International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 14, Issue 5, 2020

Legal Protection of The Rights to Privacy of Personal Data Against Algorithmic Profiling - A Comparative Study of Privacy Protection in the EU & Indonesia: Exploring Challenges and Opportunities

Sinta Dewi Rosadi[a], Andreas Noviandika[b], Helitha Novianty Muchtar[c]
[a,c] Faculty of Law, Universitas Padjadjaran, Indonesia, [b] Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia, Email: [a]sinta@unpad.ac.id.

The digital economy has gained enormous momentum. Business models driven by data or at least supported by the automated algorithmic profiling of data have become the rule and not the exception. In its application, profiling may cause some particular risks such as: de-individualisation & stereotyping, Information asymmetries, discrimination, innacuracy & abuse. This paper examine the differences and similarities between data privacy protection regulation in the EU and Indonesia. As can be known through this paper, EU legislative initiatives are more wide-ranging and more comprehensive than Indonesia counterparts. Until today, Indonesia recently has no specific provision in terms of right of privacy to personal data regarding to the automated algorithmic profiling. The main challenges found in this paper are the challenges to design arrangements for protecting personal data related to automated algorithmic profiling in countries that have multicultural social conditions, as well as the challenges to building transparent automated algorithmic profiling systems.

Key words: legal protection, data privacy ,big data, algorithmic profiling

Introduction

Artificial intelligence (AI) has rapidly developed around the globe in recent years. Today, AI tools are used increasingly by both private and public sector organizations around the world. With artificial intelligence (AI) now used in many of the apps that drive the digital workplace stimulates increased data collection, analysis & exploitation activities. As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising the analysis of personal information to new levels of power and speed (NIST Big Data Interoperability Framework, 2015). There are different types of privacy issues in public regarding the use inovation of AI, one of them is the user profiling. The American Heritage Dictionary defines the user profiling as "The recording and analysis of a person's psychological and behavioral characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people" User profiling has some advantages as it provides the recommendations of needed product to users. The user can accurately search the required information, but user profiling has security and privacy issues because it reflects the user itself. Profiling or categorization of persons can be done through different parameters, such as, gender, age and location, but the accurate profiling need some additional information along with these attributes The amounts of data collected nowadays not only offer unprecedented opportunities to improve decision procedures for and governments, but also hold great challenges. Many pre-existing data analysis tools did not scale up to the current data sizes. In its operations, AI requires a big database sourced from various data, and even one of them is a sensitive data. The technology watchdog in Europe, Norwegian Data Protection explains: 'Most uses of Artificial Intelligence require very large volumes of data (big data) to be studied and make intelligent decisions'.

Indonesia has paid some attention to the users' rights protection all along and constituted relevant laws and regulations to protect privacy rights (Sinta Dewi Rosadi, 2018). Over the last few years, Indonesia has faced a massive development in the digital ecosystem sector and hence has led to the growth of several unicorn startups in Indonesia. According to research conducted by Tracxn Technologies in early 2020, found that there are at least 69 local startups in Indonesia that have implemented artificial intelligence into their business, the growth of this digital startup has also triggered massive consumer data collection, & enhance the use of automated algorithmic profiling. However, most of these Indonesian laws and regulations do not yet provide a comprehensive regulation of personal data and the use of automated algorithmic profiling. In sharp contrast to it, the developed countries and areas with advanced information technology, for example, the EU, have established a fairly sophisticated system of the legal protection of privacy data against automatic algorithmic profiling.

In this paper, a comparative study was made on how to protect users' right to learn the provisions of automated algorithmic profiling, comparing the relevant laws and regulations in Indonesia and the EU. more attention to these regulatory differences can help society, business, government & policymakers to get a better understanding of opportunities, prospects & challenges for established individual right to privacy related to automated algorithmic profiling.

Methods

In examining the legal protection of the Rights to Privacy of personal data against algorithmic profiling in EU and Indonesia, this research use juridical normative method. Comparison between EU & Indonesia conducted to examine more closely the privacy data protection mechanism in the use of automated algorithmic profiling in these two area. Data analysis conducted in qualitative technique by legal interpretation and synchronization of the provisions of the related law. Data gathering collected by library research to select the important part of law on the privacy data protection of Rights to Privacy of personal data in the use of algorithmic profiling. Various legal materials ranging form primary, secondary as well as tertiary legal materials are used. Such legal materials include the following legal instruments as well as other journal articles relevant to the topic.

Results and Discussion

Automated Algorithmic Profiling

Automatic algorithmic profiling is a process of construction and analyzing raw data which aims to characterize some big data with the help of algorithms or other mathematical techniques that allow the discovery of patterns or correlations in large quantities of data, aggregated in databases. This process basically aims to find correlations and relationships between the variables in the data sets(M Z van Drunen, N Helberger, M Bastian, 2019: 220–235). Automated algorithmic profiling in its use has now been applied to various business lines, in order to better understand how automated algorithmic profiling works we have demonstrated it in its use on airline ticketing and hotel booking service sites, if statistically proven that at certain timescales many people want to travel or take a vacation to certain destinations, the algorithm of artificial intelligence (AI) from airline ticketing and hotel booking service companies will charge higher prices on that specific date, in the case that automated algorithmic profiling has been designed to recognize pricing related to increased demand and supply (Pujiyono, 2020: 1-11). Simply put, profiling is automated processing of personal data to evaluate certain things about an individual. Many business service products have used this technological innovation such as targeted ads, credit scoring in loan applications, and finance applications. Profiling could form part of an automated decision-making activity, but on its own culminates in intelligence and opportunity and not computer-led decisions about an individual. The possibilities for employing algorithms increase and change every day. In the last couple of years, the move from manually specified rule-based algorithms towards complex machine learning algorithms has enabled the modeling of complex social phenomena with much greater accuracy and therefore a higher level of usability. In this digital age, people can not be separated in their daily lives to consume digital content, which has now become a valuable commodity. people are surrounded by personalized news feeds, personalized campaigns, personalized advertising and personalized interactions due to automated algorithmic profiling by Artificial Intelligence(Sophie C. Boerman, 2017). Artificial Intelligence has changed the way marketers perceive the purchase journey of users & how consumers perceive a product. AI-driven personalization is able to anticipate the next step of the users & determine the consumer journey. The thing that determines whether the user profile generated by automated profiling is accurate or not depends on how the information from the user is collected and organized. So it can be said that the output of profiling depends on the user profiling process in which the information is gathered, organized, and interpreted to create the summarization and description of users to provide a personalized experience (Sumitkumar Kanoje, 2014).

Data is the most important part or instrumental in designing better AI systems. The more data is gathered and analyzed, the more accurate the profiling output. AI requires a big volume of data to be smart enough or 'intelligent' to reach its objective, and businesses will need to collect, store, and analyze a huge amount of data for that purpose (John Bauman, 2020). The potential benefits of a big volume of Personal Data follow logically from its potential uses. From a commercial perspective, data is an extremely valuable asset and a major ‘source of value creation’ and 'data powered design'. The retail sector, in particular, has embraced Big Personal Data analysis as a means of facilitating the making of predictions as to what and when people are likely to buy. In the US, for example, Walmart uses ‘sales, pricing, and economic data, combined with demographic and weather data, to fine-tune merchandising and anticipate appropriate timing of store sales’.

Nowadays in personalizing a profile more and more is done by machines, along with the decreasing amount of human involvement. Computer machines can learn from big data to find valuable knowledge (medical records, loan applications, e-commerce transactions, and the like) and then make predictions based on that data. According to Director of Machine Learning at Amazon, Ralf Herbrich, machine learning can be interpreted as: 'machine learning is the science of algorithms that detect patterns in data to make accurate predictions for future data', so on the basis of these opinions it seems appropriate to use algorithms as machine learning for the purpose of making profiles as a result of probabilistic data processing. In this case, the profile does not always represent reality but is a version of reality that originates from the process of profiling data including talking about the algorithm and data methods used, as well as the potential biases and human prejudices reflected in the data.

Even as users’ pursue bespoke experiences, they face a harsh reality: AI only works because it feeds on their data. How much of that data are they willing to give away in order to enjoy the perks of personalization? It’s a pressing question in an age where “*identity theft*” reaches far beyond bank accounts. As AI relentlessly gathers information, it learns our political ideologies, religious affiliations, and ethnic backgrounds; it knows whom we find attractive, whether we’re white or blue-collar, and how likely we are to vote; it tracks not only our banking and health information but also our favorite route to work, how many times we’ve ordered takeout, and when and where we sleep. Gathering Information There are several types of information that can be stored in a user profile is (Custers, Bart, 2013):

a. Personal information is the most obvious type of information to gather. This includes age, gender, city, country etc. When creating an account at a web shop it is not unusual that the user is asked to fill in this type of information.
b. Interests of a user are a key part of personalization. Interests can represent hobbies-related topics, work-related topics, news topics and more. These topics can be derived from various sources, such as purchasing history or browse history.
c. Behavior is a type of information that is gathered implicitly. It is important that the behavior is repetitive in order to detect patterns. For example, 'when purchasing product X, user Y usually also buys product Z'.
d. Goals of a user are important to detect when you want to optimize the convenience for the user by showing the wanted results sooner than usual. This type of information is crucial to learn from for goal prediction.

Profiling is basically the process of building a profile, the process can be made through many indicators such as country of origin, company, or process. Personal profiles are also referred to as individual profiles or commonly known as 'customer profiles', while group profiles are also referred to as 'aggregated profiles'. A personal profile is a property or collection of properties of a particular person or individual. In computer science, a property, or a characteristic, is the same as an attribute. An example of a personal profile is as follows, Mr. Viddy (age 33), who is married, has 2 children, has an income of 35,000 Euro per year, has 3 credit cards, no criminal record, and has been hospitalized with a history of asthma. In the profiling process, group profiles can contain information that basically may already be known, for example, based on analysis, people who smoke usually have a shorter lifespan than nonsmokers. But through group profiles it can also discover new facts, for example, people who live in zip code area 56798 may have a greater chance of suffering from hypertension.

The techniques used in automated algorithmic profiling are generally divided into 3 major categories, including (John Bauman, 2020):

Structure analysis

In this tehnique, the algorithm validates that the data that you have is consistent and formatted correctly. There are several different processes that you can use for this, such as pattern matching. For example, if you have a data set of phone numbers, pattern matching helps you find the valid sets of formats within the data set. Pattern matching also helps you understand whether a field is text- or number-based along with other format-specific information;

Content discovery

In this technique, the algorithm looks to check quality data more closely into the individual elements of the database. This technique can help you find areas that contain null values or values that are ambiguous or incorrect;

Relationship discovery

In this technique, the algorithm tries to gain a better understanding of the correlation between data sets starts with metadata analysis to determine key relationships between the data and narrows down the connections between specific fields.

In its implementation, automated algorithmic profiling can be applied to specific targets of individuals & groups that are the object of profiling. This is usually done for various reasons, for example for loan applications (Real-Time-Loans), which can carry out credit assessments automatically (financial history and information from credit agencies are automatically evaluated) and provide decisions (accepted or rejected) to customer within minutes. Automated algorithmic profiling in AI can be utilized to identify, track and monitor individuals across multiple devices or platforms, whether they are at work, at home, or at a public location for many business & purposes. This means that even if your personal data is anonymized once it becomes a part of a large data set, an AI can de-anonymize this data based on inferences from other devices. This blurs the distinction between personal and non-personal data, which has to be maintained under present legislation.

Opportunity Associated with Automated Profiling

The development of big data analytics technologies, such as artificial intelligence (AI) has driven the growth of data analytics industry on a large scale. In the sense of the large amount of personal data on the internet and on "the Internet of Things" has made the ability for firms operating in nearly all sectors (banking, advertising, health, insurance, etc.) to create a profile about individuals, which profile can be used to compile computational decisions or better known as 'automatic decision'.

Automated algorithmic profiling help human to manage information overload, this technological innovation gives human a better understanding of big data in effective time & efficient way.

a. predict someone’s behaviour;
b. find something about someone’s preferences, and;
c. make decisions.

Automated profiling can be very useful for organizations, government and individuals in many sectors, including healthcare, anti-terrorism, recruiting, education, financial services and marketing. Automated profiling capabilities possessed by artificial intelligence can accelerate the speed & time to process overloaded data quickly. In the security sector or government, for example, automated profiling can help police to track the whereabouts of criminals quickly, traffic ticketing systems enforcement. automated profiling can provide benefits in terms of effectiveness and efficiency in reducing operational costs.

Risks Associated with Profiling

In addition to providing a wide benefits for humans, the existence of automated algorithmic profiling owned by artificial intelligence also has serious risks and threats related to one's privacy and presence. these risks include (Custers, Bart, 2013):

a. De-individualisation & stereotyping
The risk that someone is judged on the basis of group characteristic rather than on their own individual characteristics. This becomes very dangerous if group profiles, whether it is true or false, becomes public knowledge, people may start treating each other based on that basis. For an example, when people start believing that citizens of sub-urban cities are more criminal, people may start to react and communicate with more suspicion towards citizens sub-urban cities, regardless of the correctness of such a profile;

b. Information asymmetries
Automated algorithmic profiling data can be a benefit & valuable insights for those who use it. We encounter the problem of asymmetry when data profiling is aimed at gaining more insight or preference into individuals or groups. Information asymmetries can influence the level of playing fields and the relationship between businesses and consumers, between government and citizens, upsetting the current balance of power between different parties. information asymmetries can affect individual autonomy, In the context of the relationship between government and citizens. If data profiling indeed yields actionable knowledge, the government will have more power;

c. Discrimination
Another risk posed by automated profiling is the possibility of bias analysis that leads to discrimination, the risk of invertently discriminating against particular groups or individuals. Automated profiling algorithms may "learn" to discriminate on the basis of biased data used to train the algorithm. This can occur for instance when a data profiling exercise is focused on characteristics such as race, gender, ethnicity, religion or sexual orientation;

d. Innacuracy
In personalizing someone, automated algirithmic profiling has the possibility of inaccurate output, which is related to problems of 'false positives' and 'false negatives'. Simply put there is a possibility that the fact that someone does not fit the profile is fitted within it (a false positive), or people that fit the profile are left outside of it (false negative). This can be caused by several possibilities, including due to insufficient data. False positives and false negatives are a particular problem in automated decision making since there is no human intervention, this becomes a problem in terms of proving the side of the data subject, whether they belong to a profile;

e. Abuse
Automated algorithmic profiling also has the risk of abuse by controllers, third parties or possible abuse by hackers & fraudulent purposes. Possibilities for abuse arise in particular when the profile can be linked to an identified individual. The act of abuse can be made public leading to reputational damage for the data subject.

Defining Privacy

The concept of privacy for the first time was developed by *Warren* and *Brandeis* wrote an article in the Scientific Journal, FacultyLaw, Harvard University entitled "*The Right to Privacy* ". They stated that: "Privacy is the right to enjoy life and the right to be left alone and this development of the law was invaluable and demanded of legal recognition. " Privacy is the right to enjoy life and demand the law to protect privacy, then according to *Warren*, because there are technological developments, economics and politics new emerging rights that have not been protected by Common Law. This right is related to the spiritual needs of humans that is the need to be valued for feelings, thoughts, and the right to enjoy his life or be called the right to be let alone. So that later Warren propose to the judge to recognize privacy as a right that must be protected (Graham Greeneaf, 2014). In modern communications such as social media, e-mails, and blogging bring new perspectives to privacy, helping to define a new realm of online privacy. Collegiate Professor at New York University, Tom Gerety defines privacy as “the control over or the autonomy of the intimacies of personal identity”. The right to privacy is articulated in all of the major international and regional human rights instruments. Conceptualization of privacy in the context of online or Internet communications encompasses the notion of intrusion or interest in controlling Internet access to one’s self in order to maintain solitude. Privacy is a qualified, fundamental human right.

Understanding Forms of Privacy Violation

The difference between online privacy and traditional privacy is that most of the online privacy cases involve disclosing important personal information. Online violations of privacy typically fall into the following categories (Yanfang Wu, 2011: 603-613)

a. Collecting personal information without notification
   Websites and Android / IOS applications may track users when they are online. Their footprint in the digital world or better known as cookies can be a tool to track the behavior of users. Some popular websites that exist today have on average used cookies, such as South Morning China Post, New York Times Online & ABC News;

b. Profit by selling personal information
   Websites / Apps providers can make a profit / money benefit by selling personal data / information. It should be noted that selling personal information is more harmful than illegal collection of information;

c. Personal information redevelopment
   In certain cases sometimes some companies do a collection of such information to build databases for future use (it helps sites tailor those data to enhance the website services), but this becomes a violation if the action is carried out without permission from the data owner.

Table 1 details how both the EU and the Indonesia governments have published extensive legislation on privacy data protection regulation.

Table 1
Regulatory comparison contrasting between the EU & Indonesia.

The EU

Departement/Commision	**Legislation**
National Data Protection Authorities (DPA) European Data Protection Board (EDPB) European Data Protection Supervisor (EDPS)	a. General Data Protection Regulation (GDPR) b. Data Protection Law Enforcement Directive (EU) 2016/680 c. Regulation (EU) 2018/1725

Indonesia

Departement/Commision	**Legislation**

Ministry of Communication and Informatics Directorate General of Informatics Applications (Ditjen Aptika)	a. Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (EIT Law);
	b. Regulation of The Government Of The Republic Of Indonesia Number 71 Of 2019 Concerning Electronic System And Transaction Operation (PP PSTE);
	c. MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems;
	d. And more than 30 other sectoral regulations.

Table 2 details to better understand the specifics of the forms & measures of protection provided, here we do a comparison of the arrangements regarding the protection of personal data related to automated algorithmic profiling between regulations held by the EU and Indonesia.

Table 2
Provision comparison contrasting the EU GDPR & Indonesia regulations.

	GDPR	Indonesia
Definition of Personal Data	GDPR defines personal data as "*any information relating to an identified or identifiable natural person*". The purpose of identifiable is if certain information can be a rational marker to recognize certain individuals. For example IP addresses, cellphone numbers, or location data. GDPR also distinguishes personal data relating to evidence of crime	MoCI Regulation No. 20 of 2016 defines personal data as "*certain personal data that is stored, maintained, and protected in an accurate and confidential manner*". There is no explanation about what is meant by individual data. However, it is noted that article 58 of Law No.23 of 2006 jo. Law No.24 of 2013 concerning Population Administration (Population Law) is often a reference to the definition of individual data.
Responsible party	GDPR includes the terms '*controllers*' or '*processors*' or data managers as the party responsible for guaranteeing the protection of personal data. The controller is the party that determines the purpose and objectives of managing personal data. While the manager gives instructions about why and how the data will be used.	PP PSTE uses the term ‘*electronic system organizer’*. This includes all persons, state administrators, business entities, and the public who provide, manage, and / or operate electronic systems individually or jointly to users of electronic systems for their own needs and / or the needs of other parties. There is no party differentiation like in GDPR.

PDP Authority	The European Union has a special institution called The European Data Protection Board (EDPB) , filled with representatives of supervisory authorities from each European Union member country. European Data Protection Supervisor (EDPS) Ensures that EU institutions and bodies respect people's right to privacy when processing their personal data. And, National Data Protection Authorities (DPA) in every member states.	Until today Indonesia doesn't have any single commission that have a function and authority to oversee the protection of personal data as a whole. This is because personal data protection settings are still scattered. Each institution is related to partial & sectoral rules in supervising the protection of personal data.
Profiling & Automated Decision Making	"*profiling*" is defined as any form of automatic processing of data to evaluate certain personal aspects which aim to predict aspects related to one's profile (interest, financial condition, hobbies, location, health, etc.)	Until now, there is no single regulation in Indonesia that specifically mentions automatatic decision making & data profiling.
Sanctions for violations	The sanction provisions in the GDPR regulate fines ranging from 4% of total global income worldwide to 20 million Euros if it is proven to violate GDPR standards. Also includes compensation rights for injured parties.	The sanctions provisions in the personal data protection regulations in Indonesia currently only contain administrative sanctions. Article 36 Paragraph (1) PM 20/2016 regulates the application of administrative sanctions.

EU legislative initiatives are more comprehensive and far reaching than those of their Indonesian counterparts. In terms of managing personal data, EU GDPR has provided detailed understanding of personal data as stated in Article 4 (1), which states that 'personal data' means any information relating to an identifiable natural person (data subject '); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. But unlike in Indonesia, MoCI Regulation No. 20 of 2016 defines personal data as "certain personal data that is stored, maintained, and protected in an accurate and confidential manner". There is no explanation about what is meant by 'individual data', especially what types and classes of data in an electronic system are classified as 'individual data', but article 58 of Law No.23 of 2006 jo. Law No.24 of 2013 concerning Population Administration (Population Law) is often a reference to the definition of individual data. The protection of personal data in Indonesia was initially focused on the protection from privacy perspective. Under the Indonesian Constitution, the concept of privacy rights has been recognised and protected as part of the general concept of human rights. Need to know that most of the provisions of the EIT Law focus on the electronic transactions, there is a notable provision that deals with personal data in the EIT Law. The EIT Law recognises the protection of personal data as a part of privacy rights. The article further mentions that privacy rights shall include, among others, the right to monitor the access of information concerning private life and data. To further the effort to satisfy the need for effective protection of personal data, the Minister of Communications and Informatics (the MoCI) issued MoCI Regulation No. 20/2016 on Protection of Personal Data in Electronic Systems (MoCI Regulation 20).

In the case of the party responsible. GDPR refers to the terms '*controllers*' and '*processors*' (data managers) as those responsible for ensuring the protection of personal data. 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data, the controller is the party that determines the purposes and objectives of managing personal data. While 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. or is interpreted as the manager giving instructions about why and how the data will be used for organizational needs. Different from the arrangements that are owned in Indonesia, there are no more detailed arrangements such as those owned by EU GDPR (related to 'controllers' and 'processors' terms) regarding the parties based on their intentions and objectives. Referring to the regulation of personal data protection in Indonesia, the definition of personal data in MoCI Regulation No. 20 of 2016 define as certain personal data that is stored, maintained, and maintained in an accurate and confidential manner. In this definition, it is not explicitly stated who is assigned to save, care for, maintain the truth, and protect its confidentiality, but if referring to a number of further provisions from the Permenkominfo shows that the obligation is a burden on the 'Electronic System Provider '(Article 3 MoCI Regulation No. 20 of 2016). the definition is listed in article 1 paragraph (4), which states that: "*Electronic System Provider is any person, state administrators, business entities, and community members provide, manage and / or operate Electronic Systems individually or together with Users of Electronic Systems for his own needs and / or the needs of other parties*. "

Related to automated decision making including profiling, The GDPR includes provisions to reflect organizations' increasing use of profiling and automated decision-making across a wide range of applications. These provisions are designed to protect individuals from the potential risks that this type of processing can create. In Article 4 (1) GDPR defines profiling as: "*Any form of automated processing of personal data consists of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.* " GDPR regulates at least three ways of using profiling, including: General profiling, Decision-making based on profiling & Solely automated decision-making, including profiling. EU GDPR regulates that privacy is part of a natural person or subject in the Europe, personal data is considered as a part of personal property, and right to privacy is one of basic human rights. Most of the European countries think much of privacy protection, in particular personal data protection, thus many European countries have legislations to protect personal data.

Unlike in Indonesia, the increasing number of companies and government agencies that have begun implementing AI has not yet been matched by special arrangements for automated profiling and other AI-based innovations. MoCI Regulation 20 does not recognise a number of concepts, such as, data controller, data processor, sensitive personal data, dedicated data protection officer, privacy by design, and automatic processing. However, practitioners always refer to Article 3 of the MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems, which states that:

Protection of Personal Data in an Electronic System is carried outon process:

- *a. acquisition and collection;*
- *b. **processing and analyzing**;*
- *c. storage;*
- *d. appearance, announcement, delivery, dissemination,and / or opening access; and*
- *e. annihilation.*

In the EU, the National data protection authorities of member states, European Data Protection Board (EDPB), & European Data Protection Supervisor (EDPS) assume the main responsibilities to protect privacy data. The EDPB will be at the centre of the new data protection landscape in the EU. It will help ensure that the data protection law is applied consistently across the EU and work to ensure effective cooperation amongst DPAs, while the EDPS Ensures that EU institutions and bodies respect people's right to privacy when processing their personal data. Privacy is a central element of the EU GDPR mission. This explains why privacy is considered not only to be a human right, but also a property as well. There is no specifically dedicated national data protection authority that oversees personal data protection in Indonesia. However, pursuant to MoCI Regulation 20, the MoCI (along with the Director General of Informatics Applications or Ditjen Aptika) are responsible for ensuring compliance towards the data protection regime in Indonesia (ie, EIT Law, GR 71 and MoCI Regulation 20).

The MoCI is authorised to, among others, organise governmental events related to communications and informatics; coordinate with Electronic System Operators (ESOs) for transfer of personal data overseas; settle disputes related to failure or breach of PII protection; supervise the implementation of personal data protection; request data and information from ESOs in the framework of data protection; impose administrative sanctions for violations data protection regulations; and issue Electronic System Worthiness Certificate to certify that an electronic system is functioning properly. For certain specific matters, such as, in the event of a dispute related to the failure or breach of personal data protection, MoCI may delegate its authority to Ditjen Aptika that is authorised to form a panel to settle the disputes and recommend certain administrative sanctions to be imposed by the MoCI on relevant ESOs. Ditjen Aptika is also responsible for conducting public education on matters related to personal data protection. There remain large differences in terms of people's concerns regarding online privacy between the EU & Indonesia. In the EU personal data is considered as a part of personal property, According to Article 22 of the General Data Protection Regulation (GDPR), "*the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, when it produces legal effects concerning him or her or at least it similarly significantly affects him or her*". The fact that Article 22 is structured to restrict decisions based solely on automated processing supports the concept of individuals having control of their personal data. For example, safeguards such as the requirement for individuals to be informed, specifically meaningful information about the logic involved and the significance and envisaged consequences for the individual (Articles 13 and 14), as well as the right to obtain human intervention and the right to challenge the decision (Article 22(3)). EU data protection restricts Solely automated individual decision-making (making a decision automatically without any human involvement), and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. Automated individual decision-making and profiling can lead to quicker and more consistent decisions when used responsibly. There are significant risks to individuals if used irresponsibly, however. The General Data Protection Regulation (GDPR) includes provisions specifically designed to address these risks. Individuals have the right not to be subject to a decision when: it is based on automated processing; and it produces an adverse legal effect or a significantly affects the individual.

GDPR restricts controllers from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals (see Article 22(1) of GDPR). Controllers can only carry out solely automated decision-making with legal or similarly significant effects if the decision is:

a. necessary for entering into or performance of a contract between an organization and the individual;
b. authorized by law (for example, for the purposes of fraud or tax evasion); or based on the individual's explicit consent.

Most companies or organizations think that the use of automated algorithmic profiling in marketing does not have a significant adverse effect on individuals. They are not aware that in some cases profiling activity could lead to unfair discrimination. For example, Automated algorithmic profiling that might have a small impact on individuals in general might actually have a significant effect on certain groups of people, such as minority groups or vulnerable middle-class adults. For example, someone in financial trouble regularly displays advertisements for high-interest loans, which if they decide to take the loan then would have a severely negative impact on their personal life. According to Article 22 (1), individuals have the right not to be subject to a decision based solely on automated decision-making - including profiling - which produces legal effects concerning the individual or "affected" them. As defined in article 22 (1) and (4)) the GDPR regulation specifically requires the controller to provide the data subject with fair processing information about solely automated decision-making, including profiling that has significant or legal effects, as well as:

a. meaningful information about the logic involved (categories of data to be used, source of data and why is considered relevant);
b. the significance and consequences of such processing (controller should provide information about how profiling might affect the data subject).

While in regard to considering the Effects caused by analyzing personal data, regulations owned by Indonesia have not yet provided specific arrangements, the existing arrangements seem to only provide a general context and have not clarified the limitations in using personal data, including in considering the affects which will be caused by the use of automated algorithmic profiling. Nevertheless, certain general principles in GDPR related to the processing of personal information have been adopted by MoCI Regulation 20, among others, lawfulness, confidentiality, the purpose of limitation, accuracy and storage limitation.

In terms of the imposition of sanctions it can also be seen that EU GDPR provides stricter arrangements when compared to sanctions related to violations of personal data, there are at least 2 levels of fines based on the GDPR. The first is up to € 10 million or 2% of the company's annual global turnover of the previous financial year, whichever is higher. The second is up to € 20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher. The potential fines are substantial and a good reason for companies to ensure compliance with the Regulation. Whereas in Indonesia, Breach of data protection might be subject to administrative sanctions as a rule of thumb, under MoCI Regulation No. 20 of 2016, any person that collects, processes, analyzes, stores, promotes, announces, transmits or publishes personal data without the right to do so will be subject to certain administrative sanctions, such as verbal warning; written warning; suspension of activities; or announcement on the relevant website.

Legal Challenges

Another thing to note about the legal protection of the Rights to Privacy of personal data against algorithmic profiling is that Indonesia is a state with full of socio-cultural diversity and wealth, races, ethnics, faiths, religions, local languages, and others. Although full of cultural diversity. multiculturalism in Indonesia is an issue that cannot be avoided. However, in fact, this condition is not followed by a better social condition. Even many disorders face social life in Indonesia currently causing various conflicts and stresses. In Indonesia, the relationship between regions, ethnicities, and cultures does not always distribute evenly. Conflicts between regions, ethnicities, ethnic groups, clans, various religious believers occur in a number of stages from Indonesian history (Zarbaliyev, H, 2017). Such conditions need further attention considering that if Indonesia does not immediately regulate automated algoriyhmic profiling & decision into its regulations, it does not rule out the possibility of exacerbating social horizontal conflicts over the risk of labeling & discrimination caused by automated algorithmic profiling.

Another challenge related to privacy issues related to the use of automated algorithmic profiling in the era of artificial intelligence is the issue of 'accountability' and 'transparency'. One of the key concerns regarding automated profiling is the lack of transparency and the subsequent limits of redress from automated profiling & decision making. This is a challenge & legal duty to be transparent should carry over into the design of data mining algorithms and accompanying "transparency by design" (Black, J, 2019). The possibility of bias analysis results from artificial intelligence (AI) that have the potential to cause risks such as discrimination needs to be mitigated through the programming code itself, designing program algorithms to be "aware" of computational decisions that lead to underlying risks such as discrimination. In this approach we would need to instruct the system on which information it should (or should not) base its profiling & decisions. In the case of discrimination for instance, it is desirable to have a means to "tell" the algorithm that its predictions should be independent of sensitive attributes such as sex and ethnicity. However, one thing has become clear: as a society we need to decide whether we want to live in a world that is increasingly determined by algorithms.

Conclusion

In the current digital era, artificial intelligence, machine learning and digitization play a key role in economic development and advancement. While with such technologies, automated profiling and decision making are inevitable, it is important to recognize and ensure that their use is always aimed at the welfare and benefits of humans. In addition to providing broad opportunities, on the other hand automated profiling poses a serious threat to one's privacy, including the potential for discrimination. this research shows that legislation owned by the EU related to personal data protection is far more comprehensive and provides strict protection compared to legislation owned by Indonesia. Some challenges that need further attention through comparison between these 2 regions are: First, the need to design PDP arrangements specifically related to automated profiling in countries that have social conditions that tend to be multicultural like Indonesia. Second, transparency and the subsequent limits of redress from automated decision making. mitigated through the programming code itself, designing program algorithms to become "aware" of the underlying risks such as discrimination.

REFERENCES

Bauman, John (2020). What is data profiling and how does it make big data easier?. https://www.sas.com/ru_ru/insights/articles/data-management/what-is-data-profiling-and-how-does-it-make-big-data-easier.html

Black, J., & Murray, A. (2019). Regulating AI and Machine Learning: Setting the Regulatory Agenda. European Journal Of Law And Technology, 10(3).

Boerman, Sophie C, Sanne Kruikemeier &Frederik J. Zuiderveen Borgesius. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. Journal of Advertising, 46(3). https://doi.org/10.1080/00913367.2017.1339368.

Custers, Bart & Calders, Toon & Schermer, Bart & Zarsky, Tal. (2013). Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases. 10.1007/978-3-642-30487-3.

Greeneaf, Graham. (2014). Asian Data Privacy Laws-Trade and Human Rights Perspectives. New York: Oxford University Press.

Jaelani A.K, Handayani I.G.A.K.R, Karjoko L, "Executability of the Constitutional Court Decision Regarding Grace Period In The Formulation Of Legislation", *International Journal of Advanced Science and Technology* Vol. 28, No. 15, (2019). Page. 816-823

Jaelani A.K, Handayani I.G.A.K.R, Karjoko L, "Development of Tourism Based on Geographic Indication Towards To Welfare State", *International Journal of Advanced Science and Technology* Vol. 29, No. 3s, (2020). Page. 1227-1234

M Z van Drunen, N Helberger, M Bastian, Know your algorithm: what media organizations need to explain to their users about news personalization, International Data Privacy Law, Volume 9, Issue 4, November 2019, Pages 220–235, https://doi.org/10.1093/idpl/ipz011.

NIST Big Data Interoperability Framework: Volume 1, Definitions," September 2015. http://dx.doi.org/10.6028/NIST.SP.1500-1

Nurhayati, R., Gumbira, S.W., Tejomurti, K., "Rights of freedom of expressing community organizations in Indonesia after law number 16 of 2017 concerning community organizations", *International Journal of Advanced Science and Technology*, Volume 28(20), (2020) pp. 510-518

Pujiyono, Sugeng Riyanta. (2020). Corporate Criminal Liability in the Collapse of Bank Century in Indonesia. Humanities and Social Sciences Letters**,** 8 (1)

Sinta Dewi Rosadi. (2018). Protecting Privacy on Personal Data in Digital Economic Era : Legal Framework in Indonesia. Brawijaya Law Journal, 5(1). http://dx.doi.org/10.21776/ub.blj.2018.005.01.09.

Sumitkumar Kanoje, Sheetal Girase, & Debajyoti Mukhopadhyay. (2014). User Profiling Trends, Techniques and Applications. International Journal of Advance Foundation and Research in Computer (IJAFRC), 1(1).

Yanfang Wu, Tuenyu Lau, David J. Atkin, Carolyn A. Lin. (2011). A comparative study of online privacy regulations in the U.S. and China, Telecommunications Policy, Volume 35, Issue 7, August 2011, Pages 603-616. https://doi.org/10.1016/j.telpol.2011.05.002.

Zarbaliyev, H. (2017). Multiculturalism in Globalization Era: History and Challenge for Indonesia. International (JSS), 13(1).