Joint Submission to the UN Universal Periodic Review 41st Session

THE RIGHT TO PRIVACY IN INDONESIA

Joint Submission by the Institute for Policy Research and Advocacy (ELSAM) and Access Now

ELSAM
Alia Yofira
alia@elsam.or.id
www.elsam.or.id

Access Now
Dhevy Sivaprakasam
dhevy@accessnow.org
www.accessnow.org

Introduction

1. This stakeholder report is a joint submission by the Institute for Policy Research and Advocacy (ELSAM) and Access Now.

2. ELSAM was established in August 1993 in Jakarta. Its objective is to actively participate in efforts to develop, promote and protect civil and political rights and other human rights, as mandated by the 1945 Indonesia Constitution and Universal Declaration of Human Rights (UDHR).

3. Access Now is an international organisation that works to defend and extend the digital rights of users at risk around the world. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organisation, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age.[1]

The Right to Privacy under International Law

4. The right to privacy is enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights - underlining the right to "protection of the law against arbitrary interference or attacks" against one's privacy.[2] Privacy is a fundamental right that is at the core of the exercise of human autonomy and dignity[3] and which supports and strengthens the exercise of other rights, including the rights to

[1] Access Now, *About Us*, Available at: https://www.accessnow.org/
[2] Universal Declaration of Human Rights, Article 12 (No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.xx); International Covenant on Civil and Political Rights, Article 17. The right to privacy is also enshrined in multiple other international, and regional human rights instruments, including United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.
[3] Privacy International, *What is Privacy?*, Available at: https://privacyinternational.org/explainer/56/what-privacy.

freedom of expression, information, and association.[4] Violations of privacy can also result in infringements on the rights to liberty and security, life and freedom from ill-treatment or torture.[5] Such violations are increasingly being facilitated by state abuse of surveillance technologies - including tools to conduct both mass and targeted surveillance of individuals.[6]

5. Even as the right to privacy is a qualified right upon which limitations may be permitted, such limitations must be prescribed by law, strictly necessary to achieve a legitimate aim and proportionate to the aim being pursued.[7] The Special Rapporteur on the right to privacy has clarified that limitations must be narrowly confined to only "special measures spelt out under international law as well as necessarily having a clear basis in domestic law".[8] With respect to surveillance technologies, the International Principles on the Application of Human Rights to Communications Surveillance provide further guidance that surveillance undertaken by states must be shared transparently with the public on the use and scope of measures and be subject to independent and impartial oversight - including judicial oversight and due process.[9]

6. With respect to data protection, even as the protection of personal data is distinct from the right to privacy, both are closely interconnected. It is of paramount importance in an increasingly digitalised world that personal data protection is prioritised, and adequately and effectively protected through national legal frameworks.[10] Data protection and the

---

[4] See for example, UN Human Rights Council, *Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35 ('*UNSR FoE report 2019*') detailing how surveillance impacts not only on privacy, but equally on the rights to free expression, information, and association, amongst other rights. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement

[5] Former UN Special Rapporteur David Kaye monitored how human rights defenders, journalists and opposition figures were subject to arbitrary detention, torture and possible extrajudicial killings from surveillance. See *UNSR FoE report 2019;* Access Now has also monitored, for example, increasing surveillance and violations of privacy in Myanmar by the military resulting in arrests, assaults, detention, ill-treatment, torture and killings on the ground. See: [Ongoing] https://www.accessnow.org/update-internet-access-censorship-myanmar/

[6] See for example, Access Now et. al, *Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors*, March 2022, Available at: https://www.accessnow.org/cms/assets/uploads/2022/03/2022_STAP_Guide.pdf

[7] UN Human Rights Council, *Report of the Special Rapporteur on the right to privacy*, 25 October 2018, A/HRC/37/62, Available at: https://digitallibrary.un.org/record/1656178?ln=en

[8] *Ibid.*, p24, para 4.

[9] International Principles on the Application of Human Rights to Communications Surveillance, July 2013, Available at: https://necessaryandproportionate.org/principles/

[10] See for example, Access Now, *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers* for reference, November 2018, Available at: https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf; Access Now, *The best and the worst in 2022: data protection laws across the world,* 27 January 2022, Available at: https://www.accessnow.org/data-protection-laws-in-2022/

right to privacy should also be priorities when deciding to implement national digital identity programmes.[11]

The Right to Privacy under Indonesian National Law

7. While Indonesia's 1945 Constitution does not explicitly mention privacy, it is understood to be part of rights and it is further protected in specific legislation. For instance, Article 28G (1) of the Constitution protects the right to dignity and security, which is often associated with the right to privacy. In addition, Article 21 of Law No. 39 of 1999 on Human Rights establishes that no one should be the subject of search without the consent of the person concerned.[12] This entails that everyone has the right to personal protection, family, honor, dignity, and property under their control, and has the right to a sense of security and protection from threats, which must be based on his consent.[13]

8. Additionally, Indonesia has ratified several international human rights instruments protecting the right to privacy, notably the ICCPR through Act No. 12 of 2005.

Follow up to the previous UPR

9. There was no explicit mention of the right to privacy in the National Report submitted by Indonesia in 2017, and the issue was not addressed in the report of the Working Group following the consideration of the state report in 2017,[14] despite the privacy issues being raised in Stakeholder Submission.[15] Since then a number of concerns relating to the right to privacy have arisen in Indonesia, making this issue particularly important.

10. Various recommendations were submitted on related topics developed in this report which enjoyed the support of the government including to, (a) continue its efforts to consolidate the principles of human rights and public freedoms (Yemen)[16], and (b) ensure that the freedom of speech of civil society organizations and special interest groups is promoted and respected across Indonesia so that they can, within the legal

---

[11] Access Now, *National Digital Identity Programmes: What's next?,* May 2018, Available at: https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf
[12] https://heylawedu.id/blog/hak-privasi-menurut-perspektif-hak-asasi-manusia
[13] Pradana Satya Aji Kusuma on Thesis "Protection of Data Privacy in the Digital Era (Comparative Approach Between Indonesian Law and European Union Law)", 2020, Universitas Islam Indonesia Yogyakarta, pg. 59.
[14] A/HRC/36/7 Report of the Working Group on the Universal Periodic Review, Indonesia, 3 May 2017.
[15] The Right to Privacy in the Indonesia Stakeholder Report Universal Period Review 27th Session (Sept 2016), available at: https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=3914&file=EnglishTranslation.
[16] Indonesia's Responses to Recommendations, Third Review Session 27, No. 139.13, pg. 2.

framework, voice their views and concerns, even on issues that can be sensitive (Netherlands).[17]

Areas of Concerns

11. In Indonesia, there have been various cases of violation of the right to privacy in the last few years. Notably, the absence of protections for privacy and personal data in Indonesia's domestic legal frameworks has facilitated these infringements. Some of these cases include:

Rampant Data Breach and Data Misuse Cases in Indonesia

12. In early May 2020, Tokopedia - an e-commerce platform - was hit by a data leak of more than 15 million accounts. The data that had allegedly been sold online for USD 5,000 or around 70 million Rupiah[18] can now be downloaded for free on the dark web.[19] The Indonesian Consumer Community (Komunitas Konsumen Indonesia or KKI) has filed a lawsuit in May 2020 against Tokopedia and the Minister of Communication and Informatics (MoCI) concerning Tokopedia's consumer data breach.[20]

13. Data protection regulations in Indonesia can be found in various sector-specific regulations, including in e-commerce as well as electronic systems and transactions. However, none of these regulations provide a comprehensive protection for the personal data in Indonesia. A personal data protection bill is currently being discussed by the The House of Representatives and the MoCI. However, the enactment of the data protection bill is currently hampered by talks about the oversight mechanism that the bill will establish.[21]

14. Due to the absence of a comprehensive data protection law, data protection in e-commerce sector is mainly supervised by the MoCI and regulated under the

[17] Ibid, No. 139.76, pg. 6.
[18] "Tokopedia data breach exposes vulnerability of personal data", The jakarta Post, 2020, available at: https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html.
[19] "91 Million User Data Can Still Be Downloaded, Tokopedia Affirms", Mime Asia, 2020, https://www.mime.asia/91-million-user-data-can-still-be-downloaded-tokopedia-affirms/; See also "Guessing Malicious Threats From Tokopedia's Data Leaks", VOI, 2020, https://voi.id/en/technology/8284/guessing-malicious-threats-from-tokopedias-data-leaks.
[20] "Consumer Association File Lawsuit Against Tokopedia", Tempo.co, 2020, https://en.tempo.co/read/1339873/consumer-association-file-lawsuit-against-tokopedia.
[21] "Personal Data Protection Bill Hampered by Arduous Discussions on Management", Tempo.co, 2022, available at: https://en.tempo.co/read/1574708/personal-data-protection-bill-hampered-by-arduous-discussions-on-management.

Government Regulation No. 71 of 2019 on the Operation of Electronin Systems and Transactions (GR 71/2019). Article 14 (5) of the GR 71/2019 provides data subjects with the right to be notified "*In the event of a failure in the protection of the Personal Data*". Furthermore, Article 28 of the MoCI's Ministerial Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems (MR 20/2016) regulates that the notification should be made no later than 14 days after the incident occurred. Not only that *firstly,* the time limitation of the notification is in contrast to the principle of personal data protection which requires notification without undue delay, but *secondly*, to this date, Tokopedia as an Electronic System Operator has yet to notify its users about the data breach incident. Inadequate data protection regulations topped with weak enforcement by the MoCI underlined the urgency of having an independent oversight mechanism of data protection matters in Indonesia.

15. Not only in the e-commerce sector, data breach incidents also occurred in the financial service sector. In July 2021, the data of more than two million customers of BRI Life - the insurance arm of Indonesia's national bank, Bank Rakyat Indonesia (BRI), was allegedly leaked and sold online by hackers for US$ 7,000 or around Rp. 101.5 million by.[22] The data breach includes 463,000 documents of sensitive data namely, a photo of the National Identity Card (KTP), Family Card (KK), photo of the account book, birth certificate, death certificate, proof of transfer, photo of lab results to a description of the disease.[23]

16. Data protection regulations in the financial service sector can be found under Article 2 letter d of the Financial Service Authority (OJK) Regulation No. 1/POJK.07/2013 on Consumer Protection of Financial Services. Additionally, Article 31 of the OJK Regulation also explicitly prohibits financial services business actors to provide data and/or information about their consumers to third parties. Violation of this rule will be subjected to administrative sanctions in the form of written warnings, fines and revocation of business activity permit in accordance with Article 53 (1). However, none of these provisions accommodates the right to be notified and the right to an effective remedy for consumers as data subjects.

17. Moreover, the inadequacy of data protection regulations in the financial services sector has also been disproportionately affecting women and gender minorities in Indonesia. In recent years, financial technology particularly the peer-2-peer lending (also known as

[22] "Indonesia's BRI Life probes reported data leak of 2 million users", Channel News Asia, 2021, available at: https://www.channelnewsasia.com/business/indonesias-bri-life-probes-reported-data-leak-2-million-users-2077781

[23] "Data Nasabah BRI Life Diduga Bocor dan Dijual Rp 101,5 Juta", Katadata, 2021, available at: https://katadata.co.id/desysetyowati/digital/60ffec1625b49/data-nasabah-bri-life-diduga-bocor-dan-dijual-rp-101-5-juta#:~:text=Data nasabah perusahaan asuransi%2C BRI,sekitar Rp 101%2C5 juta.

pinjol in bahasa) industry has gained popularity in Indonesia[24], especially during the pandemic.[25] However, despite the benefits offered by online lending applications, the industry is unfortunately currently underregulated. This has resulted to various harassment including online gender-based violence cases by the debt collectors. Based on data from online loan application users (to LBH Jakarta), 72.08 percent are women and 22 percent of them must have experienced online gender-based violence cases by the debt collectors.[26]

18. The OJK published several forms of harassment by pinjol applications, namely: loan disbursement without user's consent, spreading and/or threat of spreading personal data (usually a user's self-portrait holding an e-KTP which was initially collected by the app for e-KYC purposes, but can also include other personal pictures on the user's phone gallery), contacting all users' phone contacts (friends, relatives, neighbours, colleagues at work, etc) with terror or intimidation messages, as well as biling with harsh words and sexual harassment.[27] These aggresive debt-collection methods have resulted in new forms of intimidation and harassment with tragic outcomes such as people committing suicide.[28]

19. The private sector is not the only sector prone to data breach incidents. In May 2020, reports emerged of leaks from the public sector of data belonging to millions of individuals in Indonesia - allegedly leaked and shared through hacker community forums. This included leaks from the 2014 Election Permanent Voters List (DPT) (also known as the electoral roll) data, which was first revealed by the Twitter account @underthebreach on May 21, 2020.[29] The data was shared in the hacker community forum in the form of a

[24] "Consumers Face Harassment by Fintech Debt Collectors Due to Weak Data Protection", Jakarta Globe, 2019, available at: https://jakartaglobe.id/context/consumers-face-harassment-by-Fintech-debt-collectors-due-to-weak-data-protection.
[25] "The 'pinjol' trap: The horrors of payday loans in pandemic-stricken Indonesia", The Jakarta Post, 2021, available at: https://www.thejakartapost.com/life/2021/09/16/the-pinjol-trap-the-horrors-of-payday-loans-in-pandemic-stricken-indonesia.html.
[26] "Online Loans and the Absence of State Protection", LBH Jakarta's YouTube channel, Friday, September 10, 2021, available at: https://youtu.be/rnWp21PWKHA.
[27] "Still Want to Use Illegal Loans? OJK Says They Often Charge People With Rude Words and Sexual Harassment", VOI, 2021, available at: https://voi.id/en/economy/95274/still-want-to-use-illegal-loans-ojk-says-they-often-charge-people-with-rude-words-and-sexual-harassment.
[28] "Indonesia's online P2P loan sharks are driving people to suicide", South China Morning Post, 2019, available at: https://www.scmp.com/week-asia/economics/article/2188185/indonesias-online-p2p-loan-sharks-are-driving-people-suicide; see also "Indonesia: Online loan sharks intimidate and harass borrowers; activitsts call for better regulations", Business and Human Rights Resource Centre, 2019, available at: https://www.business-humanrights.org/en/latest-news/indonesia-online-loan-sharks-intimidate-and-harass-borrowers-activists-call-for-better-regulations/.
[29] "Calls mount for comprehensive audit into data breach affecting 2.3 million voters", The Jakarta Post, 2020, available at:

PDF file, with the hacking claiming to have pocketed the data of 2.3 million individuals. The electoral roll data collected includes a number of sensitive information, such as full name, family card number, Population Identification Number (NIK), place and date of birth, home address, and several other personal data. Hackers also claimed that they had 200 million Indonesian citizens' data that will be leaked in the forum.

20. Given the dualistic nature of electoral rolls data, striking a balance between transparency and the data protection aspects have been particularly challenging in Indonesia. On the one hand, voter lists are open data, which can be accessed by anyone, to ensure fair and accountable elections. However, on the other hand, these data also contain personal data content, which is subject to a number of personal data protection principles. Due to its dualistic status, the "*open to inspection by the general public with limited exception*" principle has been applied to electoral roll data. The principle has not been adequately reflected in laws in Indonesia.

21. The Indonesian electoral rolls are currently governed by two main pieces of legislation namely Law No. 7 of 2017 on Elections and Law No. 23 of 2006 on Population Administration, which together regulate that the electoral roll is replicated from the personal data collected under the National ID System (e-KTP program), and is updated every six months. Furthermore, Article 208(5) of the Elections Law also obliges the General Election Commission to provide political candidates and parties with a copy of the electoral roll. Given the scope of personal data contained in the electoral roll and the inadequate data protection provisions in the election sector, giving full access to the electoral roll data to political actors will make Indonesians prone to risks of data abuse for political purposes.

Surveillance and Digital Attacks against Human Rights Defenders

22. Surveillance tools have been abused - apparently by state-linked actors and private companies to monitor and target human rights defenders, and undermine their rights to privacy, expression, information and association. The right to freedom of expression has already been on a decline in Indonesia in recent years, which is exemplified by the increasing number of people convicted of defamation, blasphemy and *makar* (treason) simply for expressing their opinions online or organizing peaceful protests between 2014 and 2019.

23. From 2014 to 2019, were 29 incidents where students, academics, journalists and activists have been harassed and intimidated simply for criticizing the government or

https://www.thejakartapost.com/news/2020/05/22/calls-mount-for-comprehensive-audit-into-data-breach-affecting-2-3-million-voters.html.

discussing politically sensitive issues such as human rights violations.[30] Intimidation through digital means takes many forms, including credentials theft of their WhatsApp accounts, spam calls from unknown international numbers, digital harassment like distractions during online discussions - including through 'Zoom-bombing', and even direct physical violence.

24. The case of independent researcher and government critic Ravio Putra is emblematic of surveillance and digital attacks towards human rights defenders in Indonesia. On 22 April 2020, Ravio was arrested on suspicion of spreading troublesome news that incited violence and hate through the WhatsApp messaging application after his account was anonymously hacked and taken over unidentified parties, who then used it to broadcast calls for riots and looting.[31] The unidentified hackers who took over Ravio's WhatsApp account managed to bypass WhatsApp's 2-step verification and biometric fingerprint verification that Ravio has turned on his account.[32] This raised speculations that the perpetrators behind the hack have resources relating to Ravio's personal information that apparently only state institutions have access to.

25. There are numerous reports that indicate the purchases of surveillance tools by the Indonesian Government in the past. For instance, the United Kingdom's Department of Business, Innovation and Skills disclosed in its export data between February 2015 and April 2016 that Indonesia had imported IMSI Grabber Technology from companies from the UK.[33] This adds to previous purchases by the Indonesian Government in 2013 from UK-based surveillance company Gamma TSE of sophisticated wiretapping equipment.[34] Since 2012 researchers has documented the use of surveillance technologies, products, and services in Indonesia, particularly the FinFisher command-and-control (C2) targeting people in Indonesia.[35] In a follow up report published in 2013, researchers found

---

[30]"Indonesia: End Wave of Digital Attacks on Students, Journalists, Activitsts", Amnesty International, 2020, available at: https://www.amnesty.id/wp-content/uploads/2020/06/Final_Amnesty-International-Indonesia-Public-Statement-on-Digital-Attacks-17-June-2020.pdf.

[31]"Indonesia: End Wave of Digital Attacks on Students, Journalists, Activitsts", Amnesty International, 2020, available at: https://www.amnesty.id/wp-content/uploads/2020/06/Final_Amnesty-International-Indonesia-Public-Statement-on-Digital-Attacks-17-June-2020.pdf.

[32] "The Curious Case of Ravio Patra: Why Indonesian Cyberspace is a Dystopian Nightmare", The Jakarta Post, 2020, available at: https://www.thejakartapost.com/academia/2020/04/24/the-curious-case-of-ravio-patra-why-indonesian-cyberspace-is-a-dystopian-nightmare.html.

[33] "British Companies Are Selling Advanced Spy Tech to Authoritarian Regimes", Motherboard, 2016, available at: http://motherboard.vice.com/read/the-uk-companies-exporting-interception-tech-around-the-world.

[34] "TNI to step up surveillance", The Jakarta Post, 2013, available at: https://www.thejakartapost.com/news/2013/09/23/tni-step-surveillance.html.

[35] Morgan Marquis-Boire, *et.al.*, "You Only Click Twice: FinFisher's Global Proliferation", Citizen Lab, 2013, available at: https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

mobile-related evidence with a specific connection to Indonesia that is significant and deserves further scrutiny.[36]

26. These purchases by the Government of Indonesia have been carried out without a comprehensive communications surveillance law in place which reflects international human rights standards and provides sufficient regulation limiting the scope for abuse and arbitrary interference with the right to privacy.

Digital ID System: E-KTP

27. Indonesia's mandatory national ID system, e-KTP (electronic identity card), was introduced in 2009 under the Population Administration Act, which regulates about a single identification number for all citizens. In 2010, a Presidential Regulation was published to create a framework for the digitalization of the system and compulsory biometric data collection. Data collection is conducted by the Ministry of Home Affairs (MoH), which requires 31 points of personal data including sensitive data such as gender, blood type, marital status, disability information, religion and biometric data (fingerprints and iris scan). The data collected for the system is stored in a centralised database maintained by the MoH.

28. Article 84(1) of the Population Administration Act provides a very narrow definition of personal data - as it explicitly provides exhaustive list of what constitutes personal data namely: biometric data (iris scan, fingerprints, health records), signature and information that brings dishonor to the individual. Other personal data such as the e-KTP number, family card, mother's name, her e-KTP number (which is commonly used as a security question for verification means by banks), does not fall into the category of personal data in accordance to the Population Administration Act. This

29. In 2021, the MoH disclosed that 3,904 public bodies which comprise 2,178 central ministerial/agencies and 1,726 local government institutions were given access to the database.[37] In return, these bodies are required to share so-called feedback data with the MoH - that is, the personal information of people services by them (e.g. driver's licence number, national health insurance card numbers, taxpayer-identification numbers, bank account status, vehicle registration places, phone numbers, passport numbers, etc).

[36] Citizen Lab, "Islands of Control, Islands of Resistance: Monitoring the 2013 Indonesian IGF", 2014, pg. 47, available at: https://citizenlab.ca/briefs/29-igf-indonesia/29-igf-indonesia.pdf.
[37] "From 30 to 3,904 Institutions, Integration of National Data Has Progressed", Ministry of Home Affairs, 2021, available at: https://www.dukcapil.kemendagri.go.id/berita/baca/859/dari-30-jadi-3904-lembaga-pengguna-integrasi-data-nasional-sudah-berjalan.

30. Yet in 2022, the MoH announced another version of e-KTP called '*digital e-KTP*' program - which is equipped with features such as QR code.[38] So far, the program has been rolled out in 58 districts and cities in Indonesia. In simple terms, the Digital e-KTP is in the form of an application that contains the identity of a citizen, as stated on the physical e-KTP, such as the Population Identification Number (NIK), full name, date of birth, address, and so on. The Digital E-KTP requires residents to download an application and register themselves first, by matching it to the personal identity data contained in the physical e-KTP.[39]

31. In addition to personal identity, e-KTP Digital or Digital Identity will also contain other data that is integrated with NIK, such as Family Card, Covid-19 Vaccine Card, Taxpayer Identification Number (NPWP), Vehicle Ownership, and so on.[40] With Digital Identity, residents no longer need to carry a physical e-KTP. Your identity will be stored in the application on your phone. This creates privacy and cybersecurity concerns as it will allow the Indonesian government to create a centralised comprehensive profile of its citizens, all linked to a single ID number, especially considering that Indonesia currently doesn't have comprehensive laws instituting effective protections for cybersecurity act and data protection which limit how the government uses our data.

32. Back in 2017, former minister of the MoH, Tjahjo Kumolo, abused his power and share an e-KTP card of Veronica Koman, a human rights defender[41], who publicly criticizes the Indonesian Government.[42] Moreover in 2021, the MoH confirmed that 4 local governments agencies who have access to the database have been allegedly reported to suffer from data breach incidents.[43] To this date, the follow up of these data breach incidents by the law enforcement authorities remains unclear.

33. Digital identity programmes which do not take into account the domestic framework and insufficient legal safeguards not only increase risks of surveillance of individuals' personal data - particularly as Indonesia currently lacks a strong data protection legal framework - but also heighten concerns of data breaches and leaks by anonymous

[38] "Ministry of Home Affairs trial Digital e-KTP in the form of QR code", CNN Indonesia, 2021, available at: https://www.cnnindonesia.com/nasional/20211231153714-20-741099/kemendagri-uji-coba-e-ktp-digital-berbentuk-qr-code.
[39] It is unclear at the moment whether the digital e-KTP program will be made mandatory, but the e-KTP program is mandatory as of date.
[40] "Digital E-KTP Differs from Ordinary E-KTP, Do You Know the Difference?", Kontan, 2022, available at: https://nasional.kontan.co.id/news/e-ktp-digital-berbeda-dengan-e-ktp-biasa-sudah-tahu-perbedaannya-1.
[41] "Rights defenders under attack in Asia - UN experts", United Nations, 2021, available at: https://news.un.org/en/story/2021/12/1108022
[42] "The Minister of Home Affairs's act of sharing ID cards has drawn criticism", BBC, 2017, available at: https://www.bbc.com/indonesia/indonesia-39893468.
[43] "Dukcapil data in 4 regions allegedly leaked, DPR members ask the police to act", Tempo.co, 2021, available at: https://nasional.tempo.co/read/1472775/data-dukcapil-di-4-daerah-diduga-bocor-anggota-dpr-minta-polisi-bertindak/full&view=ok.

hackers for sale or other forms of abuse, which are already a pressing problem in Indonesia. In an analysis of a similar digital identity system in India, Aadhaar, glitches in the system were found to have declared as dead individuals who were still alive; and exacerbated tracking of individuals by personal characteristics, such as gender, religion, caste and political affiliations. The system also exacerbated difficulties of marginalised communities in accessing social services, increasing inequalities through increasing transaction costs for welfare recipients, delayed payments, and decreased distribution to qualified recipients.[44] These cautionary lessons are very much applicable to Indonesia - a similarly large and diverse country with existing concerns about data privacy and lack of public trust about government handling of personal data.

Health Data Governance

34. The condition of the Covid-19 pandemic has made awareness of the importance of using data in order to maximize the effectiveness of health services in Indonesia. Health data is important for contact tracing of identified Covid-19 patients and targeted vaccinations. On the other hand, the use of health data should also be balanced with adequate data protection and privacy safeguards.

35. After the COVID-19 pandemic, the monitoring process for under the skin surveillance is increasing, including in Indonesia. Take the case of PeduliLindungi contact tracing application which is operated by the Indonesian Ministry of Health[45] which excessively collect it's users data which are not necessary for the app's main features to function and violate the data minimization principle.[46] Researchers have also found that PeduliLindungi shared its user's geolocation, device identifiers, full name, and phone number to Telkom Indonesia, a telecommunications company that is majority owned by the Indonesian Government and is the app's developer.[47] None of these data transmissions are essential for contact tracing. Currently, regulations in health sectors which indirectly deals with data protection have yet to reflect not only the data minimization principle, but also other essentials data protection principles.

36. Furthermore, researchers have also found that particularly in the management of personal data related to the handling of COVID-19 in Indonesia involves many

[44] Access Now, Busting the Dangerous Myths of Big ID programs: Cautionary Lessons from India, October 2021, Available at: https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf
[45] PeduliLindungi, "Privacy Policy", 2022, available at: https://www.pedulilindungi.id/kebijakan-privasi-data?lang=en
[46] https://elsam.or.id/pentingnya-pelindungan-privasi-dalam-tata-kelola-data-kesehatan/
[47] Pellaeon Lin, *et.al*, "Unmasked II: An Analysis of Indonesia and the Philippines' Government-launched COVID-19 Apps", Citizen Lab, 2020, available at: https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/.

applications that essentially put heavier workloads for health workers and eventually hampers the access to public and health services during the pandemic.[48]

37. The current situation in Indonesia with multiple applications to manage COVID-19-related personal data, at both federal and local levels, differentiated in governance between ministries and in accordance with varying legal frameworks creates a scenario ripe for risks of data breaches and other abuses of privacy. Data minimisation, purpose limitation and limited data retention are three of the core principles for the protection of personal data and privacy, that must urgently be put in place and prioritised. This means that the collection, use, sharing, storage, and other processing of health data should be limited to what is strictly necessary to combat the pandemic; strictly limited to those who need the information to conduct relevant treatment and research for such combating measures; and the data kept strictly for the duration of the crisis and deleted thereafter, with data retention only permitted for narrow public interest purposes.[49]

Recommendations

38. For the foregoing reasons, we urge the Indonesian government to:

39. Bring into force a comprehensive legal framework for data protection with adequate and effective privacy safeguards; which will be implemented and overseen by an independent, impartial and adequately resourced data protection authority. The development of these legislations should be transparent and include public consultation with legal and technical experts specialised in the field of data protection; members of civil society, academia and the government; and seek coordination and advice from international data protection authorities and experts;

40. Ensure that the right to privacy is explicitly protected under domestic law, including through legal reform and/or amendments to existing legislation such as the Law No. 39 of 1999 on Human Rights;

41. Ensure that data protection and the right to privacy are a priority when deciding to bring into force the national ID programme, including halting the roll-out of the programme until the authorities and the public can be satisfied that the collection, use, transfer,

[48] Anesthesia Novianda, *et.al.*, "Menata Kelola Data Demi Pelayanan Publik: Studi Kasus Tata Kelola Data Sektor Kesehatan dan Pendidikan di Indonesia selama Pandemi Covid-19", CIPG and TIFA Foundation, 2022, available at: https://cipg.or.id/en/publication/tata-kelola-data/.

[49] Access Now, Recommendations on Privacy and Data Protection in the fight against COVID-19, March 2020, Available at: https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf

storage and other processing of personal data are in line with the principles of legality, necessity and proportionality, and data minimization; legal reform and/or amendments to existing legislation such as the Law No. 23 of 2006 on Population Administration;

42. Hold on to the deployment of the digital e-KTP and evaluate the need of implementing a digital ID system on the basis of an inclusive and transparent human rights impact assessment. Where there is an imperative need to have a digital identity system, adopt a legal framework to regulate the development and use of the digital e-KTP, centered on human rights, and overseen by an independent and adequately resourced authority, with a decentralized and secure infrastructure, which prioritizes the inclusion of all the population and their realities in the architecture of the system by making enrollment not mandatory;

43. Refrain from monitoring and targeting individuals deemed critical of the government, including civil society members, journalists, academics, members of the political opposition, and human rights defenders - including through the abuse of surveillance technologies;

44. Ensure that its communications surveillance laws, policies and practices adhere to international human rights law and standards including the principles of legality, proportionality and necessity;

45. Provide effective and independent oversight of surveillance by intelligence and law enforcement agencies ensuring adherence to international human rights laws and standards; and

46. Ensure that all contact-tracing efforts relating to COVID-19 prioritise the application of the principles of data minimization, purpose limitation and limited data retention; Ensure that all measures undertaken by the government to collect, use, transfer, store or otherwise process personal data collected through contact tracing measures are transparently shared with the public, and through inclusive and open consultation with independent members of the academic, healthcare and civil society sectors;