Gender Perspectives on Privacy in the Digital Era: A joint submission on sexual orientation, gender identity and expression and sex characteristics

Joint CSO submission to the Special Rapporteur on the right to privacy

30 September 2018

1. Introduction

Sexual orientation, gender identity and gender expression, as well as sex characteristics (SOGIESC) became an integral part of universal human rights standards. As earlier as in 1994, the United Nations Human Rights Committee in its groundbreaking case of *Toonen v. Australia*[1] revealed a violation of the right to privacy by criminalisation of consensual same-sex relations between adults. In 2017, the same Committee made its first decision on legal gender recognition, and it reiterated in *G. v. Australia*[2] that the right to privacy covers particularly gender identity.

New challenges posed to the human rights system by the development of modern communications and digital environment affect specifically lesbian, bisexual, trans and intersex (LGBTI) persons. The *Yogyakarta Principles +10*,[3] a document updating the 2006 Principles on the application of the international human rights law to SOGI,[4] introduced a new section on the right to the enjoyment of human rights in relation to information and communication technologies. It declares that *"[e]veryone is entitled to the same protection of rights online as they are offline. Everyone has the right to access and use information and communication technologies, including the internet, without violence, discrimination or other harm based on SOGIESC. Secure digital communications, including the use of encryption, anonymity and pseudonymity tools are essential for the full realisation of human rights, in particular the rights to life, bodily and mental integrity, health, privacy, due process, freedom of opinion and expression, peaceful assembly and association."*[5]

The present submission is aimed at revealing some concrete issues related to privacy and digital communications faced by LGBTI persons in different contexts. It includes five sections related to the use of social media and mobile applications to harass, blackmail and abuse LGBTI persons; health issues and personal data; discrimination in employment; adolescents, bullying and school environment; and specific challenges faced by transgender people. The submission also provide some examples of best practices organised by state and non-state actors to ensure protection of LGBTI persons' right to privacy in the digital environment.

The document was prepared jointly by Kazakhstan Feminist Initiative "Feminita", ODRI Intersectional rights, "Stimul" LGBT Group and Transgender Legal Defense Project (Russia), Richard Lusimbo, MPact Global Action for Gay Men's Health and Rights, Transgender Europe - TGEU, Federatie van nederlandse verenigingen tot integratie van homoseksualiteit - COC Nederland, and the International Lesbian, Gay, Bisexual, Trans and Intersex Association - ILGA.

---

[1] Communication No. 488/1992 of 25 December 1991, views of 31 March 1994, CCPR/C/50/D/488/1992.

[2] Communication No. 2172/2012 of 2 December 2011, views of 17 March 2017, CCPR/C/119/D/2172/2012.

[3] Available at: http://yogyakartaprinciples.org/wp-content/uploads/2017/11/A5_yogyakartaWEB-2.pdf.

[4] Available at: http://yogyakartaprinciples.org/wp-content/uploads/2016/08/principles_en.pdf.

[5] Yogyakarta Principles +10, Principle 36. See also annex.

2. Gendered impacts of privacy invasions on individuals of diverse SOGIESC

2.1. The use of social media and mobile apps to harass, blackmail and abuse LGBTI persons

The misuse of new communications technologies and services to harass, blackmail and abuse LGBTI persons has been addressed already by UN bodies, and specifically Treaty Bodies. For example, the Committee on Economic, Social and Cultural Rights in its Concluding Observations on Sri Lanka expressed its concerns that "*LGBTI persons have been subjected to threats and attacks on social media on the basis of their sexual orientation or gender identity*."[6] Similarly, while reviewing a periodic report of Azerbaijan, the Human Rights Committee noted "*hostility on social media targeting LGBT persons*."[7]

Media, including new media, may publish personal data of LGBTI persons and human rights defenders which place them into enormously dangerous situation and can lead to such consequences as physical violence, harassment and even murder.

Case study 1 - Uganda:[8]

> In the case of *Kasha Jacqueline and Others v Rolling Stone Ltd and Another*, the High Court of Uganda held that in regard to the right to privacy of the person and home, enshrined in the Uganda Constitution Article 27, it had no doubt, using the objective test that the exposure of identities and homes of LGBTI persons for purposes of fighting 'gayism' and the activities of gays as seen from the general outlook of the impugned publication did threaten the rights of the LGBTI persons' right to privacy and their homes, which rights they're entitled too.[9] This court ruling also used the premise that rights guaranteed by the Constitution of Uganda are to be enjoyed by all persons, regardless of SOGI. The Court also affirmed that enjoyment of rights ought to be applied to all persons, including the LGBTI persons in Uganda with prejudice, therefore the media ought to practice caution when reporting and writing about LGBTI persons in Uganda to ensure their respect their right to privacy.
>
> However, even with this progressive ruling, the Ugandan LGBTI community have continued to witness their right to privacy violated by the Ugandan media. The media abuse of the right to privacy (outing) has put lives of many perceived and actual LGBTI persons at risk, and others have lost their jobs and family. The media reporting in Uganda about LGBTI persons is often malicious and incites violence. Much of the
> reporting fuels hate toward LGBTI persons as they are presented negatively and falsely by the media.[10] The Coalition Report of 2014[11] showed instances where the Ugandan media has on numerous accounts published names, photos and contact details of perceived and actual LGBTI persons which has led to dangerous consequences for the individual named.

---

[6] Committee on Economic, Social and Cultural Rights (2017), *Concluding Observations: Sri Lanka*, E/C.12/LKA/CO/5, para. 17.

[7] Human Rights Committee (2016), *Concluding Observations: Azerbaijan*, CCPR/C/AZE/CO/4, para. 8.

[8] Lusimbo, R. (2017), *The Protection of LGBTI Persons' Right to Privacy in Uganda*: for partial fulfilment of the requirements for Mphil, Human Rights and Democratisation in Africa, Center for Human Rights, Faculty of Law, University of Pretoria, pp. 28-31.

[9] *Kasha Jacqueline and Others v Rolling Stone Ltd and Another* 2010 163 UG para (HC).

[10] Human Rights Campaign Foundation 'LGBT Uganda Today: Continuing danger despite nullification of anti-homosexuality act' (September 2015) http://assets.hrc.org/files/assets/resources/Global_Spotlight_Uganda__designed_version__September_25__2015.pdf (accessed 20 September 2017) 4.

[11] Civil Society Coalition on Human Rights and Constitutional Law 'Uganda report of violations based on sex determination, gender identity, and sexual orientation' (October 2014) Uganda Report of Violations based on Sex Determination, Gender Identity, and Sexual Orientation - uganda_violations_report_october_2014_.pdf (accessed 30 June 2017) 10.

Even after the win in the *Kasha Jacqueline and Others v Rolling Stone Ltd and Another*, David Kato, one of the LGBTI activists who featured on the cover story was brutally murdered in his home weeks later.[12] This is another reminder why the media must protect the right to privacy for LGBTI persons. If this is not observed, the consequences are fertile that can lead future loss of lives.

Different reports from the CSOs in Uganda have reported the continued abuse of the right to privacy of LGBTI persons in Uganda. Reports indicate that the lives of the LGBTI persons' whose right to privacy has been abused by the media have been evicted, lost jobs or even forced to leave the country. The SMUG Report of 2014 showed that 10 members of the LGBTI community had faced physical violence after they had been exposed by the media, 3 members of a local LGBTI dance group 'Hi 5' were evicted from their house, and due to safety concerns they had to leave the country.[13] The same report also indicated that 2 members of the LGBTI community had lost their jobs, 1 man received death threats and 3 were blackmailed.[14] The SMUG report was released at the height of the passing and signing into law of the AHA in 2014. The media failed to protect the LGBTI persons' right to privacy and was more interested in making sales.

More cases continue to be reported by LGBTI persons after the media abused their right to privacy. The 2016 SMUG Report indicated that 11 cases of media intrusion had been reported that had led to suffering of LGBTI persons including banishment by families and evictions.[15] In an interview with SMUG, Bwire relayed that after his picture had appeared in the newspaper, his sister and guardian told him to leave the home immediately and her husband had told him to leave or else he would deal with him. Bwire was left with no home and only left at the mercies of his friends whom he wandered from one to the other.[16] This is the reality that LGBTI persons continue to face in Uganda after the media has abused their right to privacy.

The abuse of the right to privacy for LGBTI persons in Uganda exposes them to a multitude of human violations. This could also lead to members of the LGBTI community being denied other human rights like right to fair trial (presumption of innocence) because of the way they are projected to the public when they share their sexuality and private information which could include pictures, addresses and names. Furthermore, their right to freedom from cruel, inhuman and degrading treatment is also abused because of the negativity light which media presents the LGBTI persons in, which has resulted in LGBTI persons being evicted[17] and others losing jobs.[18]

---

[12] Sexual Minorities Uganda (SMUG) 'And that's how I survived being killed: testimonies of human rights abuses from Uganda's sexual and gender minorities' (April 2016). http://sexualminoritiesuganda.com/wpcontent/uploads/2016/04/And-Thats-How-I-Survived_Report_Final.pdf (accessed 21 September 2017) 24.

[13] Sexual Minorities Uganda (SMUG) 'From torment to Tyranny: Enhancing persecution in Uganda following the passage of the Anti-Homosexuality Act 2014 20 December 2013 – 1 May 2014' (9 May 2014). http://sexualminoritiesuganda.com/wpcontent/uploads/2014/11/SMUG-From-Torment-to-Tyranny.pdf (accessed 20 September 2017) 5.

[14] Ibid 6.

[15] Sexual Minorities Uganda (SMUG) 'And that's how I survived being killed: testimonies of human rights abuses from Uganda's sexual and gender minorities' (April 2016). http://sexualminoritiesuganda.com/wpcontent/uploads/2016/04/And-Thats-How-I-Survived_Report_Final.pdf (accessed 21 September 2017) 24.

[16] Ibid 25.

[17] Sexual Minorities Uganda (SMUG) 'From torment to Tyranny: Enhancing persecution in Uganda following the passage of the Anti-Homosexuality Act 2014 20 December 2013 – 1 May 2014' (9 May 2014). http://sexualminoritiesuganda.com/wpcontent/uploads/2014/11/SMUG-From-Torment-to-Tyranny.pdf (accessed 20 September 2017) 5.

[18] Ibid 6.

Case Study 2 - Peru:

In Peru, two openly gay congressmen are constantly attacked, through social networks and the media, by conservative pro-life groups. These collectives do not dialogue with the ideas presented by these two congressmen, but attack them online directly with offensive comments, describing them as "aberrant", for example[19]. Moreover, there are other cases where regular people trying to assert their rights have been harassed online. That is the case of a non-binary woman whose exposure became mediatic when trying to assert the recognition of rights as a non-binary person at a law faculty of a private university[20]. She proposed that the university should respect and promote their gender expression and urged colleagues and teachers to assert their right to be recognizes as non-binary and accordingly called by their pronouns. This then led to massive attacks against their person, through Facebook[21], from where users with real accounts as those who could not be identified, created spaces to make fun of this person and destroy their reputation until today. Facebook deleted some pictures after several request raised by the student regarding the misuse of their pictures, nevertheless those pictures can still be found online using search engines such as Google using a derogatory name offenders used to mock their identity. Up to this day, even though the Facebook account is not longer, people use their pictures online promoting narratives of their “abnormality” and “sickness”[22].

Fetichizers shared through Whatsapp groups sensitive data of trans sex workers, in most cases without their consent. Fetichizers share details of HIV status, risk practices, sex pictures and prices of trans sex workers. To prevent investigation by the State or private individuals, these groups change their names continuously. There are many barriers for the prosecution of these conducts due to the stereotypes (stereotypes related to the illicit behavior of trans sex workers and fear of prosecution).

***

Another problem relates to dating applications. Many people in the LGBTI community utilize phone apps to socialize and connect with one another, but the handling of individual user data has in some instances put LGBTI people at risk. The majority of research and documentation regarding safety threats and LGBTI app use has focused on gay men, and there is a need for more research and evidence regarding the experiences of other members of the LGBTI community with regard to this topic.

Fake accounts on LGBTI dating apps and other social media platforms are being used by State and non-State actors to lure individuals to face-to-face meetings, entrap them, and subject them to arrest or other cruel and degrading treatment. Some victims have been blackmailed for money or sexual services. In 2014, investigative reporting described the tactics of violent, homophobic vigilante groups that utilize popular gay dating app *Grindr* to entrap, blackmail, and torture app users in Russia.[23] In Egypt, cases have been documented of authorities using dating apps and social media platforms to entrap and arrest gay men.[24]

---

[19] For instance, serr PT. 1: PRIDE-LESS. Available at: malastraducciones.com/2018/06/27/pride-less/

[20] For instance, Mili Palacios: “Los insultos prueban que es necesario luchar por los derechos de las personas trans”. Available at:http://somosperiodismo.com/mili-palacios-los-insultos-lamentables-la-prueba-necesario-luchar-los-derechos-las-personas-trans

[21] For instance, Estudiante transgénero de la Católica desata la furia homofóbica en redes sociales. Available at: https://peru21.pe/lima/estudiante-transgenero-catolica-desata-furia-homofobica-redes-sociales-65356

[22] Case submissions to ODRI.

[23] https://www.thedailybeast.com/the-hunted-gays-of-putins-russia-vicious-vigilantes-and-state-bigotry-close-up?ref=scroll.

[24] https://www.madamasr.com/en/2016/04/29/feature/politics/11-sentenced-to-3-12-years-in-prison-for-homosexuality/.

In response, *Grindr*, which has over 3.6 million active users globally, removed individual user location and distance on profiles, as well as began issuing warning messages to users in regions where same-sex relations are criminalized.[25] Despite these proactive measures, *Grindr* users' exact location can still be identified through "trilateration"; this has caused alarm among many privacy activists and calls for *Grindr* and other LGBTI dating apps to protect its API and limit the amount of data that can be gleaned from its servers.[26]

An *Article 19* report outlines the threats that LGBTI people face using dating apps in Egypt, Lebanon, and Iran. In all three countries, LGBTI community members have given accounts of LGBTI dating apps or pictures with the app watermark used as evidence by authorities to prosecute or blackmail gay men.[27] The report further recommends that *Grindr* and other apps partner with local and national LGBTI civil society organizations to help users connect with resources in the instance of blackmail, entrapment, or other incidents on the app.

Case study 3 - Russia:[28]

> In 2013, M.M., a founder and ideologist of the *Restrukt* neo-Nazi movement, announced the creation of the *Occupy Pedophilia* project whose stated goal was to combat pedophilia. In practice, however, the project participants acted as follows: one of them, the so-called "bait", created an account on social media, indicating his age as over 16 y.o. (the age of consent in the Russian legislation), and then started conversations, often of sexual nature, with gay and bisexual men. The "bait" asked the future victims for a date, met them and led them to an apartment, park or other secluded place where they were waited by other participants of the *Occupy Pedophilia*. The latter then announced to the victim that the "bait" was younger than 16 y.o., and therefore anyone dating with him with the purpose of having sexual contacts is subject to criminal prosecution. This was recorded on video and, in most cases, was accompanied by threats, insults, blackmail and physical violence. Subsequently, these videos were posted on the Internet, which, in turn, led to the disclosure of the victims' sexual orientation.
>
> In 2014, the *Occupy Pedophilia* declared self-dissolution, but the crimes under the described scenario continued. Their main motive is now not the homophobic hatred, but rather mercenary motive. Victims are required to pay money for a criminal case for "pedophilia" not being opened against them, and for keeping their sexual orientation in secret from their colleagues and acquaintances. Nevertheless, such crimes should still be considered hate crimes, as gay and bisexual men are attacked because their attackers believe (not unreasonably in many cases) that they will not turn to law enforcement bodies.
>
> In 2017, the *Stimul Initiative Group* documented 10 cases of "fake dates". All of them occurred according to the scenario described above, and criminals were looking for victims in mobile dating applications for gay and bisexual men and men who have sex with men (MSM). In particular, in 7 out of 10 documented cases, the victims indicated that they became connected with the attackers via the *Hornet* application. In the remaining 3 cases, the victims did not specify the name of the application or social media where the acquaintance occurred.
>
> *Hornet* is currently the most popular dating application for gay and bisexual men and MSM. When registering in it, one must confirm that they are of legal age. In all 10 cases documented by *Stimul*, the victims were contacted from accounts indicating that their owners were over 18 y.o.

[25] https://web.archive.org/web/20141002035636/https://www.grindr.com/blog/grindrs-location-security-update.

[26] https://www.queereurope.com/it-is-still-possible-to-obtain-the-exact-location-of-cruising-men-on-grindr/.

[27] https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf.

[28] Information provided by the *Stimul* LGBT Group.

In all cases, the attackers invited the victims to an apartment where several men were waiting for them. These men stated that the "bait" had not reached the age of 16, insulted the victim and in some cases used physical violence. Everything that happened was recorded on the video. After that, the attackers threatened the victim to disclose information about their sexual orientation to their friends and colleagues, and also to inform them that the victim was a pedophile. In exchange for silence, they demanded money in the amount of 50 to 300 thousand rubles (approx. 760 to 4'550 USD).

In 2017, the provision of legal assistance to victims of "fake dates" became one of the main tasks of the *Stimul*. In most cases, the victims refused to apply to the police, fearing disclosure of their sexual orientation. In those rare cases where the victims did apply to police, the institution of criminal proceedings was refused for the lack of *corpus delicti*.

Case study 4 - Egypt:

There are recorded patterns of violations of privacy that happen to LGBTIQ+ individuals in Egypt. These violations are perpetrated by both state and non-state actors. Based on the documented testimonies and obtained police reports, both state and non-state actors have been using dating applications to entrap LGBTIQ+ individuals in general, and gay men and transexual and transgender women in specific.

Police reports and available court rulings showed how the police entraps individuals from *Grindr* and *Hornet*. The process of entrapment starts with an undercover police officer from the department of the moral police on the dating application who usually lures other users to meet up for casual sex. The meeting is initially arranged in a public space where the victims are surprised with police forces arresting them. The obtained police reports showed around 15 cases in which the police attached screenshots of the conversations between the undercover police officer and the entrapped defendant as incriminating evidence. The usage of screenshots of a private conversation in all of these cases was without judge permit which is in violation of article 57[29] of the Egyptian constitution and article 309 bis[30] of the Egyptian criminal code.

The last few months witnessed an increase of cases of online entrapment in the aftermath of *Mashrou' Leila* concert which witnessed the raising of rainbow flags on 22 September 2017. Individuals who posted their pictures online with the rainbow flags were chased by the government. Two of those who posted their pictures online were arrested. Another person was arrested for posting supportive messages for the LGBTIQ+ on social media and was released shortly afterwards pending a criminal case.

Furthermore, two cases of entrapment of homosexual men on dating applications by gangs were documented. In the first case, the survivor of the entrapment was beaten up and sustained serious injuries. In the second case, the survivor was threatened, beaten up and his belongings were stolen. None of the survivors reported to the police for fear of getting arrested for their sexuality as they cannot explain the circumstances that led to the assaults. One of the survivors of gang entrapment said in his testimony, *"no matter how cautious you are, you cannot make sure you are safe while using Grindr"*. Such statement captures how these dating apps have grew to be exposed to a larger public other than the LGBTQ+ individuals who use them.

[29] http://www.sis.gov.eg/Newvr/Dustor-en001.pdf.

[30] https://www.unodc.org/res/cld/document/criminal_code_of_egypt_english_html/Egypt_Criminal_Code_English.pdf.

If it is not a police officer, it can be a gang or maybe a journalist. Last July, a local newspaper published a full-page 'investigative' piece titled *"The Documents of the Most Dangerous Online Gays' Network"* about *Grindr*, the gay dating app. The newspaper published screenshots of the accounts on the app and of the conversations that they journalist had with other users of the application. While there is no recorded case of arrests as a direct consequence of this article, the publishing of these screenshots puts those users in danger.

It is important to also highlight the new cybercrime law no. 175/2018 and the threats it will pose to the online presence of LGBTIQ+ groups. Article 25 of the newly approved law states that anyone who publishes online content that threatens society's and family values shall be punished for at least six months of prison and a fine of at least fifty thousand pounds. Such article is expected to be used to target any online content supportive of LGBTIQ+ causes.

***

By the nature of the new communications, hundreds even not thousands of people receive access to information disseminated through them, and a pure removing of the original source of information does not preclude further dissemination, therefore again and again putting the persons concerned at risk.

Case study 5 - Kazakhstan:[31]

In January 2018, two young women were secretly recorded on a phone by a stranger while kissing each other in a shopping mall. The man posted the video on his account on Facebook shortly after, and the couple started to be called by friends and relatives who watched the video on the Internet. The video has been watched more than 40'000 times, and more than 850 accounts shared this video. Numerous comments, mostly of derogatory nature, as well as threats to the couple, were posted under the video.

The young women appealed to the court. The court of first instance found that the dissemination of the video by the defendant was illegal as he did it without the women's consent. The court also ordered the defendant to pay 15'000 KZT (approx. 41 USD) to the plaintiffs for moral damages experienced by them.[32]

However, the appellate court failed to upheld the decision and rejected all claims of the plaintiffs. It ordered, particularly, that the defendant had the right to shoot the couple as they were kissing in a public space, namely the shopping mall and therefore the defendant did not interfere into their right to privacy. The court also called the defendant the "defender of the people's morals" and mentioned that "[the Kazakh] society is not ready for open sexual relations between persons of the same sex."[33]

Case study 6 - Iraq:[34]

The media has played a significant role in promoting violence against LGBT+ people in Iraq and the Kurdish Region. The use of words like "faggot", "abnormal" and other offensive terms are commonplace in the Iraqi media when referring to LGBT+ individuals. The queer community is often negatively discussed on TV, by religious leaders and psychiatrists, which is then shared through online channels. They influence the public by making sweeping homophobic and transphobic claims that lack factual basis, such as the idea that being queer is the result of rape and needs to be treated, or that LGBT+ people represent a threat to the institute of marriage and the safety of children.

---

[31] Information provided by the *Stimul* LGBT Group.

[32] Decision of the Court of the Auezovsky District of Almaty of 18 May 2018.

[33] Appellate Decision of the Almaty City Court of 17 August 2018.

[34] https://www.iraqueer.org/news/an-iraqi-tv-promotes-homophobia/, a baseline study is available upon request to COC.

Al-Sumariya TV channel, an Iraqi network, tried to show that homosexuality is an abomination in an interview with a young girl and that this phenomenon is threatening the texture of the Iraqi society, and especially the youth. This show was shared on a number of social media accounts where most of the commenters enforce and support the hate speech and the violent language towards LGBTIQ individuals; the video shared on Al-Sumariya's facebook has received 161 thousand views, 3,2 thousand likes, 2,2 thousand comments and was shared 812 times.

The Iraqi Government's Communication and Media Commission, which regulates and monitors media outlets, has not taken any noteworthy steps to hold media outlets accountable for unethical reporting and bias. Al Ahd TV has directly threatened IraQueer members. In a text message to an IraQueer member, they said "Stop defending 'hermaphrodites'-or your head will be found in trash cans like those before them," which is a reference to the LGBT+ individuals who have already been killed, many of whom were beheaded.

2.2. Health issues and personal data

Another important issue regarding app use for LGBTI people is the sharing of health data and other individual characteristics with external companies. App users have the option to share individual characteristics, such as gender identity, sexual orientation, HIV status, last date of HIV test, and age, among others. In early 2018, it was revealed that *Grindr* had shared these user data with two companies to help "optimize" the app.[35] Activists were particularly concerned about the potential ramifications of these companies sharing HIV status information, leading to discrimination, stigma, and loss of employment or healthcare.

2.3. Discrimination in employment

While it is recognised by the United Nations bodies that States have to ensure non-discrimination of LGBTI persons in employment,[36] in reality discrimination based on SOGIESC is performed by both public institutions and private companies. Development of digital communications and storage of personal data in electronic format brought here new challenges, particularly when it comes to revealing SOGIESC of factual or potential employees and following discriminatory acts committed against them.

Personal data on SOGIESC could be intentionally collected by organised anti-LGBTI groups with the aim to deliver such data to employers of the affected persons. In Russia, for instance, laws banning the so-called "propaganda of nontraditional sexual relations to minors" provoked a wave of online harassment and persecutions against LGBT individuals and LGBT rights defenders working in schools and universities. There were organized groups who collected information on such teachers, their private lives and political views on social media, websites and forums, and then forwarded this information to school administrations and educational authorities with a demand to ban teachers who "propagated perversion." One such activist alleged that he had caused 29 LGBT teachers across Russia to be fired from their jobs.[37] *Human Rights Watch* has documented seven cases where LGBT people or their supporters were threatened with dismissal or forced to leave their teaching jobs at

[35] https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy.

[36] See e.g. Committee on Economic, Social and Cultural Rights (2016): *General Comment no. 23 on the right to just and favourable conditions of work*, paras. 11, 48 and 65.

[37] *'Is my sexual orientation immoral?' Why St. Petersburg fired a gay teacher*. Available at: https://meduza.io/en/feature/2015/01/30/is-my-sexual-orientation-immoral (30 Jan 2015).

universities, schools, and educational centers for children.[38] Typically, victims resigned of their own accord, but some get fired and were not able to achieve justice through national courts.[39]

In 2015 in Kazakhstan, management of the Border Guard Service of the National Security Committee fired two female soldiers for kissing each other following an anonymous video taken from outdoor CCTV-surveillance cameras broadcasting monitor that went viral in the local social media. On the video the two women, clearly identifiable, were seen kissing at the security outpost. Following the scandal, the management of the border service instituted disciplinary proceedings against women and dismissed them, stating, as an official reason, "absence from post for 3 hours or more without a good reason." After the dismissal, the women appealed to the local court. The court found their dismissal illegal, but did not refer to its discriminatory nature.[40]

Information on social media can also be used by employees and companies to collect details of personal or family lives of employees or job applicants. For instance, in 2015 in Russia, D., a young gay man, was refused a job position after a representative of the potential employer obtained access to his account on social media and found some evidences of D.'s relations with his male partner. Even though the job interview went well, and D. was offered the position initially, the company's representative then asked him, using social media account, to "clarify his [sexual] orientation." The message also mentioned that the organization had certain "explicit criteria for its employees." D. answered that he had a stable relationship with his boyfriend, and then was responded by the company's representative that "the ideology and management of our program are such that we adhere to a traditional point of view on many questions." On the same day, D. was informed that it would not be possible for the company and him to work together.[41] D. appealed to a court, but his claims were not granted as the court did not find enough evidences of connections between a person communicating with D. on social media and via email, and the company.[42]

2.4. Adolescents/ bullying/ school environment

A study published by the Gay, Lesbian, & Straight Education Network (GLSEN)[43] revealed that LGBT youth were more likely than non-LGBT youth to be bullied or harassed online (42% vs. 15%) and twice as likely to say they had been bullied via text message (27% vs. 13%). Survey respondents also reported they were as likely to report not feeling safe online (27%) as they were at school (30%) and while traveling to and from school (29%). As was shown by the study, online victimization contributed to negative self-esteem and higher depression.

The Committee on the Rights of the Child has addressed specific risks faced by particularly LGBTI adolescents in the context of digital communications. The Committee stated that *"[t]he digital environment can [...] expose adolescents to risks, such as online fraud, violence and hate speech, sexist speech against girls and LGBTI adolescents, cyberbullying, grooming for sexual exploitation, trafficking and child pornography, over-sexualization and targeting by armed or extremist groups. This should not however restrict adolescents' access to the digital environment. Instead, their safety should*

---

[38] Human Rights Watch (2015), *License to Harm – Violence and Harassment against LGBT People and Activists in Russia*.

[39] Civil society coalition (2015), *List of issues related to the discrimination and violence against women who use drugs, sex workers, lesbian and bisexual women and transgender people in Russia*: submission to CEDAW, p. 8; Union of Independent LGBT Activists of Russia (2015), *Written submission to CEDAW related to discrimination and violence against lesbian, bisexual and transgender women in Russia*, pp. 6-7. See *Krupnova v. Russia*, a case submitted to the European Court of Human Rights (communicated on 26 October 2017).

[40] Kazakhstan Feminist Initiative "Feminita" (2018), *Situation of lesbian, bisexual and transgender women in Kazakhstan: Alternative report on implementation of the International Covenant on economic, social and cultural rights*, p. 6.

[41] Coming Out (2016), *Strategic Litigation as a Method for Defending and Advancing the Rights of LGBT People: the experience of "Coming Out" LGBT Group in Saint Petersburg (2012-2015)*, pp. 56-57.

[42] Coming Out (2016), *Report on incidents of discrimination and violence on grounds of sexual orientation and gender identity in 2015 in Saint Petersburg, Russia*, pp. 64-65.

[43] GLSEN (2013), *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet*.

be promoted through holistic strategies, including digital literacy with regard to online risks and strategies for keeping them safe, strengthened legislation and law enforcement mechanisms to tackle abuse online and fight impunity, and training parents and professionals who work with children."[44]

2.5. Transgender persons

For trans people in particular, the advent and expansion of the internet has been dramatically and dynamically impactful. Trans people use the internet to connect, but also to share resources and information on access to healthcare, to document their transitions (e.g. through video blogs), to discuss systemic transphobia, to date, and to organise. The internet has arguably been the single most influential force on the lives of trans people in the modern era. While many kinds of oppression are consistent at the family or community level, transphobia is diffuse and creates a unique kind of isolation for trans people that the internet has helped to transform. Because of this influence, trans people are also at heightened risk of privacy violations in the context of the internet, with many trans bloggers subject to "doxxing", harassment, and threats of violence due to their being openly trans online. This has an especially significant impact on trans women and trans people of colour. Thus, the internet as a tool has both served to save the lives of many trans people searching for community, information, and understanding, and also exposed trans people to increased human rights violations at the same time. While transgender people can face the same abuses on the Internet as other people, there are some specific risks and types of abuse that are faced only by transgender people because of transphobia. The Internet can be a place, where the right to privacy is violated through sharing private information of the transgender people. Transgender people are "outed" and as a consequence of loss of the privacy, harassment, blackmailing and abuse are directed against transgender individuals and communities.[45]

This section focuses on challenges in digital spaces faced by transgender people in Eastern Europe and Central Asia. Transphobia in this region manifests itself in many areas of life of transgender persons, for instance, in education, work, health care and interactions among people.[46] Trans people in this region often experience undesirable and often offensive comments, attention and harassment on the Internet.[47] Online manifestation of transphobia in the region often includes offensive and unpaid attention to the history, identity, appearance and bodies of transgender people.[48] Information about these issues are placed on the public space with the intent to inflict pain, humiliation and dehumanization of transgender people. In the highlighted region, there is an exceptional practice of outing transgender women who are often engaged in sex work, through disseminating videos, where their faces are seen, and sometimes such videos even include information about their names and addresses.[49] There is no persecution of perpetrators by the state, and in some cases, representatives of state themselves are perpetrators.[50]

In addition, such transphobic violations of the right to privacy can be committed by organizations and media agencies online. For example, in Kyrgyzstan, a trans woman was questioned by a police officer in front of the camera. The police officer asked her to tell to camera her name and address. Later, the video was shared on *Youtube* and from there by several online media in the country.[51] Apart from the

---

[44] Committee on the Rights to the Child (2016), *General Comment no. 20 on the implementation of the rights of the child during adolescence*, para. 48.

[45] Case submissions to TGEU.

[46] https://www.article19.org/stand-hate-speech-speakout4lgbt/ and https://www.amnesty.at/media/2069/less-equal-lgbti-human-rights-defenders-in-armenia-belarus-kazakhstan-and-kyrgyzstan.pdf.

[47] https://tgeu.org/wp-content/uploads/2018/05/MappingDigitalLandscapes_English.pdf.

[48] Case submissions to TGEU.

[49] Case submissions to TGEU.

[50] https://www.article19.org/wp-content/uploads/2018/03/LGBT-Hate-Speech-Report-Central-Asia_March2018.pdf.

[51] Information is shared by LGBTIAQ organization *Labrys*.

direct violation of her right to privacy by the policeman and the media, the trans woman received multiple death threats both online and in person.[52]

The consequences of all this can be devastating for individual trans people. People lose families, children and work; are abused where they live and work; and, as a result, are at high risk of mental disorder, self-harm and suicide.

Despite this practice and international human rights obligations, national legislation does not protect people from biased hate crimes and hate speech in digital spaces. Majority of the countries do not have national legislation providing protection of the right to privacy in digital spaces and protection from biased harassment and abuse of transgender people.[53] As a consequence, transgender people are often left without legal protection.

Big data makes easy to access case files and specific details about legal gender recognition judicial procedures, particularly in Chile and Peru. This type of acts, are also replicated in other more institutionalized spaces of big data such as the State judicial docket by the official newspaper, "El Peruano" that has published information about trans and intersex persons registering judicial legal recognition procedures. In the last two to four years, information regarding this very much vulnerable population has been released in a total of 100 cases related to trans people and intersex children[54]. In the case of intersex children, using search engines of judicial database, third parties can access to details of sex characteristics of children whose parents have requested gender legal recognition. Sensitive details have been exposed such as where they live, the details of genitalia and cosmetic procedures, and how they discover the children were intersex.

According to Transgender Legal Defense Project, a leading organisation in Russia providing assistance with legal gender recognition throughout the country, several cases where courts published full texts of decisions, including names of trans people, have taken place.

3. Best practice examples

3.1. Personal data of trans and intersex persons in court documentation:

In Colombia, the Constitutional Court has adopted privacy protocols to protect intersex children that have recurred for judicial protection. Several details have been deleted such as the names of claimants and defendants, relatives, localities and other details that can trace these persons and exposed them to public knowledge, and prevent revictimization[55].

In Russia, according to the Transgender Legal Defense Project, several courts removed decisions revealing personal data of trans persons upon request.

3.2. The use of dating applications to harass gay and bisexual men:

As a response to the problem described above (case study 3 - Russia), local defenders (“Coming Out” LGBT Group and “Stimul” Initiative Group) organised a range of activities to raise awareness among

[52] Information is shared by LGBTIAQ organization *Labrys*.

[53] https://www.article19.org/wp-content/uploads/2018/03/LGBT-Hate-Speech-Report-Central-Asia_March2018.pdf and https://transrespect.org/en/map/anti-discrimination/.

[54] Case submissions to ODRI.

[55] Constitutional Court of Colombia. See among other, cases T-450A/13, T-1025-02, T-675-17.

community members and to prevent violations. Such activities included, in particular, practical booklets, seminars, trainings and media publications.[56]

3.3 A safe online chatroom for young LGBTQIA+ people:

COC Netherlands, the Dutch LGBTI organisation, hosts a chatroom for lesbian, gay, bi, trans(gender), hetero, questioning, pan, non-binary, queer, intersex or asexual young people up to the age of 18 to share and discuss matters of sexual orientation, gender identity and expression and sex characteristics in a safe way. The initiative has been developed by and for young LGBTI people through the 'Jong & Out' (Young&Out) project.

Under the slogan 'safety and privacy above all', several measures have been put in place to safeguard the privacy and safety of those who join. An adult employee of COC is always present as host of the chatroom. To make sure no one is above the age of 18, each participant must show an ID or otherwise valid document with picture to verify their age and identity, which will just be shown and not stored. They receive an e-mail with precise instructions and there is also an instructional video to support them in the process. Each individual can make a profile in which they are free to decide the information they want to share. A recognizable profile picture or real name is not required, for example.

From a survey, 96,8% of the young people who take part in Jong&Out find the website safe and reliable. Many members meet new (best) friends or buddies to support and meet each other outside of the chatroom. 91,4% of the young people on Jong&Out would recommend making a profile on this website to other young people.

[56] See e.g. http://comingoutspb.com/news/kak-ne-stat-zhertvoy-vymogatelstva-na-podstavnom-svidanii/; https://meduza.io/feature/2016/04/25/obschestvo-dobrota-novye-ohotniki-na-geev.

Annex - Yogyakarta Principles +10

Principle 36: Right to the enjoyment of human rights in relation to information and communication technologies

Everyone is entitled to the same protection of rights online as they are of ine. Everyone has the right to access and use information and communication technologies, including the internet, without violence, discrimination or other harm based on sexual orientation, gender identity, gender expression or sex characteristics. Secure digital communications, including the use of encryption, anonymity and pseudonymity tools are essential for the full realisation of human rights, in particular the rights to life, bodily and mental integrity, health, privacy, due process, freedom of opinion and expression, peaceful assembly and association.

STATES SHALL:

A. Take all necessary measures to ensure that all persons enjoy universal, affordable, open, safe, secure and equal access to information and communication technologies, including the internet, without discrimination based on sexual orientation, gender identity, gender expression or sex characteristics;
B. Ensure the right of all individuals, without discrimination based on sexual orientation, gender identity, gender expression or sex characteristics, to seek, receive and impart information and ideas of all kinds, including those concerning sexual orientation, gender identity, gender expression and sex characteristics, through information and communication technologies;
C. Ensure that any restrictions to the right to access and use information and communication technologies and the internet are provided for by law and are necessary and proportionate to protect the human dignity, equality and freedoms of others, without discrimination on the basis of sexual orientation, gender identity, gender expression or sex characteristics;
D. Respect and protect the privacy and security of digital communications, including the use by individuals of encryption, pseudonyms and anonymity technology;
E. Ensure that any restrictions on the right to privacy, including through mass or targeted surveillance, requests for access to personal data, or through limitations on the use of encryption, pseudonymity and anonymity tools, are on a case speci c basis, and are reasonable, necessary and proportionate as required by the law for a legitimate purpose and ordered by a court;
F. Take measures to ensure that the processing of personal data for individual profiling is consistent with relevant human rights standards including personal data protection and does not lead to discrimination, including on the grounds of sexual orientation, gender identity, gender expression and sex characteristics;
G. Take all necessary legislative, administrative, technical and other measures, including ensuring private sector accountability, as outlined by relevant international standards, in consultation with relevant stakeholders, to seek to prevent, remedy and eliminate online hate speech, harassment and technology-related violence against persons on the basis of sexual orientation, gender identity, gender expression or sex characteristics under the framework of international human rights law.