

# MINIMISATION OF SENSITIVE PERSONAL ETHNICITY DATA OF A POPULATION IS KEY IN TRANSITIONAL JUSTICE IN RWANDA

TIMOTHY AYUO\*

## ABSTRACT

Sensitive personal data of a population in the wrong hands is dangerous data; a tool for genocide. Just to mention, the genocide against the Tutsis in Rwanda was seriously aided by uncontrolled and unfettered access to sensitive personal data of the population particularly on tribe on “indangamuntu”- Identity Document. During the 1994 genocide in Rwanda, ID cards identifying people by their so-called “ethnic group” served, for some, as an effective death sentence. The post-colonial Rwandan authority’s decision to include “ethnic group identities” on ID cards, which had originally been introduced back in 1933 by the Belgian colonial government, not only brought the very idea of rigid racial group identities to the fore, but it also “facilitated the identification of victims” and meant that the genocide took place in a terrifyingly systematic and organized way. Data gathering around sensitive topics has a long history of being used in malicious and dangerous ways including genocides. History confirms that lack of minimisation of sensitive data of a population can be a root cause for genocide. Practising data minimisation is a keystone of a rights-based, responsible data approach. The European Union (EU) Policy Framework on Transitional Justice provides principles that advocate for a Rights-Based Approach to transitional justice. In the EU under the General Data Protection Regulation article 5(c) personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Data minimisation means that you should only collect and process personal data that is absolutely necessary to fulfil your purpose. You need to implement internal procedures and routines to review this on a regular basis. Default data minimisation policy is also an option to be explored. This article is a result of qualitative research method, analyzing library resources from scholars in the field of

---

\* Timothy Samson Ayuo is a seasoned Data Protection Officer (DPO). He has served in healthcare, education, and financial sectors, offering strategic guidance on compliance with the GDPR and Kenya’s Data Protection Act (KDPa).

data protection and transitional justice. It also examines how sensitive data of a population can be weaponised for genocide as seen in 1994 Rwanda and 1938 Nazi-Germany, and further explore data minimisation and human rights-based approach to data to reverse that trend in transitional justice.

**Key words:** Personal Data, Ethnic group identity, Data minimization, Default data minimization, Transitional justice and Ethnicity data

## 1. INTRODUCTION

Ethnicity data is sensitive personal data. Ethnicity as a death sentence witnessed in massacres and genocides is a trend that must be ebbed if the 1994 genocide against the Tutsis and the 1938 genocide against the Jews in Nazi Germany is anything to go by. The underlying denominator that facilitated the genocides is ethnicity data. Accordingly, ethnic cleavage through IDs can act as a tool for genocide. An estimated over one million Tutsis were killed while thousands suffered crimes against humanity. The sanctity of the right to life is a non-derogable norm and cannot be sold at the altar of ethnic data. Identification of individual members of a targeted population group is a necessary task for perpetrators of genocide and ethnic cleansing. To accomplish this task, perpetrators either adapt existing administrative structures to their new purposes or create new structures. Identity cards are often the key element in a larger identification system. Their central position in such a system is due to their role in attaching the identity of the targeted group onto individual persons, combining individual identity information with a group profile.<sup>1</sup> In his 1996 book on Ethnic Cleansing, Andrew Bell-Fialkoff locates genocide and ethnic cleansing within a continuum of eliminationist population policies, offering the following as a definition of population cleansing:

Population cleansing is a planned, deliberate removal from a certain territory of an undesirable population distinguished by one or more characteristics such as ethnicity, religion, race, class, or sexual preference. These characteristics must serve as the basis for removal for it to qualify as cleansing.<sup>2</sup>

1 Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing Presented on 15 November 2001 to the Seminar Series of the Yale University Genocide Studies Program by Jim Fussell, Prevent Genocide International at p.6

2 Andrew Bell-Fialkoff, *Ethnic Cleansing* (New York: St. Martin's Griffin, 1996); Barnett R. Rubin, "Russian Hegemony and State Breakdown in the Periphery: Causes and Consequences of the Civil War in Tajikistan," paper prepared for the Carnegie Project on Political Order, Conflict and Nationalism in the Former Soviet Union, September 1995, p. 4.

## 1.1 EU Policy Framework on Transitional Justice

This article argues that through better data privacy and protection mechanisms for handling sensitive personal data – like on ethnicity; it can go a long way in transitional justice. Data minimisation which is later discussed in this article and a human rights-based approach to data, are key pillars in handling sensitive personal data of a population. The EU Policy Framework on Transitional Justice provides principles that advocate for a Rights-Based Approach to transitional justice. Transitional justice support is an issue that cuts across instruments. This framework provides a basis for European Union's engagement in the area of transitional justice in its external action with the following aims:

To promote a comprehensive approach to transitional justice, with the aim of achieving peaceful, just and democratic societies based on rule of law and respect for human rights, helping to recognize and redress the harms suffered by victims of human rights and international humanitarian law violations, fighting impunity, fostering trust, contributing to reconciliation and thus preventing repetition of violations or abuses in the future.

The above quotation is relevant to this article and so adaptable, it seeks to prevent callous and illegal abuse and processing of a population's ethnicity data. The EU has robust laws on data privacy and protection from the General Data Protection Regulations (GDPR), 2018 and the Modernised Convention 108. This article acknowledges that there is minimal literature that creates a convergence between data privacy and protection and transitional justice especially in Africa where there is majority of crimes against humanity. Human rights laws are universal and general and privacy rights are not an exception. However, data protection laws in Africa are in silos and are disjointed unlike in Europe.

ID cards are public documents over which the bearer has very limited rights of privacy. From the information on the ID card a person with card-viewing authority is usually required to make some judgment about whether the card bearer is eligible or permitted to engage in a given activity. When information about group identity (such as ethnicity or religion) becomes a factor in the interaction, that information alters the card-viewer's judgment. At a minimum, the presence of group classification categories on national ID cards creates and reinforces heightened awareness of group differences.<sup>3</sup>

---

3 See note 1 at p.4.

## 2. ETHNICITY DATA ON ID IN RWANDA

It is paramount to understand the history of how the ethnicity data got into the Rwandan IDs and that is exactly what this chapter explains. In 1994, genocide in Rwanda began; an ID card with the designation “Tutsi” spelt a death sentence at any roadblock. Along with the prior training of militias, stockpiling of weapons, direction of the massacres by hate radio, the prior existence of ethnic ID cards was one of the most important factors facilitating the speed and magnitude of the 100 days of mass killing in Rwanda.<sup>4</sup>

### 2.1 The rigid Belgian ID Classification system

Prior to the rigid Belgian classification system imposed after 1926 on Rwandans through ID cards, the census and in employment and education quotas, the Hutu and Tutsi could have best been described as social caste groups and not separate ethnic groups. Hutus and Tutsis in Rwanda share a common language and religious affiliations. Physical differences sometimes exist, but not always. Inter-marriage between the groups has always occurred with some frequency.<sup>5</sup> Most writers on the 1994 genocide against the Tutsi note the introduction of group classification on ID cards by the Belgian colonial government in 1933, an action most significant because it introduced a rigid racial concept of group identity where it had not previously existed. It is important to note that the post-colonial Rwandan authorities retained the group classifications on ID cards.<sup>6</sup>

Worth noting, is that the card-bearer’s name appeared on page one, the name could not be seen together with the photograph and ethnicity, except by turning back to the first page. Below the ethnicity entry pages 2 and 3 of the card included entries for place of birth, date of birth, profession, place of issue, name of spouse, signature of the issuing official and the names and birth dates of up to 12 children. The ethnicity item on the ID card first appeared on ID cards issued by Belgian colonial authorities after 1933. The entry for ethnicity on ID cards was retained after Independence in 1962. Before April 1994, it was believed that about 85% of the population were Hutu, 14% Tutsi, and less than 1% Batwa (Twa). “Ethnicity” (“Ubwoko” in Kinyarwanda and “Ethnie”

4 Jim Fussell, *Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing*, presented on 15 November 2001 to the Seminar Series of the Yale University Genocide Studies Program, Prevent Genocide International.

5 *Ibid.*

6 *Ibid.*

in French) appeared immediately beneath the card bearer's photograph as the uppermost item on page two of the Rwandan ID card. Four possible "ethnic" categories appeared with the issuing official striking a line through all but the applicable category, for example "Ubwoko (Hutu, Tutsi, Twa, Naturalisé)". The term "Naturalisé" applied to naturalized citizens.

## 2.2 Hutu Manifesto, 1957

Prior to independence, nine Hutu leaders declared their intention to retain such classifications in the Hutu manifesto of 24 March 1957, writing: "we are opposed vigorously, at least for the moment, to the suppression in the official or private identity papers of the mentions 'muhutu', 'mututsi', 'mutwa'. Their suppression would create a risk of preventing the statistical law from establishing the reality of facts. By "statistical" the authors meant dominance by the Hutu majority population group. One of the nine authors of the 1957 Manifesto, Gregoire Kayibanda, became the first President of Rwanda in 1961 and under his leadership the Rwandan carte d'identité continued to display the "ubwoko/ethnie" group affiliation of the card bearer.<sup>7</sup>

His successor, after a 1973 coup d'état, President Juvénal Habyarimana also retained the cards until 13 November 1990. On that day, at the same time he announced a new multi-party system, President Habyarimana announced his intention, which he never acted upon, to abolish ethnic identity cards. He was later encouraged in April 1991 to follow through with this statement by United States Ambassador Robert A. Flaten, but Philip Gourevitch the French Ambassador opposed the plan. Alison De Forges reports that in July 1991 independent consultants encouraged France and other governments giving

7 The full paragraph from the Hutu Manifesto reads: "Les gens ne sont d'ailleurs pas sans s'être rendu compte de l'appui de l'administration indirecte au monopole tutsi. Aussi pour mieux surveiller ce monopole de race, nous nous opposons énergiquement, du moins pour le moment, à la suppression dans les pièces d'identité officielles ou privées des mentions "muhutu", "mututsi", "mutwa". Leur suppression risque encore davantage la sélection en le voilant et en empêchant la loi statistique de pouvoir établir la vérité des faits. Personne n'a dit d'ailleurs que c'est le nom qui ennuie le Muhutu; ce sont les privilèges d'un monopole favorisé, lequel risque de réduire la majorité de la population dans une infériorité systématique et une sous-existence imméritée" from "Manifeste des Bahutu: Note sur l'aspect social du problème racial indigène au Ruanda: 24 mars 1957" in C.M. Overdulve, Rwanda: Un peuple avec une histoire, (Paris, l'Harmattan, 1997), p. 98-111.

Loosely translated, "The people have not failed to notice the indirect support of the administration for the Tutsi monopoly. Therefore, to better monitor this racial monopoly, we strongly oppose, at least for the moment, the removal of the mentions 'muhutu', 'mututsi', 'mutwa' from official or private identity documents. Their removal would further risk obscuring selection and preventing statistical law from establishing the truth of the facts. Moreover, no one has claimed that it is the name that bothers the Muhutu; it is the privileges of a favored monopoly, which risks reducing the majority of the population to systematic inferiority and undeserved sub-existence." [Author]

aid to Rwanda to require the removal of group affiliation from ID cards as a prerequisite for assistance, but those governments failed to take that advice.<sup>8</sup>

It is imperative that sensitive personal data is defined in this article to enable the reader understand whether ethnicity data falls in that category.

### 3. DEMYSTIFYING SENSITIVE PERSONAL DATA

Under EU law, there are special categories of personal data which, by their nature, may pose a risk to the data subjects when processed and need enhanced protection. Such data are subject to a prohibition principle and there are a limited number of conditions under which such processing is lawful. Within the framework of Modernised Convention 108 and the GDPR<sup>9</sup>, the following categories are considered sensitive data:

(a) personal data revealing racial or ethnic origin; (b) personal data revealing political opinions, religious or other beliefs, including philosophical beliefs; (c) personal data revealing trade union membership; (d) genetic data and biometric data processed for the purpose of identifying a person; and (e) personal data concerning health, sexual life or sexual orientation.<sup>10</sup>

From the above definition, here-below is a case buttressing the definition of personal data, Bodil Lindqvist case:

Bodil Lindqvist<sup>11</sup> concerned the reference to different persons by name or by other means, such as their telephone number or information on their hobbies, on an internet page. The Court of Justice of the European Union (CJEU) stated that “reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health”.<sup>12</sup>

The GDPR contains several important adaptations and innovations concerning sensitive data. Most obviously, it has within article 9(1) both confirmed a closed list of “special categories of personal data” and enlarged the scope of protection adding three more special categories of personal data: “[G]enetic data,” “biometric data for the purpose of uniquely identifying a natural person,” and “data concerning a natural person’s sexual orientation.”<sup>13</sup> The use of a

8 Philip Gourevitch, *We Wish To Inform You That Tomorrow We Will Be Killed With Our Families: Stories from Rwanda*, (Farrar Straus and Giroux, New York, 1998), p. 90;

9 (Article 9).

10 (Article 6).

11 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 November 2003, para. 51.

12 Former Directive 95/46/EC, Art. 8 (1), now General Data Protection Regulation article 9(1).

13 “genetic data” was added to the list of sensitive data.

regulation has to a certain extent ended the question of which categories of data should be sensitive in nature. Member States can no longer create further categories of sensitive data, as they could under Directive 95/ 46/EC, though the GDPR now includes the most common ones that Member States had themselves added, such as genetic data.<sup>14</sup> This has, to a certain degree, reduced the problems that were created by the heterogeneous legal landscape that was permitted under Directive 95/46/EC. Whilst this exception does not cover all of the forms of sensitive data described within article 9, it does nonetheless apply to important categories that are central to many critical areas including security, healthcare, and scientific research.<sup>15</sup>

EU Data Protection Directive-95/46/EC—which employed *prima facie* a heavily context-based approach. In its general prohibition on the processing of sensitive personal data, it states: Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. This formulation appears to leave little room for the role of purpose or intent, appearing totally focused on an objective, context-based definition of what could constitute personal data.<sup>16</sup> The GDPR calls for a contextual understanding of most categories of personal data and a purposeful understanding of only a few categories of data. It states in article 9:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, bio-metric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.<sup>17</sup>

Justifications that have been put forward often relate to the need to prevent harm such as discrimination and stigmatization. There is furthermore an argument that the regulation of sensitive data with specific legal frameworks is a fundamental rights requirement, in other words linked to the right of

14 Paul Quinn and Gianclaudio Malgieri, The difficulty of defining Sensitive Data—the concept of Sensitive Data in the EU Data protection Framework; Cambridge University Press on behalf of the German Law Journal, 2021 at p. 1589.

15 *Ibid.*

16 The Article 29 working Party Opinion on Sensitive Data is notable for not even discussing this point. Given this there is little evidence to suggest that article 8 should be read in a way that differs from its literal meaning which is seemingly very context-based. See article 29 Data Protection Working Party, Advice Paper on Special Categories of Data (“sensitive data”), (European Commission, Working Paper 444105, 2011).

17 GDPR article 9.

privacy. The risk of harms in these areas is arguably greater for the processing of sensitive data. Irrespective of any basis justification, sensitive data is undergoing a transition which has intensified in recent years.<sup>18</sup>

Article 8 of the EU Charter of Fundamental Rights (the Charter) not only affirms the right to personal data protection, but also spells out the core values associated with this right. It provides that the processing of personal data must be fair, for specified purposes, and based on either the consent of the person concerned or a legitimate basis laid down by law.

### 3.1 Is Ethnicity Data Sensitive Personal Data?

GDPR under article 9 in the previous subtopic is clear that ethnic data is sensitive personal data. In *Digital Rights Ireland*,<sup>19</sup> the CJEU was called upon to decide on the validity of Directive 2006/24/EC in light of the fundamental rights to personal data protection and respect for private life, affirmed in the EU Charter of Fundamental Rights. The directive required providers of publicly available electronic communication services or public communication networks to retain citizens' telecommunication data for up to two years, to ensure that the data were available for the purposes of preventing, investigating and prosecuting serious crime. The measure only concerned metadata, location data and data necessary to identify the subscriber or user. It did not apply to the content of electronic communications. The CJEU deemed the directive an interference with the fundamental right to personal data protection "because it provides for the processing of personal data".<sup>20</sup>

In addition, it found that the directive interfered with the right to respect of private life.<sup>21</sup> When taken as a whole, the personal data retained pursuant to the directive, which could be accessed by competent authorities, could allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social

---

18 P1610-1611.

19 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and Kärntner Landesregierung and others* [GC], 8 April 2014.

20 *Ibid.*

21 *Ibid.*

environments frequented by them”.<sup>22</sup> The interference with the two rights was wide-ranging and particularly serious.

The CJEU declared Directive 2006/24/EC invalid, finding that even though it pursued a legitimate aim, the interference with the rights to personal data protection and private life was serious and not limited to what was strictly necessary.

A caselaw directly relevant on ethnicity data at the European Court of Human Rights, is *Ciubotaru v Moldova*,<sup>23</sup> where the applicant complains under article 8 ECHR (right to respect for private and family life and for correspondence) about the authorities’ refusal to register his Romanian ethnic identity in his identity papers. His application was denied.

### **3.2 Sensitive Personal Data on Ethnicity, A Tool in the 1994 Rwanda Genocide**

In spite of the Arusha Accord of 1993 requesting the Rwanda government to expunge ethnicity details from the I.D., the call was never heeded and spelt a death sentence to the Tutsis in Rwanda. In massacres northwestern Rwanda in early 1993, ethnic categories on ID cards facilitated the identification of victims. When this event occurred, negotiations were in progress for power-sharing under a Transitional Government. Among the provisions in the 4 August 1993 Arusha Accord was the following: “The Broad-Based Transitional Government shall, from the date of its assumption of office, delete from all official documents to be issued any reference to ethnic origin.”<sup>24</sup> This continued presence of group classification on ID cards, even after their role in facilitating genocidal massacres in 1993, shows that both moderates and future killers recognized in advance the important function these cards might play in ethnically targeted mass killing, such as later ensued in April 1994.

Clearly therefore, the massacres which occurred in Rwanda in 1994 had a specific objective, namely the extermination of the Tutsi, who were targeted

---

<sup>22</sup> *Ibid.*

<sup>23</sup> 27 April 2010 27138/04.

<sup>24</sup> Arusha Accord (Peace Agreement between the Government of the Republic of Rwanda and the Rwandese Patriotic Front), August 1993, Article 16: “Deletion of reference to Ethnic Group in Official Documents: The Broad-Based Transitional Government shall, from the date of its assumption of office, delete from all official documents to be issued any reference to ethnic origin. Documents in use or not yet used shall be replaced by those not bearing any reference to ethnic origin,” Arusha Accord (Peace Agreement between the Government of the Republic of Rwanda and the Rwandese Patriotic Front), 4 August 1993.

especially because of their Tutsi origin and not because they were RPF fighters. In any case, the Tutsi children and pregnant women could, naturally, not have been among the fighters.<sup>25</sup>

Paragraph 7 of the indictment alleges that the victims in each paragraph charging genocide were members of a national, ethnic, facial or religious group. The Chamber notes that the Tutsi population does not have its own language or a distinct culture from the rest of the Rwandan population. However, the Chamber finds that there are a number of objective indications of the group as a group with a distinct identity. Every Rwandan citizen was required before 1994 to carry an identity card which included a definition for ethnic group (*ubwoko* in Kinyarwanda and *ethnie* in French), the ethnic group being Hutu, Tutsi or Twa. The Rwandan Constitution and laws in force in 1994 also identified Rwandans by reference to their ethnic group. Article 16 of the Constitution of the Rwandan Republic, of 10 June 1991, reads, “All citizens are equal before the law, without any discrimination, notably, on grounds of race, colour, origin, ethnicity, clan, sex, opinion, religion or social position”. Article 57 of the Civil Code of 1988 provided that a person would be identified by “sex, ethnic group, name, residence and domicile.” The Civil Code provided that birth certificates would include “the year, month, date and place of birth, the sex, the ethnic group, the first and last name of the infant.”<sup>26</sup> The Arusha Accords of 4 August 1993 in fact provided for the suppression of the mention of ethnicity on official documents.<sup>27</sup>

Two facts, in particular, which suggest that it was indeed the Tutsi who were targeted should be highlighted: Firstly, at the roadblocks which were erected in Kigali immediately after the crash of the President’s plane on 6 April 1994 and, later on, in most of the country’s localities, members of the Tutsi population were sorted out. Indeed, at these roadblocks which were manned, depending on the situation, either by soldiers, troops of the Presidential Guard and/or militiamen, the systematic checking of identity cards indicating the ethnic group of their holders, allowed the separation of Hutu from Tutsi, with the latter being immediately apprehended and killed, sometimes on the spot. Secondly, the propaganda campaign conducted before and during the tragedy by the audiovisual media, for example, “Radio Television des Mille

25 See: International Residual Mechanism for Criminal Tribunals, The Prosecutor V Jean Paul Akayesu, Case No. ICTR-96-4-T, available at <https://ucr.irmct.org/LegalRef/CMSDocStore/Public/English/Judgement/NotIndexable/ICTR-96-04/MS44787R0000619822.PDF> para. 125.

26 Article 18.

27 See note 17 para. 170. See article 16 of the Protocol on diverse questions and final disposition.

Collines”(RTLM), or the print media, like the Kangura newspaper. These various news media overtly called for the killing of Tutsi, who were considered as the accomplices of the RPF and accused of plotting to take over the power lost during the revolution of 1959. Some articles and cartoons carried in the Kangura newspaper, entered in evidence, are unambiguous in this respect.<sup>28</sup>

### 3.3 Comparative Jurisprudence

The Nazi Germany equally abused ethnic data as a tool for genocide against the Jews. As elaborated in the abstract of a scholar. Nazi persecution of racial victim groups presupposed not only precise legal definitions and close cooperation among multiple governmental agencies, but also sophisticated technical procedures for locating those groups according to complex age, occupational, and racial criteria. This article shows how a variety of administrative tools – including two national censuses, a system of resident registration, and several special racial databases were used to locate groups eventually slated for deportation and death, as well as the possible role played in this process by Hollerith tabulation technology. Patterns in the expulsion of Jews from Germany suggest that aggregate census data may have been used to guide this process as well. The precise role played by punched-card tabulation technology remains a matter of speculation. However, it is certain that as early as 1933, Nazi officials and statisticians envisioned a future in which the racial characteristics and vital statistics of every resident would be monitored through tabulation technology in a system of comprehensive surveillance. While the “final solution” was in no sense caused by the availability of sophisticated census-taking and tabulation technologies, concrete evidence suggests that Hollerith machines rationalized the management of concentration camp labor, an important element in the Nazi program of “extermination through work.”<sup>29</sup>

The most elaborate identification system created was that of Nazi Germany, though it was not applied uniformly in all territories occupied by Germany.<sup>30</sup> Raul Hilberg describes that system and its impact upon Jews in especially great detail in his 1985 edition of “The Destruction of the European Jews”, summarised as:

28 See note 17 at para.123.

29 D. Luebke and S. Milton, “Locating the Victim: An Overview of Census-Taking, Tabulation Technology, and Persecution in Nazi Germany” in IEEE Annals of the History of Computing, vol. 16, no. 03, pp. 25-39, 1994. url: <https://doi.ieeecomputersociety.org/10.1109/MAHC.1994.298418>

30 See note 6 at p.11.

The whole identification system, with its personal documents, specially assigned names, and conspicuous tagging in public, was a powerful weapon in the hands of the police. First, the system was an auxiliary device that facilitated the enforcement of residence and movement restrictions. Second, it was an independent control measure in that it enabled the police to pick up any Jew, anywhere, anytime. Third, and perhaps most important, identification had a paralyzing effect on its victims. The system induced the Jews to be even more docile, more responsive to command than before. The wearer of the star was exposed; he thought that all eyes were fixed upon him. It was as though the whole population had become a police force, watching him and guarding his actions. No Jew, under those conditions, could resist, escape, or hide without first ridding himself of the conspicuous tag, the revealing middle name, the telltale ration card, passport, and identification papers. Yet the riddance of these burdens was dangerous, for the victim could be recognized and denounced. Few Jews took the chance. The vast majority wore the star and, wearing it, were lost.<sup>31</sup>

The role played by group classification on national identity cards in crimes of genocide against the Tutsi in Rwanda and in Nazi Germany should trouble all persons concerned with prevention of genocide. In Nazi Germany in July 1938, only a few months before Kristallnacht, the infamous “J-stamp” was introduced on ID cards and later on passports. The use of specially marked “J-stamp” ID cards by Nazi Germany preceded the yellow Star of David badges. In Norway, where yellow cloth badges were not introduced, the stamped ID card was used in the identification of more than 750 Jews deported to death camps in Poland. (1) Ethnic classification on ID Cards in Rwanda instituted by the Belgian colonial government and retained after independence, was central in shaping, defining and perpetuating ethnic identity. Once the 1994 genocide in Rwanda began, an ID card with the designation “Tutsi” spelled a death sentence at any roadblock. (2) No other factor was more significant in facilitating the speed and magnitude of the 100 days of mass killing in Rwanda.

Classification on ID cards is only one method perpetrators might use to identify a population group during genocide or ethnic cleansing. Group classifications did not appear on ID cards in the former Yugoslavia, for example. Other means of identifying a group such as creation of lists, marking buildings or mandating the display of distinguishing cloth badges can be used instead of or together with ID cards. Unlike these other means of identifying groups,

31 Raul Hilberg, *The Destruction of the European Jews*, (Holmes & Meier Publishers, New York, 1985), 173-180; Einführung der Kennkarte für Juden ab 1.1.1939 (Introduction of the identification card for Jews starting from 1.1.1939), 23. Juli 1938, Reichgesetzblatt I 1, 922; Verordnung Reisepässe von Juden vom (Regulation of passports of Jews), 5. Oktober 1938 Reichgesetzblatt I. I, 1342.

however, group classification on ID cards has been a more universally accepted or tolerated practice, perceived as a normal and legal governmental function. The world did not respond to the presence of religious categories on the Afghanistan ID booklet, but responded vocally to the announcement in May 2001 that Hindus in that country would be required to wear distinguishing yellow badges. Where a particular identity is stigmatised or vilified, it is of minimal difference that a person must carry that identity on the outer clothes, or must display it upon demand on a card.

This confirms that crimes against humanity and genocide are not isolated to Africa but are global menaces that must be tackled swiftly and effectively. Below, the author sheds light on the definition of data minimisation principle.

#### **4. DATA MINIMISATION PRINCIPLE**

The principle of data minimisation is to the effect that only such data shall be processed as are “adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed”.<sup>32</sup> The categories of data chosen for processing must be necessary in order to achieve the declared overall aim of the processing operations, and a controller should strictly limit collection of data to such information as it is directly relevant for the specific purpose pursued by the processing. This article argues that the inclusion of ethnicity data in an ID is in blatant defiance of this data minimisation principle since it is irrelevant and excessive.

Furthermore, by making use of special privacy-enhancing technology, it is sometimes possible to avoid using personal data at all, or to use measures to reduce the ability to attribute data to a data subject (for instance, through pseudonymisation), which results in a privacy-friendly solution. This is particularly appropriate in more extensive processing systems.

Article 5(1) of the Modernised Convention 108 contains a proportionality requirement for processing personal data in relation to the legitimate purpose pursued. There must be a fair balance between all interests concerned at all stages of the processing. This means that “[p]ersonal data which is adequate and relevant but would entail a disproportionate interference in the fundamental rights and freedoms at stake should be considered as excessive”.

The Organisation for Economic Cooperation and Development (OECD) on its part states that, “Personal data should be relevant to the purposes for

---

32 Modernised Convention 108, Art. 5 (4) (c); General Data Protection Regulation, Art. 5 (1) (c).

which they are used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.”

The minimisation principle requires that those processing data to consider what the minimum amount of data necessary to achieve the purpose would be. Processors should hold that and no more – it is not acceptable to collect extra data because it might be useful later on, or simply because no thought has been given to whether it is necessary in a specific scenario.

The principle of data minimisation is even more integral in the age of big data, where advancement in technology has radically improved analytical techniques for searching, aggregating, and cross-referencing large data sets in order to develop intelligence and insights. With the promise and hope that having more data will allow for accurate insights into human behaviour, there is an interest and sustained drive to accumulate vast amounts of data. There is an urgent need to challenge this narrative and ensure that only data that is necessary and relevant for a specific purpose should be processed. Data minimisation principle and handling of sensitive personal data is not alien to Rwanda and its data privacy and protection laws have robust provisions that embrace this principle as highlighted below.

#### **4.1 Rwanda laws on Processing Sensitive Personal Data**

Rwanda’s Law relating to the protection of personal data and privacy<sup>33</sup> laws provides for grounds for processing sensitive personal data.<sup>34</sup> They include data subjects’ consent, necessity for carrying out obligations of the data controller, processor or exercising specific rights of a data subject in line with the law, processing necessary for protection of vital interests of the data subject, processing necessary for public health and safety and lastly, processing necessary for archiving purposes in public interest.

Rwanda’s Law relating to the protection of personal data and privacy<sup>35</sup> provides for principles relating to processing of personal data.<sup>36</sup> It is succinct that the data controller and the data processor ensure that the data subject’s personal data: are collected for explicit, specified and legitimate purposes and

33 N° 058/2021 of 13 October 2021.

34 Article 10 from sub articles 1-5.

35 N° 058/2021 of 13 October 2021.

36 Article 37.

not further processed in a manner incompatible with those purposes.<sup>37</sup> In addition, are related to the purposes for which their processing was requested.<sup>38</sup>

The saving grace is that ethnic data has since been expunged from the IDs in Rwanda and the assurance that data protection laws were implemented and enforced starting in 2023 confirms that going forward, processing of sensitive personal data must be a legal preserve.

## **4.2 Human Rights-Based Approach to Data Processing**

EU Policy Framework on Transitional Justice provides principles that advocate for a Rights-Based Approach to transitional justice. In line with the minimisation principle highlighted above, a human rights-based approach guided by the United Nations Human Rights' Based Approach to Data principles suits handling sensitive data of a population. Considering the fact that data protection has been acknowledged as a human right both by international and constitutional law. The Office of the High Commissioner for Human Rights (OHCHR) launched a human rights-based approach to data (HRBAD) document.<sup>39</sup> The HRBAD can be defined according to OHCHR, "[...]as the use of data and statistics consistently with international human rights norms and principles". The OHCHR elected six principles as the most important ones regarding data collection, namely, Participation; data disaggregation; self-identification; transparency; privacy and accountability. This article has briefly explained what each principle entails when processing data of a population.

### **4.2.1 Participation**

Participation is central to a human rights-based approach. It is instrumental to the realisation of all components of the HRBAD, as well as retaining trust in official and other relevant data and statistics. All data collection exercises should include means for free, active and meaningful participation of relevant stakeholders, in particular the most marginalised population groups. Participation should be considered in relation to the entire data collection process: from strategic planning through identification of data needs; selecting and testing an appropriate collection methodology; data collection (for instance, hiring interviewers from particular communities to improve response rates); and to

37 Article 37 sub. Article 2.

38 Article 37 sub article 3.

39 <https://www.ohchr.org/documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf>.

data storage, dissemination, analysis and interpretation. Consider a range of processes that facilitate and encourage participation. Clearly communicate how participatory processes are conducted and the outcomes of these exchanges. Ensure that the views of vulnerable or marginalized groups, and groups who are at risk of discrimination, are represented. Maintain knowledge holdings and institutional memory in relation to information gathered through participatory processes.

#### **4.2.2 Disaggregation**

A HRBAD requires a move from traditional data collection and analysis, which concentrates on national averages and risk masking underlying disparities. A HRBAD incorporates data on the most-disadvantaged or marginalised in national/large-scale data collections. As a result, it provides data that identify and measure inequalities among population groups.<sup>40</sup> Disaggregation of data allows data users to compare population groups, and to understand the situations of specific groups. Disaggregation requires that data on relevant characteristics are collected.<sup>41</sup>

More detailed data than national averages is key in identifying and understanding inequalities. Data should be disaggregated by key characteristics identified in international human rights law. Collection of data to allow disaggregation may require alternate sampling and data collection approaches. Birth registration is foundational for robust datasets that allow accurate disaggregation.

#### **4.2.3 Self-identification**

The respect and protection of personal identity is central to human dignity and human rights. Categorisation of populations in statistics, and the detailed data collection that makes disaggregation possible, are important in identifying and addressing inequality and social issues. These processes are not norm- or value-neutral, however, and data collectors should remain cognisant of the norms

40 Application of the three perspectives of average, deprivation and inequality has been recommended and illustrated in “Human Rights Indicators: A Guide to Measurement and Implementation” (HR/PUB/12/5) available in Arabic, English, French and Spanish, pp. 127–128.

41 Office of the United Nations High Commissioner for Human Rights (OHCHR). A Human Rights-Based Approach To Data: Leaving No One Behind in the 2030 Agenda For Sustainable Development, 2018. <https://www.ohchr.org/documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf>. Last accessed on 3 January 2023 p.7.

and values that inform their decision-making in relation to personal identity characteristics.<sup>42</sup>

The overriding human rights principle do no harm should always be respected. Historically, there have been cases of misuse of data collected by National Statistical Offices (and others), with extremely detrimental human rights impacts.<sup>43</sup> When data is collected for reasonable statistical purposes, it is kept safe and used only for the benefit of the groups it describes and society as a whole.

In some cases, it may be necessary for logistical, political or other reasons to use demographic characteristics to identify a particular population. For example, if a particular ethnic minority is not recognized by the State but is understood to reside exclusively in one location. In this case, data about an individual's place of residence may be thought to denote, *ipso facto*, their ethnicity. Where data is used in this way to identify particular groups, data collectors should ensure that their handling and publishing of that data does not imply self-identification where disclosure of personal information relating to ethnic identity has not occurred. Data should be accurately described to make clear that the parameters established for a particular group have been set according to place of residence, in this example, and not the self-identification of group members.

#### 4.2.4 Transparency

The principle of transparency is closely linked with those of participation (see first section) and accountability in a HRBAD.<sup>44</sup> Also referred to as the right to information, it is a fundamental attribute of the freedom of expression. The freedom to seek, receive and impart information is specified in international human rights treaties.<sup>45</sup> The United Nations Fundamental Principles of Official Statistics state that statistics play a fundamental role in the information system of a democratic society, and beyond serving the Government and the economy, in honouring a population's entitlement to public information.<sup>46</sup> Civil Society

42 See note 27 at p.11.

43 Luebke, D. & Milton, S. 1994. 'Locating the Victim: An Overview of Census-Taking, Tabulation Technology, and Persecution in Nazi Germany'. IEEE Annals of the History of Computing, Vol. 16 (3).

44 See note 27 pp.14-15.

45 Article 19 of the International Covenant on Civil and Political Rights.

46 The Fundamental Principles of Official Statistics were endorsed by the United Nations General Assembly on 29 January 2014 (A/Res/68/261). In the context of discussions on SDG indicators, this right to public information was increasingly referred to, in particular by civil society groups, who underlined a role for official statistics that should go beyond own government's needs.

Organizations (CSOs') access to data and reports informing them of existing inequalities among population groups is essential to the realisation of the right to information, and the monitoring and realisation of human rights more generally. Such data may relate to, for instance, access to education, health, protection from violence, work, participation, social security and justice. The legal, institutional and policy frameworks under which national chief statisticians and statistical systems operate should be publicly available. This helps ensure trust in the statistical information produced.<sup>47</sup>

#### **4.2.5 Privacy**

Data disclosed to data collectors should be protected and kept private, and confidentiality of individuals' responses and personal information should be maintained.<sup>48</sup> The right to privacy is closely linked with self-identification and personal identity issues. The Human Rights Committee defined privacy as a sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone.<sup>49</sup> Data should not be published or publicly accessible in a manner that permits identification of individual data subjects, either directly or indirectly. Access to information must be balanced with the rights to privacy and data protection.

#### **4.2.6 Accountability**

Data collectors are accountable for upholding human rights in their operations, and data should be used to hold States and other actors to account on human rights issues. Accountability from a human rights perspective means that the State, or those in authority, must be held accountable to the population affected by their decisions and actions.<sup>50</sup> This relates to the obligations of the State, or those in authority, under international human rights law (duty-bearers) and the corresponding rights of the population (rights-holders) under the same standards.<sup>51</sup> Accountability is central to a human rights-based approach. In the

47 Principle 7 of the United Nations Fundamental Principles of Official Statistics.

48 See note 27 at p.16.

49 Human Rights Committee, *Coeriel and Aurik v the Netherlands* (1994), Communication No. 453/1991, para. 10.2.

50 See note 27 at p.18.

51 About accountability, see *Who will be accountable? Human Rights and the Post-2015 Development Agenda*, Joint publication from OHCHR and the Center for Economic and Social Rights, 2013.

context of the HRBAD, it refers to data collection for accountability as well as accountability in data collection.

Data Minimisation principle laced with the HRBAD approach is the best possible way to handle sensitive personal data in case, for any legal reason, such data has to be processed.

## 5. CONCLUSION

Minimising the collection and use of sensitive ethnicity data is crucial for Rwanda's transitional justice efforts. Given the country's history, strict safeguards are needed to prevent ethnic profiling, discrimination, and misuse of personal data, ensuring peace, reconciliation, and human rights protection.

A Human Rights-Based Approach (HRBA) to data processing aligns with international frameworks, such as the EU Policy on Transitional Justice, emphasising non-discrimination, transparency, and accountability. Rwanda's Law Relating to the Protection of Personal Data and Privacy reinforces these principles, mandating data minimization, purpose limitation, and proportionality to prevent misuse and uphold privacy rights.

The importance of data minimisation is highlighted by the tragic role ethnicity data played in the 1994 genocide. If such data had not been included on national IDs, systematic targeting of the Tutsi would have been significantly hindered. Therefore, ethnicity data should only be processed when strictly necessary, such as for legal purposes like genetic family tracing, and must be safeguarded through pseudonymisation or blockchain storage to prevent unauthorised access.

Privacy-enhancing technologies, including pseudonymisation and encryption, help limit data exposure while ensuring compliance with global privacy laws. However, the growing shift from traditional IDs to biometric identification raises new privacy concerns, particularly regarding unique identifiers that can link data across multiple databases, potentially leading to excessive surveillance. International legal precedents emphasize that consolidating personal information across multiple government databases threatens individual freedoms.

To balance data protection and governance, Rwanda can learn from Estonia's X-Road system, which allows data exchange while enabling citizens to monitor how their personal data is accessed. Additionally, the UN General Assembly Resolution on Privacy in the Digital Age underscores the necessity for strict safeguards in collecting and processing biometric data.

Ultimately, implementing privacy-by-design principles and human rights-centered policies will help Rwanda navigate the complexities of ethnicity data processing while ensuring justice, reconciliation, and compliance with both domestic and international legal frameworks.