OHCHR MULTI-STAKEHOLDER CONSULTATION ON ACCESS TO REMEDY IN THE TECH SECTOR

Session 3: Understanding the perspectives and needs of affected stakeholders when attempting to seek remedies

Part II: Case Studies[1]

Guiding questions

- What type of harm has occurred? Did the business enterprise cause the harm, contribute to the harm, or is it involved solely because the impact is directly linked to its operations, products or services?
- Which options for remedy can be considered/which pathway for remedy is the most promising/effective one to try to get access to remedy?
- Why would you recommend that pathway to be chosen over other mechanisms?
- Is the set-up of that mechanism and process of the mechanism transparent for you, and why/why not? Can you anticipate the process of the mechanism?
- Are there any examples of good practice where effective remedies have been available in similar situations?

Case Study 1: Racial bias in AI and ADM systems used in the criminal justice system

Background: Artificial intelligence (AI) and automated decisionmaking (ADM) systems are increasingly used by law enforcement and criminal justice agencies for a range of tasks, including profiling individuals and predicting the likelihood of criminal offending or re-offending. While used by state actors, the systems are often developed by, or alongside, private companies. Concerns have been raised that these systems are built on biased datasets and thus produce biased and discriminatory outcomes, particularly on the basis of ethnicity, race and nationality.

Human rights engaged: Decisions made by AI and ADM systems which are discriminatory or which disproportionately disadvantage individuals on the basis of characteristics such as race, ethnicity or nationality engage the right to non-discrimination (Articles 2(1) and 26, ICCPR). By predicting behaviour related to criminality, these systems also engage the right to a fair trial, which includes the presumption of innocence (Article 14, ICCPR).

Source: Fair Trials International, "Automating Injustice: The Use of Artificial Intelligence & Automated Decision-making Systems in Criminal Justice in Europe", 2021

[1] These case studies were developed by Global Partners Digital for the purposes of discussion during this consultation.

Case Study 2: Sensitive data exposure

Background: Many tech companies and the apps that they develop rely on the collection, storage and processing of personal data. This data can sometimes be extremely sensitive, for example where it records a person's self-expressed sexual orientation and gender identity, particularly in contexts where LGBTI individuals face persecution and discrimination within society or by state actors. In recent years, dating apps targeted at LGBTI individuals have been involved in data breaches and data exposures, causing concern that individuals' private information could be made public and put them at risk.

Human rights engaged: Any situation whereby individuals' personal data are used or shared without their consent raises issues under the right to privacy (Article 17, ICCPR). The potential consequences, which may include violence and discrimination, engage the rights to freedom from torture or to cruel, inhuman or degrading treatment or punishment (Article 7, ICCPR), the right to security (Article 9, ICCPR) and the right to non-discrimination (Article 26, ICCPR). In the most extreme cases, the right to life could even be engaged (Article 6, ICCPR).

Source: Recorded Future, "Online Surveillance, Censorship, and Discrimination For LGBTIQA+ Community Worldwide", 2020

Case Study 3: Online gender-based violence

Background: Many groups that might be at heightened risk of vulnerability or marginalization, or that have been historically disadvantaged, face higher levels of abuse, harassment and violence online. Women, in particular, face a range of hostile and threatening behaviours ranging from trolling and pile on to doxing and death threats. This trend appears to have been exacerbated during the COVID-19 pandemic. While most major social media platforms have policies preventing these behaviours, many groups consider that the policies are either insufficient, or are not enforced quickly and effectively enough.

Human rights engaged: Online gender-based violence engages the right to security (Article 9, ICCPR) and, due to its discriminatory impact, the right to non-discrimination (Article 26, ICCPR). Gender-based violence – whether online or offline – is also a particular form of discrimination against women for the purposes of Article 1 of the Convention on the Elimination of All Forms of Discrimination against Women, engaging a range of rights under the treaty (CEDAW Committee, General Comment No. 19 and 35).

Sources: UN Women, "Online and ICT-facilitated violence against women and girls during COVID-19", 2020; World Wide Web Foundation, "The impact of online gender-based violence on women in public life", 2020