United Nations A/HRC/58/58/Add.1

General Assembly

Distr.: General
15 January 2025

Original: English

Human Rights Council
Fifty-eighth session
24 February–4 April 2025
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Visit to Mauritius

Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères*

Summary

The Special Rapporteur on the right to privacy, Ana Brian Nougrères, carried out a visit to Mauritius from 27 November to 4 December 2023. Mauritius, which possesses one of the most robust and comprehensive regulatory systems for privacy and data protection, in alignment with the General Data Protection Regulation of the European Union ((EU) 2016/679), is the first country in Africa to sign and ratify the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe. In the present report, the Special Rapporteur examines the protection of personal data, including health data, biometric data, financial data and the cross-border sharing of data, the right to privacy in the context of cybersecurity, surveillance by intelligence and law enforcement agencies and the balancing of the right to privacy and freedom of expression, gender identity and reproductive rights and children's privacy in the digital age. Domestic legislation in Mauritius aligns with a robust international framework on the processing of personal data and privacy and the Government clearly places a high value on privacy. However, regarding the privacy of vulnerable groups (older persons, persons with disabilities, persons on lower incomes, children and LGBTQI+ persons), the Special Rapporteur finds additional steps need to be taken to further strengthen efforts to promote sensitivity and respect for personal dignity in order to ensure the right to privacy, both online and offline. The Special Rapporteur believes that Mauritius can be a leading example in the region on adopting a human rights-based approach and building an international framework that embraces both technological and social progress while balancing security with the right to privacy. The Special Rapporteur outlines recommendations regarding the various issues examined in her report.

* The summary of the report is being circulated in all official languages. The report itself, which is annexed to the summary, is being circulated in the language of submission and French only.

Annex

Report of the Special Rapporteur on the right to privacy on her mission to Mauritius

I. Introduction

1. The Special Rapporteur on the right to privacy, Ana Brian Nougrères, conducted a country visit to Mauritius from 27 November to 4 December 2023. The present report builds on the preliminary observations contained in the end-of-mission statement issued on 7 December 2023[1] and reflects updated information gathered from engagement with all stakeholders.

2. The Special Rapporteur thanks the Government of Mauritius for its support and for the constructive manner in which the discussions were held. She also thanks all stakeholders who presented her with detailed information and additional documentation in follow-up to her visit.

3. The Special Rapporteur held meetings with representatives of the Ministry of Foreign Affairs, Regional Integration and International Trade; the Office of the Prime Minister, including the Defence and Home Affairs Division; the Counter-Terrorism Unit; the National Security Service; the Police Force; the Independent Police Complaints Commission; the Prison Service; the Attorney General's Office; the Office of the Director for Public Prosecutions; the Ministry of Education, Tertiary Education, Science and Technology; the Ministry of Gender Equality and Family Welfare; the Ministry of Health and Wellness; the Ministry of Information Technology Communication and Innovation; the Ministry of Social Security; the Ministry of Labour and Human Resources; the Supreme Court; the National Human Rights Commission; the Office of the Ombudsperson for Children; and the Economic Development Board. She also met with the United Nations Resident Coordinator and representatives of the United Nations country team and civil society organizations.

4. Mauritius, which was the first African country to ratify the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe,[2] has a strict data protection system. It is for this reason that the Special Rapporteur sought an invitation to conduct a country visit, which she hoped would provide an opportunity to identify good practices in promoting and protecting privacy that other countries in Africa may be interested in incorporating. She is grateful to the Government of Mauritius for extending the requested invitation.

II. International, regional and national law regarding privacy

International and regional law

5. The right to privacy is enshrined in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, which state that no persons shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon their honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks. Mauritius ratified the International Covenant on 12 December 1973. Mauritius has also ratified the Convention on the Rights of the Child, which enshrines the right to privacy in article 16, and the African Charter of Human and People's Rights, although the African Charter does not contain a specific provision protecting the right to privacy.

[1] See https://www.ohchr.org/en/press-releases/2023/12/un-expert-says-mauritius-leads-privacy-region-challenges-remain.

[2] See https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

National law

6. Article 9 of the Constitution of Mauritius (adopted in 1968 and revised in 2016) provides for the protection of privacy of home and other property,[3] including the right not to be subjected to the arbitrary search of one's person or property. The Mauritian Civil Code enshrines the right to respect of one's private life and empowers competent jurisdictions to take action to repair any violations of that right. Such measures may be ordered, if necessary, by a Chamber Judge.[4]

Privacy and personal data

Protection of personal data

7. Mauritius possesses one of the most robust and comprehensive regulatory systems for privacy and data protection, as provided under its Data Protection Act 2017, promulgated through Proclamation No. 3 of 2018 and made effective on 15 January 2018, which aligns with the General Data Protection Regulation of the European Union ((EU) 2016/679). On 4 September 2020, Mauritius became the first country in Africa to sign and ratify the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

8. The processing of personal data must be lawful, fair, transparent, adequate, kept for as long as required and proportionate to the purposes for which is it being processed.[5] Pursuant to section 27 of the Data Protection Act, controllers shall destroy data as soon as is reasonably practicable in cases where the purpose for keeping such personal data has lapsed.

9. The Data Protection Office, established under section 4 of the Data Protection Act, is an independent and impartial advisory office, which is led by the Data Protection Commissioner. The Commissioner exercises control of data-processing operations, investigates complaints of violations under the Act and issues and approves codes of practice or guidelines to implement the Act. This includes ensuring "that there is no significant risk or adverse effect of any developments on the privacy of individuals" and examining "any proposal for automated decision-making or data linkage that may involve an interference with, or may otherwise have an adverse effect on, the privacy of individuals and ensure that any adverse effect of the proposal on the privacy of individuals is minimized". In addition, the Commissioner may authorize the investigation of complaints and direct individuals to attend hearings to decide matters related to an investigation.

10. The Data Protection Act also empowers authorized officers to enter and search any premises and examine documents, records or data in order to carry out their duties under the Act (and several other pieces of financial legislation), provided that they obtain a warrant issued by a Magistrate and show the warrant to the owner or occupier of the premises.

11. The Data Protection Office, which is under the administration of the Ministry of Information Technology, Communication and Innovation, has independent functions but does not have independent funding. In 2023, owing to a lack of funding, there were only two Data Protection Officers on staff to process 423 claims. While the Office has published numerous guidelines it is evident that more coordination is needed between the Ministry of Education and other ministries as many of the topics are cross-cutting issues.

12. The Data Protection Office works closely with the Attorney General's Office to ensure compliability and has requested police officers to be seconded to the Office as enforcement presents the greatest challenge. It is mandatory for corporations to have Data Protection Officers although in practice many do not.

[3] See https://cdn.accf-francophonie.org/2019/03/maurice-constitution2016.pdf.
[4] See Civil Code, article 22 https://www.mcci.org/media/35747/code-civil-mauricien.pdf.
[5] See Mauritius.pdf (ohchr.org).

Cross-border sharing of data and privacy of information

13. Section 36 of the Data Protection Act defines the rules for transfer of personal data abroad.[6] A controller or processor may transfer personal data outside Mauritius if the Data Protection Commissioner is provided with proof confirming that there are appropriate safeguards in place for the protection of personal data. Personal data may also be transferred outside Mauritius if, prior to such transfer, the data subject has been informed of any possible risks of the transfer and has given explicit consent for the transfer. If the controller or processor cannot provide for the appropriate safeguards in relation to the transfer of personal data to another country, the controller or processor, as applicable, must obtain the prior authorization of the Data Protection Commissioner.

14. The transfer of personal data to another jurisdiction can also be allowed on such terms as the Data Protection Commissioner may approve for the protection of the rights of the individual in question. The Commissioner has the power to suspend or prohibit the transfer of data to another jurisdiction if the processor or controller is not able to demonstrate either the effectiveness of safeguards, or the existence of compelling legitimate interest.

15. In addition, under the Guidelines on Outsourcing by Financial Institutions (revised in March 2018) issued by the Bank of Mauritius, a series of conditions are imposed during the process of storing customers' information on cloud-based services by financial institutions.[7]

16. As a member of the the Southern African Development Community (SADC), Mauritius is also guided by the provisions of the SADC Model Law, which provides a guideline for Member States on how to develop, draft and harmonize data protection laws.

Use of personal data by business enterprises

17. In sections 23, 28 and 44 (1) of the Data Protection Act there are important safeguards on the access of State authorities to data collected by private companies. In line with section 23 of the Act, an individual must be informed of the purpose of data-sharing at the time of the collection of personal data. Section 28 of the Act establishes the legal basis required for processing such data, including obtaining the consent of the subject before sharing.

18. The Government of Mauritius has promoted and disseminated the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, including by hosting a webinar in September 2023 to help companies promote and protect human rights as well as privacy and data protection within all business activities.[8] There was an acknowledgment that greater awareness and more robust complaints mechanisms were needed.

19. The Special Rapporteur noted a good practice by the Economic Development Board, which is independent body from both the State and the corporations responsible for facilitating commerce, in the appointment of a National Contact Point to coordinate policy coherence and actively promote the Guiding Principles on Business and Human Rights.

Data protection in financial services

20. The Financial Services Commission regulates the non-banking financial services sector in Mauritius and ensures that institutions, within its mandate, abide by the requirements that a controller handle the collection, processing and transfer of personal data. In accordance with section 87 of the Financial Services Act 2007, every record of the Commission must be kept for a period of at least 7 years after the completion of the transaction to which it relates. However, given the specific functions of the Commission, some personal data may be required to be kept for more than 7 years. Furthermore, section 87 of the Financial Services Act also provides for exchange of information, mutual assistance and confidentiality. Owing to the global rise in virtual assets, Mauritius enacted the Virtual

[6] See CFI-RTP-Mauritius.docx (live.com).

[7] See Mauritius - Data Protection Overview | Guidance Note | DataGuidance.

[8] See Commonwealth and Mauritian Government host webinar to help businesses protect human rights | Commonwealth (thecommonwealth.org).

Asset and Initial Token Offering Services Act 2021, which came into force on 7 February 2022. The Act provides protections for personal data in virtual transactions during the digital transferring, processing, storing and trading of information.

21. The complexities of virtual assets expose users to the possibility of data breaches since virtual asset transactions occur exclusively on the Internet. While users on virtual currency platforms may remain anonymous when trading, their full transaction history is nonetheless publicly available and accessible from multiple jurisdictions. A data breach may therefore result in the likelihood that a particular user's personal information, for example their mailing address, may be released to the public without their consent or knowledge.

22. Data protection concerns in the financial sector are challenging as they span multiple sectors of government, the private sector and often involve cross-border transactions and multiple jurisdictions so that the application of a particular jurisdiction's data protection laws may be difficult to ascertain. As virtual assets operate through a decentralized network, permanent blockchains are created to record trading history. These blockchains are in large part unalterable by data controllers/processors, whose responsibilities include amending inaccurate data and destroying obsolete personal data.

23. The Financial Services Institute partners with the Data Protection Office to provide training sessions on data processing for professionals, but more resources and investment are needed as the private sector is very devolved. It is vital that both bodies work closely with the Ministry of Information Technology, Communication and Innovation to ensure the highest level of data protection. In November 2023, the Data Protection Office issued guidelines on data protection in the financial sector[9] to manage the rapid growth of data-driven technologies, cyberthreats and the impact on privacy.

24. Mauritius has also been proactive in ensuring that it meets the latest artificial intelligence trends in financial technology. The Financial Services Commission introduced a Robotic and Artificial Intelligence Enabled Advisory Services licence in 2021 to better protect service users and providers from data breaches.[10] The Government informed the Special Rapporteur that it intends to study the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,[11] with the aim of domesticating this principle as it is important to have a prudent and harmonized approach to artificial intelligence.

Artificial intelligence and health data

25. In April 2020, the Data Protection Office issued a "Guide on Data Protection for Health Data and Artificial Intelligence Solutions in the Context of the COVID-19 Pandemic".[12] In the Guide, the Office recognized that although data protection rights are not absolute and can in no way be a barrier to save human lives, it is equally crucial to reiterate that the fundamental rights to privacy and data protection are still applicable. The Office has acknowledged that many of the techniques used to mitigate the spread of the coronavirus disease (COVID-19) pandemic could implicate storage and processing of personal data. Therefore, the Office stressed the need for organizations to comply with the requirements set out in sections 28 and 29 of the Data Protection Act and to use the principles of necessity and proportionality to guide their decisions regarding collecting health data, which is a singular type of personal data.

26. The Special Rapporteur reviewed the Guide on Data Protection and noted: that it provided useful guidance regarding the importance of anonymizing all personal data processed by artificial intelligence and incorporating the use of pseudonyms to facilitate this goal; that artificial intelligence should be used to process data only when guided by the principles of necessity and proportionality; and that artificial intelligence data processing methods must be made transparent to individuals. The Guide stressed the need for informed

[9] See https://dataprotection.govmu.org/Documents/Draft%20_Financial_Guide_UpdatedV7.pdf.
[10] See Data Protection & Privacy 2023 - Mauritius | Global Practice Guides | Chambers and Partners.
[11] See https://rm.coe.int/1680afae3c.
[12] See https://dataprotection.govmu.org/Communique/Guide%20on%20Data%20Protection%20for%20health%20data%20and%20AI.pdf.

consent when using artificial intelligence assisted data processing and established that measures used to process personal data during the COVID-19 pandemic are exceptional and should be consistently reevaluated so that any undue infringement of the rights and privacy of individuals do not become the norm.

27. The Special Rapporteur welcomes the Government's "One Patient, One Record" project,[13] launched on 27 January 2024, with the support of the United Nations Development Programme, to modernize the public healthcare services, which serve 75 per cent of the population. A pivotal aspect of the project is the implementation of a patient portal and patient administration system, providing healthcare professionals with access to accurate and up-to-date information about patients. This technological advancement is expected to eliminate challenges associated with lost or misplaced medical files, offering instant access to crucial patient data with a simple click. The e-health programme is the beginning of a larger digitalization plan across other sectors of Government (including finance and social services). Currently, 157 health institutions in Mauritius, which previously did not share information, now capture, store, manage and transmit the health data of individual patients. Diagnosis, reports, scans and hospital records are stored on a cloud server, the information on which can only be accessed by authorized persons and exchanged among healthcare providers.[14] The Special Rapporteur noted that the legal and regulatory framework around e-systems needs to evolve and to be strengthened in order to minimize risks; there is no privacy without security.

Biometric data

28. In 2021, the decision of the Human Rights Committee in communication No. 3163/2018 (*M.M. v. Mauritius*, 24 March 2021),[15] found that the National Identity Card Act 2013 violated citizens' privacy rights as there were insufficient guarantees that fingerprints and other biometric data stored on the identity cards could be securely protected.

29. Given the lack of sufficient information provided by the authorities of Mauritius concerning the implementation of measures to protect the biometric data stored on identity cards from being copied without the holder's knowledge, the Committee found that the right to privacy of the individual in question was violated and called on Mauritius to review the safeguards for storing and retaining fingerprint data on identity cards and to provide M.M. with an effective remedy. The National Identity Card (Mobile ID) Regulations 2024 came into force in January 2024 without requirements for fingerprint data or photographs. However, the Government has yet to provide a formal response to the Human Rights Committee regarding the use of data and the necessary safeguards and security measures.

30. In December 2021 the Government proclaimed regulations on information and communication technologies (the registration of subscriber identity module (SIM) cards), but had to postpone the registration exercise as the three major telecommunication companies, Mauritius Telecom, Emtel and Mahanagar Telephone Mauritius Limited, said that they lacked the infrastructure to store the data from a mass, nationwide registration exercise that would include biometric information, including photographs for each user. In June 2023, the Information and Communication Technologies Authority of Mauritius passed revised regulations for mandatory SIM re-registration[16] and the registration process took place from 31 October 2023 to April 2024. The Authority announced that the registration campaign was intended to ensure that each SIM card was registered in the name of its user in order to protect subscribers against all types of fraud, identity theft and other offenses.

31. There are two cases before the Supreme Court challenging the constitutionality of the regulations regarding the registration of SIM cards as they impose a legal obligation upon citizens to give sensitive, biometric data for the purpose of the registration of SIM cards

[13] See https://www.undp.org/mauritius-seychelles/news/undp-supports-launch-one-patient-one-record-ehealth-project-enhanced-public-healthcare.

[14] See https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2023/mauritius/trends-and-developments.

[15] See CCPR/C/131/D/3163/2018.

[16] See https://www.icta.mu/faq/.

without any parliamentary debate, which may infringe on protections in sections 1, 2, 3, 9 and 12 of the Constitution.[17]

32. The Government's justification for this anti-crime initiative was based on the report of the Commission of Inquiry on Drug Trafficking Report (2018),[18] which highlighted the issue of SIM cards used by tourists and foreign workers coming into the possession of jailed drug traffickers and being recycled and sold to traffickers.

33. The re-registration exercise requires citizens to provide personal details contained in identification cards and passports, including proof of address and photographs, for deposit with telecommunication companies, which store the biometric information in a database that can be accessed by the Information and Communication Technologies Authority. Civil society organizations expressed concerns to the Special Rapporteur that the data may be collected, retained and used for other purposes and that there were other, less intrusive ways for the Government to address the SIM card issue, namely through better coordination between law enforcement and prison authorities to control the use of illegal mobile devices. The Special Rapporteur is concerned that the measures taken by the Government may not have been proportional as they affect all citizens, who are obliged to comply with the mandatory re-registration and the sharing of personal data; if they do not comply, their mobile phones may be deactivated for non-compliance.

Cybersecurity and cybercrime

34. The Cybersecurity and Cybercrime Act (2021),[19] which replaced the Computer Misuse and Cybercrime Act (2003), aligns with the Council of Europe Convention on Cybercrime (2001)[20] (Mauritius was the first African country in 2014 to accede to the Convention), as well as with the African Union Convention on Cybersecurity and Personal Data Protection.[21]

35. The Cybersecurity and Cybercrime Act includes offences related to cyberbullying (article 17) and revenge pornography (article 19) and outlines the investigation procedures to collect and intercept traffic and content data and/or require service providers to record certain data to aid in the collection and interception processes (articles 29 and 30). While article 41 of the Act establishes the conditions for the exchange of information, the Government may request that the information be kept confidential or only be disclosed according to specified conditions. Article 42 of the Act provides for the storage of computer data for the purpose of enabling foreign States to request the search, access, seizure, securing or disclosure of data.

36. Building on the National Cybersecurity Strategy (2014–2019), the Government has developed a new National Cybersecurity Strategy (2023–2026)[22] to strengthen the legal framework and security of critical information infrastructure against cyberthreats and cybercrime, improve law enforcement capability and effective criminal justice framework, promote innovation and strengthen education through regional and international partnership.

37. In addition, in relation to cybercrime, the Government has established the Mauritian Cybercrime Online Reporting System, which allows the public to report cybercrimes occurring on social media securely. It also provides advice to help in recognizing and avoiding common types of cybercrime that take place on social media websites. The online system is connected to other stakeholders, namely the Data Protection Office, the Cybercrime Unit of the Mauritian Police Force and the Ministry of Information Technology, Communication and Innovation.

[17] See https://lexpress.mu/s/what-pazhany-rangasamys-case-against-sim-card-registration-is-about-531505.
[18] See https://pmo.govmu.org/SitePages/viewAllReports.aspx?RType=Reports+and+Publications.
[19] See https://moic.gov.sl/wp-content/uploads/2022/08/Cyber-Crime-Act-2021.pdf.
[20] See https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[21] See https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
[22] See National Cybersecurity Strategy 2023-2026 - Maurice Info.

38. In September 20024 the Government also launched its Digital Mauritius 2030 strategy,[23] which is aimed at making government services more efficient and accessible while ensuring strong data protection. One of the objectives of the strategy is to develop digital skills across the population to support the transition into a knowledge-based and technology-driven economy.

III. Intelligence and law enforcement safeguards on right to privacy

Intelligence services

39. The relationship between national security and data protection continues to evolve rapidly as the world moves towards digitization. National security involves the collection and storage of an immense amount of personal data of individuals. Mauritius does not have one overarching intelligence act, rather, investigations are carried out by investigatory authorities subject to different legislative frameworks. Section 9 of the Financial Intelligence and Anti-Money Laundering Act 2002,[24] which created the Financial Intelligence Unit, focuses uniquely on financial intelligence gathering regarding the proceeds of crime, money-laundering and the financing of activities related to terrorism. The Financial Intelligence Unit has broad powers to access information but also strict protocols and judicial safeguards.

40. The Mauritius Police Force, governed by the Police Act 1974,[25] is responsible for all other aspects of security and intelligence gathering. Article 18 of the Act established the National Security Service, with the designated function to obtain, correlate and evaluate intelligence relevant to national security. Notably, section 18 (2), which contains an apparent safeguard against the surveillance of protestors/dissenters, states that: “No police officer nor any person referred to in [the above sections] shall: (a) trail any individual on account of the involvement of the individual in any political activity or in any other form of lawful protest or dissent; (b) act as a political activist, or engage in any political activity, or interfere in any manner with any electoral process”.

Law enforcement powers

41. The Police Act contains several articles relevant to the exercise of powers that affect privacy in criminal investigations. Law enforcement personnel have a broad set of tools, such as wiretapping, geolocation and tracking, data mining and physical and electronic surveillance. Section 14 of the Act provides that search warrants and medical examinations can be issued and/or instituted by a police officer (not below the rank of Assistant Superintendent) without communicating with a magistrate if there are exigent circumstances or if communicating with a magistrate would cause a delay in achieving justice.

42. Aware that there is a high level of illegal drug activity that continues to plague Mauritian society, the Special Rapporteur is concerned that, owing to the need for a number of drug investigations, the police may routinely cite exigent circumstances for the conduct of a search; the only requirement is for police officers to go to their superior officer rather than going to court and seeking a judicial order.

43. Under national law, judges and magistrates are allowed to authorize the interception of private communications in limited circumstances where the enforcement agency, for example the Mauritius Police Force, has made an application for such a warrant. Various legal provisions outline the procedures for applying for a search warrant, the conditions for granting it and the execution of the search, in accordance with the necessary safeguards and

[23] See https://ncb.govmu.org/ncb/strategicplans/DigitalMauritius2030.pdf.

[24] See https://www.fiumauritius.org/fiu/wp-content/uploads/2023/02/financial-intelligence-and-anti-money-laundering-act-2002.pdf.

[25] See https://www.policinglaw.info/assets/downloads/1974_Police_Act_of_Mauritius.pdf.

obligatory redress and remedies, should the search be conducted unlawfully or without proper authority.

44. The Criminal Investigation Division, which is a specialized unit of Mauritius Police Force, advised the Special Rapporteur that it routinely gets access to digital devices (for example, mobiles and tablets) by requesting and obtaining the permission of the owner. The Director of Public Prosecutions is also involved in such cases. The Special Rapporteur was further informed that the Criminal Investigation Division has never had to request surveillance interception from the court. The Special Rapporteur would like to analyse the latest annual statistics from the Commissioner of Police regarding requests for surveillance, wiretapping, the number of search warrants requested and granted, the number of requests to examine digital devices (including mobile phones and computers) and the percentage breakdown regarding judicial authorisation of those various investigative tools.

45. In the Office of the Director of Public Prosecutions (which also has a Cybercrime Unit), senior prosecutors working on sensitive and high security cases have specialized training and sign confidentiality agreements.

Mass surveillance for purposes of law enforcement: use of closed-circuit television

46. Public concern about safety and crime has risen in recent years, in particular owing to an illicit drug epidemic, which has resulted in a demand for increased security. Because tourism is one of the major pillars of the economy, the Government, in order to promote its reputation as a safe destination, has implemented the "Safe City Project"[26] through the installation of 4,000 high-functioning closed-circuit television (CCTV) surveillance cameras in major tourist zones, with plans to extend the network to other urban and high-risk areas. The Special Rapporteur was advised that some of the installations are equipped for the use of video surveillance cameras that employ facial recognition technology to help establish an individual's identity to assist the Mauritius Police Force in investigating incidents and resolving criminal cases. Because of the serious privacy implications of facial recognition technology, further assessment is essential and a clear legal regulatory framework needs to be implemented.

47. Regarding the regulation of the data collected through CCTV, section 31 of the Data Protection Act states that controllers and processors (service providers/third parties) have the duty to implement all appropriate security measures to prevent any unauthorized access, alteration, disclosure, accidental loss or destruction of personal data (images captured by CCTV camera). This includes only allowing authorized personnel to gain access to the CCTV room, having an audit trail to monitor staff access to footage, using password protection to manage staff access to stored footage, transmitting and storing footage in encrypted form and carrying out regular audits of system security.

48. Section 34 of the Data Protection Act refers to the use of "data protection impact assessments", which are designed to balance privacy interests with the overall national interests of safeguarding the public. Such assessments provide a mechanism to protect personal data and mitigate the risks of potential infringements on the privacy rights of citizens.

49. In cases where the processing of surveillance operations is on a large scale, for example the systematic monitoring of a publicly accessible area, impact assessments are required owing to the high risk of infringements to the privacy rights and freedoms of data subjects by virtue of their nature, scope, context and purposes, such as: extensive evaluation of personal aspects related to individuals, including profiling; and large scale processing of special categories of data or large scale systemic monitoring of public areas. In such instances, all controllers or processors must, prior to the processing of data, carry out an assessment of the envisaged processing operations to determine if they are lawful, necessary and proportionate. In support of the Safe City Project, the Data Protection Office issued a

[26] See https://www.securityvision.io/wiki/index.php/Safe_City_deployments_in_Mauritius.

"code of practice" for the officers involved to ensure that any activity performed is in accordance with the law and holds public confidence.

50. The Data Protection Act permits data controllers to disclose surveillance information to law enforcement personnel when the purpose is to prevent and detect crime, but it would not be appropriate to place such information on the Internet or disclose information about identifiable individuals to the media. Subject to section 37 of the Act, individuals whose images are recorded have a right to view CCTV images/footage of themselves and to be provided with a copy. If there are other identifiable people in the footage, it is necessary to seek options to protect their privacy, for instance by masking their images on the footage.

51. Section 37 (6) of the Data Protection Act, establishes that if a controller refuses to take action on the request of a data subject (individual), it shall, within one month of the receipt of the request, inform the data subject, in writing, of the reason for the refusal and about the possibility of lodging a complaint with the Data Protection Commissioner.

52. Private citizens have also begun using CCTV surveillance systems and the Data Protection Office has seen an increase in complaints about surveillance cameras and the invasion of privacy and security of others. Of the complaints processed by the Office in 2022, 93 per cent involved the unauthorized use of CCTV cameras.[27]

Remedies

53. The Data Protection Act includes remedies for those whose privacy has been violated though the exposure of their personal data. Individuals have the right to lodge a complaint with the Data Protection Office if they believe there has been a violation of the law under the Data Protection Act and can seek redress to the Supreme Court. If a person is found to violate any provision of the Act, depending on the offence, they can receive a fine not exceeding 200,000 rupees and a term of imprisonment not exceeding 5 years. Citizens can also file a civil suit directly to the court, including on constitutional grounds, and can seek damages.

54. The position of the Ombudsman, which is enshrined in the Constitution,[28] has been established since March 1970. The role of the Ombudsman is to investigate administrative actions of government officials and other public bodies that have caused harm, prejudice, injustice or loss to citizens. The recommendations are not legally binding, but the Ombudsman can propose remedies and raise awareness. The Special Rapporteur learned that it is possible for a citizen to make an anonymous complaint and to have the recommendations posted on the Ombudsman's website without revealing the identity of the complainant.

55. The Government reported that it plans to introduce a National Human Rights Action Plan 2023–2030. The Special Rapporteur welcomes an update on: the status of the implementation of the plan; information on the jurisdiction, including monitoring and investigating powers, of the National Human Rights Committee in its implementation; and how the various complaints mechanisms will complement each other, without creating an overlap, should a citizen allege a violation. In the view of the Special Rapporteur, keeping accurate statistics on the various complaints raised can be a good indicator of a well-informed population; awareness and education are indispensable. If there are no privacy claims, this may mean that people lack knowledge about the foundations of privacy and have a limited understanding of their rights.

Balancing the right to privacy and freedom of expression

56. Mauritius is a leading State in the African region in upholding political rights and civil liberties.[29] However, as is the case in many democratic countries, the Internet and social

[27] See Data Protection Office, Annual report 2022, p. 31 (https://dataprotection.govmu.org/Documents/AR22%20DPO.pdf).

[28] Ombudsman Act sections 96–97.

[29] See https://freedomhouse.org/countries/freedom-world/scores.

media have created global problems. Mauritius has attempted to increase national regulations over the Internet as there is, to date, no international framework.

57. When the new law on cybersecurity and cybercrime took effect in December 2021, the Special Rapporteur learned that opposition politicians criticized the law's vague language, suggesting it gave authorities a broad mandate to crack down on online content they deemed harmful or inaccurate. In addition, the legislation increased the power of law enforcement officials to seize computer systems or devices.[30]

58. The Special Rapporteur received information that, in 2022, the police in Mauritius allegedly used wiretapping to access information from mobile phones and e-mails of journalists and opposition politicians. Reportedly, some political activists noted an increase in attempts to hack their social media accounts.[31]

59. In 2018, amendments to the Information and Communication Technologies Act:[32] allowed people to file complaints and seek damages for a post, share or even a "like" that "is likely to cause or causes annoyance, humiliation, inconvenience, distress or anxiety"; lifted the requirement that prosecutors need to demonstrate an intent to harm; and increased the maximum penalty for infractions from 5 to 10 years in prison.

60. The Special Rapporteur learned that there may be further amendments to the Information and Communication Technologies Act to increase surveillance powers over social media platforms, including the creation of a National Digital Ethics Committee whose role would be to identify and flag harmful content. Furthermore, it has been proposed that a Technical Enforcement Unit be established to operate a surveillance mechanism to eavesdrop on all social media traffic.

61. Major websites and social media platforms have implemented secure communication channels to encrypt the traffic between the end users' devices and servers. No one, not even an Internet service provider, can access the content of the traffic transiting through its network. The technical toolset proposed by the Information and Communication Technologies Act would decrypt, store and then re-encrypt web traffic between an end user in Mauritius and social media platforms by using a proxy server. The latter would act as a middlebox between the end users and the Internet, capturing, archiving and forwarding all traffic passing through it. In technical terms, this amounts to performing a "machine-in-the-middle" attack.

62. To comply with the proposal of the Information and Communication Technologies Act, if implemented, all Internet service providers in Mauritius would need to instruct their users to install a custom certificate that contains a unique but unverifiable key to enable the redirection of social media communications to a designated server. Without the installation of such a certificate, access to selected websites would be denied.[33]

63. The Regional Office of the United Nations High Commissioner for Human Rights (OHCHR) for Southern Africa has analysed the proposed amendments to the Information and Communication Technologies Act. The Special Rapporteur shares some of the concerns raised as they may infringe upon citizens' rights under article 17 International Covenant on Civil and Political Rights and article 9 of the Constitution, namely:

(a) The fact that the National Digital Ethics Committee and the Technical Enforcement Unit would have unfettered access to all decrypted incoming and outgoing social media traffic/data for every online user, allowing their tracking by Internet Protocol (IP) address, beyond what is considered "harmful or illegal" content posted online, impedes both the right to privacy and to freedom of expression owing to the risk of arbitrary or unlawful interference or attacks. This access could also enable targeted surveillance of dissenting opinions from civil society, including human rights defenders, journalists and opposition parties, and could put them at risk of intimidation or harassment;

[30] United Nations country team submission, p. 8. See also CEDAW/C/MUS/CO/8, para. 27.
[31] U.S. State Department, *2022 Country Reports on Human Rights Practices: Mauritius* (https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/mauritius).
[32] See https://ifex.org/mauritius-amends-law-to-include-harsh-penalties-for-online-content/.
[33] See Internet Society, "Mauritius Must Not Fall into the 'Mass Surveillance' Trap".

(b) The proposed amendment does not mention how long information will be archived by the National Digital Ethics Committee or how decrypted and archived user data will be protected from data breaches, thus posing a threat to the security of all online users in the country.

Gender identity and reproductive rights

64. The right to the free development of personality is protected under articles 22 and 29 of the Universal Declaration of Human Rights. Moreover, the Human Rights Council, in its resolution 34/7, makes the explicit link that the right to privacy can enable the enjoyment of other rights and the free development of an individual's personality and identity.

65. In a landmark judgment, the Mauritius Supreme Court issued a decision on 4 October 2023 decriminalizing the offence of sodomy between consenting same-sex partners. The Court ruled that the prohibition on discrimination on grounds of "sex" in the Constitution should be interpreted to include "sexual orientation". The court emphasized that the recognition of sexual orientation as a category of protection is based on the idea that "the Constitution is a living document and must be given a generous and purposive interpretation".[34]

66. The Special Rapporteur welcomes the Government's National Gender Policy 2022–2030 [35] and the National Sexual and Reproductive Health Implementation Plan 2022–2027. [36] However, the Special Rapporteur was briefed by various sources about ongoing concerns regarding gender, in particular the limited availability of education on sexual and reproductive health and rights and the high incidence of adolescent pregnancy and unsafe abortion.[37] From a privacy and perspective, it was concerning to learn that girls under age 18 must be accompanied by an adult in order to have access to contraceptives provided by a medical professional.

67. The legal landscape for transgender persons in Mauritius is complex and, in many respects, inadequate; there are no comprehensive legal recognition and protections for transgender persons, in particular concerning gender identity. The legal framework, the Civil Status Act (1981), permits name changes but the process is overly bureaucratic as it not only requires the publication of a notice in newspapers but also a police investigation, including questioning about a person's hormone intake and medical history related to gender transition. Such intrusive procedures have been criticized for violating the privacy and dignity of transgender persons, further exacerbating the stigma and discrimination they experience.[38] Furthermore, the Civil Status Act (1981) does not allow for the alteration of the sex/gender marker on official documents, such as birth certificates and national identity cards, leaving transgender persons in a legal vacuum.[39]

Children, privacy and digital space

68. The Children's Act of 2020, effective as of 24 January 2022, gives effect to both the Convention on the Rights of the Child and the African Charter on the Rights and Welfare of the Child under domestic law.[40]

[34] See Mauritian Court Finds Sodomy Law Unconstitutional, Discriminatory | Human Rights Watch (hrw.org).

[35] See https://gender.govmu.org/Documents/2022/NationalGenderPolicy2022-2030.pdf.

[36] See https://health.govmu.org/health/wp-content/uploads/2023/03/National-Sexual-and-Reproductive-Health-Implementation-Plan-2022-2027.pdf.

[37] United Nations country team submission, p. 8. See also CEDAW/C/MUS/CO/8, para. 27.

[38] See https://africlaw.com/2024/08/23/miss-universe-mauritius-2024-a-landmark-in-the-legal-battle-for-transgender-equality/.

[39] See https://youngqueeralliance.com/wp-content/uploads/2021/08/2021.07.27-Policy-Brief-Administrative-recognition-of-trans-people-in-Mauritius.pdf.

[40] Children's Act 2020, subpart II, part A (https://gender.govmu.org/Documents/2021/children's%20act%202020.pdf).

69. In accordance with the overarching principle of "the best interests of the child", the Children's Act elevates the status of the child from a subject under the law to the recipient of rights, including the right to privacy. Under article 27 of the Children's Act, people are prohibited from taking any action that affects the privacy of a child. The Act also prohibits the publishing or broadcasting in the media of any information in any form identifying a child witness, child victim or child offender who has passed away, unless authorized by the parent of the child, where no court proceedings have been instituted or by a court if a matter is pending before it. The Act empowers courts to order that children be referred to by initials, or by a pseudonym, and empowers the courts to exclude persons from court or hold a closed session to protect a child's privacy in legal proceedings.

70. There are several other articles of the Children's Act related to privacy. Article 32 states that the police may enter any place where a child is present and interview a child without the consent of, or in the absence of, its parent. Article 32 (2) also allows officers, in instances where children may be exposed to harm, represent a danger to themselves or to others or are suffering from a mental disorder, to interview children without the consent of, or in the absence of, their parents, and also permits officers to request health/social/educational or other children's service providers to provide information related to such services. Article 33 allows authorized officers to "enter, at any reasonable time and, where the circumstances so require, with the assistance of the Police, any place where the child is or was living, or such other place which the child usually visits".

71. Under the Children's Act, an array of offences in respect of children are criminalized, including child pornography, child grooming and bullying and online harassment, In addition, a Children's Court has been created with the power to grant care and protection orders and to determine cases involving criminal offences.

72. The Special Rapporteur heard from numerous interlocutors about the increasing importance of protecting the privacy rights of children, especially in cases of sexual exploitation, child trafficking and cyberbullying, as well as about the security risks to children's personal information when using and posting on social platforms.

73. The National Children's Council works with both the Ministry of Education and the Ministry of Gender and Child Protection Services, which employ specialized investigators who have signed confidentiality clauses to access data and are trained to protect sensitive information. However, the Special Rapporteur was informed that, in practice, as Mauritius is a small country, it is challenging to keep the information private, even if conveyed in a more generic format, as everyone knows everyone.

74. The Government has released several mobile apps, including the Family Welfare Mobile App, which allows anyone to report cases of child or domestic abuse. The app features a prominent "help me now" panic button when someone needs urgent assistance, which immediately locates the victim using a Global Positioning System. Action in response is taken by a group of first responders at the Ministry of Gender Equality, Child Development and Family Welfare.

75. The Special Rapporteur was informed that the Ministry of Gender Equality, Child Development and Family Welfare had set up a technical committee to study the phenomenon of child revenge pornography, with a view to, inter alia, setting up a system for data collection that would improve standard operating procedures for institutional interventions and enhance protection measures for victims.

76. The Ombudsperson for Children Act (2003) established the Office of the Ombudsperson for Children, which has the primary responsibility for carrying out investigations in an impartial, independent and non-discriminatory manner and for promoting the best interests of the child. The office also provides a free and transparent complaint service. Complaints can be made by and on behalf of children in relation to alleged violations by any public or private institution. Data regarding any complaint received by the office must be retained for 20 years. In addition, there is a minimalization of data (access is only permitted to the minimum information necessary) and health data is kept solely by the Ministry of Health and is not shared with other Ministries.

77. Of the 1.2 million children in Mauritius, there are approximately 500 to 600 children living in residential homes; those children have a right to privacy, including knowledge of their identity and family background. While the confidentiality of retained data is a fundamental right, there is also a concern regarding the absence or lack of data regarding children as it can deny them the right to know their family history and their own identity. This information is also important as it allows children to gain an understanding of their family medical history. Professionals rely on administrative records, including medical documentation, to obtain a comprehensive picture of the care provided to a child. If no data is retained or shared by the various institutions (including the Ministry of Health, the Ministry of Education and the Office of the Ombudsperson for Children) through a secure process, authorities may not be able to fully understand the patterns of abuse that a child may have been subjected to. Furthermore, such information can be leaked, causing irreparable damage.

78. The Minister of Education is committed to e-education and recognizes that digital skills and access to technology is a human right. There is a progressive learning curve: children in grades 1 to 3 use tablets that remain at school, and in grades 4 to 6 they use tablets to enhance their personalized learning. By secondary school, students are well versed in digital tools and have a sound understanding of how to protect their personal data. The use of social media is a particular challenge, including how to ensure a coherent approach that involves parental support and also protects children's privacy; children and teenagers are not only users of technology but also, increasingly, producers as they generate content and post on social media. Social platforms have their own regulations and rules, which, once accepted, put children's privacy at risk. The challenge is not that the laws in place are inadequate but that there is a low complaint rate and a lack of investigation and accountability. In discussions with authorities, the Special Rapporteur noted a gender bias; girls are more likely than boys to be subjected to cyberbullying and sexual exploitation.

IV. Conclusions and recommendations

79. **Mauritius, strategically located at the crossroads of Asia and Africa, has embraced emerging technologies while demonstrating a strong commitment to privacy to further elevate its economic and social development.**

80. **The Special Rapporteur welcomes the comprehensive legal framework (Data Protection Act 2017), which aligns domestic legislation with a robust international framework on the processing of personal data and privacy. This should be considered a good practice as Mauritius is one of the few States outside Europe to incorporate data protection laws in line with the General Data Protection Regulation of the European Union ((EU) 2016/679). The challenge for Mauritius is not in the recognition or regulation of the right to privacy, which appear to be exhaustive, but more in the lack of proper implementation of control procedures. Notably, violations of personal data protection occur owing to the inadequate implementation of data security measures in the information systems of both the private and public sectors, in particular with regard to sensitive health data.**

81. **While Mauritius clearly places a high value on privacy, additional measures are needed to balance innovation, security and privacy by strengthening and coordinating oversight powers.**

82. **Further Government collaboration among the national institutions and partnerships with the private sector are crucial to ensure respect for and protection and enhancement of the right to privacy, identify best practices and find solutions to advance towards a global harmonization of privacy regulations.**

83. **Regarding the privacy of vulnerable groups, the Special Rapporteur finds that additional steps need to be taken to further strengthen efforts to promote sensitivity and respect for personal dignity in order to ensure the right to privacy, online and offline, for older persons, persons with disabilities, persons on lower incomes, children and LGBTIQ+ persons, as well as to combat intolerance, prejudice, bullying and discrimination in the public sphere. A key factor is a mechanism to ensure that policies and laws are effectively implemented.**

84. **The Special Rapporteur places great emphasis on the importance of awareness, education, cooperation, harmonization and standardization at the regional and international levels and notes that Mauritius is already well placed in this regard.**

85. **With the continued support and collaboration with the United Nations country team, including the OHCHR Regional Office for Southern Africa, the Special Rapporteur believes that Mauritius can be a leading example in the region in using a human rights-based approach and building an international framework that embraces both technological and social progress while balancing security with the right to privacy.**

Recommendations on personal data protection

86. **The Special Rapporteur notes the high level of diligence exercised by the Data Protection Office to act in accordance with the principles of the General Data Protection Regulation of the European Union ((EU) 2016/679) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in order to ensure that personal data is processed fairly, accurately, securely and for a specific purpose, in accordance with a legitimate legal basis and utilizing a data protection framework; this represents best practice. However, the Office requires more financial resources[41] to improve public awareness and education so that individuals are better informed on how to protect their fundamental right to privacy.**

87. **Data is an important asset, and citizens need confidence and trust in their personal data. The protection of personal data is a shared responsibility that must be balanced with the right to access and disclosure; if data is overprotected, it can inadvertently enable corruption. Thus transparency, privacy by design (minimalization of data collection and retention), privacy impact statements and regional and international standards for data protection mechanisms are essential tools.**

88. **The Government recognizes the challenges related to e-systems and is creating an office of e-government to centralize and secure information and develop plans to improve the digital skills of the population. It is critical to implement preventive measures to address the challenges related to digitalization, which can undermine the ability to protect one's privacy.**

89. **To ensure that the legal framework on data protection remains strong and resilient, it must align with technological developments and ensure that legal safeguards are harmonized with international norms, as outlined in a previous report of the Special Rapporteur.**[42]

90. **The Government's cooperative work on data protection with the Council of Europe is a good practice. Several African States, including Cameroon, Côte d'Ivoire, Rwanda, Seychelles, Uganda and the United Republic of Tanzania, and have sought technical assistance and harmonization projects with Mauritius.**

91. **The Networking Forum for Data Protection Officers, launched in May 2023, facilitates the regular exchange of experiences, challenges and insights on the implementation of regulations and evolving best practices in data protection. It also provides opportunities for collaboration and training where privacy can be enhanced through the implementation of the Guiding Principles on Business and Human Rights.**

92. **Welcomes the commitment of the United Nations country team, led by the office of the Resident Coordinator for Mauritius and Seychelles, to support the efforts of the Government to take a leadership role on digital rights and to implement strategies to "leave no one behind", as enshrined in the 2030 Agenda for Sustainable Development and its Sustainable Development Goals. This effective partnership represents a good**

[41] Data Protection Office, Annual Report 2022, pp. 37–38 (https://dataprotection.govmu.org/Documents/AR22%20DPO.pdf).

[42] A/HRC/55/46, para. 124.

practice for States in Africa and Asia to promote cooperation and protect the right to privacy in an increasingly digital age.

93. **The Special Rapporteur recommends that the Government organize workshops to enhance a deeper understanding on the part of the public of safety and privacy when accessing various online services and using digital devices in order, inter alia, to close the digital divide, especially regarding vulnerable groups.**

94. **On 8 August 2024, Member States reached an agreement on a draft United Nations Convention against Cybercrime,[43] which was adopted by the General Assembly in its resolution 79/243, on 24 December 2024, as the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. The Convention includes an article on the reasonable expectation of privacy in the non-consensual dissemination of intimate images. The Special Rapporteur encourages Mauritius to become a signatory to the Convention.**

Recommendations on privacy and health data

95. **The COVID-19 pandemic provided an opportunity for a significant reflection on the positive and negative impacts of the increasing use of applications and digital solutions in patient healthcare. The Special Rapporteur urges the Government to consider and implement the recommendations on implementation of the principles of purpose limitation, the deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the COVID-19 pandemic.**[44]

96. **The Special Rapporteur welcomes the Government's "One Patient, One Record" initiative, which, while placing a strong emphasis on information exchange systems, also stresses the importance of robust security measures to ensure secure collaboration among healthcare providers managing sensitive health data. The transition to e-health records and the use of artificial intelligence and technology requires stringent measures and the standardization and harmonization of patient's data needs in order to adhere to the highest standards of privacy.**

97. **The Special Rapporteur emphasizes that the Ministry of Health must ensure the confidential treatment by health professionals and personnel to respect patient's right to privacy and dignity and to take all measures to ensure that systems, procedures, records and data collection protect the confidentiality of all medical and other related treatments.**

98. **The Special Rapporteur encourages the Government to consider the comprehensive recommendations regarding the protection and use of health-related data outlined in the report of her predecessor.**[45]

99. **The Special Rapporteur also encourages the Government to endorse the provisions of article 9 (2) of the General Data Protection Regulation of the European Union ((EU) 2016/679), which outlines the grounds on which special categories of data can be processed. One category is the consent of the data subject in order to protect personal health data related to reproductive health, sexual orientation and gender identity.**

Recommendations on surveillance and oversight

100. **The Special Rapporteur commends the efforts made by Mauritius to strengthen the legal framework to prevent privacy infringements by applying oversight standards**

[43] See A/AC.291/L.15.
[44] A/HRC/52/37 paras. 27–32.
[45] A/74/277, annex.

to unwarranted surveillance and encourages additional resources for an independent judicial oversight mechanism to increase investigative competence and technical expertise of law enforcement and intelligence experts.

101. **The Special Rapporteur recommends that the Government take the following measures regarding surveillance:**

(a) **Ensure adequate judicial powers to check for compliance ex ante, before surveillance or interception measures are undertaken, and to ensure that law enforcement personnel, prosecutors and judges receive adequate training to enable them to undertake privacy impact assessments and evaluate the quality of the data so that they better understand the possible consequences of the technologies they are regulating;**

(b) **Ensure that independent oversight agencies for all types of surveillance, whether intelligence or law enforcement, guarantee that an a posteriori inspection is not carried out by the same body that granted an a priori authorization of surveillance;**

(c) **Reinforce the independent supervisory role of the oversight bodies responsible for surveillance at all stages by strengthening their enforceable powers to terminate interception and/or destroy material by specifying accountability obligations and ensuring cooperation;**

(d) **Where Mauritius shares personal information and/or intelligence with other countries, ensure that it installs or reinforces adequate privacy safeguards for cross-border intelligence sharing;**

(e) **Seek funding to strengthen the capacity of all security systems, networks and data technology so they are upgraded in accordance with the regulations of the International Criminal Police Organization (INTERPOL).**

102. **Regarding facial recognition technology, owing to its potential to have a negative impact on the right to privacy, the Special Rapporteur strongly recommends that it be further studied and thoroughly tested before being considered for deployment.**

103. **While decisions by the National Human Rights Commission are non-binding, the Commission can play a pivotal role in raising greater awareness by robustly monitoring infringements and violations and ensuring that the judiciary and administrative bodies meet their legal obligation to impose sanctions and provide effective remedies in an era of increasing digital surveillance.**

Balancing the right to privacy and freedom of expression

104. **The right to privacy and the right to freedom of information are interrelated and must be weighed and balanced when assessing the effectiveness of personal data protection monitoring mechanisms. Thus, the Special Rapporteur recommends a review of the Information and Communications Technologies Act to ensure that it is implemented in a manner that does not infringe on the right to privacy and freedom of expression.**

105. **Freedom of information and expression is guaranteed under section 12 (1) of the Constitution of Mauritius and section 12 (2) provides for limitations. In order to respect the dignity and privacy for all citizens, in particular children, more robust measures are needed to ensure ethical reporting by the media.**

Recommendations on gender and reproductive rights

106. **Mauritius has ratified the International Covenant on Civil and Political Rights and the African Charter on Human and Peoples' Rights. The Special Rapporteur encourages the Government to recognize that the right to privacy includes the right to self-determination on gender and the freedom of individuals to make autonomous decisions about their bodies.**

107. **The Special Rapporteur urges the Government to follow up on the landmark decision of the Mauritius Supreme Court of 4 October 2023,**[46] **which ruled that it was unconstitutional to criminalize the private and intimate life of LGBTQI+ people by advancing and adopting legislative and regulatory measures to fully protect their privacy rights and combat discrimination against people based on their sexual orientation or gender identity.**[47]

108. **The Special Rapporteur reminds the Government of the view expressed by the Human Rights Committee that the right to privacy covers gender identity.**[48] **Mauritius has a duty to uphold the right to privacy in relation to gender identity.**[49] **The Special Rapporteur recommends that the principles outlined by her predecessor regarding gender identity and legal recognition**[50] **be respected and implemented.**

109. **The Special Rapporteur welcomes the Government's national gender policy, the national strategy on gender-based violence and the commitment to establish a Gender-Based Violence Management Information System, with a central database to enhance the harmonization of data collection by service providers, and to share data across diverse agencies to improve services to those subject to gender-based violence,**[51] **and urges the implementation of robust security measures owing to the sensitive nature of the personal data.**

110. **The Special Rapporteur concurs with the recommendation by the Committee on the Elimination of Discrimination against Women to include in school curricula mandatory, age-appropriate, scientifically accurate education for girls and boys on sexual and reproductive health and rights. The limited availability of educational material on sexual and reproductive health and rights has resulted in high adolescent pregnancy rates and restricted access to safe abortions owing to restricted legalization in certain circumstances (Criminal Code (Amendment) Act 2012, sect. 235A).**[52]

111. **The Special Rapporteur calls on the Government to be guided by the Yogyakarta Principles on the Application of International Human Rights Law in relation to Sexual Orientation and Gender Identity and the subsequent Additional Principles and State Obligations on the Application of International Human Rights Law in Relation to Sexual Orientation, Gender Identity, Gender Expression and Sex Characteristics to Complement the Yogyakarta Principles to ensure legal recognition of individuals' gender identity without imposing intrusive and onerous requirements.**

112. **The Special Rapporteur urges the Government to ensure that personal information relating to sex and gender is protected through regular vulnerability assessments of information management systems and regular training for staff on data privacy and data security.**

Recommendations on children and privacy

113. **Mauritius has undertaken efforts to promote and protect children's privacy, in accordance with the rights and values of the Convention on the Rights of the Child. However, to further safeguard their autonomy, in both the digital and non-digital spheres, it is necessary to strengthen policies, laws and regulations to incorporate specific strategies that reflect child privacy impact assessments before introducing innovations, including those intended to reduce the risks of cyberbullying, online exploitation and abuse of children and young people, to avoid inadvertent and harmful impacts and ensure that children have effective remedies against privacy infringements.**

[46] See https://www.humandignitytrust.org/wp-content/uploads/2023/10/Judgment-AH-SEEK-.pdf.
[47] A/HRC/56/8, para.153.294.
[48] See CCPR/C119/D/2172/2012.
[49] Resolution 34/7, para. 5 (g).
[50] A/HRC/43/52, paras. 35–36.
[51] CEDAW/C/MUS/FCO/8, para. 18.
[52] CEDAW/C/MUS/CO/8, paras. 23 (e) and 27 (a).

114. **The Special Rapporteur endorses the recommendation of the Committee on the Rights of the Child that Mauritius strengthen the implementation of the legislative provisions in place to protect the privacy of children, ensure that the media and other relevant professionals were appropriately trained on such regulations and policies and apply deterrent sanctions for violations of children's right to privacy.**[53]

115. **The Special Rapporteur supports the recommendation made by the Committee on the Rights of the Child to establish a mechanism to systematically involve civil society organizations working in the field of children's rights in the development, implementation, monitoring and evaluation of laws, policies and programmes**[54] **to protect the dignity and privacy rights of children.**

116. **The Special Rapporteur concurs with the assessment of the Special Rapporteur on the sale, sexual exploitation and sexual abuse of children that the Government should work more closely with the Office of the Ombudsperson for Children and act on recommendations contained in her report.**[55]

117. **The recommendations of the Ombudsperson are sent to Parliament but are not legally binding. However, 75 per cent of the Ombudsperson's recommendations are followed. It is important to implement those recommendations to ensure adequate protections and remedies for children's privacy.**

118. **The Special Rapporteur reminds the Government of the invaluable guidance provided by the Committee on the Rights of the Child in its general comment No. 25 (2021) on children's rights in relation to the digital environment.**[56] **In the same general comment, the Committee also recommends that the business sector undertake child-rights due diligence and child-rights impact assessments and implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services.**

119. **The Special Rapporteur recommends that the Ministry of Education, in coordination with the Ministry of Health, educate teachers and provide specialized counsellors to implement a comprehensive age-appropriate sexual education programme, which also addresses specific needs of children with disabilities, varying cognitive abilities and cultural and linguistic diversities, to inform children of the importance of understanding that they control their sphere of privacy (namely their body) and to mitigate teenage pregnancies, the threat of sexual violence and online activities aimed at the sexual exploitation of youth.**

120. **In the implementation of the Convention on the Rights of the Child, which Mauritius ratified in 2011, the Committee on the Rights of the Child urged States to repeal all laws criminalizing or otherwise discriminating against individuals on the basis of their sexual orientation, gender identity or intersex status and to adopt laws prohibiting discrimination on those grounds.**[57]

121. **The Special Rapporteur encourages the Government to take into consideration the recommendations of her predecessor on children and privacy.**[58]

122. **The Special Rapporteur recommends that the Government prioritize digital education to children, in age-appropriate language, on exercising their rights to privacy and to ensure there are provisions for counselling and administrative and judicial complaint mechanisms.**

---

[53] CRC/C/MUS/CO/6-7, para. 20. See also A/HRC/52/31/Add.1, para. 119 (s).
[54] CRC/C/MUS/CO/6-7, paras. 13 and 24.
[55] A/HRC/52/31/Add.1, para. 119 (ii).
[56] CRC/C/GC/25.
[57] CRC/C/GC/20, para. 34.
[58] A/HRC/46/37, para. 127.