identify areas that warrant further attention and, where necessary advocate for amendments to address these deficiencies.

International standards

European Union

EU laws and regulations relevant to cyberviolence mainly fall under broader frameworks related to cybersecurity, data protection, digital rights and online content regulation.

On 8 March 2022, the European Commission adopted an EU-wide proposal for a Directive to combat violence against women and domestic violence.[9] The proposed Directive, was

[9] Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence. (COM (2022) 105 final). Available here.; The approved version by the European Parliament available here.

approved on 24 April 2024[10] and makes the first comprehensive legal instrument at the EU level to tackle violence against women, criminalizes physical violence, as well as psychological, economic and sexual violence against women across EU, both offline and online. The Directive includes important definitions including that of violence against women and domestic violence. Importantly, it foresees measures to remove certain online material; on specialist support to victims, and on how to document the cybercrime and information on judicial remedies and remedies to remove online content related to the crime.[11]

Several pieces of EU policy focus on the issue of online and technology facilitated violence against women, acknowledging the issue and developing roadmaps to respond to it. Such is the EU Gender Equality Strategy 2020 – 2025,[12] where among key objectives is ending gender-based violence, including protecting women's safety online. In line with the Gender Equality Strategy aspirations, as of 1 October 2023 the EU became a party to the Council of Europe Istanbul Convention and is now bound by the comprehensive standards deriving from it.

With the prospect of EU accession, significant EU policies and legislation influence the Albanian legal and policy landscape regarding cybercrime and violence. Key documents include:

- EU Directive 2011/36 – Anti-Trafficking Directive[13]
- EU Strategy on combatting trafficking in human beings 2021 – 2025
- EU Directive 2012/29 – Victim's Rights Directive[14]
- EU Victim's Rights Strategy 2020 – 2025
- Council Directive 97/80/EC on the burden of proof in cases of discrimination based on sex[15]
- General Data Protection Regulation (GDPR)[16]
- EU Gender Equality Strategy 2020 – 2025
- Code of Conduct on Countering Illegal Hate Speech Online

Council of Europe

The standards deriving from the Council of Europe offer extensive guidance and tools, which assist states in addressing cyberviolence. The Council of Europe has a set of treaties and protocols in place including the European Convention on Human Rights, Budapest Convention

[10] European Parliament. (2024). Press Release: Parliament approves first ever EU rules on combating violence against women. Available here.
[11] See Directive (approved version of April 2024).
[12] A Union of Equality: Gender Equality Strategy 2020 – 2025. Available here.
[13] EU Directive 2011/36 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA. Available here.
[14] EU Directive 2012/29 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA. Available here.
[15] Council Directive 97/80/EC of 15 December 1997 on the burden of proof in cases of discrimination based on sex. Available here.
[16] EU Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available here.

on Cybercrime and the Convention on preventing and combatting violence against women and domestic violence, which Albania has ratified (Istanbul Convention).[17]

The Istanbul Convention provides guidance on substantive criminal laws that protect women from abuse and violence. While the Convention itself does not explicitly refer to the digital dimension of violence against women, GREVIO General Recommendation No 1 on the digital dimension of violence against women[18] clears out any ambiguity about the Convention's application in the digital dimension.[19]

The Budapest Convention[20] requires parties to criminalize offences perpetrated against or by means of computer data and systems, as well as aspects of cyber violence, secure evidence and engage in cross-border international cooperation to investigate and prosecute online violence against women. The First Additional Protocol[21] on xenophobia and racism focuses on dissemination of racist and xenophobic material through computer systems, while the Second Additional Protocol focuses on enhanced cooperation and disclosure of electronic evidence.[22]

Of relevance for the analysis, the Committee of Ministers Recommendation CM/Rec (2019)1 on preventing and combating sexism, is unique as it brings the first internationally agreed definition of sexism, including online sexist hate speech.[23] The Recommendation notes that sexist hate speech may escalate to offensive and threatening acts, including sexual abuse or violence, rape or potentially lethal action, loss of resources, self-harm or suicide – and can occur in the full range of human activity including cyber space. The Recommendation reaffirms the intersectional dimension of sexism and underlines aggravating circumstances such as power relations and the reach and repetitiveness of the abuse.

It is important to note that the standards outlined in the aforementioned documents guide the analysis of the Albanian legal framework, as presented in the following Sections.

Other relevant binding and soft law instruments which inform a comprehensive legal framework include:

- Council of Europe Convention on Action Against Trafficking in Human Beings (Warsaw Convention);
- European Convention on the Compensation of Victims of Violent Crimes;
- Convention 108+ with regards to the processing of personal data;
- Committee of Ministers Recommendation CM/Rec(2018)2 on the rules and responsibilities of internet intermediaries in carrying out their mandate;

[17] Albania has also ratified the Lanzarote Convention on Protection of Children against Sexual Exploitation and domestic violence. This Convention is not included in the analysis, as it falls outside the scope of the study which is specific to violence against women.
[18] The Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO). (2021). General Recommendation No 1 on the digital dimension of violence against women. Available here.; See also the explanatory report to the Convention, para. 363, which underlines that the Convention harmoniously coexists with other treaties, and its aim is to assure the victim with the highest level of protection.
[19] GREVIO considers that the term violence against women in its digital dimension and the digital dimension of violence against women is comprehensive enough to comprise both online acts of violence and those perpetrated through technology, including technology yet to be developed.
[20] Albania ratified the Budapest Convention with Law No 8888/2002. Available here.
[21] Albania ratified the First Additional Protocol with Law No 9262/2004.
[22] In February 2023 Albanian signed the Second Additional Protocol to the Convention on enhanced co-operation and disclosure of electronic evidence.
[23] Text of the Recommendation (2019)1 available here.

- Committee of Ministers Recommendation CM/Rec(2007)17 on gender equality standards and mechanisms, which provides detailed guidance to member States to give priority to the development, adoption and enforcement of effective national gender equality legislation, and to the integration of a gender perspective into all areas of governance, both in laws and policies;
- European Commission against Racism and Intolerance (ECRI) General Policy Recommendation No 15 on Combating Hate Speech;
- Committee of Ministers Recommendation CM/Rec(2022)16 on Combating Hate Speech;
- Committee of Ministers Recommendation CM/Rec(2014)6 on a Guide to Human rights for internet users;
- Council of Europe Gender Equality Strategy 2024 – 2029.

Parliamentary Assembly of the Council of Europe

The Parliamentary Assembly of the Council of Europe (PACE) has issued two resolutions with relevance to this analysis: Resolution 2144(2017) on cyber discrimination and online hate, and Resolution 2177(2017) on ending sexual violence and harassment of women in public space.

United Nations

The Convention on the Elimination of All Forms of Violence against Women (CEDAW) stands as an important treaty in the fight against gender-based violence. The Committee on the Elimination of Discrimination against Women (CEDAW Committee), through its General Recommendation No. 35, acknowledges the evolving nature of gender-based violence against women, extending to technology-mediated environments such as the internet and digital spaces. This recognition emphasizes the importance of addressing contemporary forms of violence occurring online.

In addition, International Labour Organization (ILO) Convention No 190 on Violence and Harassment in the world of work is the first international treaty to recognize the right of everyone to a world of work free from violence and harassment, including gender-based violence and harassment.[24]

Other relevant documents include the Convention on the Rights of Persons with Disabilities, Human Rights Council (HRC) Resolution 32/13 of 2016 on the promotion protection and enjoyment of human rights on the internet as well as the 2018 Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.

An analysis of the Albanian legal and policy framework

This section with analyse the Albanian legal and policy framework on cybercrime and violence against key international standards.

Legal Framework

[24] Albania ratified the ILO Convention No 190 on 3 February 2022.

Criminal Code

The Albanian Criminal Code, as amended, is only partially aligned with the Istanbul Convention, Budapest Convention and EU Directive 2013/40.[25] *While strides have been made, particularly in addressing certain cybercrimes, discrepancies remain, particularly concerning provisions related to cyber violence against women.*

In consonance with the Istanbul Convention, there is an imperative for the criminalization of sexual harassment online and perpetrated through digital means, stalking committed in the digital sphere, and online psychological violence. Such practices necessitate legal recognition and robust penalties to deter perpetrators effectively.

The definition of **sexual harassment** encompasses various forms of unwelcome sexual conduct, including non-consensual image or video sharing image sharing, non-consensual taking, producing or procuring of intimate images or videos, exploitation, coercion and threats, sexualised bullying and cyber flashing. Also recognized as a precursor to physical violence, sexist behaviour such as sexist hate speech, perpetuate a climate of humiliation and degradation, can escalate to overtly threatening acts falling within the purview of the Istanbul Convention, including sexual violence or rape. Criminal Code Article 108/a provides the definition of sexual harassment as "Commitment of actions of a sexual nature which infringe the dignity of a person, by any means or form […]", which allows for statutory interpretation.

Yet, the Albanian Criminal Code falls short in explicitly addressing technology-facilitated sexual harassment and behaviours falling under the definition.

Online stalking practices, or stalking via modern communication tools and information and communication technology devices, perpetrated in the digital sphere encompass a wide range of behaviours, including threats of a sexual, economic, physical or psychological nature, as well as actions resulting in reputational damage. Perpetrators engage in monitoring and gathering of private information on the victim, often resorting to identity theft, solicitation for sexual favours, impersonation and harassment with the aid of accomplices.

Under Article 121/a of the Criminal Code, as amended, stalking is limited to physical actions only. Regardless of this limiting aspect of the legal provision, case law shows that in the majority of cases, stalking is not limited to physical actions but also through the use of phone,[26] social media,[27] or a combination of phone and social media.[28] There are also cases that stalking is merely done through the use of social media.[29]

There is gap in Albanian legislation to address the myriad ways in which stalking manifests itself in the online realm, which leaves the victims vulnerable to prolonged harassment and psychological trauma, increasing the anxiety and isolation from public and social sphere,

[25] EU Directive 2013/40 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available here.
[26] See Tirana District Court Decision No 78, dated 19.01.2017, Decision No 587, dated 28.02.2017, Decision No 674, dated 06.03.2017; Decision No 252, dated 02.02.2016; Decision No 382, dated 11.02.2016; Decision No 1776, dated 30.05.2016; Decision No 2328, dated 11.07.2016. Available here.
[27] See Tirana District Court Decision No 425, dated 16.01.2017; Decision No 552, dated 23.02.2017; Decision No 1648, dated 20.05.2016; Decision No 1697, dated 24.05.2016; Decision No 3252, dated 27.10.2016; Decision No 3429, dated 08.11.2016. Available here.
[28] See Tirana District Court Decision No 1883, dated 03.06.2016; Decision No 2997, dated 04.10.2016; Decision No 3511, dated 15.11.2016. Available here.
[29] Tirana Disctrict Court Decision No .683, dated 06.03.2017. Available here.

contravening thus the protective measures outlined in both the Istanbul and Budapest Convention.

Online psychological violence, manifesting through intimidation and shaming, presents another critical challenge, exacerbated by factors like mob mentality and anonymity. Economic abuse, as a form of psychological violence, entails control over a woman's financial resources, poses also significant threat to a victim's well-being and independence. *Under the current legal framework, it would be deemed appropriate to demand legislative attention and adequate protective measures, seeing online psychological violence often as an indispensable element of cyber stalking practices and technology facilitated (sexual) harassment, and importantly of domestic violence.*

When analysing the Albanian Criminal Code, it is important to conduct it against the Budapest Convention substantive criminalization section (Articles from 2 to 11 of the Budapest Convention).

Article 2 (illegal access)**,** Article 3 (illegal interception)**,** Article 4 (data interference), Article 5 (system interference), Article 6 (misuse of devices) and Article 9 (child pornography) of Budapest Convention are seen with a more direct connection to cyberviolence.[30]

The Albanian Criminal Code, and specifically Article 293/b on data interference and Article 293/c on system interference need to be further refined to align with the set standards. Both data and system interference in a critical system may cause death or physical or psychological injury.[31] **Data interference** is also seen, for example, to alter a person's social media posting to attract hostility; while in the context of domestic violence, this form of abuse could manifest itself in an abusive partner or ex-partner destroying or deleting the victim's tools, devices or content for a matter of control or revenge.[32] With regards to **system interference** an attacker may have sufficient control over a computer system that a victim may be unable to preserve any evidence related information or communication – for example in the case of stalking tactics used in domestic violence.[33] *All these mentioned elements have to be considered carefully, and changes to the legislation as such need to address the vulnerability of women as usual victims of cyber threats and violence.*

Article 293/a of the Albanian Criminal Code on **illegal interception**, is also partially in line with Article 3 of the Budapest Convention,[34] which aims to protect the right to privacy and data communication. Technically speaking, interception relates to monitoring or surveillance of content of communications. Traffic interception is also done for the purpose of committing

[30] See for further information on definitions: Explanatory Report to the Convention on Cybercrime. (2001). Available here.; Note that: Article 9 on Child Pornography is outside the scope of this analysis.
[31] These crimes could target any person, not just women. It is also important to note here the concept of intentional conduct, meaning the offender must have acted intentionally/must have the intent to seriously hinder.
[32] Council of Europe. (2021). Protecting Women and Girls from Violence in the Digital Age – The relevance of the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. p. 35. Available here. "The notion of "serious harm" should be understood in the broader context of domestic violence and should always be an aggravating circumstance. This article [Article 4 Budapest Convention] has a facilitating as well as a direct connection to violence, similar to Article 5 [of the Budapest Convention on System Interference]".
[33] Ibid. p. 36. "In the case of stalking tactics used in domestic violence, the interference with and destruction of a victim's data, without right, by a perpetrator. The "serious harm" result of this action and "serious hindering" should be appreciated in terms of impact on a victim in a domestic violence context."
[34] This provision describes the action of intercepting a victim's (non-public) personal data without right, either by installing software on their devices to intercept those data or by penetrating their devices by technical means.

privacy violations, which then amount to cyberviolence. A gendered approach would be beneficial when addressing further improvements to this Article.

With regards to **misuse of devices** (Article 6 of the Budapest Convention); the corresponding Article 293/ç of the Albanian Criminal Code requires further alignment with the international standards in place. Similarly, those Articles in the Criminal Code related to attempt and aiding or abetting (Article 11 of the Budapest Convention). It may be useful to address cyberviolence, in relation to the above articles.[35]

Unauthorized access is addressed in the Criminal Code under Article 192/b, yet further refinement is needed to ensure compliance with the Budapest Convention Article 2. Illegal access shows to be common in cyberthreats, cyberstalking and sextortion, and other forms of privacy violations amounting to cyberviolence, including theft of intimate data for the purpose of dissemination and intimidation, among other reasons.

The above-mentioned Articles need to also address the standards as set by the Istanbul Convention, and introduce a consideration to the gender-related aspect. Having said that, it is important to refine aggravating circumstances to explicitly acknowledge cyber-violence against women as an aggravating circumstance.

Here, it is crucial to highlight that currently, there is no systematic and thematic monitoring of cases, hindering thus our understanding of the frequency of occurrence of cyber violence. However, a superficial analysis of court rulings on domestic violence cases under Article 130/a of the Criminal Code reveals numerous instances where the court administers evidence related to cyber violence. *This again underscores the urgency of incorporating provisions for cyber violence as a form of gender-based violence against women into legislation, including in the Criminal Code and other relevant laws as discussed throughout this document.*

In addition, it may be considered transposing definitions into national law would also enhance legal clarity and efficacy in prosecuting cyber violence cases.

Provisions such as Article 74(a), 84(a), 119(a), and 119(b) align with the First Additional Protocol to the Budapest Convention, targeting offenses like dissemination of materials promoting genocide or racial hatred through computer systems.[36]
Noting that the ongoing revision of the criminal code is anticipated to align with international standards; a finalized version available for public consultation is yet to materialize.

Criminal Procedure Code

Overall the Criminal Procedure Code (CPC), as amended, aligns with Section 2 of the Budapest Convention, namely Procedural Law. *Yet, adjustments are required regarding search and seizure procedures, production orders and interception of content. Consideration should also be given to the collection of traffic data in real-time to be regulated in the law in precise and foreseeable manner, in line with international standards.*

[35] See for further information: Explanatory Report to the Convention on Cybercrime. (2001). Available here.
[36] More specifically: Article 74(a) Computer dissemination of materials favoring genocide or crimes against humanity; Article 84(a) Threats due to racist and xenophobic motives through the compute system; Article 119(a) Dissemination of racist or xenophobic materials through the computer system; Article 119(b) Insulting due to racist or xenophobic motives through the computer system.

In line with Article 16 and 17 of the Budapest Convention, the CPC covers expeditious preservation of stored computer data, and preservation and partial disclosure of traffic data, CPC Article 299/a and 299/b respectively.

When there are reasons to believe that data may be lost, damaged or altered, CPC Article 299/a empowers the prosecutor to issue preservation orders, with the obligation resting upon data controllers to maintain the integrity of the data for a maximum of 90 days, renewable once.[37]

CPC Article 299/b is in line with Article 17 of the Convention. The measure aims to ensure that in case of multiple service providers have been involved in the transmission of communication, sufficient amount of traffic data is disclosed in order to enable identification of service providers and path of communication. *It is important that reference to measures that ensure validity and authenticity of stored data under Article 299/b is guaranteed as it may potentially affect their admissibility as evidence in criminal proceedings.*[38]

Furthermore, for service providers located abroad, but offering services in the territory, it is imperative to adhere to Article 18(1)(b) as interpreted by the by the Cybercrime Convention Committee (T-CY) Guidance Note on Production orders for subscriber information.[39] In line with Article 18(3) of the Convention, there is need for a definition on 'subscriber information'.

Criminal Procedure Code, as amended, includes Article 208(a) on seizure of data or computer system, and provides rules on seizure and confiscation of proceeds of crime. The scope of the measure is limited to the offences related to information technology. In practice, general provisions on seizure of evidence are used for phones or other electronic devices in offences. The scope of this provision needs to be considered, and assessed whether the current framework provides for an expeditious manner to extend the search. In addition, in such cases the prosecutor can order the seizure, however for the search of a device a court order is needed. *This element would need to be further assessed whether it creates unnecessary boreoarctic hurdles.*

There is no specific provision on real time collection of traffic data under CPC. There is a generic provision on interception of content foreseen under CPC Article 221. Traditionally the collection of traffic data in respect of telecommunications has been a useful investigative tool to determine the source or destination and related data of illegal communications. Similarly, the collection of content data has been useful tool to determine that communication is of illegal nature (communication constitutes a criminal threat or harassment). In line with this, it is important the current provisions of the CPC are in line with international standards in place, and if deemed necessary introduce standalone procedural measures.

[37] Note that: Pursuant to Article 101 of the Law No 9918/2008 on Electronic Communications, as amended, network operators are obliged to preserve the data records of their subscribers for a period of two years, and in accordance with the CPC. Available here.
[38] Council of Europe. (2021). Compliance of cybercrime legislative framework of Albania with procedural provisions of the Budapest Convention (Articles 16 to 21) and relevant EU/CoE standards with respect to collection and processing of personal data and transborder data flows – Report of Albania. [IProceeds-2 Project of the European Union and the Council of Europe on Targeting crime proceeds on the Internet and securing electronic evidence in South East Europe and Turkey].
[39] Available here.

CPC contains only several references to personal data. Most of references relate to the situation where personal data entails data identifying the perpetrator.[40] Any reference to personal data in the context of cybercrimes or cyberviolence is not covered by the CPC.

Albania's signing of the Second Additional Protocol on 27 February 2023[41] necessitates thorough analysis of its impact on legislation; possibility for a direct request to Albanian Internet Service Providers (ISP) is a novelty that would require changes of CPC (international cooperation), legislation on ISPs (obligations to provide the data), and possible additional 24/7 contact point in prosecution service for emergency requests etc.

Law on Measures against Violence in Family Relations

The amendments of 2018 and 2020 to the Law No 9669/2006 "On measures against violence in family relations"[42] incorporated relevant provisions based on the Istanbul Convention and CEDAW.

Taking note of the Albania State Report of June 2023 submitted to the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), municipalities report increased trends in online violence while managing cases of domestic violence. Therefore, the protection measure imposed by the court is prohibition of any form of harassment and violence on social networks, via telephones or any other form.[43]

In this regard, the reasoning of the European Court of Human Rights in the case of Buturugă v. Romania is of particular relevance – a case that saw the first explicit recognition of cyberviolence by ECtHR. It concerned allegations of domestic violence and of violations of the confidentiality of electronic correspondence by the former husband of the applicant who complained of shortcomings in the system for protecting victims of this type of violence. The court noted that cyber-harassment is currently recognized as an aspect of violence against women and girls and that it can take various forms, including cyber-violation of privacy, intrusion into the victim's computer and the capture, sharing and manipulation of data and images, including private data.

Following the above, it is important the Law on measures against domestic violence welcomes further amendments in light of the advancements of online violence, and its forms thereof. This entails incorporating GREVIO Recommendation No 1, which emphasizes the importance of understanding cyber violence and training of relevant entities, including the judiciary and the prosecutor's office.

Labour Code and the Law on Safety and Health at Work

Women and girls may experience gender-based violence against women in all aspects of their lives, including in their families and intimate relationships, by friends and acquaintances, within their communities, places of work, including remote working as well as work provided on/through platforms.

[40] In Albanian language: "gjeneralitetet e të pandehurit dhe të dhënat e tjera personale". See also: Article 103 paragraph 4 on publication of personal data of minors (defendants and witnesses).
[41] See here.
[42] Available here.
[43] Report submitted by Albania pursuant to Article 68, paragraph 4 of the Council of Europe Convention on preventing and combating violence against women and domestic violence (1st thematic evaluation round). Received by GREVIO on 30 June 2023. Available here. All cases of digital domestic violence involve women and girls as victims, with the perpetrators being intimate partners, cohabitants or husbands.

Sexual harassment at work has seen many forms perpetrated also online.

The ILO Convention No 190 on violence and harassment, ratified by in February 2022, needs to be integrated in the Albanian legislation both in the Labour Code and Law No 10 237/2010 on Safety and Health at Work.[44] The ILO analysis of 2020 on the compatibility between the Albanian legal framework and ILO Convention No 190 provides in detail recommendations for further alignment of the legislation.[45]

Law on Protection from Discrimination

The amendments introduced in 2020 to the Law No 10 221/2010 on protection from discrimination welcomed several provisions to approximate it with the EU anti-discrimination legislation, including expansion of gender-related grounds for discrimination such as gender identity, sexual orientation and sex characteristics, etc.[46]

Recent changes have added sexual harassment as a form of discrimination. The law defines sexual harassment as unwanted behaviour, verbal or non-verbal, of a sexual nature, which has the purpose or effect of violating the dignity of the person and creating an environment of intimidation, hostility, contempt, humiliation or offence.[47]

To ensure the victim-cantered approach, the burden of proof is reversed – from the applicant to the party against which the complaint is brought – in complaints submitted to the Commissioner for Protection from Discrimination or to the courts.

The scope of the law needs to be revisited, to foresee guaranteeing protection of all forms of discrimination, including discrimination taking place online. The Commissioner for Protection from Discrimination is entrusted to monitor the implementation of both the Law on Protection from Discrimination and the Gender Equality Law, but details on how this monitoring process will take place and with what resources is lacking and needs to be addressed.

Law on Gender Equality

The Law No 9970/2008 on Gender Equality, at the time of its adoption, played an instrumental role in establishing a strong normative framework on equality between women and men. At the time, it was largely based on existing international standards, which have seen further advancement in the years since its adoption.

Having said that, as recognized by the CEDAW Concluding Observations on the fifth periodic report of Albania of November 2023[48] the Committee recommends Albania to consider revising Law No 9980/2008 in accordance with the commitment made in the National Strategy on Gender Equality 2021 – 2030. The European Commission 2023 Report for Albania[49] also calls for intensification of implementation of the law and the national Strategy; while the

[44] Law No 10 237/2010, as amended, on Safety and Health at Work. Available here.
[45] Reference can be made to the document: Mandro, Arta. (2020). Analizë e legjislacionit shqiptar mbi dhunën dhe ngacmimin në punë kundrejt përputhshmërisë me Konventën 190 të ILO.
[46] Article 1 of the Law No 10 221/2010. Available here.
[47] Article 3, point 14 of the Law No 10 221/2010.
[48] See CEDAW Concluding Observations on the fifth periodic report of Albania. (November 2023). para. 12(a). Available here.
[49] Full text of the Report available here.

Report of Albania for 2022 notes that the national legal framework needs to be harmonized with the provisions of the ILO Convention No 190.[50]

The Gender Equality Law does not recognize gender-based violence as a form of discrimination, and does not provide women and girls with a possibility to seek remedy when authorities fail to protect them.

The current legislation does not include protection of women facing intersecting forms of discrimination such as women with disabilities or other disadvantaged groups. On the same note, the Committee on Rights of Persons with Disabilities[51] expresses concern regarding the lack of a comprehensive gender equality policy and strategy that addresses the multiple and intersecting forms of discrimination faced by women and girls with disabilities.[52]

The Gender Equality Law needs to recognize forms of gender-based violence as a serious obstacle towards achieving gender equality and protection from discrimination, and ensure legal measures to prevent and protect women and girls.

It is necessary that the Law on Gender Equality establishes cohesive connections with the Law on Protection from Discrimination. Gender Equality is affected by both violence and discrimination that can take place online and offline, thus harmonization between these two pieces of legislation is essential to ensure comprehensive and uniform legal coverage.

As mentioned earlier, the Commissioner for Protection from Discrimination is entrusted to monitor the implementation of the Gender Equality Law and the Law on Protection from Discrimination, but details on how this monitoring process will take place and with what resources are lacking and need to be addressed.

As a country undergoing accession negotiations, Albania needs to ensure that its national legislation on gender equality and non-discrimination is fully compliant with the EU acquis. An important aspect of this, is that the Law on Gender Equality addresses gender bias and violence against women in politics.

Albanian Electoral Code

The Law No 10 019/2008 "On the Electoral Code of the Republic of Albania" has undergone several amendments. In 2020, the Working Group on Gender and Equality in Decision-Making submitted a set of recommendations to the Albanian Parliament in the context of ongoing political discussions of amendments to the Code. Among recommendations, the Working Group addressed the largely neglected issue of violence against women in elections, proposing specific provisions in the code to prevent and fight this form of gender-based violence.

Other relevant pieces of legislation

- Law No 10 193/2019 on Jurisdictional Relations with Foreign Authorities in Criminal Matters, which regulates mutual legal assistance.[53]

[50] EC 2022 Report Albania. p. 34. Available here.
[51] The Committee of the Convention on the Rights of Persons with Disability.
[52] Committee on the Rights of Persons with Disabilities. (14 October 2019). Concluding Observations on the initial report of Albania. Available here.
[53] In 2021, Albania implemented a new database for automated processes and template for MLA requests, using the Council of Europe Committee of Experts on the operation of European Conventions on Cooperation in

- Law No 152/2013 On Civil Servant[54]
- Law No 2/2017 on Cyber Security
- Law No 9918/2008 on Electronic Communications
- Law No 10/2023 On classified information.
- Law No 10 273/2010, on Electronic Document.
- Law No 107/2015 on Electronic identification and trusted services
- Law No 40/2016 on the Order of the Psychologist.
- Law No 9887/2008 Law on Protection of Personal Data.[55]
- Audiovisual Broadcasting Code[56]

Policy Framework

Considering cybercrime through a gender-based lens is essential for developing gender-sensitive prevention strategies and fostering a more holistic approach to combatting cyber violence. By integrating gender equality considerations into prevention and control measures, effective responses, interventions, and services can be tailored to address the specific dynamics of cyber violence. This approach ensures that efforts to combat cyber violence are inclusive and responsive to the diverse experiences and vulnerabilities of women and girls.

Two key strategies (should) inform the policy direction in the field of cyber violence and cybercrime in Albanian, namely the Strategy on Gender Equality and on Cyber Security. A number of other strategies, as listed below, may also consider more explicitly cyberviolence.

National Strategy on Gender Equality 2021-2030, approved with DCM No 400, dated 30.06.2021[57] foresees four strategic goals inspired by the EU's Gender Equality Strategy 2020 – 2025 and the Gender Action Plan (GAP III) 2021-2025.

It is important there is a systematic link between the Strategy and the legislation on domestic violence, gender equality as well as other concerning laws mentioned throughout this analysis.

criminal matters (PC-OC) templates; while T-CY templates are not integrated into the system yet, however those are available to prosecutors.

[54] Law No 152/2013, as amended, aims to ensure the protection of the moral, physical integrity and dignity of the civil servant and the obligation of the institution where the civil servant works to protect him during the performance of his duty and even the involvement in this protection of other specialized bodies if the case arises. Article 33 provides for (1) the right to suitable working conditions to protect civil servants during the exercise of their duties, thus ensuring the conditions for the protection of the physical, moral integrity and dignity of civilians, and (2) the obligation of state institutions to ensure the protection of the civil servant during the exercise of the duty or in relation to it, requesting, if necessary, the support of specialized bodies according to the law.

[55] The Law is aligned with EU General Data Protection Regulation (GDPR) and EU Directive 2016/680 – Law Enforcement Directive. The general principle of the legislation in force on personal data protection is the lawful processing of personal data by respecting and guaranteeing human rights and fundamental freedoms and in particular the right to privacy.; A series of ratified legal acts in the field of personal data protection include: Law No 9288 dated 7.10.2004 On the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Law No 9287 dated 7.10.2004 On the Ratification of the Additional Protocol[55] to the Convention regarding supervisory authorities and transborder data flows. Law No 49/2022 On the Ratification of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[56] Decision No 60, dated 10.07.2023. Available here. The Code aims to improve the application of the right to gender equality, to tackle hate speech, and to address disinformation.

[57] Available here.

An ongoing issue remains the lack of adequate financial and human resources of the Gender Equality Mechanism, thereby hampering the implementation of the strategy. Further effort is needed to complete the collection of data envisaged by the strategy to allow adequate monitoring by the Commissioner for Protection from Discrimination.[58]

The National Strategy on Cyber Security 2020 – 2025[59] promotes and supports the cyber protection of the individual and citizens, and more specifically it places children at its focus.

The Strategy strives for enhanced legal framework in the field of cyber security, awareness raising not only among the Albanian society but also within key institutions.
Albania should adopt legal and sub-legal acts in line with its Cyber Security Strategy 2020-2025.[60]

The strategy does not make specific reference to cyber violence against women. Consideration could be given to linking measures of the Action Plan with international standards and policies in the area of cyberviolence against women.

Other National Strategies of importance that should incorporate the digital dimension of violence include:

1. National Action Plan for LGBT 2021-2027.[61] In line with the Action Plan, Albania needs to take measures to ensure systematic reporting, sanctioning and effective redress in cases of discrimination, hate speech and physical violence against LGBT persons.
2. Strategy for Equality, Inclusion and Participation of Roma and Egyptians 2021 – 2025
3. Strategy Against Organised Crime and Serious Crime 2021 – 2025
4. National Action Plan for Persons with Disabilities. The Committee on the Rights of Persons with Disabilities notes that: insufficient efforts have been made with regards to reviewing the existing legislation and bring it in full compliance with the Convention; derogative and discriminatory terms continue to be present in the national legislation, public documents or different public discourse.[62]
5. National Strategy on Health[63] foresees awareness campaigns in schools aimed at preventing violence and e-addiction as well as mental heal. No gender specific targets are identified in the plan.
6. The Action Plan for Mental Health 2023 – 2026 recognizes mental health and personal well-being are at risk by a number of factors including, violence, social exclusion and bullying. The Action Plan does not make reference to cyber violence. *It however notes the prevalence of irritability and low mood increases with age in girls*.[64] Disaggregated data on the underlying causes of this are missing, and would be crucial to develop targeted interventions. The Action Plan foresees development of manual/guideline for mental health of victims of trafficking and violence and abuse.[65] It would be constructive to foresee increased training of professionals which deal with cases of violence, including cyberviolence.

[58] European Commission. 2023 Country Report – Albania. Available here.
[59] Council of Ministers Decision No 1084, dated 24.12.2020 on 'Adoption of the National Strategy on Cyber Security and its Action Plan 2020 - 2025'. Available here.
[60] See: Specific Objective: Improvement of legal framework in the field of cybersecurity and further harmonization with EU Directives. Available here.
[61] Approved with DCM No 700, dated 18.11.2021. Available here.
[62] Available here. pg. 70.
[63] Available here.
[64] See Action Plan for Mental Health 2023 – 2026. pg. 9.
[65] See specific Objective 1.4. pg. 26. Available here.

Institutional framework

When analysing the institutional framework of Albania there are also a number of overarching themes that come about, and which require attention of the Albanian authorities, as well as those international organizations operating in the field and supporting further advancement of the country in countering cybercrime and cyber violence against women.

Generally speaking, several barriers are observed to impede the investigation and prosecution of cyber violence cases:

1. Victims lack awareness of their rights and struggle to access assistance;
2. Law enforcement agencies are not adequately equipped and trained to aid victims due to resource constraints;[66]
3. Cyber violence is often deprioritized by law enforcement due to workload pressures.

Below, an analysis of key actors involved and with a stake on addressing cybercrime and cyber violence cases.

Referral Mechanism

The amendments to the Law No 9669/2006 in measures against violence in family relations in 2018 (with Law No. 47/2018) and 2020 (with Law No 125/2020) were followed by a series of secondary legal acts aimed at clarifying and supporting the effective implementation of the Law, in compliance with the Istanbul Convention. Law No 9669/2006 provides a list of administrative institutions at the central level (Article 5-8) and at the local level and the courts that have jurisdiction to adjudicate these cases.

The Decision of the Council of Ministers (DCM) No. 327, date 2.06.2021[67] governs the standard basic procedures for the coordination of work between the authorities responsible for prevention of domestic violence, protection, provision of support, and rehabilitation services to victims, while guaranteeing human rights and promotion of gender equality, and elimination of all forms of discrimination against women.

This Decision regulates the most important standards of case management at the local level, based on a victim-cantered approach. This DCM also consolidates the job position and duties of the Domestic Violence Coordinator (DVC) in managing and referring domestic violence cases, at the local level.[68] The Decision creates space for the Coordinated Referral Mechanisms to engage, where appropriate, not only in cases of domestic violence, but also in cases related *to other forms of gender-based violence*. The DCM pays a particular attention to the collection, retention and disclosure of data related to these cases, by means of a dedicated electronic system for data management (REVALB).

[66] See also: Committee of the Parties – Istanbul Convention. (2021). Conclusions on the implementation of recommendations in respect of Albania as adopted by the Committee of the Parties to the Istanbul Convention. Available here. The conclusions of the Committee of the Parties to the Istanbul Convention of December 2021 noted progress but urged Albania to increase resources to put legal provisions into practice.

[67] Approved by DCM No. 327, dated 02.06.2021, repealing DCM No. 334/17.2.2011, National Coordinated Referral Mechanism for reporting and handling the domestic violence cases and the rules of proceedings.

[68] The response to cases of gender-based violence is coordinated by Referral Mechanisms Against Domestic Violence established in 61 Municipalities.

The Coordinated Referral Mechanism[69] for cases of domestic violence is set up at each municipality and its task is to prevent and handle the cases of domestic violence. Not all Coordinated Referral Mechanisms established in municipalities are effectively functioning. Specialist support services are understaffed, under-budgeted, insufficient, and *not tailored to treat all forms of violence including cyber violence and the very specifics of cyber violence in different groups of women.*[70]

This DCM includes an update of the list of institutions in charge of managing cases of domestic violence at the local level, and specifies their tasks to ensure a better coordination and harmonization of the working standards in all municipalities.

Education of all actors part of the Referral Mechanism needs to be ensured to increase awareness that domestic violence does not only occur offline but also online; and provide them with the necessary tools to deal with such cases.

The National Council on Gender Equality (NCGE) primary task is to lead, define and develop state policies on gender equality as well as to coordinate, implement, monitor and evaluate policies and measures for preventing and combatting all forms of violence covered by the Istanbul Convention. The Ministry of Health and Social Protection is responsible for gender equality and issues related to gender-based violence. Gender equality focal points are nominated in line ministries while at the local level the responsibilities lie with the gender equality officers/local coordinators against domestic violence in Municipalities. In some municipalities it is the same person, whereas in big municipalities they are two different people.

The Commissioner for Protection from Discrimination should ensure data collection and research on the prevalence and nature of cyber violence in Albania. It would be beneficial the Commissioner takes an active role in fostering partnerships with technology companies and social media platforms to develop tools and policies for preventing and addressing cyber violence against women. This can also take place done in cooperation with the Information and Data Protection Commissioner.

The Ministry of Interior has established a working group to make online violence a criminal offence. Consideration is given whether there should be a new legislation or development of sub-legal acts to address the current gaps in legislation.[71]

Within the (general) Prosecution and Judicial service there are cybercrime trained and specialized professionals. Most cybercrime cases are dealt with in Tirana district. The school for Magistrate is playing an active role in training judges and prosecutors.

The Prosecutor, for the purpose of a specific criminal investigation, has the power to establish investigation teams consisting of representatives of relevant institutions. The relevant

[69] The work of the Coordinated Referral Mechanism is based and adheres to a number of principles, including: easily accessible and approachable services; treating the victims with respect and dignity; c) prohibition of victimization, re-victimization and secondary victimization; ç) confidentiality and protection of personal data; d) life and health safety for the victims; dh) prohibition of discrimination; e) effective and individual care; and support and partnership.
[70] See also: UN Women. Albania Country Gender Equality Brief 2020. (2020). Available here.
[71] See: Top Channel. (2024). Dhuna ndaj grave edhe online – Ligj i ri dhe një aplikacion për të denoncuar rastet. Available here.

legislation provides a solid basis for inter-agency cooperation for the search, seizure and confiscation of online crime proceeds.

Albania should raise awareness among the prosecutors to enhance the use of the 24/7 points of contact network established by the Council of Europe Convention on Cybercrime. The prosecutor sends a request with a court order to the Police 24/7 point of contact unit, and these requests should also be recorded in the Ministry of Justice database.

Section for Cybercrime Investigation is part of the General Directorate of the State Police. In order to increase the quality of the investigation of cybercrime and crimes related to electronic evidence in the country, the cybercrime investigation structure needs to ensure that they are equipped with the necessary technical expertise and tools to provide rapid and professional response to the prevention, prosecution and investigation of crimes in cyber space.[72] Importantly, it is necessary to ensure smooth and enhanced cooperation, with national and international strategic partners in the field of cybercrime investigation.

Although there is a link on the State Police website to an online cybercrime reporting system, it seems that currently the system is not functioning. Thus, the Police is relying on various common communication means to receive complaints: phone, email, social networks, etc.

School of Magistrates continues to offer specialized obligatory training modules at the intersection of cyber violence, cybercrime and data protection. These training modules should be provided to practicing and in-training judges and prosecutors. It is important to raise awareness among all judges and prosecutors that crimes traditionally committed offline – not only against women but in general – have gained a new dimension.

Academy of Security should also provide, as part of their training curricula, information on technology-facilitated cyber violence and cybercrime.

The Public Administration Department together with the police and armed forces should ensure that policies and procedures against violence, harassment and sexual harassment, include recognition to gender-based online (sexual) harassment. In this context, awareness raising trainings to staff – to women and men – should be provided on regular basis, informing them on their rights and consequences, as well as available paths for reporting.

The National Authority for Electronic Certification and Cyber Security (AKCESK/NAECCS) monitors the implementation of Law No 9980/2008 on Electronic Signature, Law No 107/2015 on Electronic Identification and Trusted Services and Law No 2/2017 on Cyber Security, as well as by-laws issued for their implementation.

AKCESK acts as the National Computer Security Incident Response Team (CSIRT) and has a number of competencies in the field of cybersecurity including, but not limited to, establishing cybersecurity measures; providing assistance and methodological support to operators in the

[72] UNICEF. (2019). Faktori Web: Vlerësimi i kuadrit ligjor dhe gatishmërisë institucionale për trajtimin e abuzimit dhe shfrytëzimit seksual të fëmijëve në hapësirën kibernetike në Shqipëri. Available here. The UNICEF study states that neither the police nor the prosecution is fully equipped with the infrastructure for the efficient investigation of cases. The Cybercrime Investigation Unit appears to lack capabilities to conduct active online surveillance, undermining their ability to initiate ex officio and proactive investigations.
The Study focuses specifically on sexual abuse of children online. Yet, observations it makes regarding the functioning of set-in-place structures is also relevant in the context of gender-based online violence analysis.

field of network security; performing analyses of weaknesses in the field of internet security.[73] It is also responsible for conducting awareness-raising and education activities in the field of cybersecurity. In accordance with the legislation in force, the National CSIRT coordinates its activities with security and defence institutions and is required to cooperate with sectoral CSIRTs and international authorities in the field of cybersecurity.[74]

The National CSIRT organizes informal meetings with private sector entities to discuss new trends in terms of cyber threats, cybercrime techniques as well as prevention mechanisms and awareness.

It is important the Agency is vested with the necessary human and financial resources, and ensure a sufficient level of cyber security education, research and training, as well as to support internal needs for cyber security professionals.[75] In addition, it is equally important to facilitate establishment of a hub for close cooperation and information sharing between service providers and criminal justice authorities.

In the webpage, AKCESK provides for a form to report online illegal/harmful content aimed at providing a safe online environment for children and youth. It may be beneficial to provide something similar specifically for women, as victims of gender-based sexual violence and harassment online.

Statistics

Collection of statistics is important to inform the formulation of gender-equality legislation and policies.[76] Albania last produced a gender equality index in 2020. Having an up-to-date gender equality index is important for evidence-based policy-making in the sector. The same holds true for the periodical surveys on violence against women produced by INSTAT, which has not produced any update since 2018. Albania needs to ensure systematic and updated collection of disaggregated data.[77]

It is important to ensure that data on suicides or suicide attempts and on gender-based killings of women and their children include information on the history of harassment, including at the workplace, stalking or psychological violence perpetrated in the digital sphere.

The Femicide Observatory established at the People's Advocate marks the first of its kind, and is expected to collect and analyse data in order to improve policies and mechanisms to prevent the killing of women and girls.

[73] For more information see here.
[74] See Article 5 and 7 of Law No 2/2017 on Cyber Security. Available here.
[75] See also the Strategy on Cyber Security 2020 – 2025. Available here.
[76] This was also a pressing issue identified in the CEDAW Concluding Observations – Fifth Periodic Report for Albania. (November 2023) Available here.
[77] Albania – 2023 Screening Report. Cluster 1: Fundamentals. Available here.; See also: CEDAW Concluding Observations on the fifth periodic report of Albania. (November 2023). Available here

Key findings of the analysis

The analysis of the Albanian legal and policy framework on cybercrime reveals discrepancies with key international standards, including the Istanbul Convention, Budapest Convention, and EU Directive 2013/40.

Although the Albanian Criminal Code has made strides in addressing certain cybercrimes, it falls short in explicitly criminalizing technology-facilitated sexual harassment, online stalking, and psychological violence, leaving victims, particularly women, vulnerable to prolonged harassment and psychological trauma. Current legislation inadequately addresses online manifestations of these offenses, despite the Istanbul Convention's imperative for robust legal recognition and penalties for sexual harassment, stalking, and psychological violence perpetrated through digital means.

Further analysis against the Budapest Convention highlights the need for refinement in the Albanian Criminal Code to effectively combat cyberviolence and protect victims. Recommendations include incorporating specific provisions for cyber violence as gender-based violence, refining aggravating circumstances to acknowledge cyber-violence against women, and enhancing legal clarity through transposing international definitions into national law. Ongoing revisions to the Criminal Code are expected to address these gaps and align with international standards.

The Albanian Criminal Procedure Code (CPC), while largely aligned with the Budapest Convention's procedural law section, requires adjustments regarding search and seizure procedures, production orders, and interception of content. The CPC lacks specific provisions requires further alignment with international standards, including definitions and protocols for subscriber information and real-time collection of traffic data. Additionally, while the CPC includes measures for the seizure of data and computer systems, these provisions are limited and may require expansion to cover broader scope of cybercrime effectively.

Further legislative amendments are needed to the Law on Measures against Violence in Family Relations to address advancements in online violence, incorporating GREVIO Recommendation No 1, which emphasizes the importance of understanding cyber violence and training of relevant entities, including the judiciary and the prosecutor's office. Additionally, integrating ILO Convention No 190 into the Labour Code and the Law on Safety and Health at Work is essential to combatting online sexual harassment and ensuring safer workplaces for women.

The Law on Protection from Discrimination needs to be revisited to guarantee protection against all forms of discrimination, including online discrimination. The Commissioner is responsible for monitoring the implementation of this law and the Gender Equality Law, but details on the monitoring process and resource allocation are insufficient and need addressing.

The Law on Gender Equality, originally instrumental in establishing equality norms between men and women, requires updates to reflect advancements in international standards and to address gaps identified in recent reports. The CEDAW Committee and the European Commission have both recommended revisions to align with the National Strategy on Gender Equality 2021-2030 and the ILO Convention No 190. The law currently does not recognize gender-based violence as a form of discrimination nor provide remedies for women when authorities fail to protect them. Additionally, it lacks provisions for intersecting forms of

discrimination faced by women with disabilities and other disadvantaged groups. For effective implementation, it is essential that the Gender Equality Law and the Law on Protection from Discrimination are harmonized, and in coherence with one another, to ensure comprehensive legal coverage and that adequate resources are allocated for monitoring and enforcement.

The institutional framework in Albania faces several barriers in addressing cyber violence and cybercrime, which require attention from both national authorities and international organizations. Key challenges include victims' lack of awareness of their rights, insufficient resources and training for law enforcement. To improve the handling of such cases, the Referral Mechanism at the municipal level has been established to manage domestic violence cases, including cyber violence. However, many of these mechanisms are not effectively functioning, and specialist support services are often understaffed and under-budgeted. Training and awareness for all actors involved in these mechanisms are necessary to handle both offline and online violence adequately.

Key institutions like the National Council on Gender Equality (NCGE), the Commissioner for Protection from Discrimination, and the Ministry of Health and Social Protection play vital roles in defining, coordinating, and monitoring gender equality policies and measures against violence. There are also specialized cybercrime units within the State Police and the judicial system, but they require better equipment, training, and inter-agency cooperation. The National Authority for Electronic Certification and Cyber Security (AKCESK) oversees cybersecurity measures and works with various stakeholders to address cyber threats. However, there is a need for enhanced resources and a hub for cooperation between service providers and criminal justice authorities. Improved data collection, including statistics on cyber violence and gender-based crimes, is essential for informed policy-making and effective prevention strategies.

IV. Final Remarks and Recommendations

Technology-facilitated violence against women stands as a human rights violation, which shares its root causes with other forms of violence against women; and should be dealt within the broader context of the elimination of all forms of discrimination against women.

Different EU countries have adopted different approached in relation to cyber violence.

Some Member States, including Romania and France, combine the cyber and gender perspective, however their provisions do not clearly encompass all aspects and types of gender-based cyber violence. In Romania, ‘cybernetic violence’ is recognized as a form of domestic violence under the legislation on domestic violence.[78] Others criminalise specific types of cyber violence without addressing the gender angle, such as Belgium, Czechia, Spain and France.[79]

On cyber bullying, Italy addresses the protection of minors and some provisions of the Criminal Code can be used for combating violence online, even though it does not directly mention it (such as stalking).

[78] See: European Parliamentary Research Service. (2021). Combating Gender-based Cyber Violence. Available here.
[79] All Member States criminalise child pornography.

On cyber harassment, Austria is at the forefront criminalising the persistent harassment involving telecommunication or computer system.

Hate speech without a specific gender component is criminalised in Spain, the Netherlands, Bulgaria, Greece, Croatia, Portugal and Malta. These countries explicitly criminalise hate speech online. A number of Member States use existing provisions not specific to online crimes. These countries include Germany, Spain, Finland and the Netherlands. For example, Germany uses provisions that are not specific to cyber violence to tackle the issue, such as those for stalking and harassment.[80]

The legal analysis shows Albania has a very comprehensive legal framework, which serves as a strong basis for further amendments tailored to substantively incorporate those elements that address gender based cyberviolence and crime. By complementing this with the implementation of a framework law on cyberviolence, a number of advantages can be attained including legal clarity and consistency as well as enhanced information for and protection of victims.

Below a set of recommendations divided in clusters, in addition to the specific recommendations addressed throughout the study.

Recommendations

Legislative

1. Enhance legislative frameworks.

1.1 Address gaps in the current legislative framework, including in the Criminal Code and Criminal Procedure Code, as well as other pieces of legislation as examined throughout this analysis, such as Law on Protection from Discrimination, Law on Gender Equality, Labour Code etc (Reference to section:
An analysis of the Albanian legal and policy framework).

1.2 Define gender-based cyber violence. Address the lack of a harmonized legal definition of gender-based cyber violence and lack of a 'cyber' perspective in existing legislation.

1.3 Address the intersectional perspective in existing legislation.

1.4 Combine legal and non-legal policy options to generate the greatest added value and ensure that legal and policy frameworks support implementation of one another.

Key actors: Parliament of Albania, Council of Ministers, Ministry of Justice, Ministry of Interior, Ministry of Health and Social Protection, Civil Society Organizations.

Mechanisms and inter-institutional cooperation

2. Reform and strengthen monitoring and cooperation mechanisms.

[80] For a more detailed analysis see also: European Institute for Gender Equality. (2022). Combating Cyber Violence against Women and Girls. Chapter 3: Overview of the legal and policy framework on cyber violence against women and girls at the EU, international and national levels. p. 19 – 29. Available here.; See also: European Parliamentary Research Service. (2021). Combating Gender-based Cyber Violence. Available here.

2.1 There is need for the reorganization and strengthening of monitoring and governing mechanisms, at the central and local level, also through the strengthening of advocacy skills in this field.

2.2 Engage with platforms and recognize the important role of the Information and Data Protection Commissioner.

2.3 Clarify responsibilities for enforcement of court decisions, protection orders. Clear outline of the responsibilities of law enforcement actors, ISPs and online platforms in enforcing court decisions and protection orders in cases of cyber violence.

2.4 Promote cooperation across sectors. Increase cooperation between the private sector, civil society and law enforcement institutions.

Key actors at the central level: Council of Ministers; responsible Ministries at the central level including Ministry of Interior and Ministry of Health and Social Protection, General Directorate of the State Police *(cybercrime investigation), Information and Data Protection Commissioner, AKCESK, Civil Society Organizations.*

Key actors at the local level: all the actors part of the referral mechanism.

3. Improve victim support.

3.1 Address the issue of inadequate victim support by law enforcement.

3.2 Standardize mental health support services. Standardization of cross-sectoral services for mental health and psychosocial support, through clear referral routes, in order to improve the provision of this service.

Key actors: Ministry of Interior, Ministry of Health and Social Protection, Ministry of Justice, Order of the Social Worker; Order of the Psychologist, Civil Society Organizations.

Training and capacity building

4. Comprehensive training for stakeholders.

4.1 Judges, prosecutors, judicial police, police officers, attorneys, all actors of the referral mechanism at the central and local level, NGO, Commissioner for Protection from Discrimination, Labour Inspectorate and other actors with a stake on prevention/protection from cybercrime and violence, should be trained on types of and responses against technology-facilitated violence.

4.2 Improved training for criminal justice authorities. Provide better training and awareness raising for criminal justice authorities regarding cyberviolence, including its investigation, prosecution and sanctioning, where it constitutes a criminal offence, in line with obligations deriving from the Budapest Convention and Istanbul Convention.

4.3 Develop template courts decisions per type of cybercrime/cyberviolence to increase efficiency of justice.

Key actors: School of Magistrates, ASPA, School of Advocate, Academy of Security, Order of the Psychologist, Order of the Social Worker, International Organizations and Civil Society Organizations.

Prevention/Education

5. Raise awareness and address underreporting of cyberviolence through technology education and digital literacy.

5.1 These efforts should empower individuals with the knowledge and skills necessary to identify, address, and report instances of cyber-violence effectively. By enhancing digital literacy, users can better navigate online spaces, seek support, and prevent further victimization.

5.2 Raise awareness among women and girls. Implement targeted awareness campaigns to educate women and girls about reporting mechanisms and available remedies for addressing cyber-violence.

5.3 Include educational curricula on information technology and its risks, as well as criminal implications of technology-facilitate violence.

5.4 Support media as a key actor in raising awareness on cyber violence and its risks.

Key actors: Ministry of Education and Sport, the media.

Data Collection

6. Ensure the well-functioning of a centralized data keeping system, and systematic collection of disaggregated data.

Key actors: Ministry of Justice, Ministry of Health and Social Protection, Commissioner for Protection from Discrimination, National Council on Gender Equality, INSTAT.

Research

7. Allocate resources for research.

7.1 Invest in research and comprehensive understanding of various aspects of the phenomenon of gender-based cyber violence. Currently, there is limited quantitative data available on the social and economic impacts of gender-based cyber violence on victims.

7.2 Develop research that informs development of policies and strategies, such as a study of media habits of adults in Albania.

7.3 Understand current de jure and de facto gaps. Initiate a study to assess the existing capacities for enforcement of court decisions and protection orders in cases of cyber violence.

Key actors: Ministry of Education and Sport, Academy of Science, Universities (Faculty of Law, Academy of Security, etc.)