*Journal of International Relations, Volume 6, Nomor 2, 2020, hal 173-180*
***Online di** http://ejournal-s1.undip.ac.id/index.php/jihi*

# European Union's Data Protection in Cyberspace for Gender Minority

**Rakha Hifzan Priwansyah**
Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro
Jalan Prof. Soedarto, SH, Tembalang, Semarang, Kotak Pos 1269
Website: http://www.fisip.undip.ac.id Email: fisip@undip.ac.id

## *ABSTRACT*

Data in the 21st century becomes one of the most valuable things an individual could ever possess, and protect. The purpose of this study is to determine the actions taken by European Union to secure gender minority sensitive data in cyberspace. In this research there will be analyses of 29 European Union member states institution responsible in collecting discrimination data towards gender minority individuals. This research uses the concept of human security, to be specific citizen personal security introduced by Costa Rican Human Development Report. Based on the using of citizen personal security concept, the results of this research show that European Union introduced data protection policy, such as General Data Protection Regulation, resulting in 8 principals which needs to be satisfied in order to consider the process and use of gender minority data lawful and safe. Each of these 8 principals have passes as the form of securitibility in protecting gender minority individuals' sensitive data in cyberspace according to the citizen personal security concept as they have reduced the probability of unlawful and misuse of sensitive data to happen.

***Keywords***: European Union, Gender Minority, Sensitive Data, Human Security, Citizen Personal Security, General Data Protection Regulation

## INTRODUCTION

The different conception of gender, sex, and sexual orientation is a problem for many to understood. While gender refers to the internal experience of individual, which might or might not related to their sex that is assigned at birth (adapted from International Commission of Jurists, 2007, p6). Gender, or gender expression, is commonly expressed through several ways, including but not limited to name, clothe, hairstyle, attitude, voice, or any other expressions. On the other hand, sex refers to the differences based on biological characteristics which can be seen from the difference of chromosome on one individual, and/or another physical attributes such as genital. Lastly, sexual orientation refers to one attraction towards certain sex or gender, both sexually and/or emotionally (The United Nations Statistics Division, 2017, pp. 1–3).

Gender minority usually be referred with the acronym LGBTI that stands for Lesbian, Gay, Bisexual, Transgender and Intersex (European Commission, 2018). In broader sense, gender minority is an umbrella term encompassing all individual that are self-identified as a non-heterosexual and other non-gender conforming individuals. In the real world, an individual whose sex, gender expression, and sexual orientation identities are fall under those consider minority, can be referred to gender minority, are more prone towards discrimination. The 2015 Eurobarometer on discrimination shows that just about 60 percent of European Union, hereinafter EU, citizens

see discrimination on the basis of sexual orientation and gender expression are widespread. Gender minority individuals still suffer from widespread discrimination, hate speech and hate crimes within the European Union.

These days, with the advancement of technology, cyberspace is already part everyone's everyday lives. This advancement does not only bring betterment towards the society, but it also come at a cost. The gender-based discrimination is also coming towards, or from, the realm of cyberspace. The information of one's individual can be looked through not only in real world but also in cyberspace. Personal data is all information that is linked to an individual, at the time when the collection of the information is gathered can identify a specific individual (European Commission, n.d.). While sensitive data is information that is related to an individual's ethnicity, political choice, religious or philosophical beliefs, health, sexual life and gender, and also genetic and biometric data (A&L Goodbody, 2016). These categorizations are beneficial in determining the limitation and additional protection that can be given toward the protection of data through regulation.

Limitation and protection are an important aspect in the protection within the cyberspace, because unlike in real world where things are tangible, those within cyberspace often be very vague. The purpose of the web and therefore the cyberspace is to extend the accessibility of individuals and information. Moreover, traveling within cyberspace makes the user at risk of tracking and tracing by national governments, business sectors, and employers. Still, several conditions of relative unavailability shield key aspects of laptop users' identities from unwanted revealing to others (Allen, 2000, p. 1186). The relative unavailability, or in other words limitation, gives an extra level of clarity on what an actor can and cannot do with one's information or data. While both personal data and sensitive data have certain level of protection, sensitive data requires an actor to give an extra protection while handling them.

Before talking about EU's data protection policy, it needs to be clarified first what are the differences between data protection and cybersecurity as both are sometimes being used intertwined with each other by the public. National Initiative for Cyber Security Careers and Studies defines cybersecurity as a strategy, policy, and standards regarding the security of an operations in cyberspace (Vishik et al., 2016, pp. 221–222). On the other hand, data protection means rules that regulate on how an individual's data can be accessed and used, including the protection of an individual's data from unintended modification, destruction or disclosure (Blume, 2015; experian, 2020). When we're talking about cybersecurity, it is also about the whole safety and resiliency of physical manifestation that makes cyber world could work properly such as the cables, computers, data centers, and etc. While the data protection is a narrower concept where it specifically talking about the safety and resiliency of an individual's data from unintended access and use. Thus, in this research, author will focus on how EU's policy in the area of data protection.

The traditional notion of security that emphasizing on the security of state is not enough in answering the problems, or security, of an individuals; as such, the concept of Human Security is introduced. Henk (2005) as cited from UNDP stated that human security is a people-centered that tries to protect an individual from chronic threats such as famine, illness, political repression, and also protection from any sudden and destructive disruption in one's live. This people-centered concept resulting in several dimensions that human security tries to cover, Shinoda (2004) citing the Report stated that the concept of human security has seven essential dimensions: economic security, food security, health security, environmental security, personal security, community security, and also political security.

Focusing on the security of gender minority's sensitive data requires this research to specifically use one dimension of human security, which is personal security. Focusing on the definition of citizens personal security brought by Costa Rican Human Development Report (HDR) as the personal, objective and subjective conditions of being free from violence or from the threat of intentional violence or dispossessions by others. In essence, it refers to effective protection of the right to life and personal integrity, as well as other inherent rights of personal privilege, such as the inviolability of the home, freedom of movement and the enjoyment of patrimony (Gasper & Gómez, 2015, p. 12; UNDP Costa Rica, 2005, p. 15).

Objective threat means the actual occurrence of acts of violence and dispossession. Dispossession means depriving an individual's property or rights, and in this era an individual's property no longer means to something that is tangible such as house, land, or car but also something that the eyes can't see such as data in cyberspace. Also, an individual's rights not only something that we (should be) able to do in real life such as to organize ourselves or our rights to freedom of speech but also to something such as our rights to knowing what our data is being used (European Union, 2012). Subjective threat means probability attributed to the occurrence of such acts according to specific individuals or group of people, here in this case is Gender Minority individuals. Lastly, the securitibility means the actions taken by state institution that should more evidently contribute in preventing threats to citizen security and protecting the population (UNDP Costa Rica, 2005).

This research will try to look at how citizen personal security concept, as one of dimension from human security, is actually beneficial in analyzing how EU's data protection is actually the securing the gender minority individuals data in cyberspace. Objective and subjective threats, and also securitibility are going to be the tool in helping answering author's research question.

## DISCUSSION

*Objective and Subjective Threat of Data in European Union*

Objective threat in the case of data in cyberspace correlates as if the data is being process lawfully according to the existence regulation or not, and if it is not is there any actions taken towards it. In the past several years there has been couple of unlawful process of data happened in EU, with two the biggest cases are the unlawful process of data relating to UK citizens at times of EU referendum, and the bigger one which is a scandal done by Cambridge Analytica and Facebook. in the case of UK citizens' data's misused when the referendum on EU was happening it can be categorized as depriving UK citizens' right on knowing what their data (property) is being used. In the Eldon Insurance case, where they shared several customers' personal data to people working for Leave.EU without the consent of the data subject it clearly breaches the concept of consent from the data subject regarding what their data is being used for (Information Commissioner’s Office, 2018, pp. 46–48). Same thing goes to when Emma's Diary unlawfully collected personal data belongs to more than 1 million people UK citizen and sold them to the UK Labour Party without disclosing that what the data is being used for. While it might be lawful, according to the regulations that the data is being used to carry out the contract between two parties between the data subject, or customers, and Emma's Diary as controller, it became unlawful when those data is being used for purposes outside those contract; such as political marketing or even sell the data to the third party (in this case UK Labour Party). Both of the case deprives the right of data subject to know what their data is being used and exploits on the unknowing data subject for the beneficial of data controller, in this case Eldon Insurance and Emma's Diary. Both cases

also unlawful as it goes against the EU DPD and UK Data Protection Act (Information Commissioner's Office, 2018, p. 60).

In the case of Cambridge Analytica, where more than 1,5 million EU citizens, including UK, German, and Italian (Information Commissioner's Office, 2018; Privacy International, 2019), it was more than collecting personal data, it goes even further to the collection of sensitive data; which under the DPD and GDPR has to have extra measures in the processing those data. The data that is unknowingly collected by Cambridge Analytica are: name, birth date, gender, email addresses, tagged photos and liked pages, posts, friends lists, and even their friends' data. It deprives the rights of data subject because they are unaware that their personal and sensitive data are being collected by the Cambridge Analytica through their Facebook accounts. They also exploited those data to draw inferences of data subjects' opinions on political issues, their voting behavior and preferences; which under the DPD and GDPR considered as sensitive data. Because the data subject did not know that their data is being collected and exploited, under the DPD and GDPR it was considered as unlawful and thus breaching the law.

Both of cases are considered an objective threat according to citizen personal security because it is: (1) it deprives an individual's right of what is their data used for; (2) it exploits and individual's data; (3) it is unlawful; but because of these acts happening not to specific individuals it is important to see the subjective threat. Subjective threat which means subjective probability of violence or dispossession not actually occurring yet but the possibility is high. In this case, the probability of unlawful and misused of gender minority data, and the impact it might have on gender minority individuals.

In the EU gender minority survey conducted by European Union Agency for Fundamental Rights (FRA) it is shown that gender minority individuals face obstacles to enjoy their fundamental rights. It is clearly shown that discrimination, violence, and harassment happen throughout their daily life, from education and employment even in public spaces. Yet, gender minority individuals rarely report any of those incidents, knowing that most of those reports might just go unnoticed by the authorities. They are also afraid that their sexual orientation identity might be exposed, because majority of them are actually not open about it (European Union Agency for Fundamental Rights, 2014). As discrimination, violence, and harassment are rampant in the life of gender minority individuals, it is surely can be considered a threat too in the case of gender minority individuals' data. Since an unlawful process of their data (which is considered sensitive) might result in more discrimination, harassment, and violence in real life. When their data is being unlawfully process, without extra measures of protection, it is also possible that those data can be accessed by the public which results in exposing their identity. If it actually happens, only resulting to more threats including, but not limited to, violence based on sexual orientation, eviction from property or public places by an argument of (different) sexual orientation, and even discrimination on the employment which might result in the gender minority individuals being fired from their job.

*Securitibility by European Union's Data Protection Policy*

In regards to the Data Protection Policy, EU had Data Protection Directive which was firstly enacted in 1995. Later on, in 2018 the new regulation namely General Data Protection Regulation effectively replaced Data Protection Directive in the matter of Data Protection Policy throughout EU Member States. Within General Data Protection Regulation (GDPR) there are further classification between data that is considered personal, and sensitive. Data that is considered sensitive requires extra layer of protection in the form of 'what is consider lawful' in the matter of gathering, preserving, processing, disclosing and transferring individual data.

Sensitive data requires more protection because of the vulnerability of information that it contains, and one of the examples of sensitive data is an information of individual sex, gender, and sexual orientation. In this chapter researcher will show how sensitive data of gender minority is actually being secured by extra layer of protections provided by Data Protection Policy, such as GDPR.

Author concludes securitibility that is done through GDPR can be simplified into several principals; these principals are important to know how can the process of gender minority data can be considered lawful. Those are: (1) principal of safeguarding measures; (2) principal of data minimization; (3) principal of public interest (scientific, historical, or statistical purposes); (4) principal of specific aimed purposes (no third party involved); (5) principal of secrecy; (6) principal of obligation to judicial institution; (7) principal in prevention of serious danger; (8) principal of explicit consent.

Principal of safeguarding measures is considered securitibility according to the concept of citizen personal security because it could prevent any objective and subjective threat to occurs. It prevents any objective threat to occur, because to be able to use personal and sensitive data of any individuals only lawful if it is to carry obligations under law/agreement, which the individual has an awareness on. It is also beneficial in preventing any subjective threat to occurs to gender minority individuals because specific measures are given to make sure that the gender minority data is protected enough, and aspects that is being protecting is including human dignity, freedoms, and citizens' right that are important to the gender minority because their freedoms in being themselves (part of LGBTI community) while their dignity and rights are also protected, so discrimination is unlawfull because it undermines gender minority individuals dignity and rights.

Principal of data minimization is considered securitibility according to citizen personal security concept where objective and subjective threat are prevented through these measures. It prevents objective threat to occur, because it is only lawful to access sensitive data if it is for several appropriate conditions including: taxation, social security, public health, reporting crimes, humanitarian, safety of products, and election campaign. It also benefits gender minority individuals as it emphasized the use of sensitive data should be as minimum as possible, and there should be technical and organizational measures to prevent any unwanted access. The access of minimum data and safeguarding measures are securitibility because of their purpose to prevent any subjective threat occurs to the gender minority sensitive data (Cormack, 2019; Intersoft Consulting, 2019).

Principal of public interest is considered securitibility because it helps prevent any future objective threat by stating that the access of sensitive data is only lawful if it is necessary for scientific, historical, and statistical purpose (which can be considered as greater good). While also preventing the same threat happening in gender minority sensitive data because the use of their data should not disregard the rights and freedom of gender minority data and even if their data is needed, appropriate safeguarding measures are obligated to be provided (European Commission, 2014).

Principal of specific aimed purposes are considered securitibility as it is aimed to prevent subjective threat to occurs to the gender minority individuals as it further specifies on what specific conditions that the use of data is acceptable (morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, and the causes of mortality) and whom can and cannot use the data of gender minority individuals. More importantly, it is also aimed to minimize the probability of misusing gender minority data by an actor that could benefits from it such as employers and companies (International Lawyers Network, 2016).

Principal of Secrecy considers as securitibility by making sure objective threat is prevented through providing conditions in which it is lawful and acceptable to use and access sensitive data such as prevention, investigation, treatment and alleviation of illness and assessing employees' fitness for work (Faculty of Occupational Medicine, 2019; The Walton Centre, 2019). Other than those conditions, health, social, and employer are prohibited to use and access sensitive data. Subjective threat is prevented as the accessing and using of gender minority sensitive data should only be done by someone with professional duty with high level of secrecy. It means that no other persons can access the sensitive data, and with this reducing the probability of the misuse of gender minority sensitive data.

Principal of obligation to judicial institution is considered securitibility as it aims to prevent objective and subjective threat to occur. The misuse of sensitive data is prevented through this principal because it is considered lawful to use gender minority sensitive data when judicial insititutions have given their approval. Judicial insitutions are usually giving approval after being assured that an actor will not use the data for their own self-benefit, and data subject rights are being protected.

Principal in prevention of serious danger is considered as securitibility according to citizen personal security concept as it aims to prevent objective and subjective threat to occur. The use of sensitive data is considered lawful only if the gender minority individuals unable to give their consent or in order to prevent serious danger or death to occur to them. Other than these circumstances, the access or use of sensitive data is unlawful.

Principal of explicit consent is considered as securitibility as its purpose it prevents the objective and subjective threat to occur. Explicit consent means that gender minority individuals know and understand to what extent that their consent applies (Vollmer, 2018). So, if the data subject sees their data as vulnerable towards misuse, they can retract their consent or not giving consent at all (i-SCOOP, 2019). This prevents both objective and subjective threat to occur towards the gender minority sensitive data.

## CONCLUSION

Analyzing from the data provided with the theoretical frameworks used, this research finds the answer for the research problem. According to the citizen personal security concept, that author uses in this research the answer to the research question is found. This research finds the means that is being done by EU in order to protect the sensitive data which through the creation of extra layer of protections and measures in order to make the processing and use of gender minority data can be consider lawful. The extra layer of protections and measures are described in EU GDPR, the latest data protection policy enacted by EU. Several principals are being analyzed by author in order to make extra layer of protections and measures easily categorized. Those are: (1) principal of safeguarding measures; (2) principal of data minimization; (3) principal of public interest (scientific, historical, or statistical purposes); (4) principal of specific aimed purposes (no third party involved); (5) principal of secrecy; (6) principal of obligation to judicial institution; (7) principal in prevention of serious danger; (8) principal of explicit consent. It is to be considered lawful then the processing of gender minority data must satisfy at least one of the principals above. The eight principals above have shown that they are, at the very least, successes in curbing the probability of unlawful and misuse of gender minority individuals' data from the lens of citizen personal security, as it successfully minimizing or preventing both objective and subjective threat that has been explained.

**REFERENCE**


A&L Goodbody. (2016). *The GDPR A Guide for Businesses*.

Allen, A. L. (2000). Gender and Privacy in Cyberspace. *Stanford Law Review*, *52*(5), 1175. https://doi.org/10.2307/1229512

Blume, P. (2015). Data Protection and Privacy – Basic Concepts in a Changing World. *Scandinavian Studies In Law*, 14.

Cormack, A. (2019, October 23). *GDPR: What's your justification?* Joint Information Systems Committee. https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-whats-your-justification

European Commission. (n.d.). *What is personal data?* [Text]. European Commission - European Commission. Retrieved March 20, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

European Commission. (2014). *Article 29 Data Protection Worker Party*.

European Commission. (2018, May 17). *JUST Newsroom—LGBTI Equality—European Commission*. https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605456

European Union. (2012). C 326. *Official Journal of the European Union*, *55*, 412. https://doi.org/10.3000/1977091X.C_2012.326.eng

European Union Agency for Fundamental Rights (Ed.). (2014). *EU LGBT survey: European Union lesbian, gay, bisexual and transgender survey ; main results*. Publ. Off. of the Europ. Union.

Experian. (2020). *What is Data Security? | Experian Business*. Experian. https://www.experian.co.uk/business/glossary/data-security/

Faculty of Occupational Medicine. (2019). *Guidance on the General Data Protection Regulation*. https://www.fom.ac.uk/media-events/news/guidance/guidance-on-the-general-data-protection-regulation

Gasper, D., & Gómez, O. A. (2015). Human Security Thinking in Practice—'Personal Security', "Citizen Security", Comprehensive Mappings. *Contemporary Politics*.

Information Commissioner's Office. (2018). *Investigation into the use of data analytics in political campaign*.

International Lawyers Network. (2016, January 16). Non-Profit Body [Text]. *European Encyclopedia of Law (BETA)*. https://lawlegal.eu/non-profit-body/

Intersoft Consulting. (2019). Recital 112—Data Transfers due to Important Reasons of Public Interest. *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/recitals/no-112/

i-SCOOP. (2019). *Explicit consent and how to obtain it—New GDPR consent guidelines*. I-SCOOP. https://www.i-scoop.eu/gdpr/explicit-consent/

Privacy International. (2019, April 30). *Cambridge Analytica, GDPR - 1 year on—A lot of words and some action*. Privacy International. http://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action

The United Nations Statistics Division. (2017). *Statistical Standard for Gender Identity*. 12.

The Walton Centre. (2019). *The Walton Centre—Lawful Basis for the Processing of your information*. https://www.thewaltoncentre.nhs.uk/498/lawful-basis-for-the-processing-of-your-information-.html

UNDP Costa Rica. (2005). *Overcoming Fear: Citizen (In)security and Human Development in Costa Rica*. National Human Development Report.

Vishik, C., Matsubara, M., & Plonk, A. (2016). *Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms*. 22.
Vollmer, N. (2018, September 5). *Recital 42 EU General Data Protection Regulation (EU-GDPR)* [Text]. http://www.privacy-regulation.eu/en/recital-42-GDPR.html