GUIDE TO SURVIVE:

HOW TO DEFEND YOUR ONLINE SPACES AGAINST ONLINE GENDER BASED VIOLENCE

sflc.in unesco

Guide to Survive- How to Defend Your Online Spaces Against Online Gender Based Violence, 2024
By SFLC.in in partnership with UNESCO

Published by: SFLC.in
K9, 2nd Floor, Birbal Road, Jangpura Extension, New Delhi – 14, India.

Email: mail@sflc.in

Website: https://www.sflc.in

X: @SFLCin

WHAT DOES OGBV MEAN?

Gender based violence refers to targeted actions against people because they belong to a certain gender, and are committed with the intent to cause harm. When this takes place on online platforms, it is called **Online Gender Based Violence**. To keep things simple, let's call it **OGBV.**

WHAT ARE THE INGREDIENTS OF OGBV:

- ❑ **It takes place online**
- ❑ **Based on one's gender**
- ❑ **Causes harm**
  - Psychological, damage to reputation, physiological (ex: harassment)
  - Impact on financials economic harm (ex: online extortion, property damage)
  - Social isolation (ex: defamation)

GENERAL DEFINITIONS

There are a few common terms you'll find in the law when it comes to defining an offence. We've simplified that here for your reference:

a. Obscene: something so repugnant or offensive to current standards of morality/decency that it is not considered acceptable by the general public.

b. Sexually explicit: nudity, depictions of actual or simulated sexual acts.

WHAT IS THIS BOOKLET, WHY DO I NEED IT?

This guide is designed to help you understand:

1. What OGBV is.
2. If you have experienced OGBV yourself.
3. How the law can help you take action against the perpetrators of OGBV.

NAVIGATING THE GUIDE

PART 1

Part 1 explains Online Gender Based Violence (OGBV).

PART 2

Part 2 discusses the available legal recourse for those subjected to OGBV.

PART 1: OGBV CHECKLIST

This checklist serves as a tool to identify if someone has experienced Online Gender Based Violence and are seeking information about the corresponding legal consequences for such actions.

1. ONLINE SEXUAL HARRASSMENT

An extension of sexual harassment that takes place in-person and physically.

- **A** Is someone making remarks that are sexual in nature to you?
- **B** Are they demanding or requesting sexual favours from you?
- **C** Are they forcing you to watch pornographic content?
- **D** Are they continuing to make advances?

If any of this from A to D is true, and is happening online and without your consent, then this behaviour constitutes online sexual harassment.

IPC, Section 354A

Sexual harassment: Imprisonment for up to 3 years, and/or a fine.
Sexual remarks: 1 year imprisonment and/or a fine.

Applicable to: Women being subject to such behaviour by men online.

2. CYBERFLASHING

- **A** Has someone been sending you obscene or explicit content online?
- **B** Do they include private images, or pornographic material for instance?
- **C** Are they doing this without your consent?

If you've checked all of the above, then it is likely a case of cyberflashing.

IT Act, 2000, Section 67

First time offence: 3 years imprisonment + fine upto INR 5 lakh.
Repeat offence: 5 years imprisonment + fine upto INR 10 lakh .

IT Act, 2000, Section 67A

First time offence: 5 years imprisonment + fine up to INR 10 lakh.
Repeat offence: 7 years of imprisonment + a fine that could go up to INR 10 lakh.

Applicable to: Anyone experiencing this.

3. CYBERSTALKING

A Is someone repeatedly trying to have a conversation with you online?

B Is this continuing despite you making it clear that you are not interested?

C Do you think they are monitoring your activity? i.e. they see you online and reach out, keep track of how many times you are active on an app etc.

D Were you informed that this was done to prevent a crime? Were you told that someone was doing their duty? (ex as a police officer undercover for a case) or were you given a reasonable justification for this behaviour?

E Did you ask for any ID for situations mentioned in points C and D? (While it is not mandatory, it is recommended that you ask for an ID to verify someone's identity and their statement, especially if someone is claiming to be a police officer).

If you have checked A, B & C, then this is likely a case of cyberstalking. If the last was true, then please note that the previous activities would likely not be considered cyberstalking since there was a lawful justification for it.

IPC, Section 354D

First time offence: 3 years imprisonment + fine.
Repeat offence: 5 years imprisonment + fine.

Applicable to: Women being cyberstalked by men.

4. NON-CONSENSUAL DISSEMINATION OF INTIMATE PHOTOS AND VIDEOS

A Is someone sharing intimate photos and/or videos of you online?

B Have you not consented to this?

C Additionally but not mandatorily: Did a romantic partner/former romantic partner do this?

If you have checked off A & B, it is likely a case of non-consensual dissemination of intimate photos and videos.

IT Act, 2000, Section 66E

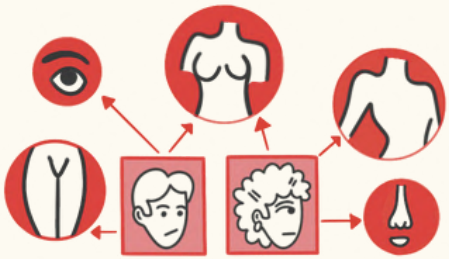
3 years imprisonment + fine up to INR 2 lakh.

IT Act, 2000, Section 67A

First time offence: 5 years imprisonment + fine up to INR 10 lakh.
Repeat offence: 7 years of imprisonment + a fine that could go up to INR 10 lakh.

The laws mentioned above apply generally. In case a romantic partner did this to you, it may be revenge porn, which is a form of intimate partner violence. It is important to remember that you are not to blame for any reason whatsoever in such situations, and to reach out to family/friends you can trust to support you. We cover more of this in the recourse section.

Applicable to: Anyone experiencing this.



5. DOXING

A Did you find private information about yourself online? Such as photos, videos, or text that were not publicly shared or posted by you, or personal details about you such as your address, Aadhar number, medical information that you do not want to be seen by anyone?

B Did this happen without your knowledge and consent?

C Is that information being used against you? Are you being harassed and bullied/ threatened?

If you check all of the above, then it is likely a case of doxing.

IT Act, 2000, Section 67A
First time offence: 5 years imprisonment + fine up to INR 10 lakh. Repeat offence: 7 years of imprisonment + a fine that could go up to INR 10 lakh.

IT Act, 2000, Section 66E
3 years imprisonment + fine up to INR 2 lakh.

IPC, Section 499
2 years imprisonment and/or fine

Applicable to: Anyone experiencing this.

6. MORPHING/ TRANSMOGRIFICATION

A Did you find photos that you posted online being edited onto other photos that you didn't take? Do you see that your face is replacing someone else's on videos, and to make it look like the person in the video is actually you?

B Was this done without your consent and knowledge?

C Was the content obscene content/sexually explicit content?

D Do you believe it could also have been deep fake/artificially generated sexually explicit content? [not mandatory to have been the case for it to be morphing]

If you checked off everything from A to C, then it is likely a case of morphing.

IT Act, 2000, Section 66E
3 years imprisonment + fine up to INR 2 lakh.

IT Act, 2000, Section 67A
First time offence: 5 years imprisonment + fine up to INR 10 lakh. Repeat offence: 7 years of imprisonment + a fine that could go up to INR 10 lakh.

IT Act, 2000, Section 66D
3 years imprisonment + fine up to INR 1 lakh.

Applicable to: Anyone experiencing this.

7. VOYEURISM

A Were photos/videos or other content of you made when you were unaware?

B Did it involve a private moment where you expected privacy?

C Even if you allowed for it to be captured, was it shared or posted online without your consent?

If you have checked off everything above, then it is likely a case of voyeurism.

IPC, Section 354C

First time offence: 1 year up to 3 years imprisonment + fine.
Repeat offence: increase up to 7 year imprisonment + fine.

IT Act, 2000, Section 67

First time offence: 3 years imprisonment + fine upto INR 5 lakh.
Repeat offence: 5 years imprisonment + fine upto INR 10 lakh .

Applicable to: Women who have been subjected to this by men.

8. ONLINE SEXPLOITATION+ SEXTORTION

A Are you being made to undress against your will by someone? Do you feel threatened or fear an injury if you don't and fear for your safety if you do not do what they want?

B Is this person doing this through the internet and forcing you to engage in such acts on the internet?

C Are you being threatened into doing sexual favours, sharing more private images or videos? Is someone blackmailing you into doing so? Do they warn you that your private details, images or videos will be circulated online or shared if you do not do what they say?

If you've checked off the above, it is likely a case of sexploitation and sextortion.

IPC, Section 354

First time offence: 2 years imprisonment and/or fine.

IT Act, 2000, Section 66E

3 years imprisonment + fine up to INR 2 lakh.

IPC, Section 507

Pertaining to anonymous criminal intimidation: i.e. Threatening harm to someone's person, reputation, or property: 2 year imprisonment and/or fine.
Threatening to harm someone with the intention to cause a serious injury or death: up to 7 year imprisonment and/or fine.

IPC, Section 503

Criminal intimidation–i.e. Threatening to cause harm to another person, their reputation or their property: imprisonment for a period of up to 2 years and/or a fine.
If there was an intent to cause a serious injury or death, then the imprisonment could be for a term of up to 7 years and/or a fine.

Applicable to: Anyone who experiences this. Section 354 applies to women.

9. GENDER-BASED HATE SPEECH

A Have you been the target of violent, offensive, or discriminatory content online including gender based slangs? Do you believe people are sending you such hateful messages because you belong to a particular gender?

B Do you see this content harming or potentially causing harm to you, your reputation, your property and others associated with you?

C Has any of the content threatened to cause serious injury to you, or even death?

If you've checked off A & B, it is likely an instance of gender-based hate speech.

IPC, Section 499

2 years imprisonment and/or fine.

IPC, Section 503

Criminal intimidation: i.e. Threatening to cause harm to another person, their reputation or their property: imprisonment for a period of up to 2 years and/or a fine. If there was an intent to cause a serious injury or death, then the imprisonment could be for a term of up to 7 years and/or a fine.

IPC, Section 507

Pertaining to anonymous criminal intimidation: threatening harm to someone's person, reputation, or property: 2 year imprisonment and/or fine. Threatening to harm someone with the intention to cause a serious injury or death: up to 7 year imprisonment and/or fine.

IPC, Section 509

3 years imprisonment + fine

Applicable to: Anyone experiencing this.
Section 509 specifically applies to women.

10. IDENTITY THEFT

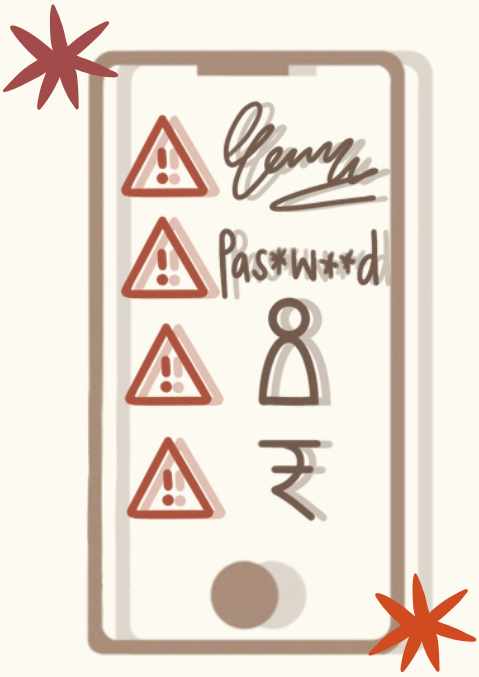
A Was your password, electronic signature or other unique information about you used by someone else to pretend to be you?

B Has anyone made any communication, representations or statements to engage in fraudulent activity?
ex: did you find that new loans were being taken in your name?

If you have checked any of the above, it is likely a case of identity theft.

IT Act, 2000, Section 66C
upto 3 years imprisonment + fine up to INR 1 lakh.

Applicable to: Anyone experiencing this.



11. OFFENCES SPECIFIC TO MINORS

A Are there texts or images or other forms of content being created online?

B Are text/image/other forms of material being collected?

C Is the subject of such material a child/children?

D Are they being depicted in an obscene/sexually explicit manner?

If all the above are true, then it constitutes an offence against minors.

E Is such material being advertised/exchanged/distributed?

F Is such material being downloaded?

G Is such material being browsed?

H Are children being induced into developing relationships online in a manner that would offend a reasonable adult? (aka evidence of grooming/predatory behaviour)

I Is the distribution of this content being facilitated?

If any of the above from A to D are true, then the act would be a punishable offence under 67B of the Information Technology Act, 2000. E to I provide additional context to the commission of the offence.

IT Act, 2000, Section 67B
First time offence: 5 years imprisonment + fine up to INR 10 lakh.
Repeat offence: 7 years imprisonment + fine upto INR 7 lakh.

Applicable to: Any child/children.

PART 2: RECOURSE

WHAT DO I DO NOW?

DOCUMENT EVERYTHING

Take screenshots. Document every interaction, every site on which you see instances of OGBV taking place, date of the incident, every profile that is partaking in such incidents and posting it online. Remember this is all evidence of the offence that is being committed, be as thorough as you can.

REPORT

- See if there's a 'report' option. This allows you to tell the site/social media site (like Facebook, Instagram) to take action and remove that content. You will find certain categories under which you can report this content- usually 'inappropriate', 'bullying/harassment', 'violence' and so on. As per the law in India, social media sites are required to acknowledge your complaint and take appropriate action within 24 hours of receiving it. Do ensure it is reported, and request trusted friends and family to report the content as well. In the meantime, please block the account you are receiving this content from so they cannot contact you any further.

- You would receive an update about the decision on your account. If you are unhappy with it, you also have the option to request that they review their decision.

- If after requesting reviews and getting their decisions, you believe the social media site has not taken the right decision, you can file a complaint with the government's Grievance Appellate Committee, on: https://gac.gov.in/

- To understand how your application will be reviewed by them, it is recommended you also take a look at some of the FAQs on the link below. They make the final decision about what needs to be done with the content.

https://gac.gov.in/CMSData/FAQs?qs=+WcLOPiE4QBLh0NRiMqmqQ==

- The Government also has a National Cyber Crime Reporting Portal where you can report these incidents- the link to the site is: https://cybercrime.gov.in/Webform/crmcondi.aspx.

The helpline number is 1930. The women's helpline number is 181.

Before you file your complaint on the portal, take a look at their FAQs as well: https://cybercrime.gov.in/Webform/FAQ.aspx.

We recommend you take the above mentioned steps in a timely manner. When filing an FIR at the cyber police station, they may request these steps too. You can take all of these actions while your report with the platform is being addressed.

FILE AN FIR

- If you want to file an FIR with the police, go to your nearest police station or the cybercrime unit if your city has one. The locations are usually available on Google Maps. In case they try to discourage you from filing, please reiterate that you have done what is required and you wish to have this on record.

- In case you face a situation where they refuse to file your FIR, you can file a complaint with the Superintendent of Police under section 154 (3) of the CrPC.

- You also have the option to go to another police station- even if they do not have jurisdiction, they can still file it and transfer it to the relevant station (this is called a Zero FIR). You can also approach the local district magistrate to file the complaint in the event that this doesn't work.

Please remember that you have the RIGHT to register a complaint under the law.

- Filing an FIR: Please try to write what happened as clearly as possible. Include relevant details. You can even tell them about the incident orally and the officer will write it down. Please check that it is accurate- they will also read it out to you; in case they don't, request them to do so. Ensure that you have received a copy of the FIR with a stamp on it (with the police diary number, 'DD No.', on it), and make sure to note down the FIR number, the filing date, and the name of the police station. The police are required to investigate this once this is done.

APPENDIX

IPC - Indian Penal Code
IT Act, 2000 - Information Technology Act, 2000

IPC, Section 499
Relating to criminal defamation, punishes individuals who (by either speaking or writing) intends to cause harm to the reputation of another person, or knows their actions will cause harm to their reputation.

IPC, Section 354
The exploitation and extortion of women: It punishes anyone who assaults or forces a woman to act in a manner that would outrage her modesty.

IPC, Section 354A
Defines and penalises behaviours that qualify as sexual harassment.

IPC, Section 354C
Punishes any man who secretly or intrusively captures the image of a woman engaging in a private act. Punishes any man for sharing or distributing these captured images without the woman's consent.

IPC, Section 354D
Deals with the offence of stalking. IPC 354D was introduced to criminalise the act of stalking, particularly in the context of electronic communication or monitoring of an individual's online activity.

IPC, Section 503
Pertaining to criminal intimidation: i.e. Threatening to cause harm to another person, their reputation or their property.

IPC, Section 507
Deals with criminal intimidation Threatening to cause harm to another person, their reputation or their property by an anonymous communication.

IPC, Section 509
Punishes insults to the modesty of a woman or which breaches the privacy of a woman.

APPENDIX

Section 154(3) in The Code Of Criminal Procedure, 1973
(3) Any person aggrieved by a refusal on the part of an officer in charge of a police station to record the information referred to in subsection (1) may send the substance of such information, in writing and by post, to the Superintendent of Police concerned who, if satisfied that such information discloses the commission of a cognizable offence, shall either investigate the case himself or direct an investigation to be made by any police officer subordinate to him, in the manner provided by this Code, and such officer shall have all the powers of an officer in charge of the police station in relation to that offence.

IT Act, 2000, Section 66C
Deals with the punishment for identity theft. This section specifically addresses the crime of using someone else's identity dishonestly with the intent to cause harm or commit fraud.

IT Act, 2000, Section 66D
Anyone who cheats by personating another individual through a communication device or a computer will be punished.

IT Act, 2000, Section 66E
anyone who shares images of a private area of any person online without their consent is liable to be punished because it breaches their bodily privacy.

IT Act, 2000, Section 67
Penalises publishing or transmitting obscene material in electronic form.

IT Act, 2000, Section 67A
Penalises publishing or transmission of material containing sexually explicit content in electronic form.

Misuse of 67 & 67A:
These sections impose significant punishment, and with words such as ‘obscene’ and ‘sexually explicit’ having ambiguous interpretations, they have been routinely misused and led to indiscriminate arrests. The sections punish the transmission and publication of such material. They also do not separate consensual acts from non-consensual acts, either could apply to these offences.

IT Act 2000, Section 67B
Deals with the punishment for publishing or transmitting material depicting children in sexually explicit acts.

sflc.in unesco