European Commission

The EU Mutual Learning Programme in Gender Equality

Combatting digital forms of violence against women

Finland, 6-7 February 2025

Discussion paper – Iceland

ösb Consulting
Ein Unternehmen der ÖSB Gruppe.

The information and views set out in this paper are those of the author(s) and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Justice

This publication is supported by the European Union Citizens, Equality, Rights and Values Programme (2021-2027).

This programme is implemented by the European Commission and shall contribute to the further development of an area where equality and the rights of persons, as enshrined in the Treaty, the Charter and international human rights conventions, are promoted and protected.

For more information see: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/cerv

Combatting and preventing digital forms of gendered abuse. Perspectives from Iceland

María Rún Bjarnadóttir

Rune Consulting

1. Combatting and preventing digital violence in Iceland

1.1 Background

Despite high ranking on international indexes measuring gender equality, violence against women remains a challenge in Iceland. To respond to reports of increased numbers of digital violence against women, the Government of Iceland set out legal and policy reforms, aimed at both improving response to and preventing digital forms of violence against women in 2021. These were implemented through a top down multi stakeholder model, relying on a wide range of actors and actions on a national level.

The Government of Katrín Jakobsdóttir already set out in their 2017 coalition platform plans to criminalise non-consensual sharing of intimate images. Their second term platform from 2021 addressed plans to systematically prevent sexual abuse, including in digital forms. A steering committee was formed with the participation of relevant ministers and external experts. The committee commissioned a report on digital forms of sexual abuse in Iceland. The report's findings were that the existing legal framework was not fit for purpose and suggested a "comprehensive response to enhance the protection of sexual privacy in Iceland", calling for "a criminal law reform combined with a threefold policy reform addressing preventative measures, victim support and adjustments to the process and resources attributed to the issue within the criminal justice system."

The parliament passed changes to the General Criminal Code defining the protection of sexual privacy in February 2021. These include a general update of the relevant provisions and introduced a special provision on sexual privacy under in the chapter on sexual violence, ensuring victims have access to all available support and free legal aid. In April the same year, the Ministers of Justice and Children and Education co-operatively tasked the National Commissioner for the Icelandic Police with rolling out holistic and wide-ranging policy measures aimed at supporting the effective implementation of the criminal reform.

2. Criminal reform

The parliament approved amendments to the General Criminal Code in February 2021. The bill was drafted on the foundation of academic research and explicitly rooted in the human rights obligations of the state under the European Convention System. The provisions were aimed at framing the interest of sexual privacy under the criminal code in a way that acknowledges the twofold nature of such violations as both a manifestation of sexual violence that disproportionally affects women and as a privacy breach protected under Art. 8 of ECHR.

2.1 Article 199. a. in the General Penal Code

Up until the February 2021 criminal reform, existing criminal provisions were applied to violations of sexual privacy, depending on the circumstances of the case. Judicial analysis exposed gaps and overlaps in the legislation, where provisions including criminal clauses were applied in somewhat inconsistent manner. The two main provisions applied were a general provision of privacy, describing that anyone who unlawfully discloses messages or images concerning another person's private matters shall be fined or imprisoned (Art. 228) and a broad "indecency offense" aimed at covering sexual offenses that fall outside other legislation and acts of indecent exposure (Art. 209).

A bill, based on the UK legislation, had been put forward in Icelandic Parliament in 2016 with the aim to criminalise "revenge porn", as it was referred to at the time.[1] This had opened up the political debate, allowing for the proposal that became law in 2021 to take place in a fairly well-developed political landscape.

The introduction of Article 199. a. in the General Penal Code in 2021 explicitly addresses sexual privacy as a protected interest, irrespective of the means applied to violate the right.

The clause reads:

> Anyone who prepares, obtains for themselves or for others, distributes or publishes images, text or similar material, including fake material, of nudity or sexual conduct of another person without their consent shall be subject to a fine or imprisonment of up to 4 years.

[1] The term revenge porn refers to similar acts as currently are addressed as violations of sexual privacy, non-consented intimate images (see i.e. stopnciiorg), image-based sexual abuse (McGlynn, Rackley et. al. 2018) and digital forms of gender-based abuse. However, the term revenge porn carries with it loaded notions that can be attributed to victim-blaming, misogyny and normalisation of pornography in a way that is harmful to victims. Although it was used in early stages of the development of the issue (i.e. Bjarnadóttir 2016), this terminology is no longer appropriate and should only be used to contextualise the issue.

> The same punishment shall be imposed on anyone who threatens as described in paragraph 1, provided that the threat is likely to cause fear or anxiety in the person to whom it is directed.
>
> If the offence is committed through negligence, it shall be punishable by a fine or imprisonment of up to 1 year.

At the heart of the clause lies the consent of the person whose rights are at stake. Diverging from other legal reforms, such as in the UK, regarding image based sexual abuse the focus is not on the intent of the perpetrator to harm with their actions, rather on the lack of consent of the victim. This emphasis underlines the issue is not female nudity or one rooted in morale. It focuses on the important personal rights that the clause aims to protect, not the social and moral context the provisions previously scarcely applied rely on. This approach further mirrors the recently reformed legal definition of rape under the Icelandic Criminal Code, where the lack of consent drives the assessment of the violation rather that the intent of the perpetrator.

The provision addresses any form of expression and is not limited to image or video format. This is essential to ensure victims are not discriminated against due to the means used to violate them or the manifestation of the acts in question, and that they enjoy the protection of the law irrespective of the means of violations their perpetrator takes.

Addressing fake material “futureproofs” the clause, envisioning that violations may take place through virtual reality (VR) or be created with the assistance of Artificial Intelligence (AI). This ensures the clause applies both to sharing and producing fake material of nudity or sexual conduct of another person without their consent. In essence this covers what has been referred to as “deepfakes”. With the fast-evolving pace of the technology, the legal provision is tailored to meet the most immediate evolving forms of abuse and is framed in a technology and medium neutral way to address the underlying interests at stake.

By addressing threats specifically in the clause, no room is left for interpretation or a circumstantial assessment on whether the victim is protected if threats are levelled at her regarding sexual content. The framing of threats as a stand-alone offence is an important tool when such threats are a part of a domestic abuse pattern and used to keep them at bay rather than seeking help.

The criminal liability test under the article is twofold, specifically addressing negligence as a qualifying standard to create criminal liability. This serves as a standard setting instrument in a normative context while focusing on the interest of the victim and the harm the offence poses to them.

The sexual offence classification ensures victims access to legal aid and recognises the socio-cultural context of sexual harm.

2.2 Further legal amendments

The legislation introducing Article 199.a. included further legal amendments to support the new clause. This includes:

- revised core clauses on privacy: Articles 228 and 229 on privacy were amended to reflect the increasingly digital nature of criminal privacy violations. The wording is updated to highlight a broader set of privacy standards, including sexual privacy, but does not provide the full protection of privacy the digital age calls for. As an example of this, digital identity theft does not enjoy the protection of the criminal code.
- Amending Article 242 to allow for public prosecution for privacy violations. Victims of sexual privacy violations should not have to rely on private prosecutions of privacy violations as was the case before the amendment.
- Changes to the Code of Criminal Procedure amending Article 88 to allow for police investigatory powers in sexual privacy violation cases.

3. Holistic policy measures developed in an inclusive manner and rolled out on a national level

3.1 A threefold action plan rolled out through broad partnership

In a co-operative effort between the Ministers of Justice and Children and Education, the National Commissioner for the Icelandic Police (NCIP) was tasked with rolling out holistic and wide-ranging policy measures aimed at supporting the effective implementation of the criminal reform. The efforts were ranging, implemented on a national level, with strong political and operational leadership backing. The measures were developed with the aim of reflecting both issues raised by victims and victim support groups representatives through interviews and media, as well as issues highlighted by the police and stakeholders from academia and within the criminal justice system.

3.2 Targeted preventative measures

3.2.1 Children

An age responsive prevention campaign was developed and delivered in schools across the country starting in the autumn term of 2021.

Age: Considering data indicating that a significant jump is in the number of teenage girls reporting feeling pressure to share their nude images at the age of 14, and the legal age limit for having a social media account is 13, the decision was made to target students in the 8th grade (13–14-year-old students).

Delivery: The material is on slides and video that is hosted centrally and online to ensure appropriate updates and uniform messaging to students. It is in Icelandic, but also available with English and Polish text. It is supported with guidelines for teachers and school staff.

In collaboration with the steering group set up under the National Prevention Strategy for Gender-based and Sexual Violence amongst Children and Young People teaching material about violence against children, including in sexual and digital forms, was collected and systematically made available. This includes material regarding digital forms of sexual abuse.

During the first year of the campaign, 2021-2022, designated regional and/or local community police officers delivered the material during their visits. As they did not have capacity to visit every school, the material was released to schools and teachers through the preventive hub of the local authorities to all directors for education in municipalities.

Key message of the preventive material and what is emphasised during the school visits is that:

- Consent is a core factor in all communication, but essential in sexual and digital communication.
- Children have the right to be safe – both online and offline
- Support is available
- It is important to report abuse, and there are many ways available to children to do so.

3.2.2 Parents/the general public

In relation to school viewings of the prevention material, information about it was sent out to parents and guardians. This was made available in Icelandic, English and Polish.

An online parents meeting was held in November 2022, and all material made available through online channels. 1000 participants signed up to the event, the maximum number the webinar platform licence allowed for. The interest far exceeded the registrations.

Through funding from Meta community fund, targeted ads on social media directed people onto information sites on the 112 website. The website has been updated to include information for parents regarding safe online use for children, safe internet use in general, and general parenting advice.

3.2.3 Perpetrators

In 2023, a programme for perpetrators of sexual abuse and people with inappropriate sexual thoughts about children was set up and funded by public authorities. The programme draws inspiration from the UK based services Stop it Now and affords services and support for perpetrators under the name "Taktu skrefið", meaning take the step.

An awareness campaign was run on social media with funding from Meta, targeting 18-35-year-old men with a YouTube video encouraging men to seek help if they are showing signs of inappropriate sexual interest online. The targeting group reflects the most common group of perpetrators of sexual abuse in police and prevalence studies

domestically. The launch of the services was further highlighted by various media engagements including publishing of articles.

Information for perpetrators and other concerned about their sexual behaviour online was developed in collaboration with leading experts in the field and made centrally accessible on the 112 website.

3.3 Update the criminal justice system

3.3.1 Training police officers

The Icelandic police education programme underwent significant changes in 2016, when the education was moved to a university level. During this transition, online criminal activity was given a bigger role in the education material and digital forms of sexual and gender-based violence against women became a part of the core curriculum of the programme in 2018. Investigation and evidence gathering in digital sexual abuse cases is now taught and addressed in two modules in the foundational police education course; the cybercrime module and the violence and power structures module. Despite the reshaping of modules in the police education programme from 2025 onwards, these issues remain a core section of the programme.

Under the measures introduced in 2021, the education regarding digital forms of sexual and gender-based violence against women were also made mandatory in the curriculum for training routes to become investigators or shift commanders that are available through the Police Training and Continuous Education Centre. This ensures that no police officer progresses into an executive position without training on digital abuse. The training addresses the underlying issues of gender-based violence and how these manifests in different ways, including digital. The training also includes investigative protocols, evidence gathering and information about access to services and support for victims.

Further, the Police was awarded funding under the National Action Plan on Cyber Security to introduce training for prosecutors and judges on issues of cybercrime, including on digital forms of sexual and gender-based violence. These partly rely on existing training available, such as the Council of Europe Help programme on cybercrime, but an adapted version of the police education material has been developed in the domestic context, relying on existing case law and standards.

3.3.2 Revising investigative protocols

The aim was to also include a revision of all investigative protocols. During the time the time the programme was in place, the Ministry of Justice issued a new action plan on Combatting and Preventing Sexual Abuse in Iceland where one of the main actions was to introduce new investigative protocols for sexual abuse, including digital sexual abuse.

3.4 Comprehensive victim support

3.4.1 Build on existing support services

Rather than creating new routes of information sharing, reporting or support services, it was decided to lean on existing structures and support this operation in updating their operations to include digital forms of abuse.

In Iceland, the NGO sector is strong and has for a long time provided support services for women victims of abuse. Further, the domestic support system on local levels includes support for children and women alike, available to all irrespective of background or means. This is deployed through services on local level, including schools, social services and child protective services that already have a well-established mechanism for supporting victims of abuse. Rather than introducing new avenues for support for victims of digital forms of abuse, the existing support services were upgraded to include mechanism for information and support regarding digital abuse.

The 112.is violence information hub was updated to include information regarding digital forms of abuse, safe use of technology and issued an app that allows for direct reporting and location sharing.

3.4.2 Introduce technical victim support domestically

In 2021, two international platforms that help limit the spread of non-consensual imagery were mainstreamed. The Icelandic police was an early supported and adapter of the services, the stopncii.org and takeitdown.ncmec.org.

Introducing accessible ways to limit the spread of images addresses the concern of victims and possible victims. The aim of systematically include internationally operating services in domestic victim support is to:

- Empower victims
- Utilize already existing instruments
- Contribute to a unified approach for victims

To introduce the methods, the police gave lectures and talks for all interested stakeholders. This includes the largest municipality in Iceland, Reykjavík, collaborative platform for social workers and psychiatrists, staff from safe houses and NGO´s and prevention officers from schools. Talks and training was conducted for all staff members of women´s support services, Domestic Abuse shelters and NGO´s operating in the field.

Further, the police produced and made available standardised responses for young people experiencing digital forms of sexual harassment, pressure to share sexual images or being sent unwanted sexual images.

3.4.3 Co-operation with industry stakeholders

As Meta owns the biggest platforms used in Iceland, the police arranged for training for staff members of women's support services and domestic abuse shelters from

Meta about the safety measures available for women through their platforms.[2] This is not least to respond to victims of domestic abuse that have left the home for the domestic abuse shelter that continue to experience digital forms of threats and violence when in the shelter. By enhancing the staff knowledge about the safety and security measures available on the platform, they can better support the victims.

In collaboration with Pornhub, the most popular platform for pornography in Iceland, information about the perpetrator programme Taktu skrefið is made available via a direct link should a user of the platform with an Icelandic IP-address seek out content linked to illegal sexual behaviour.[3]

4. Strengths and challenges

4.1 Strengths

4.1.1 Long term approach in legal reform

The legislative reform is centred around consent, or lack thereof, and does not focus on the intent of the perpetrator. The legal protection protects the interest at stake, irrespective of the form it takes or if it is fake or real. This is particularly important in light of the fast pace technical development. The clause is narrowly tailored to fit the existing legal framework, while plugging gaps and avoiding overlaps within the criminal code.

4.1.2 Political priority

As the legislation was passed and the Government rolled out the programme with the direct participation of two ministers and the National Commissioner for the Icelandic Police, it showed that the project has high level support to back up both funding and commitment to the project. This was important strategically, but also from a media standpoint that gave the project important media coverage and helped with raising awareness.

4.1.3 Builds on academic research

The measures were proposed with strong theoretical and practical backgrounds, allowing for trust to be established within and between different stakeholders on common ground of research.Importantly, the academic research built on explored existing standards and practices from other countries. By examining the legal framework in the other Nordic countries, England and Wales, Scotland, Australia and the United States, the research reflects a range of practical and scholarly approaches

[2] Facebook and Instagram are the platforms most used by adults in Iceland. See data from the Icelandic Media Commission

[3] This led to 15 people seeking help in the year of 2024.

to the issue of digital forms of sexual abuse that were of paramount importance when drafting the legal reform.

Further, the research provided a strong foundation for the rights-based approach adopted in the legal drafting. In particular, the standards under the European Convention System including the European Convention on Human Rights and the Istanbul Convention proved useful in this context.

4.1.4 Collaborative approach involving many stakeholders

Rather than addressing the issue of digital sexual abuse as a single issue, an effort was made to highlight the links between it and existing and recognised patterns of behaviour and well-established criminal concepts. This prevented power struggles and allowed for the inclusion of a range of stakeholders with various experience.

4.1.5 Measuring progress

For the implementation of the project, it was decided against setting up a specific metric unit to measure to progress of actions taken as a part of the project, rather than relying on a range of existing and reliable metric sources. This provides a broad perspective on the results acknowledging the issue calls for actions from a variety of stakeholders that use different sticks of measurement.

An example of how the data is used to illuminate the programme activities is the following:

- At the time of the project launch in 2021, there had been a significant increase in child victims in cases of sexual violations reported to the police, with 61% under the age of 18 in all cases reported in 2021. In 2024 the number was 46%.
- In 2021 teenage girls reported strong and mounting pressure to share sexual images from the age of 14 years, with 25% of girls 15-17 having been pressured to share intimate images and nearly 18% having the images shared further without consent. In the findings from 2023 12% of 15–17-year-old girls reported being pressured and 9% had had their images shared without their consent.

4.1.6 Holistic approach

By following up the legal reform with policy measures, an effort is made to implement the legal changes. This is essential to the success of the project.

Involving a range of stakeholders that have different interests and entry points to the issue has proven valuable and helpful to strengthen both new and existing collaborative platforms.

By implementing measures that are aimed at reducing the number of violations through perpetrator prevention, supporting and empowering existing victims and hopefully preventing further harm as well as raising awareness among the public, the issue of digital sexual abuse should not be seen as a single issue anymore.

4.2 Challenges

4.2.1 Ensuring long-term implementation of the policy measures

Following the introduction of the measures and their implementation, it remains to be seen if there will be consistency in the approach on a long-term basis. Despite some mitigating measures being put in place, there is a risk the efforts will be approached as a one-off and that skills and training will not keep up with evolving manifestations of digital forms of violence. This both applies to all sectors of the criminal justice system, as well as within the support services available to victims.

4.2.2 Funding

A weakness in the programme was that it was only specifically funded for one year, with the intent of the actions becoming mainstream and non-reliant on programme funding. Additional funding was awarded to the programme, but formally the programme's actions are coming to an end early 2025, with the foresight that all actions have taken place, and some will have become a standardised practice moving forward.

4.2.3 Streamlining and sustainability of school prevention campaign material

As schools are faced with reginal and local challenges, they have different needs for education and preventative actions from their local community police officers. In a bid to be responsive to the needs of the school environment, the community police officers have found it challenging to deliver the material in a uniform manner within and between regions. Further, as there is not specific funding set aside for this kind of training to take place, it runs the risk of falling to the back of what is interesting at any given time rather than being addressed as a core issue.

5. Summary

The Icelandic approach to preventing and responding to digital forms of sexual abuse disproportionally affecting women relies on broad collaboration and a range of measures aimed at a common goal rooted in gender equality and respect for human rights. As measurements show, progress has been made to reach this goal both from a legal and a practical standpoint. This has however not eradicated the practice, and new forms of technology facilitated gendered abuse continue to come to light. Continued implementation of existing measures and consistent application of the criminal law thus is of great importance. Further, despite successful implementation of the actions discussed in this paper, public authorities must continue their commitment to preventing and responding to digital manifestations of gendered abuse in an agile and responsive manner.