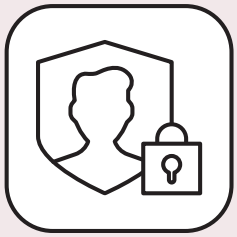

PERSONAL SAFETY AND DATA PRIVACY

Everyone has a right to control information about themselves and to secure protection from digital harms.

↓

The right to privacy underpins our use and enjoyment of other human rights. It encompasses the right to privacy in family life, the home, and correspondence, and freedom from attacks on a person's honor or reputation.

In the digital realm, the right to privacy is not just about the right to be left alone. With our personal data increasingly being extracted and analyzed to inform and fuel algorithmic decisions that affect every aspect of our lives, the right to privacy is also about protecting our rights to justice, dignity, and autonomy.

Digital privacy is also about safety. The internet is rife with bullying and harassment, while the online exploitation and abuse of women, girls, and children has reached unprecedented global proportions. At the same time, digital technologies and services are increasingly being used for manipulation and suppression of dissent, including through the use of smart devices by domestic abusers to monitor and control women's behavior.

The lack of recognition and enforceability of the digital right to privacy results in women, girls, and other discriminated-against groups and marginalized people lacking protection from – and redress for – serious harms to their careers, safety, and social freedom, as well as to their dignity, bodily integrity, and autonomy.

THE DIGITAL PRINCIPLES

- Everyone has the right to the protection of the data that concerns them – and to be able to understand, in very simple terms, how that data is processed.
- No one shall be subjected to arbitrary interference of this right, and any limitation of this right shall be reasonable, necessary, proportionate, and justifiable.
- Any processing of data shall be fair, lawful, and transparent, adhering to data processing principles set out in international norms and standards.
- Particular attention should be afforded to the structural issue of intimate privacy violations against women, girls, and people of marginalized genders.
- Everyone has a right to protection against unfettered forms of surveillance, including in places of work and education and during civic participation. The use of facial recognition or biometric technologies must be regulated, necessary, and proportional.
- Everyone has the right to encryption and online anonymity. Sharing of data with third parties, including law enforcement agencies and the private sector, must be limited to what is reasonable, necessary, and proportional.
- Everyone has the right to control their digital legacy and to decide what happens with the publicly available information that concerns them after their death.
- Digital service providers must be held accountable as more than mere conduits for user-generated content, particularly that involving hate speech, incitement to cause harm, and/or the exploitation and abuse of women, girls, and other discriminated-against groups and marginalized people.
- States must accept an obligation to safeguard citizens from online abuse, misogyny, and hate crime, including by conducting swift, cross-jurisdictional investigations and upholding the right of victims to obtain appropriate and holistic remedies.
- Protection from abuse should include all forms of online sexual exploitation and abuse, including sexual harassment, stalking and tracking, coercive control, technology-enabled sex trafficking, livestreaming of sexual abuse, child sexual abuse material, and image-based sexual abuse, including through deepfake sex videos.