UDAYANA JOURNAL OF LAW AND CULTURE

UDAYANA JOURNAL OF LAW AND CULTURE

Vol. 03, No. 1, January 2019, pp. 95-122
Available at: https://ojs.unud.ac.id/index.php/UJLC/issue/view/3028
E-ISSN 2549-0680

Data Profiling and Elections: Has Data-Driven Political Campaign Gone Too Far?

Alia Yofira Karunian[*]
Institute for Policy Research and Advocacy (ELSAM), Indonesia.

Helka Halme[**]
Faculty of Law University of Helsinki, Finland.

Ann-Marie Söderholm[***]
Faculty of Law University of Helsinki, Finland.

Article Received: 12nd December 2018; Accepted: 28th January 2019; Published: 31th January 2019

Abstract

In the age of digitalization, data-driven political campaign has rapidly shifted into sophisticated data profiling and big data analysis. In Indonesia, the privacy implications of data profiling for political purposes have not been thoroughly studied, much less regulated. This paper aims to conduct a comparative regulatory study between the European Union General Data Protection Regulation (EU GDPR) and Indonesian laws concerning personal data protection in facing the growing practice of data profiling for political purposes. In conclusion, in order to prevent unfair and non-transparent data profiling for political purposes in the upcoming 2019 general election, Indonesia should enact a comprehensive data protection law which provides data subjects with the right to information related to profiling and establishing independent supervisory authority.

Keywords: *Big Data; Data Profiling; Data Protection; Election*

How to cite (Chicago-16th): Karunian, Alia Yofira, Helka Halme, and Ann-Marie Söderholm. "Data Profiling and Elections: Has Data-Driven Political Campaign Gone Too Far?"*Udayana Journal of Law and Culture*3, no. 1, 95-122. https://doi.org/10.24843/UJLC.2019.v03.i01.p05.

doi: https://doi.org/10.24843/UJLC.2019.v03.i01.p05

[*]Email/Corresponding Author: alia@elsam.or.id
[**] Email :helka.halme@hotmail.com
[***]Email :ann-marie.soderholm@helsinki.fi

1. Introduction

1.1. Background

The way Cambridge Analytica transformed Facebook 'likes' into a lucrative business by poisoning countries' political system has been significantly increasing public discussions around the topics of data profiling and elections all around the world.[2] The British Political Consulting Firm has reportedly had a role not only in 2016 US election but also in 2013 and 2017 Kenya election. Big data has been taking old data-driven political campaign techniques to whole another level. Big data itself refers to the collection and aggregation of large quantities of data produced by and about people, things or the interactions between them.[3] Big data is characterised by 3V, *volume, velocity* and *variety*.[4] Volume means big data comprises large amounts of data. Velocity means the data streams coming at great speed, updated on a real-time basis. While variety means data come from different data sources, both internal and external data source.

Thanks to big data, the volume, variety and velocity of data used in data-driven political campaigns have been developing significantly. From the seemingly mundane data, politicians can now predict the personality traits, financial condition, and most importantly, the political belief, meaning that politicians know exactly who will be voted in the upcoming election.[5] And all of this often happens, without us, the data subjects[6], fully understand how and by whom, our personal data is being processed and analysed, as well as which decisions can be drawn from it. Big data analysis, therefore, raises a

[2] Balázs Bodó, Natali Helberger, and Claes H. de Vreese. "Political Micro-Targeting: a Manchurian Candidate or Just a Dark Horse?." *Internet Policy Review* 6, no. 4 (2017): 3. See also for example, The Guardian, "India to investigate alleged Cambridge Analytica data breach", https://www.theguardian.com/world/2018/jul/26/india-to-investigate-alleged-cambridge-analytica-data-breach-facebook; Kompas.com, "1 Juta Data Pengguna Asal Indonesia Bocor, Menkominfo Panggil Facebook", https://nasional.kompas.com/read/2018/04/05/17361101/1-juta-data-pengguna-asal-indonesia-bocor-menkominfo-panggil-facebook; The New York Times, "Cambridge Analytica Had a Role in Kenya Election, Too", https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html; Reuters, "What are the links between Cambridge Analytica and a Brexit campaign group?", https://www.reuters.com/article/us-facebook-cambridge-analytica-leave-eu/what-are-the-links-between-cambridge-analytica-and-a-brexit-campaign-group-idUSKBN1GX2IO.

[3] Primavera de Filippi, "Big Data, Big Responsibilities", *Internet Policy Review* 3, no. 1 (2014): 1.

[4] Rob Kitchin and Gavin McArdle, "What Makes Big Data, Big Data? Exploring the Ontological Characteristics of 26 Datasets", *Big Data & Society* 3, no.1 (2016): 1.

[5] David W. Nickerson and Todd Rogers, Political campaigns and big data." *Journal of Economic Perspectives* 28, no. 2 (2014):6.

[6] Article 4(1) GDPR defines data subject as an identified or 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.

series of privacy concerns to the extent that – even if users did actually consent to the processing of some of their personal data – they did not explicitly consent to the collection (or, in this case, the extrapolation) and processing of information which has been derived from it by means of big data analysis.[7]

The problem becomes more intricate because the big data analysis for political purposes is often conducted by data brokers. These data brokers typically collect consumers' public and non-public data that are available both online and offline.[8]With the help of data brokers, for years, political campaigns have been able to combine public voter files with commercial information, to develop detailed and comprehensive profile of voters[9] and further use it to craft tailored campaign messages. The role of data broker here is therefore essential. However, the business model of the data brokers is known to be very complex and opaque or lack of transparency, thereby raising privacy concerns.[10]The data brokers typically collect, manipulate, and share consumers' data without interacting directly with the data subjects, resulting in data subjects' unawareness about data brokers' roles in these practices.[11]As soon as the data subjects ask for more information, data brokers decline to answer, arguing that their data practices constitute trade secrets and must, therefore, be protected and kept secret.[12]

In Indonesia itself, personal data protection issue within election context recently has been gaining public's attention when one of Indonesian political parties, Gerindra, sent a legal warning (surat somasi) to Indonesia General Election Commission (KPU). This happened because KPU had previously denied Gerindra's request of access to KPU's voter list that contains voters' uncensored national identity card number and family card number.[13] Gerindra's action has been widely criticized by Indonesian civil society organizations, especially Indonesia Coalition of Personal Data

[7] Primavera de Filippi, *op.cit.,* 4.

[8] Federal Trade Commission. "Data Brokers: A Call for Transparency and Accountability". May 2014, 46-47.https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

[9] Jeff Chester dan Kathryn C. Montgomery, "The Role of Digital Marketing in Political Campaigns", *Internet Policy Review Journal on Internet Regulation*, Vol.6, Issue 4, (2017), 3.

[10]Federal Trade Commission, *op.cit.*,3.

[11]*Ibid.*

[12] Wolfie Christi and Sarah Spiekermann, "Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy", 121-123, http://crackedlabs.org/en/networksofcontrol;See also Wolfie Christi, "How Companies Use Personal Data Against People: Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information", 8.https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf,

[13]Farisa, Fitria Chusna. "Somasi KPU, DPD Gerindra DKI Dikritik". Kompas.com. last modified November 30, 2018 https://nasional.kompas.com/read/2018/11/30/18085861/somasi-kpu-dpd-gerindra-dki-dikritik

Protection, who stated that Gerindra has violated Law No.23 of 2006 on Population Administration that classify national identity card number and family card number as citizens' personal data that must be protected by State.[14] Another political party, Golkar, has also publicly declared that its campaign strategy for the upcoming 2019 election would be the utilization of Big Data Analysis combined with Political Micro-Targeting.[15]

1.2. Purpose

This paper addresses two main legal issues: firstly, what is the nexus between data profiling and elections, and secondly, how data subjects can control their personal data from the practice of data profiling by companies for the purpose of political campaign. This paper aims to analyse how does the existing legal framework of the European Union (EU) and Indonesian laws concerning personal data protection help to prevent the practice of unfair and non-transparent data profiling for political campaign purposes. The writers choose the EU for the comparative study because the EU General Data Protection Regulation 2016 (GDPR) is considered as the "world's toughest personal data protection law".[16]

1.3. Research Methodology and Structure

Research method applied in this paper is normative legal research, using a combination of comparative, statutory, analytical and conceptual approach. A comparative-statutory study between the European Union and Indonesia was conducted in order to further understand the existing legal framework regulating the practice of data profiling, whilst analytical and conceptual approach were conducted by analysing books, academic journal articles, organization reports, news, *etc*, concerning data protection in general, as well as data profiling and elections in particular.

Section 2.1. of this paper provides analysis regarding the concept of data profiling as well as the nexus between data profiling and elections. Furthermore, Section 2.2 provides a comparative analysis between the EU and Indonesia regulation on personal data protection, especially concerning the right of data subjects relating to data profiling for political purposes.

[14] Koalisi Perlindunngan Data Pribadi: Pemilu Demokratis Harus Menjamin Perlindungan Data Privasi Pemilih". ELSAM. https://elsam.or.id/2018/12/koalisi-perlindungan-data-pribadi-pemilu-demokratis-harus-menjamin-perlindungan-data-privasi-pemilih/

[15] Golkar Manfaatkan Big Data untuk Pemenangan Legislatif 2019. Tribunnews. last modified December 21, 2018 www.tribunnews.com/nasional/2018/12/21/golkar-manfaatkan-big-data-untuk-pemenangan-legislatif-2019

[16] Adam Satariano. G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. The New York Times. last modified March 24, 2018. https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

1.4. Theoretical Framework

1.4.1. The Right to Privacy and Data Protection

The right to privacy is a fundamental right enshrined in many constitutions around the world, as well as in international human right slaw.[17] Article 12 of the Universal Declaration of Human Rights 1948 (UDHR) proclaims that: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence...... Everyone has the right to the protection of the law against such interference or attacks.*"

The UDHR itself is generally agreed to be the foundation of international human rights law and has served as the basis for major international human rights treaties[18] which similarly enshrine the right to privacy including, International Covenant on Civil and Political Rights 1966 (ICCPR) in Article 17, European Convention of Human Rights 1950 in Article 8 and American Convention on Human Rights 1969 in Article 11.

Comprehensive personal data protection regulation is critical to help minimise state and corporate surveillance as well as data exploitation.[19] Personal data protection has long been recognized as a fundamental aspect of the right to privacy, for instance, in 1988, UN Human Rights Committee recognized the need for data protection laws to safeguard the fundamental right to privacy:[20]

> "*The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.... Every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individual or bodies control or may control their files. If such files.... Have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.*"

Furthermore, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression issued reports similarly noting that "*the protection of personal data represents a special form of respect for the right to privacy*"[21] and that the right to privacy includes "*the*

[17] Privacy International, "The Keys to Data Protection: A Guide for Policy Engagement on Data Protection", 2018, 4.https://privacyinternational.org/data-protection-guide

[18] The Foundation of International Human Rights Law. United Nations. www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html

[19] Privacy International (2018), *op.cit.,* 9.

[20] UN Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17, ¶10.

[21] UN Doc. A/HRC/17/27, ¶58 (May 16, 2011).

ability of individuals to determine who holds information about them and how […] that information is used."[22]

In December 2016, the UN General Assembly passed a resolution (by consensus) on the Right to Privacy in the Digital Age, which reaffirmed previous UNGA resolutions regarding the importance of data protection to safeguard the right to privacy.[23] As of January 2018, over 100 countries around the world have enacted comprehensive data protection legislation, and around 40 countries are in the processing of enacting such laws.[24] Indonesia has not yet enacted the personal data protection bill and is currently in the process of drafting the bill.[25]

1.4.2. Data Profiling

Data, particularly when aggregated, can reveal a lot about a person.[26] Including one's political belief. Political opinion is considered sensitive data and is subject to specific processing conditions.[27] GDPR defines profiling in Article 4 as:

> "*Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*"

Valeria Ferraris *et.al.* distinguish between group and individual profiling, as well as between direct and indirect profiling.[28] *Group profiling* identifies a group of individuals. Members of a group can either share a certain attribute (distributed profiling), or profiling can group people into a group without necessarily having the same attributes or without sharing all attributes (Non-distributive profiling).[29] While *personalised or individual profiling* aggregates information about an individual and/or uses that

[22] UN Doc. A/HRC/23/40, ¶22 (Apr. 17, 2013).

[23] UN Doc. A/RES/71/199, 3; see also UN Doc. A/HRC/34/7.

[24] Privacy International (2018), *op.cit.,* 17.

[25] Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, "Rancangan Undang-Undang tentang Perlindungan Data Pribadi", https://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html.

[26] Data Is Power: Profiling and Automated Decision-Making in GDPR.Privacy International. 2017,2. https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

[27] The General Data Protection Regulation 2016/679 of the European Union (GDPR), Art.9(1).

[28] Valeria Ferraris *et.al.*, "Defining Profiling", http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf, 8-9.

[29] Privacy International (2017), *op.cit.,* 3.

information to derive, infer, or predict unknown characteristics or future behaviour.[30]

Both individual and group profiling may be conducted directly or indirectly. *Direct profiling* occurs when the end user and the original data subject used to define the virtual person with its profile are the same.[31]While *indirect profiling* aims at applying profiles deduced from other data subjects to an end user. [32] In general, data profiling was conducted for several purposes. For instance, to infer or predict information, to score, rank, evaluate and assess people, to make or inform a decision about an individual as well as a decision that personalises an individual's environment:[33]

i. *Profiling to infer or predict information*

Through profiling, highly intimate information, including sensitive information, can be inferred, derived or predicted from personal and often non-sensitive data at varying degrees of accuracy. *E.g.* personality traits, such as the big-five personality traits (extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience), can be predicted from standard mobile phone logs, such as call logs and contact data. [34] Researchers were able to use cell phone usage history (call logs, contact data and location) to predict users' socioeconomic status.[35]

ii. *Profiling to score, rank, evaluate and assess people*

Profiling does not just result in descriptive profiles but through profiling individuals may also be measured against benchmarks of

[30] *Ibid.*

[31] David-Olivier Jaquet-Chiffelle, "Direct and indirect profiling in the light of virtual persons." in *Profiling the European Citizen: Cross-Disciplinary Perspectives* edited by Mireille Hildebrandt and Serge Gutwirth, 35-40, (Germany: Springer, 2008); Direct profiling can be used to uniquely characterise a person within a population or to infer, for example, future behaviour, needs or habits of a specific target.

[32] *Ibid.*; In indirect profiling, data is collected from a large population. Groups and categories of subjects with similar properties emerge from the collected data. Each group has its own identity defined through a small amount of information. The typical member of one group can be modelled using the concept of virtual persons. It is then sufficient to identify a subject as a member of the group, i.e., with the corresponding virtual person to be able to infer, for this subject, knowledge inherited from the group itself: probable behaviour, attributes, risks, etc.

[33] Privacy International (2017), *op.cit.,* 4-6.

[34] Yves-Alexandre de Montjoye, Jordi Quoidbach, Florent Robic, and Alex Sandy Pentland. "Predicting Personality Using Novel Mobile Phone-Based Metrics." In *International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction.* (Berlin, Heidelberg: Springer, 2013), 53.

[35] Joshua Blumenstock, Gabriel Cadamuro, and Robert On, "Predicting Poverty and Wealth from Mobile Phone Metadata," *Science* 350, no. 6264 (2015): 1073.

"predefined patterns of normal behaviour"[36] to establish whether and to what extent they deviate from such patterns. *E.g.* in 2016, IBM launched a tool that would help governments separate "real asylum seekers" from potential terrorists by assigning each refugee a score that would assess their likelihood to be an imposter.[37]

iii. *Profiling to make or inform a decision about an individual*
Profiling generates information which may in turn be used to make or significantly inform decisions about individuals. Such decisions can be taken with varying degrees of human intervention and automation. *E.g.*A hiring company assigns software to automatically scores and sorts resumes as well as ranks applicants. The hiring company only considers applicants that score above a certain threshold.[38]

iv. *Profiling to make or inform a decision that personalises an individual's environment*
Profiling is also used to automatically personalise experiences and information exposure, both online and increasingly offline. Real-time personalisation gears information towards an individual's presumed interests. *E.g.* Billboards on the Tokyo Express way—on one of Japan's busy expressways— detect and identify cars to then select and display content based on the types of cars.[39]

When an inaccurate or otherwise systematically biased profile is used to inform or feed into a decision that affects individuals, such inaccuracies may result in harm.[40] UN Human Rights Council reaffirmed this by stating that automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights.[41]

[36]Fanny Coudert, "When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies." *Computer Law & Security Review* 26, no. 4 (2010): 377-384.

[37]Patrick Tucker, Defense One, "Refugee or Terrorist? OBM Thinks Is Software Has the Answer". defenseone.com. last modified January 27, 2016.http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-hasanswer/125484/

[38] Alex Rosenblat*et.al.*, "Networked Employment Discrimination", https://datasociety.net/pubs/fow/EmploymentDiscrimination.pdf

[39]Intel, *et.al.*, "Deep Learning Enables Intelligent Billboard for Dynamic, Targeted Advertising on Tokyo Expressway", https://builders.intel.com/docs/storagebuilders/deep_learning_enables_intelligent_billboard_for_dynamic_targeted_advertising_on_tokyo_expressway.pdf

[40] Privacy International (2017), *op.cit.,* 7.

[41] UN Doc. A/HRC/34/L.7/Rev.1

2. Result and Analysis

2.1. Data Profiling and Elections: The Shift of Political Campaigns Methodology

2.1.1. Political Micro-Targeting and Political Behavioural Targeting

In order to effectively deliver their campaigns messages to respective constituents, political candidates and parties have long been identifying its 'voter market'. This practice of classifying and segmenting the 'voter market' is called Political Micro-Targeting (PMT). PMT demonstrated a partial retreat from undifferentiated mass audiences in favour of tailoring messages to the "needs, wants, expectations, beliefs, preferences, and interests" of a target audience as determined by data profiling.[42] In short, PMT's core concept is the use of data and analytics to craft and convey a tailored message to a subgroup or individual members of the electorate.[43]PMT has been widely implemented by political actors because it allows political parties to allocate their resources efficiently[44] and it supports new ways of delivering individualized messages using both old media (traditional narrowcasting methods like direct mail, door-to-door canvassing, and phone calls) and new media (targeted email, personalized phone calls, and targeted political ads via social media).[45]

Another phenomenon of data profiling and elections was introduced by, Tom Dobber, as Political Behavioural Targeting (PBT). PBT refers to the creation of voters' profile based upon voters' online behaviour and other data provided by data brokers, as well as the use of this profile to target the voters' individually with tailored political ads.[46] PBT itself originates from the commercial marketing system. The rise of big data has led campaign operatives to harness digital technologies and tools to mobilize voter turnout, engage young people, raise money, and support grassroots ground operations.[47] Electoral politics has now become fully integrated into a growing, global commercial digital media and marketing ecosystem that has already transformed how corporations' market their products and influence consumers.[48] For instance, many of the digital strategies, tools, and

[42]Ira S. Rubinstein, "Voter Privacy in the Age of Big Data", *Wis. L. Rev.* (2014): 882.

[43]Balázs Bodó, Natali Helberger, and Claes H. de Vreese, *loc.cit.*

[44] Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns*, (Portland: Broadway Books, 2012), 12.

[45] Ira S. Rubinstein, *op.cit.,* 883.

[46]Tom Dobber, Damian Trilling, Natali Helberger, and Claes H. de Vreese. "Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques." *Internet Policy Review* 6, no. 4 (2017): 2-3.

[47] Jeff Chester, *op.cit.*, 2.

[48]Election 2016: Marriage of big data, social data will determine the next president. Wired. https://www.wired.com/insights/2013/05/election-2016-marriage-of-big-data-social-data-will-determine-the-next-president/

techniques employed in the 2016 US election were initially developed, deployed, tested, and refined by the commercial sector.[49]

PMT and PBT share similarities. Both PMT and PBT use digital campaigns as one of the core strategies, because it enhances campaign effectiveness and cost efficiency.[50] Both PMT and PBT starts with data profiling to profile prospective voters then continued with the delivery of a tailored message that matches with the prospective voters' profile. Data brokers and analytics companies, social media platforms, online messenger applications, perhaps are the main actors of today's PMT and PBT. Data brokers and analytics companies took part in data profiling and analytics of the prospective voters, while the social media platforms and online messenger applications took part in delivering the tailored campaign message (A research shows that the use of WhatsApp messaging app to spread political messages has led to large increases in voter turnout among younger voters in Brazil).[51]

The increasingly central role of commercial digital marketing in contemporary political campaigns is reshaping modern-day politics in fundamental ways, altering relationships among candidates, parties, voters, and the media.[52]There are several risks associated with the practice PMT and PBT, which also mirrors concerns raised in the commercial advertising domain, *inter alia*: profiling entails a loss of user privacy, targeting opens the door for selective information exposure, potential manipulation,[53] and enables campaigns to send tailored messages directly to citizens, thereby avoiding scrutiny from journalists.[54] As a result, campaigns can potentially make opposite promises to different people, without anyone noticing.[55]

2.1.2. How Does Data Profiling Affect Elections: Lesson Learned From Cambridge Analytica

While the practice of data-driven political campaign is actually nothing new, manipulating the entire country's psychology to help a certain candidate to win the election, is obviously detrimental to the very existence of democracy. This section provides an example of cases in which PMT and PBT were implemented by Cambridge Analytica, to influence voters during US and Kenya election.

[49] Jeff Chester, *loc.cit.*.

[50] Mauricio Moura and Melissa R. Michelson, "WhatsApp in Brazil: Mobilising Voters Through Door-To-Door and Personal Messages", *Internet Policy Review* 6, no. 4 (2017):3.

[51] *Ibid.*

[52] Jeff Chester, *op.cit*, 7.

[53] Balázs Bodó, Natali Helberger, and Claes H. de Vreese, *op.cit,* 4.

[54] Tom Dobber, Damian Trilling, Natali Helberger, and Claes H. de Vreese *op.cit,* 2.

[55] *Ibid.*

2.1.2.1. The 2016 US Election

Cambridge Analytica scandal was perhaps Facebook's biggest data breach ever. The data was initially collected for academic purposes through an app called thisisyourdigitallife, developed by Aleksandr Kogan.[56] Facebook users who took personality tests on the app were paid and agreed to have their data (and their friends' data, too) collected by Kogan.[57] Cambridge Analytica then entered into an agreement with Kogan and used the 50 million Facebook data to create personality profiles for voters and used it to target individuals with specifically tailored content.[58]

One example of manipulation caused by Cambridge Analytica during the US 2016 presidential elections was to identify specific Hillary's voters and target them with psychographic messaging designed to discourage them from voting.[59]Unlike the EU GDPR, the US does not have a dedicated data protection law, but instead regulates primarily by industry, on a sector-by-sector basis.[60]

2.1.2.2. The 2013 and 2017 Kenya Election

Kenya has a long history of ethnically divided politics and election-related violence. The weeks of bloodletting took place in 2007, where it is estimated 1,200 people were killed and 600,000 fled their homes during the inter-ethnic violence after a disputed election.[61] For this reason, Kenyans prepare for elections in the same way other prepare for war or natural disasters.[62] As the memories of the 2007 elections linger, tensions have

[56] Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. last modified March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[57] *Ibid.*

[58] Sean Llling. Cambridge Analytica, the shady data firm that might be a key Trump-Russia link, explained. Vox. last modified April 4, 2018 https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-facebook-alexander-nix-christopher-wylie

[59] Jeff Chester, *op.cit.*, 8; see also Green, Joshua and Sasha Issenberg. Inside the Trump bunker - meet the people powering his campaign. The Irish Examiner. last modified November 5, 2016. https://www.irishexaminer.com/viewpoints/analysis/inside-the-trump-bunker--meet-the-people-powering-his-campaign-429091.html

[60] Rosemary P Jay, *Data Protection & Privacy*, 2015, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/04/DDP2015_United_States.pdf, 208.

[61] Kenya president's election campaign used firm hired by Trump: privacy group. Reuters. last modified December 15, 2017. https://www.reuters.com/article/us-kenya-politics/kenya-presidents-election-campaign-used-firm-hired-by-trump-privacy-group-idUSKBN1E82QS

[62] Amid fears of election violence, Kenyans seek a way past inter-ethnic conflict. The Guardian. last modified August 4, 2017. https://www.theguardian.com/commentisfree/2017/aug/04/fear-election-violence-kenya-ethnic-divisions-hope-new-generation

risen in western Kenya and parts of Nairobi amid confusion and discrepancies surrounding the country's repeated presidential election on October 2017, with deadly violence breaking out in some areas.[63]

Kenya National Commission on Human Rights (KNCHR) published a statement reporting that 24 people were killed during the election period, between August 8 and August 12, 2017.[64] Human Rights Watch further reported that over 100 people were injured later that month.[65] Furthermore, the KNCHR recorded 25 deaths from 1 - 25 October 2017, with the second election taking place on October 26.[66]

On March 2018, the Kenyan daily, The Star, reported that Cambridge Analytica confirmed its involvement in not only in 2017, but also in 2013 Kenyan presidential elections.[67] Later it was disclosed that Cambridge Analytica's strategy for Mr. Kenyatta, was "divisive propaganda," raising ethnic enmity.[68] The 2017 presidential candidates were, Uhuru Kenyatta, a Kikuyu, the largest ethnic group, while Raila Odinga, a Luo, a major community whose members chafe at years of exclusion, primarily at the hands of Kikuyu elites.[69]

It is reported that during the campaign season, Kenyan citizens received targeted text messages which led to the speculation that individuals' voter registration information, social media data and telephone numbers were being independently linked.[70] It also manipulated voters with

[63]Jina Moore, Violence Flares and Tensions Rise After Kenya Presidential Vote. The New York Times. last modified October 28, 2017 https://www.nytimes.com/2017/10/28/world/africa/kenya-election-uhuru-kenyatta-raila-odinga.html.

[64] Justina Crabtee. "Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections". CNBC.com. last modified march 23, 2018.https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html

[65]Nairobi. "Kenya: Post-Election Killings, Abuse". Human Right Watch. last modified August 27, 2017, https://www.hrw.org/news/2017/08/27/kenya-post-election-killings-abuse.

[66] CNBC, *loc.cit.*

[67]Cambridge Analytica confirms involvement in Kenyan elections. The Star. last modified March 20, 2018 "https://www.the-star.co.ke/news/2018/03/20/cambridge-analytica-confirms-involvement-in-kenyan-elections_c1732986.

[68]Moore, Jina. Cambridge Analytica Had a Role in Kenya Election, Too. The New York Times. last modified March 20, 2018. https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html

[69] Amid fears of election violence, Kenyans seek a way past inter-ethnic conflict. The Guardian. last modified August 4, 2017. https://www.theguardian.com/commentisfree/2017/aug/04/fear-election-violence-kenya-ethnic-divisions-hope-new-generation

[70]Moore, Jina. Cambridge Analytica Had a Role in Kenya Election, Too. The New York Times. last modified March 20, 2018. https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html

disinformation, apocalyptic attack ads and smeared Kenyatta's opponent Raila Odinga as a violent, corrupt and dangerous political figure.[71] The absence of a comprehensive data protection law safeguarding how data should be collected, processed, stored and retained, has also contributed to making the situation even worse. An improvement on personal data protection in Kenya took place in 2015 when data protection bill was tabled in Parliament, however, the bill has not yet passed until today.[72]

2.2. Data Protection Law as a Toolkit to Control Data Profiling: A Comparative Study betweenthe European Union andIndonesia

2.2.1.The European Union

Data protection has been acknowledged as a distinct fundamental right under EU law. It is affirmed, for instance, in Article 16 of the Treaty of the Functioning of the EU as well as Article 8 of the EU Charter of Fundamental Rights. Furthermore, the adoption of the EU GDPR in April 2016 marked a major development on personal data protection in Europe. As EU regulation, the EU GDPR became directly applicable law in all EU's Member States and didn't require implementation by the Member States. However, some national legislation has been enacted in the Member States to complete privacy protection legislation on a national level.

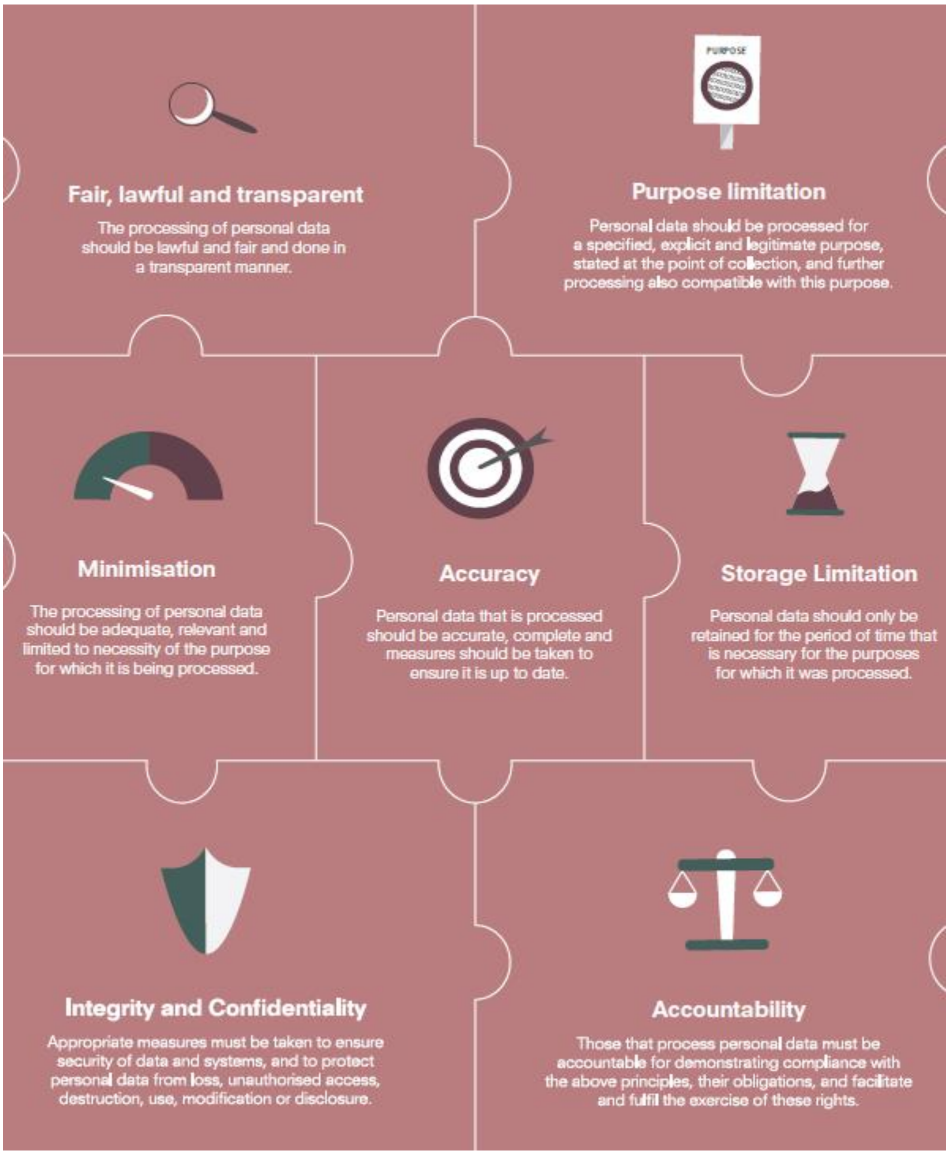
The GDPR that entered into force on 25 May 2018, is comprehensive, covering almost all personal data processing. It is also significant, as its implementation will affect not only data controllers based within the EU, but also those that offer goods or services to or monitor the behaviour of, EU citizens.[73] Or in other words, GDPR has extraterritorial effect. Privacy International, a UK-based organization which aims to "fight for the right to privacy across the world", outlines seven key principles of data protection that can be found in GDPR:

[71] Larry Madowo. How Cambridge Analytica poisoned Kenya's democracy. The Washington Post. last modified March 20, 2018 https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/?noredirect=on&utm_term=.4cf283c6a0ed

[72] State of Privacy Indonesia. Privacy International. January 2018, https://privacyinternational.org/state-privacy/1003/state-privacy-indonesia

[73] Privacy International (2018),*op.cit.,* 17.

Illustration 1
Data Protection Principles



Fair, lawful and transparent
The processing of personal data should be lawful and fair and done in a transparent manner.

Purpose limitation
Personal data should be processed for a specified, explicit and legitimate purpose, stated at the point of collection, and further processing also compatible with this purpose.

Minimisation
The processing of personal data should be adequate, relevant and limited to necessity of the purpose for which it is being processed.

Accuracy
Personal data that is processed should be accurate, complete and measures should be taken to ensure it is up to date.

Storage Limitation
Personal data should only be retained for the period of time that is necessary for the purposes for which it was processed.

Integrity and Confidentiality
Appropriate measures must be taken to ensure security of data and systems, and to protect personal data from loss, unauthorised access, destruction, use, modification or disclosure.

Accountability
Those that process personal data must be accountable for demonstrating compliance with the above principles, their obligations, and facilitate and fulfil the exercise of these rights.

(Source: Privacy International, The Keys to Data Protection, 2018)

The existence of these principles automatically gives rise to several rights of the data subject. At minimum, the rights of data subject should include the following rights:[74]

A. Right to information

EU data protection laws require personal data processing to be done in a fair and transparent manner. All individuals must be informed about the purpose of processing their data and the risks involved.[75] All information must be provided in advance

[74] Privacy International, *op.cit,* 51.

[75] GDPR, Art.12,13,14.

and in clear and plain language to allow all individuals to easily understand the rules, risks, safeguards and rights involved.

B. Right to access

GDPR also provides the data subject with the right to access their data that has been processed.

C. Rights to rectify, block and erasure

Everyone also has the right to have their data rectified or removed if the data is inaccurate or erased if their data is being processed illegally. Every person has the right to temporarily restrict processing if it's not done in the right way. The accuracy of personal data is essential to ensure a high level of data protection for the individuals[76].

D. Right to object

Article 21 (1) of the GDPR empowers everyone to raise objections on grounds relating to their personal situation. Article 21 (2) of the GDPR provides a specific right to object to the use of personal data for the purposes of direct marketing.

E. Right to data portability

Individuals should have the right to obtain all of their personal data from a data controller in a universally machine-readable format or for that data to be ported to another service should they request it.

F. Rights related to profiling and automated-decision making

Everyone has the right not to be subjected to decisions based solely on automated processing, including profiling, that have legal effects or that significantly affect him or her[77]. Automated decisions are decisions taken using personal data processed solely by automatic means without any human intervention. If such decisions are likely to have a significant impact on the lives of individuals as they relate, for example, to credit worthiness, e-recruitment, performance at work, or the analysis of conduct or reliability, then special protection is necessary to avoid negative consequences.

[76] GDPR, Art. 15(1)(c), 15(1)(f),16,17(2), 21, Recital 65.

[77] GDPR, Recital 71, Art.4(4),22

G. Right to an effective remedy
Individuals should have the right to an effective judicial remedy where they consider that their personal data was not processed in compliance with the law

H. Right to compensation and liability
Data subject whose rights have been found to be violated has a right to compensation for the damage - material or non-material – suffered.

Now, how does GDPR, as data protection law, help to prevent opaque data profiling practice by data brokers? One of the GDPR principles that are relevant to the practice of profiling is the **fair, lawful and transparent principle**. This principle is related to the **right to information and access**, as these rights are essential to ensure fair and transparent processing of data. Right to information of profiling is enshrined in Article 13(2)(f) and Article 14(2)(g) GDPR, while Article 15(1)(h) GDPR provides the data subject with the right to access or obtain such information relating to profiling. All three articles regulate that data controller is obliged to provide meaningful information about the logic involved in profiling, as well as the significance and the envisaged consequences of such processing for the data subject.[78]

Providing such information related to profiling would prevent data profiling actors to use and process data subjects' personal data in unimaginable ways, help data subjects to understand more on how their data is used to create a profile, and what are the risks and consequences of the existence of such profiles. It is highly important to notify such risks and consequences of profiling because profiling itself has the potential to lead to the exclusion or discrimination of individuals.[79] A 2015 study by Carnegie Mellon University researchers found that Google's online advertising system showed an ad for high-income jobs to men much more often than it showed the ad to women.[80] Considering its inevitable risk to the enjoyment of human rights, transparency of profiling is therefore, paramount to the data subjects.

Aside from providing the data subject with the right to information related to profiling, adequate supervision mechanism is one way to control the way companies are using data. Supervisory authorities can, if necessary, for example, reprimand or even fine the company, who is breaking the personal data protection regulation. EU's Member State's national

[78] GDPR, Art.13(2)(f), 14(2)(g), 15(1)(h).

[79] Privacy International (2018),*op.cit.*, 57.

[80]A. Datta and M. C. Tschantz, "Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice and Discrimination", https://arxiv.org/pdf/1408.6491.pdf, 21.

authorities have issued several fines under the GDPR. For instance, France data protection authority or known as (CNIL) *La Commission nationale de l'informatique et des libertés* fined Google with €50 million (almost US$57 million) on January 2019. According to CNIL, Google's data consent policies are not easily accessible and transparent, and therefore against the EUGDPR.[81]

2.2.2. Indonesia

The 1945 Constitution of the Republic of Indonesia does not specifically mention the right to privacy, however, Article 28G protects the right to dignity and "to feel secure", concepts that are often related to the right to privacy in national constitutions.[82] Moreover, Indonesia has also ratified ICCPR,[83] which *ipso facto* means that Indonesia guarantees the right to privacy enshrined in Article 17 ICCPR. While the EU has GDPR which serves as the umbrella law that provides personal data protection, Indonesia currently has no comprehensive personal data protection law yet. However,on November 2018, Indonesian Government announced that Personal Data Protection Bill has officially been included in the list of the Priority Bill in the 2019 National Legislation Program and the final draft is expected to be finalized before the end of the year.[84] Although no specific personal data protection law has been passed, guarantees of several aspects of personal data protection (for instance, information about the purpose of data processing, data retention duration, the disclosure of personal data to a third party, etc.) have been incorporated in several sectoral laws in Indonesia.[85] Example of several sectoral laws that mention personal data protection in Indonesia are, *inter alia*:[86]

1. Law No. 1 Year 1946 concerning the Criminal Code (KUHP);
2. Law No. 8 Year 1981 concerning the Criminal Procedure Code (KUHAP);
3. Law No. 8 Year 1997 concerning Corporate Documents (Corporate Documents Law);
4. Law No. 10 Year 1998 concerning Banking (Banking Law);

[81] The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. CNIL. Last modified january 21, 2018.https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[82] State of Privacy Indonesia. Privacy International. January 2018, https://privacyinternational.org/state-privacy/1003/state-privacy-indonesia.

[83] Act No. 12 Year of 2005 concerning the Ratification of International Covenant on Civil and Political Rights of Indonesia.

[84] UU Data Pribadi Masuk Prioritas 2019". Kominfo. https://kominfo.go.id/content/detail/15264/uu-data-pribadi-masuk-prioritas-2019/0/sorotan_media

[85] ELSAM's research found that there are at least 30 regulations which are related with the protection of personal data in Indonesia; see Wahyudi Djafar, *et.al.,* Protection of Personal Data in Indonesia (ELSAM: 2016): 28-49.

[86] *Ibid.,* 29.

5. Law No. 8 Year 1999 concerning Consumer Protection (Consumer Protection Law);
6. Law No. 23 Year 1999 concerning Bank of Indonesia (Bank of Indonesia Law);
7. Law No. 31 Year 1999 concerning the Eradication of the Crime of Corruption (Anti-Corruption Law);
8. Law No. 36 Year 1999 concerning Telecommunications (Telecommunications Law);
9. Law No. 39 Year 1999 concerning Human Rights (Human Rights Law);
10. Law No. 30 Year 2002 concerning the Commission for the Eradication of Corruption (Anti-Corruption Commission Law);
11. Law No. 15 Year 2003 concerning Stipulation of GR in Lieu of Law No. 1 of 2002 concerning the Eradication of the Crime of Terrorism (Anti-Terror Law);
12. Law No. 18 Year 2003 concerning Legal Advocates (Advocate Law);
13. Law No. 29 Year 2004 concerning the Medical Practice (Medical Practice Law);
14. Law No. 23 Year 2006 concerning Population Administration (Population Administration Law);
15. Law No. 21 Year 2007 concerning the Eradication of the Crime of Human Trafficking (Anti-HumanTrafficking Law);
16. Law No. 11 Year 2008 concerning Electronic Information and Transaction (EIT Law);
17. Law No. 14 Year 2008 concerning Freedom of Information (FOI Law);
18. Law No. 21 Year 2008 concerning Islamic Banking (Islamic Banking Law);
19. Law No. 35 Year 2009 concerning Narcotics (Narcotics Law);
20. Law No. 36 Year 2009 concerning Health (Health Law);
21. Law No. 43 Year 2009 concerning Archiving (Archival Law);
22. Law No. 44 Year 2009 concerning Hospitals (Hospital Law);
23. Law No. 8 Year 2010 concerning the Prevention and Eradication of the Crime of Money Laundering (Anti-Money Laundering Law);
24. Law No. 17 Year 2011 concerning State Intelligence (State Intelligence Law);
25. Law No. 18 Year 2011 concerning the Amendment of Law No. 22 of 2004 concerning the Judicial Commission (Judicial Commission Law);
26. Law No. 21 Year 2011 concerning the Financial Services Authority (Financial Services Authority Law);

27. Law No. 9 Year 2013 concerning the Prevention and Eradication of the Crime of Terrorism Funding (Financing of Terrorism Law);
28. Law No. 7 Year 2014 concerning Commerce (Commerce Law);
29. Law No. 18 Year 2014 concerning Mental Health (Mental Health Law); and
30. Law No. 36 Year 2014 concerning Medical Personnel (Medical Personnel Law).

As can be seen above, various regulations which mention about personal data come from several different sectors, ranging from human rights, media and telecommunications, defence and security, judiciary, health, population administration, commerce and industry, as well as commerce.Comparison of provisions on personal data protection in all 30 sectoral regulations will be further elaborated in a table below:

Table 1
Comparison of Provisions on Personal Data
in Various Legislations in Indonesia

LEGISLATION	RECOGNITION OF PERSONAL DATA	LIMITATIONS	MECHANISMS OF PROTECTION
I. Human Rights			
Criminal Code	Articles 430-434	-	Articles 430-434
Human Rights Law	Article 29(1)	Article 32	Articles 76(1) and 89(3)
Anti-Human Trafficking Law	Article 33	Articles 29, 32	Article 31
II. Media and Telecommunication			
Telecommunication Law	Articles 40-42(1)	Articles 42(2), 43	Articles 56-59
Electronic Information and Transaction Law	Articles 26(1), 31(1)-(2) dan 43(2)	Articles 31(3), 43(3)	Articles 26(2), 38, 47
Freedom of Information Law	Articles 6(3)(c), 17(g)-(h), 19	Article 18(2)	Articles 23, 26(1), 54
III. Defence and Security			
Anti-Terrorism Law	-	Articles 30-31	-
State Intelligence Law	-	Articles 31-34	Articles 15(1), 47
Financing of Terrorism Law	Article 9(1)	Article 9(3)	Article 9(2)
IV. Judiciary			
Criminal Procedural Code	Articles 48(2)-(3)	Article 47	Article 47(1)

Anti-Corruption Law	-	Articles 26, 29, 30	Article 31
Anti-Corruption Commission Law	-	Articles 12(a), (c), (f)	Article 47(1)
Advocate Law	Articles 19(1)-(2)	Article 19(1)	-
Judicial Committee Law	Article 20A (1) (c)	Articles 20 (3)-(4)	Article 20A(2)
V. Archiving and Population Administration			
Population Administration Law	Articles 1 (22), 2 (c) and 84-86	Article 87	Articles 2(f), 95, 98(2)
Archival Law	Articles 5, 6 (5), 7 (g), 9, 34-35, 40, 44, 49 (b), 51-52, 66 (2), (5)- (6)	Articles 66 (1), (3) (i), (7)	Articles 80 85-86
VI. Health			
Medical Practice Law	Articles 46, 47, 48 (1) 51 (c) and 52 (e)	Article 48 (2)	Articles 64, 66-70, 79 and Chapter IX
Narcotics Law	-	Articles 75(i), 77-78, 80	-
Health Law	Articles 8, 57 (1) and 189 (2) (c)	Article 57 (2)	Articles 58 (1) and 182-188
Hospital Law	Articles 29 (1) (h), (l), (m), 32 (i), 38 (1) and 44	Article 38 (2)	Articles 54-55
Mental Health Law	Articles 68(d), 70(1)(e)	Articles 71-72, 74	-
Medical Personnel Law	Articles 58 (1) (c) and 70-73 (1)	Article 73 (2)	Article 82 (1)
VII. Finances and Banking			
Banking Law	Articles 1 (28), 40 (1)	Articles 40-44A	Articles 29 (1), 47 and 47A
Central Bank Law	-	-	Articles 24, 27, 34, 35
Islamic Banking Law	Article 41	Articles 42-49	Articles 42(2), 50, 57, 60, 61
Anti-Money Laundering Law	Articles 11 (1), 40 (b), 42, 54 (2) and 83 (1)	Articles 11 (1), (3), 28, 41 (1) (a), (2), 44 (1) (h), 45, 72	Articles 11 (2), 72 (5) and 83 (2)
Financial Service Authority Law	Article 33 (1)-(3)	Article 33 (1)-(3)	Articles 5, 6 (a), 7, 33 (4) and 52

VIII. Commerce and Industry			
Corporate Documents Law	Articles 4, 11(3)-(4)	Articles 11(5), 18, 19(2), 21	-
Consumer Protection Law	-	-	-
Trade Law	Article 65(3)	-	Articles 65(5)-(6)

(Source: Wahyudi Djafar, *et.al.*, Personal Data Protection in Indonesia)

Several regulations acknowledged that the right to privacy can be restricted by the interests of law enforcement by certain agencies and for the acceptance of certain positions.[87] Moreover, the authority to oversee the implementation of data management without specifying the protection mechanisms is also present in several regulations.[88]In circumstances where privacy right of the data subject is violated, several regulations providedifferent sanctions ranging from criminal to administrative sanctions.[89]

Aside of the 30 regulations above, Indonesian government on 2012, issued the Government Regulation No. 82 of 2012 on Electronic System and Transaction Operation, that mentions about personal data protection on 'Electronic System'.[90] Moreover, in 2016, the Minister of Communication and Informatics issued Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems. However, unlike the EU GDPR which specifically provides the data subjects the right to information relating to profiling and establishes independent supervisory authority mechanism, all Indonesia'ssectoral regulations that mentions personal data protection that have been mentioned above, do not provide the data subjects with the right to information relating to data profiling and establish any independent supervisory mechanism.With no right to information relating to data

[87] For instance, the Criminal Code gives authorisation to the police to access personal letter relating to a crime, or the Health Law excludes the principle of confidentiality of patient health records only for the interests of law enforcement and when the patient is applying for a certain position or profession; see Wahyudi Djafar, *op.cit.*, 50.

[88]Only several regulations govern in detail the mechanism of protection of personal data in varied ways. For instance, in the Criminal Procedural Code and EIT Law, the police authority must be based on the decision of the Chair of the District Court. While the Anti Money Laundering Law and the Anti-Corruption Commission Law, the authority of PPATK and KPK to access personal data are not subject to permission from the Chair of the District Court, but simply based on adequate evidence and the permission of the head of these institutions internally; see *Ibid.*

[89]For example in the Telecommunications Law and the Terrorism Financing Law, leakage of data protection is threatened with imprisonment. While, the National Intelligence Law and the KPK Law, abuses of authority through wiretapping, resulting in the intervention of privacy rights of citizens, can be punished and fined; see *Ibid.*

[90]Article 1(1) of the Government Regulation No. 82 of 2012 on Electronic System and Transaction Operation defines Electronic System as a series of devices and electronic procedures that serve to prepare, collect, process, analyze, store, display, publish, transmit, and/or distribute Electronic Information.

profiling and, it would be hard for Indonesians to understand more on how their data is used to create a profile, and what are the risks and consequences of the existence of such profiles. Furthermore, the absence of independent supervisory mechanism would open the door fordata profiling actors to use and process Indonesians' personal data in unimaginable ways for political purposes.

Once profiles have been created, the next stage would be sending tailored political messages to targeted individuals. As explained above,[91] both PMT and PBT use digital campaigns (especially social media) as one of the core strategies. As for Indonesia, the government allows the possibility of social media being used as one of the means to influence voters during the election campaign season. This provision can be found in Article 287(1) of Law No. 7 Year 2017 concerning General Elections, where Indonesian Government clearly stipulates that the advertising of elections campaign can be conducted through social media. Article 1(30) of General Elections Commission Regulation No. 23 Year 2018 further defines campaigns ads as:

> *"....**the delivery of campaign messages through** printed media, electronic media, network media, **social media**, and broadcasting institutions, in written form, drawing, animation, promotion, sound, demonstration, theatrics, debates, and other forms **intended to introduce Election Candidates or convince voters to support the Election Candidates**."*

However, Article 37 of General Elections Commission Regulation No. 23 Year of 2018 imposes limitations to political ads circulated in social media, by limiting its ad spot to only 1 (one) spot and with a maximum duration of 30 (thirty) seconds for every social media per day. However, even with the restrictions, the absence of a comprehensive data protection law that provides the data subjects the right to information related to data profiling in Indonesia would make Indonesia prone to unfair and non-transparent data profiling for political purpose.

3. Conclusion and Recommendation

Electoral politics has now become fully integrated with commercial digital media and marketing ecosystem. This has taken the term data-driven political campaign to whole another level. A vast amount of data is being collected, analysed, and used to craft tailored political messages to each individual. This results on violation of data subject's right to privacy, opens potential manipulation and enables campaigns to send tailored messages directly to citizens, thereby avoiding scrutiny from journalists.

[91] See section 2.1.1.

Under GDPR, data profiling is not forbidden, however, the implementation of data profiling must be transparent and easily accessible, where GDPR's safeguards are properly considered and data subjects have agreed to have their data collected for this specific use. For this reason, data protection serves as a tool to prevent unfair and non-transparent data profiling practices by imposing data controller to provide data subject about meaningful information about profiling and establishing an adequate supervisory mechanism.

The EU GDPR regulates that data controller is obliged to provide meaningful information about the logic involved in profiling, as well as the significance and the envisaged consequences of such processing for the data subject. Providing such information would help data subjects to understand risks and consequences of profiling as profiling itself has the potential to lead to the exclusion or discrimination of individuals. Indonesia, on the other hand, have no comprehensive personal data protection law. Several aspects of personal data protection principles can be found in several sectoral regulations in Indonesia, but still, these regulations are deeply flawed as it does not comprehensively protect personal data in Indonesia. For instance, there is no regulation that provides the data subjects with the right to information related to data profiling in Indonesia. Moreover, there is no clear and adequate supervisory mechanism over companies who collects and process personal data in Indonesia.

The absence of a comprehensive data protection law in Indonesia would, therefore, make Indonesia vulnerable to unfair and non-transparent data profiling for political purpose. *Ergo*, having in mind that Indonesia is currently gearing up for the 2019 general election, a comprehensive data protection law is urgently needed.

BIBLIOGRAPHY

Book

Djafar, Wahyudi, *et.al., Protection of Personal Data in Indonesia*, ELSAM: 2016.

Jaquet-Chiffelle, David-Olivier, "Direct and indirect profiling in the light of virtual persons." in *Profiling the European Citizen: Cross-Disciplinary Perspectives* edited by Mireille Hildebrandt and Serge Gutwirth, Germany: Springer, 2008.

Issenberg, Sasha, *The Victory Lab: The Secret Science of Winning Campaigns*, Portland: Broadway Books, 2012.

de Montjoye, Yves-Alexandre, Jordi Quoidbach, Florent Robic, and Alex Sandy Pentland. "Predicting Personality Using Novel Mobile Phone-Based Metrics." In *International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction*, 48-55. Springer, Berlin, Heidelberg, 2013.

Journal Article

Blumenstock, Joshua, Gabriel Cadamuro, and Robert On. "Predicting Poverty and Wealth from Mobile Phone Metadata." *Science* 350, no. 6264 (2015): 1073-1076. https://doi.org/10.1126/science.aac4420

Bodó, Balázs, Natali Helberger, and Claes H. de Vreese. "Political Micro-Targeting: a Manchurian Candidate or Just a Dark Horse?." *Internet Policy Review* 6, no. 4 (2017). https://doi.org/10.14763/2017.4.776

Chester, Jeff, and K. Montgomery. "The role of digital marketing in political campaigns." *Internet Policy Review* 6, no. 4 (2017).https://doi.org/10.14763/2017.4.773

Coudert, Fanny. "When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies." *Computer Law & Security Review* 26, no. 4 (2010): 377-384. https://doi.org/10.1016/j.clsr.2010.03.007.

Dobber, Tom, Damian Trilling, Natali Helberger, and Claes H. de Vreese. "Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques." *Internet Policy Review* 6, no. 4 (2017). https://doi.org/10.14763/2017.4.777

De Filippi, Primavera. "Big Data, Big Responsibilities." *Internet Policy Review* 3, no. 1 (2014). https://doi.org/10.14763/2014.1.227

Kitchin, Rob, and Gavin McArdle. "What Makes Big Data, Big Data? Exploring the Ontological Characteristics of 26 Datasets." *Big Data & Society* 3, no. 1 (2016). https://doi.org/10.1177/2053951716631130

Moura, Mauricio, and Melissa R. Michelson. "WhatsApp in Brazil: Mobilising Voters through Door-to-Door and Personal Messages." *Internet Policy Review* 6, no. 4 (2017). https://doi.org/10.14763/2017.4.775

Nickerson, David W., and Todd Rogers, "Political Campaigns and Big Data", *Harvard Kennedy School Faculty Research Working Paper*, No.

RWP13-045, (2013): 6. doi: http://dx.doi.org/10.2139/ssrn.2354474.

Rubinstein, Ira S. "Voter Privacy in the Age of Big Data." *Wis. L. Rev.* (2014): 861-936.

Legal Documents

European Union. The General Data Protection Regulation 2016/679 of the European Union.

Indonesia. Law No. 12 Year 2005 concerning the Ratification of International Covenant on Civil and Political Rights of Indonesia

Indonesia. Law No. 7 Year 2017 concerning General Elections

Indonesia. Government Regulation No. 82 Year 2012 on Electronic System and Transaction Operation

Indonesia. Minister of Communication and Informatics Regulation No. 20 Year 2016 concerning Personal Data Protection in Electronic Systems

Indonesia. General Elections Commission Regulation No. 23 Year 2018 concerning Campaign of General Elections

Other Documents

Alex Rosenblat, Tamara Kneese, and danahboyd. “Networked Employment Discrimination”. https://datasociety.net/pubs/fow/EmploymentDiscrimination.pdf.

Christi, Wolfie and Sarah Spiekermann, “Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy”. Crackedlab.org. http://crackedlabs.org/en/networksofcontrol.

Christi, Wolfie. "How Companies Use Personal Data Against People: Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information". Crackedlab.org. https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf.

Datta, A., and M. C. Tschantz, “Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice and Discrimination”, https://arxiv.org/pdf/1408.6491.pdf.

Federal Trade Commission.”Data Brokers: A Call for Transparency and Accountability”. May 2014.https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

Intel. “Deep Learning Enables Intelligent Billboard for Dynamic, Targeted Advertising on Tokyo Expressway”.https://builders.intel.com/docs/storagebuilders/deep_learning_enables_intelligent_billboard_for_dynamic_targeted_advertising_on_tokyo_expressway.pdf.

Jay, Rosemary P.*Data Protection & Privacy*. 2015, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/04/DDP2015_United_States.pdf

Privacy International. "The Keys to Data Protection: A Guide for Policy Engagement on Data Protection".https://privacyinternational.org/data-protection-guide

UN Doc. A/HRC/17/27

UN Doc. A/HRC/23/40

UN Doc. A/HRC/34/7

UN Doc. A/RES/71/199

UN Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17

V. Ferraris AMAPOLA F. Bosco, G. Cafiero, E. D'Angelo, and Y. Suloyeva. "Defining Profiling", http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf.

Website Content

Amid fears of election violence, Kenyans seek a way past inter-ethnic conflict. The Guardian. last modified August 4, 2017. https://www.theguardian.com/commentisfree/2017/aug/04/fear-election-violence-kenya-ethnic-divisions-hope-new-generation

Cambridge Analytica confirms involvement in Kenyan elections. The Star. last modified March 20, 2018 "https://www.the-star.co.ke/news/2018/03/20/cambridge-analytica-confirms-involvement-in-kenyan-elections_c1732986

Data Is Power: Profiling and Automated Decision-Making in GDPR.Privacy International. 2017,https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

Election 2016: Marriage of big data, social data will determine the next president. Wired. https://www.wired.com/insights/2013/05/election-2016-marriage-of-big-data-social-data-will-determine-the-next-president/

Farisa, FitriaChusna. "Somasi KPU, DPD Gerindra DKI Dikritik". Kompas.com. last modified November 30, 2018 https://nasional.kompas.com/read/2018/11/30/18085861/somasi-kpu-dpd-gerindra-dki-dikritik

GolkarManfaatkan Big Data untukPemenanganLegislatif 2019. Tribunnews. last modified December 21, 2018 www.tribunnews.com/nasional/2018/12/21/golkar-manfaatkan-big-data-untuk-pemenangan-legislatif-2019

Green, Joshua and Sasha Issenberg. Inside the Trump bunker - meet the people powering his campaign. The Irish Examiner. last modified November 5, 2016. https://www.irishexaminer.com/viewpoints/analysis/inside-the-trump-bunker--meet-the-people-powering-his-campaign-429091.html

India to investigate alleged Cambridge Analytica data breach. The Guardian. last modified July 26, 2018. https://www.theguardian.com/world/2018/jul/26/india-to-investigate-alleged-cambridge-analytica-data-breach-facebook

Justina Crabtee. "Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections". CNBC.com. last modified march 23, 2018.https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html

Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, "Rancangan Undang-Undang tentang Perlindungan Data Pribadi", https://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html

Kenya president's election campaign used firm hired by Trump: privacy group. Reuters. last modified December 15, 2017. https://www.reuters.com/article/us-kenya-politics/kenya-presidents-election-campaign-used-firm-hired-by-trump-privacy-group-idUSKBN1E82QS

Koalisi Perlindungan Data Pribadi: Pemilu Demokratis Harus Menjamin Perlindungan Data Privasi Pemilih". ELSAM. https://elsam.or.id/2018/12/koalisi-perlindungan-data-pribadi-pemilu-demokratis-harus-menjamin-perlindungan-data-privasi-pemilih/

Kuwado, Fabian Januarius. 1 Juta Data Pengguna Asal Indonesia Bocor, Menkominfo Panggil Facebook". Kompas.com. last modified April 5, 2018 https://nasional.kompas.com/read/2018/04/05/17361101/1-juta-data-pengguna-asal-indonesia-bocor-menkominfo-panggil-facebook

Llling, Sean. Cambridge Analytica, the shady data firm that might be a key Trump-Russia link, explained. Vox. last modified April 4, 2018 https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-facebook-alexander-nix-christopher-wylie

Madowo, Larry. How Cambridge Analytica poisoned Kenya's democracy. The Washington Post. last modified March 20, 2018 https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/?noredirect=on&utm_term=.4cf283c6a0ed

Nairobi. "Kenya: Post-Election Killings, Abuse". Human Rights Watch. last modified August 27, 2017, https://www.hrw.org/news/2017/08/27/kenya-post-election-killings-abuse

Moore, Jina. Cambridge Analytica Had a Role in Kenya Election, Too. The New York Times. last modified March 20, 2018. https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html

Moore, Jina. Violence Flares and Tensions Rise After Kenya Presidential Vote. The New York Times. last modified October 28, 2017 https://www.nytimes.com/2017/10/28/world/africa/kenya-election-uhuru-kenyatta-raila-odinga.html

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. last modified March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

UU Data PribadiMasukPrioritas 2019". Kominfohttps://kominfo.go.id/content/detail/15264/uu-data-pribadi-masuk-prioritas-2019/0/sorotan_media

Satariano, Adam. G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. The New York Times. last modified March 24, 2018. https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

State of Privacy Indonesia. Privacy International. January 2018, https://privacyinternational.org/state-privacy/1003/state-privacy-indonesia.

State of Privacy Kenya. Privacy International. January 2018, https://privacyinternational.org/state-privacy/1005/state-privacy-kenya#dataprotection

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. CNIL. Last modified january 21, 2018.https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

The Foundation of International Human Rights Law. United Nations. www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html

Tucker, Patrick. Defense One, "Refugee or Terrorist? OBM Thinks Is Software Has the Answer". defenseone.com. last modified January 27,2016.http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-hasanswer/125484/

What are the links between Cambridge Analytica and a Brexit campaign group?.Reuters. last modified March 22, 2018. https://www.reuters.com/article/us-facebook-cambridge-analytica-leave-eu/what-are-the-links-between-cambridge-analytica-and-a-brexit-campaign-group-idUSKBN1GX2IO