BRAWIJAYA LAW JOURNAL
Journal of Legal Studies
e ISSN 2503-0841
p ISSN 2356-4512
Volume 5 No 1, April 2018
Nationally Accredited No. 32a/E/KPT/2017 Dated 26th April 2017

Implementation of Resolution no. 4/2016 of the ICPO-INTERPOL Concerning Biometric Data Sharing: Between Countermeasures Against Terrorist Foreign Fighters (FTFS) and Protection of the Privacy of Indonesian Citizens

Amira Paripurna[1], Masitoh Indriani[2], Ekawestri Prajwalita Widiati[3]

[1] Department of Criminal Law, Faculty of Law Universitas Airlangga
E-mail : amira@fh.unair.ac.id

[2] Department of International Law, Faculty of Law Universitas Airlangga
E-mail : masitoh@fh.unair.ac.id

[3] Department of Constitutional Law, Faculty of Law Universitas Airlangga

Submitted: 2018-03-01 | **Accepted**: 2018-04-04

Abstract: *This study aims to identify and explore the challenges in the implementation of Resolution No. 4/2016 of the ICPO-INTERPOL concerning sharing and exchanging biometric data among the members of ICPO-INTERPOL in order to counter terrorist foreign fighters (FTFs). This research also aims to elaborate and describe the mechanism of collecting, recording, storing, and exchanging biometric data conducted by the Indonesian government.*

The mechanism of collecting, recording, and storing biometric data works through 3 main doors, namely: 1) in the process of making electronic Resident's ID Cards (e-ID Cards); 2) in the process of making SKCK (Certificates of Police Record); 3) in the process of making e-Passports. In the implementation of Resolution No. 4/2016 of ICPO-INTERPOL, the most obvious obstacles and challenges are the absence of regulations concerning the protection of personal data, and also the fact that the biometric data system itself is still relatively new and the database is not fully developed. Until today, the INTERPOL National Central Bureau *(NCB) for Indonesia does not have its own biometric database system; instead they are using the database that is centralized at Pusinafis Polri (the Indonesian National Police's Center of Automatic Fingerprint Identification System).*

The results of the study reveal that the biometric data recorded, collected, and stored are big data, but so far in supporting law enforcement and crime prevention processes the data have only been used as comparative data. In addition, there have also been found indications of violations of personal data and privacy, for example in relation to the absence of mechanism for data retention, consent, processing, notification, and disclosure.

Keywords: *INTERPOL, Biometric Data, Intelligence Sharing, Data Privacy, Terrorism*

I. INTRODUCTION

When dealing with the complexity of terrorism and transnational-organized crimes (hereinafter abbreviated as TOC), such as narcotics crime, counterfeit money crime, etc., oftentimes the law enforcement officers become overwhelmed. This is because in terms of speed the law enforcement officers are far behind the perpetrators in executing their criminal intent, destroying evidence, and running away. In addition to the increasingly sophisticated methods, perpetrators of these crimes can operate and move from country to country freely.

In the aspect of early detection, preventing and thwarting acts of terrorism have become more complicated compared to acts of TOC. Terrorism has a higher complexity than other acts of TOC. Many events have shown the facts that although the intelligence has retained information on the movements and networks of terrorism, the *tempus* and *locus delicti* of terrorism events are always unexpected. This is in contrast to drug crime, for example, whose movements, narcotics deliveries and organized networks can be traced online. Real examples of the successful eradication of organized narcotics networks are already commonly known, which is not so with terrorism. The bombing events in Bali, Kuningan, and Marriot on Thamrin Street in Jakarta, as well as terrorism attacks of WTC Building in New York, in Madrid and London, are real examples of how difficult it is to prevent terrorism in any other countries.

In the context of Indonesia, even though the law enforcement officers have succeeded in combating the largest terrorist networks in the country, namely the network of Santoso's (the leader of the East Indonesia Mujahidin) and the Jama'ah Islamiyyah network, it does not mean that the problem of terrorism in Indonesia is over. Terrorism continues to be a threat given the growing influence of radicalism everywhere, one of the problems being the emergence of ISIS as a new power, and not to mention the newly emerging problem of the return of the FTFs to their respective countries of origin. The FTFs who return to their home countries are suspected of having great potential to spread out their experience and their influence, and ultimately recruit new members.

The international communities have acknowledged that not a single country in the world is able to deal with terrorism and TOC without the support of other countries. Therefore, the international communities have established a number of international cooperations such as the ICPO-INTERPOL, Europol, and others. In these international forums, a number of decisions and agreements are adopted to facilitate the coordination of cooperation in the police sector in order to combat terrorism and TOC.

One of the international cooperations the ICPO-INTERPOL has recently agreed on the implementation of biometric data sharing among its member countries. In the 85th INTERPOL General Assembly convened on 7-10 November 2016 in Bali, the INTERPOL member countries made an agreement to conduct biometric data collection and sharing of data/information. The contents of the agreement in the 85th INTERPOL General Assembly include conducting systematic collection and recording of the DNAs and fingerprints of suspects or defendants as well as collecting and sharing biometric data to help member countries in their efforts to arrest foreign terrorist fighters (FTF) crossing the border under fake names and travel documents.

The main objective is to address terrorism and transnational crimes. With this agreement, it is expected that each member country can identify and conduct early prevention of potential threats of terrorism

and TOCs. This step is taken because there are significant weaknesses in the collection and exchange of biometric data in relation to terrorism at the international level, as well as the alertness to the potential danger of the return of foreign terrorist fighters to their home countries.[1] These weaknesses are considered to have created loopholes for interferences that are harmful to the security of each member country.

The biometric system has been around since one century ago. Biometric technology is commonly used to identify individuals so that they can access certain facilities. However, the use of this system as one of the instruments to assist law enforcement officers in their strategy to prevent crimes (policing) only became widely known in the past two decades. With biometric technology, for example, law enforcement officers can identify and store unique identifiers such as fingerprints, DNAs, retinal and iris scans, and face recognition. The facial recognition system has now become quite predominantly used for the counter-terrorism purposes.[2]

In connection with counter-terrorism, especially in the pro-active counter-terrorism whose strategy is focused on the pre-crime aspects such as preventing and stopping, and disrupting terror plots, exchange of biometric data among law enforcement officers across the countries becomes highly relevant. With the growing use of false aliases, falsification of travel documents, tactics of deception misleadingly suggesting a person has died in a conflict area, and even the basic issues associated with translations have exacerbated the challenges faced by law enforcement officers in the field.

Biometric data exchange becomes important especially for identifying the whereabouts of perpetrators. This is certainly related to the functions of the ICPO-INTERPOL, i.e. to provide global police communication services that allow the police forces of member countries to request and transmit information. This will let the police have an efficient way to share and access information. INTERPOL functions to maintain and update databases that can be accessed and used by international police forces. These databases contain a wide range of information including lists of wanted individuals, lists of stolen documents, and forgery trends.

The information available to law enforcement officers at the frontline level, through INTERPOL, is expected to help identify suspects accurately and release innocent individuals or minimize false arrests of terrorism suspects. To date, INTERPOL already has 9,000 data on FTFs, including those in conflict zones, and only about 10% of the data currently possessed are complemented with biometric data and high-

[1] Toni Bramantoro, 'Koordinasi Antar Negara Adalah Kunci Untuk Mencegah Aksi Foreign Terrorist Fighter', Tribunnews (online), 11 August 2016 <https://www.tribunnews.com/nasional/2016/08/11/koordinasi-antar-negara-kunci-untuk-mencegah-foreign-terrorist-fighter>; see also INTERPOL, '*Foreign Terrorist Fighters,*' <https://www.INTERPOL.int/Crime-areas/Terrorism/Foreign-terrorist-fighters>; see also Muhammad Saifulloh, 'BNPT Pimpin Negara ASEAN Bahas Foreign Terrorist Fighter', Okezone (online), 11 August 2016, <http://news.okezone.com/read/2016/08/11/337/1460830/bnpt-pimpin-negara-asean-bahas-foreign-terrorist-fighter>

[2] Since the 9/11 terror attacks in the USA, face recognition has been used in the majority of airports. This system is also installed in all areas that require high levels of security. See also, Carlos Delano Buskey, *How Face Recognition Will Be Used to Counter Terrorism*, Biometrics Report (2001), 3; John D. Woodward, Jr, *Facing up to Terrorism*, (RAND Publication, 2001), 6-7.

resolution images, which can be used in the facial recognition method.[3]

As an INTERPOL member country, on the one hand the law enforcement officers in Indonesia are obligated to comply with the terms of the agreement, but on the other hand biometric technology systems are still relatively newly adopted in Indonesia and counter-terrorism policing in Indonesia is still being developed to achieve the most efficient model that is also in conformity with the principles of law and human rights. Therefore, with the agreement established among the ICPO-INTERPOL member countries to collect, record and share biometric data, it is important to identify and analyze challenges and obstacles in the implementation of Resolution No. 4/2016 of ICPO-INTERPOL related to sharing and exchange of biometric data among ICPO-INTERPOL members. Since the biometric technology system is still relatively newly adopted by the Indonesian government, knowledge and understanding of the mechanism of collection/gathering, recording and sharing of biometric data are needed from the perspective of legal protection of data and privacy of citizens.

II. LEGAL MATERIALS AND METHODS

This research is descriptive-analytic qualitative research. The purpose of this research is to make descriptions, illustrations, identification and analysis systematically, factually and accurately of facts, characteristics and relationship between phenomena concerning the application of biometric data sharing in the police as well as among the ICPO-INTERPOL member countries, and the mechanism of collecting and recording biometric data, and the utilization of biometric data for law enforcement purposes primarily for the prevention of terrorism.

Primary data are data generated from interviews with research subjects. In-depth interviews were conducted with the International Communication Division of Indonesia's INTERPOL NCB Secretariat of the Indonesian National Police's International Relations Division, and the Pusinafis (Centre of Automatic Fingerprint Identification System) of the Indonesian National Police's Criminal Investigation Agency. Meanwhile, secondary data consist of legal and non-legal documents and materials. Legal materials consist of the national laws and regulations, legal provisions existing both at the national and international levels, and also technical rules in the field in the implementation of the system. As for secondary legal sources, in this case they consist of studies concerning the legal aspects of the collection, storing, sharing and use of biometric data for law enforcement purposes, as well as studies concerning aspects of protection of data and privacy either in the form of books or journals. Furthermore, this research also uses non-legal materials to add to and enrich the legal materials that have been gathered before.

III. RESULTS AND DISCUSSIONS

Collection, Storing and Sharing of Biometric Information Under Resolution No. 4/2016 of the ICPO-INTERPOL ('Bali Resolution')

The 85th INTERPOL General Assembly held on 7-10 November 2016 in

[3] Justin Lee,'INTERPOL says Lack of Biometric Data on Terrorists a Security Vulnebaribility', Biometricupdate (online), 10 November 2016 <http://www.biometricupdate.com/201611/INTERPOL-says-lack-of-biometric-data-on-terrorists-a-security-vulnerability>.

Bali resulted in a resolution No.4/2016[4] (hereinafter referred to as 'Bali Resolution') to reinforce the implementation of biometric information sharing among the ICPO-INTERPOL members in dealing with terrorists' mobility. This resolution (hereinafter referred to as 'Bali Resolution') basically encourages each member country to give maximum contribution to the ICPO-INTERPOL's efforts in compiling data related to terrorism, particularly in the matter of coordination with NCBs (ICPO-INTERPOL members) through INTERPOL diffusions and international notice as well as INTERPOL's Crime Analysis File aimed at dealing with foreign terrorist fighters (hereinafter referred to as FTFs).[5] It is through this 'Bali Resolution' that member countries are also encouraged to perform cross-check systematically on the information already retained in the ICPO-INTERPOL information systems and issue INTERPOL International notice and diffusions.

Systematic collection and storing of biometric information is an integral part of the terrorist profiles shared through the ICPO-INTERPOL channels [6] The focus of the systematic collection and storing of biometric information is the unique identifiable attributes, which include fingerprints and DNA profiles of individuals in the following categories[7]:

1. Individuals known to have connections with, or have reached/entered into conflict areas with the aim of providing support or joining terrorist groups;
2. Individuals who are deported, detained or subjected to court decisions for committing crimes related to terrorism, including individuals traveling with the aim of committing, planning, preparing, and participating in acts of terrorism;
3. Individuals who provide or receive terror training, as well as who are connected to armed conflicts;
4. Individuals returning from conflict areas who in the judgment of and investigation by the authorities have a high risk of cross-border mobility and a high risk of re-offending.

Currently, the INTERPOL databases have recorded nearly 8,000 profiles of individuals known or suspected as FTFs.[8] These efforts are continuously improved to facilitate successful investigations, monitor and prevent terrorists' mobility, as well as prevent the growing gaps of security among international countries. The 'Bali Resolution' can thus be seen as a form of awareness of all member countries of the vital role of positive identification of terrorist suspects in the field, thereby promoting more efficient law enforcement and increased border security as needed, as well as minimizing the impact on other screened individuals on a broad scale.

Upon biometric data collection, the biometric data can then be used to identify suspected perpetrators of serious crimes as well as terrorism. This can be done in several ways, which among others include:[9]

1. Screen visa applicants, internally displaced persons, asylum seekers,

[4] Resolution No. 4 AG-2016-RES-04.
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid.*
[9] 'Roundtable on Biometric Data Sharing for Identity Verification: Introduction To The Regional Data Sharing Initiative,' Baliprocess.net (online), October 2014 <http://www.baliprocess.net/UserFiles/baliprocess/File/Discussion%20Paper%20on%20Biometric%20Data%20Sharing.pdf>.

residency applicants, and transit passengers. This screening is required to find out if the persons in question are:

a) suspected terrorists, or engaged in terrorist activities (including foreign fighters/FTFs),
b) human trafficking victims,
c) engaged in serious crimes or engaged in fundraising/collecting donations for organizations that are on the list of terrorist organizations or engaged in other transnational crimes;

2. Screen visa applicants and persons seeking refuge to find out whether they filed asylum claims in multiple jurisdictions and "shopping forums";
3. Detect persons (asylum seekers or displaced persons) who have received asylum from a third country (the country of the first asylum) or have been registered as refugees by UNHCR;
4. Re-document original visa or passport holders whose travel documents are lost/stolen/retained;
5. Check travel documents against whitelists and blacklists issued for troubled countries or organizations.

Biometric Data Collection and Storage Mechanism in Indonesia

Biometrics is an authentication method that uses the verification and validation of physical characteristics and characteristics of human behavior. Verification and validation are conducted using fingerprint scan, iris/retinal scan, digital signature, face/face shape recognition, dental shape, and voice recognition to identify one's identity.

Since 2009, the Indonesian Government has introduced and developed the use of Electronic Resident's Identity Card (e-ID Card) nationwide. This e-ID Card must be held by every citizen who has reached the age of 17 years and above. This e-ID Card uses biometric technology to load security codes and electronic records as a means of verifying and validating the identity data of a resident. Before the new policy concerning the use of e-ID Card was issued, the ongoing practice of conventional ID Card making system had enabled someone to hold more than one ID card. This was due to the absence of an integrated database that collects population data from all over Indonesia. Possession of multiple ID Cards was in many cases used to evade taxes, make certain passports that could not be made in every city, as well as disguise/conceal the identity of terrorists and perpetrators of other crimes.

As a matter of fact, the use and collection of biometric data has been practiced long before the e-ID Card was introduced, particularly when someone applied for a driver's license (SIM). Even so, the collection of the Indonesian citizens' biometric data was not done as massively as it has been since the issuance of the policy in respect of e-ID Card use. Hence, it is noted that since 2009 biometric data collection in Indonesia has been conducted through 3 doors, namely:

1. Biometric data collection through e-ID Cards where the process of collecting and storing the database is under the responsibility of the Ministry of Home Affairs;
2. Biometric data collection through Electronic Passports where the process of collecting and storing the database is under the responsibility of the Directorate General of Immigration and the Ministry of Law and Human Rights;
3. Biometric data collection through Certificates of Police Record (SKCK),

where the process of collecting and storing the database is under the responsibility of the Indonesian National Police (Polri).

The biometric data collected through these 3 doors are mainly in the form of fingerprints. There are at least three main reasons why fingerprints are used in authentication: in addition to being the most economical and low-cost compared to other biometric data and systems, fingerprints are not easily deformed and are unchangeable, and they have unique properties in that they are different from one individual to another.[10]

The storage center for biometric data (especially fingerprints) within the police structure is at the Pusinafis. The technical procedures for biometric data storage are carried out by the sub-divisions within the Pusinafis, which can be described as follows:[11] Technically, the principal division in charge of administering non-criminal fingerprint information management system whether manually, centralized and nationwide is the Biddaktium (the General Dactyloscopy Division). This division is in charge of performing and supervising the fingerprinting process on an AK-23 card, and developing fingerprint formulation as well as sorting the AK-23 fingerprint cards and AK-24 name cards,[12] and after going through the processing stages the fingerprint data are stored and verified (through a retrieval process) manually.[13]

Sharing and Exchanging Biometric Data at the National Level

One of the functions of biometric data is to support the law enforcement process. Article 58 paragraph 4 of Law No. 24 of 2013 on Amendment to Law Number 23 of 2006 on Population Administration, regulates the utilizations of the population data collected from electronic Resident's ID Cards, one of which is to support law enforcement and crime prevention. Considering the significant role of electronic e-ID Card data in the law enforcement sector, and in line with the mandate of the Law, the Ministry of Home Affairs and INP have signed a memorandum of understanding (MoU) on the utilization of electronic Resident's ID Card data.

With respect to the identification of biometric data (fingerprints), the Indonesian National Police (INP) has its own Centre of Automatic Fingerprint Identification System (known as Pusinafis), under the INP's Criminal Investigation Agency which has a function to provide technical support to investigators in criminal interrogation and investigation.

Pusinafis has a database system that stores all biometric data of Indonesian citizens who have applied for a Certificate of Police Record (known as SKCK) as well as data of perpetrators of crime and recidivists. The role of electronic Resident's ID Card data to support the law enforcement can be illustrated as follows. When a police investigator conducts an investigation of a suspect, they will need to first examine the suspect's identity,[14] to help in the further steps of investigation.[15] This identity check is primarily based on the identification owned

[10] Kementerian Dalam Negeri RI, 'Apa dan Mengapa E-KTP (What e-ID Cards Are and Reasons (for their use))', e-ktp (online), 20 June 2011 <http://www.e-ktp.com/2011/06/hello-world/>.

[11] Interview with Nurul Tristiati, 16 August 2017.

[12] This task is carried out by the Fingerprint Processing Subdivision (the Prosiri Subdivision)

[13] This task is carried out by the Fingerprint Documentation Subdivision (the Doksiri Subdivision).

[14] Article 7 paragraph 1, letter c of the Criminal Procedure Code.

[15] Mirna Rahmaniar, Lucky Endrawati and Milda Istiqomah, 'Analisis Yuridis Data Kependudukan Kartu Tanda Penduduk Elektronik Untuk

by the suspect, which is generally a Resident's Identity Card.

Prior to the existence of electronic Resident's ID Cards (e-ID Cards), it was easy to make a fake ID card, and one person could possibly have two identities. Now, the fact that e-ID Cards apply the principle of one National Identification Number for one ID Card, and contain biometric data, makes it difficult to produce fake electronic e-ID Cards and closes the possibility of someone having two identity cards.[16] Thus, in an investigation of a suspect, it is almost impossible for the suspect to give a false identity, because the authenticity of each e-ID card can be verified through SIAK (Population Administrative Information System),[17] and the biometric data of the suspect collected during the investigation can be compared with the biometric data stored in the e-ID card.

Furthermore, in the investigation process implemented to date, especially in order to reveal a criminal whose identity is yet to be known but his facial description or fingerprints have been known, the investigators use comparative data in the form of data of ex-prisoners, recidivists or fugitives that are currently stored in the database of Pusinafis. However, since there is an MoU between the Indonesian National Police (INP) and the Ministry of Home Affairs,[18] the comparative biometric data are no longer limited to the data owned by the Pusinafis (collected in the process of producing Certificates of Police Record (known as SKCK) and data on prisoners/recidivists/fugitives). INP can now have access to the Ministry of Home Affairs' database system where biometric data of most Indonesians who are required to have resident's identity cards are stored. As for the final step, if there are no data matching the identity of the perpetrator, the police will put the perpetrator in the wanted list.[19]

Meanwhile, the biometric data that have been collected in the e-passport making process have not been used optimally in the effort to support the law enforcement process because the current system has not contained complete data, and this is because old user data have not been included in the biometric database.[20]

Furthermore, this section will specifically discuss the scope of cooperation outlined in the memorandum of understanding (MoU) between INP and the Minister of Home Affairs which is then followed up with a cooperation agreement signed by the Indonesian National Police (INP)'s Criminal Investigation Agency and Directorate General of Population and Civil Registration of the Ministry of Home Affairs. This cooperation is basically established to regulate the use of population data in the effort to improve the effectiveness of police duties in community service and law enforcement. The scope of this cooperation

Penyidikan Tindak Pidana (Juridical Analysis of Population Data on Electronic Identity Cards for Criminal Investigation)' (2014) Jurnal Hukum Fakultas Hukum Unversitas Brawijaya, 3-5 <http://hukum.studentjournal.ub.ac.id/index.php/hukum/issue/view/31>.

[16] *Ibid.*

[17] *Sistem Informasi Administrasi Kependudukan* (SIAK) or Population Administrative Information System is a system for collecting, processing and presentating population data in a quick and accurate manner to produce appropriate population information to assist the government in the development and provision of services to the citizens.

[18] Memorandum of Understanding between the Minister of Home Affairs of the Republic of Indonesia and the Chief of Indonesian National Police No. 471.12/382/SJ, B/6/I/2013 concerning Cooperation on the Utilization of Resident's Identification Number, Population Data and Electronic Resident's Identity Card within the Scope of Duties of Indonesian National Police

[19] *Ibid.*

[20] *Ibid.*

covers the utilization of electronic Resident's ID card data, NIK (National Identification Number) and Population Data.

With this cooperation, the Ministry of Home Affairs as the owner of the database basically grants authorization to access[21] the population data including fingerprint data to INP, but this authorization to access is limited to the Indonesia National Police officers in charge of data management (in this case Pusinafis).[22] The Population Database recorded through the SIAK contains a number of data and information including: residential data; family data; citizens' biodata; civil registration data; passport size photo (3 x 4 cm) data, fingerprint data, and citizens' signatures.[23] This cooperation is valid for a period of 5 years (2013-2017) and may be extended upon the agreement of the parties.

Table 1. Cooperation between the Indonesian National Police's Criminal Investigation Agency and Directorate General of Population and Civil Registration of the Ministry of Home Affairs of Indonesia in Sharing Data related to Utilization of Electronic Resident's ID Card Data, NIK (National Identification Number) and Population Data.

No	Indonesian National Police's Criminal Investigation Agency	Directorate General of Population and Civil Registration of the Ministry of Home Affairs of Indonesia
1	Grants authorization to have the key to the Secure Access Module (SAM);	Provides a card reader and the key to SAM;
2	Authorized to access population data (with the authorization limited to an INP's dedicated unit with respect to this matter) as needed;	Grants access to the data communication network only to the authorized INP unit;
3	Authorized to access fingerprint data as needed, without any time limitation for the purpose of investigation and community service;	Monitors the usage and utilization of data such as e-ID card data, National Identification Number and Population data;
4	Authorization granted is limited to officers in charge of data management;	Monitors and grants approval upon a recommendation from INP of officers who are authorized to access data;
5	Authorized to include National Identification Number (NIK) whose data integrity has been verified in every document issued by INP to citizens;	Provides technical guidance and assistance, as well as technical personnel to provide guidance and mentoring;
6	Authorized to utilize demographic data (including fingerprint data) to add to the fingerprint data that have been stored in the Centre of Automatic Fingerprint Identification System (Pusinafis) of the INP's Criminal Investigation Agency;	Holds periodic coordination and evaluation meetings between the parties at least once a year;
7	Is required to keep the confidentiality, integrity and authenticity of the data accessed.	

The existence of the memorandum of understanding and the cooperation between the Indonesian National Police's Criminal Investigation Agency and Directorate

[21] According to Government Regulation No. 37 of 2007 Article 1 (37) stating that an authorization to access data is granted by the Minister to officers in charge in the Operating and Implementing Agency to be able to access the population database in accordance with the permission granted.

[22] *Supra* note 18.

[23] Regulation of the Minister of Home Affairs of the Republic of Indonesia No.25 of 2007 Articles 4-10.

General of Population and Civil Registration of the Ministry of Home Affairs shows that there is a mechanism of information or data sharing and coordination between the institutions that have been formally regulated. With the formally set out agreement, the cooperation becomes non-incidental, and consequently it can better facilitate the coordination process since each party now has a clear written scope of their respective rights and responsibilities, and the agreement also provides a clear picture of what data to be shared and when such data should be shared.

In implementing the terrorism prevention function (the pre-crime aspect in counter-terrorism), coordination and sharing of information or data among law enforcement institutions and other related institutions, play a crucial role. Searching, collecting and obtaining sensitive and important data or information help law enforcement officers in carrying out their terrorism prevention function. The prevention function focuses on early detection, to the maximum extent possible to narrow the terrorists to execute their plans.

Sharing and Exchanging Biometric Data at the International Level

One of INTERPOL's most important functions is to enable police to share crime-related information.[24] The success of an investigation conducted by ICPO-INTERPOL relies on the availability of up-to-date global data. Therefore, INTERPOL has criminal databases and this allows INTERPOL's member countries to be able to have an instant and direct access to a number of criminal databases. All of the databases, except IBIN (INTERPOL Ballistic Information Network), can be accessed in real-time through the I-24/7 network connecting databases from INTERPOL to National Central Bureaus (NCBs).[25] The INTERPOL web server has been developed and improved so that in addition to being accessible to NCBs, it can also be accessed by front-line law enforcement officers, such as border guards, allowing them to search for databases of wanted persons, stolen and lost travel documents.[26]

In addition, INTERPOL also has an international notice system that is used to issue international notices for fugitives, suspected criminals, persons associated with or of interest in an ongoing criminal investigation, persons and entities subject to UN Security Council sanctions, potential threats, missing persons and unidentified bodies. Member countries' National Central Bureaus (NCBs) may also use INTERPOL's international notices system to alert law enforcers in other countries about potential threats of crime or to request assistance in dealing with a crime case. In addition, similar to international notices, there is also a diffusion circulated for the same purpose as a notice but it is circulated directly by member countries or international entities to the countries of their choice. Diffusions are also recorded in police databases. International notices and diffusions contain two main types of information: personal details (physical descriptions, photographs, fingerprints, identification number, etc.); and judicial information (indictments, arrest warrants or judgments and court decisions,

[24] Interview with Nina Naramurti, International Communication Division of Indonesia's Interpol NCB Secretariat, International Relations Division of Indonesia National Police, Jakarta, 15 August 2017; See also INTERPOL, '*Forensics*' <https://www.interpol.int/INTERPOL-expertise/Forensics/Fingerprints>.

[25] INTERPOL, '*Data Exchange*' <https://www.interpol.int/INTERPOL-expertise/Data-exchange>.

[26] *Ibid.*

etc.). The Secretariat General will publish notices upon a request from member countries' NCBs or authorized international entities. All notices are published on the INTERPOL's website once the compliance checks have been completed.[27] At the request of member countries or international entities, extracts of notices may also be published on INTERPOL's website. The Secretariat General will only publish international notices and diffusions after the legal requirements are met, for example, a notice will not be published if it violates the INTERPOL's constitution, which prohibits the organization from undertaking activities of a political, military and religious or racial character.

The INTERPOL forensic database system consists of fingerprints, DNA profiles and facial images.[28] Authorized users in member countries may view, submit and cross-check fingerprint records in the fingerprint database via a user-friendly automatic fingerprint identification system (AFIS). This DNA profile database contains DNA profiles from crime offenders or suspects, crime scenes, missing persons and unidentified bodies. INTERPOL does not store any nominal data linking a DNA profile to any individual.

Facial Recognition System Database is a database providing a dedicated platform to store and cross-check images in order to identify fugitives, missing persons and persons of interest. In addition, INTERPOL also has Edison (Electronic Documentation and Information Systems on Investigation Networks) which provides examples of original travel documents to help identify fakes. Edison contains images, descriptions and security features of original travel and identity documents issued by countries and international organizations. The entire details of data containing personal data and criminal record history of a person are stored in a database known as the INTERPOL Criminal Information System.[29] In this case each INTERPOL member country (NCBs) is authorized to be a user as well as an owner of INTERPOL criminal information system as well as INTERPOL forensic database system and is bound by INTERPOL rules.[30] Being a user means that NCBs are authorized to have direct and instant access to INTERPOL's database, while being an owner means that NCBs may upload criminal data and information onto INTERPOL's criminal information database system and INTERPOL's forensic database system.[31]

Personal Data Protection and Privacy Issue in Large Scale of Biometric System

The rise of new technology creates massive data and recently called as big data. Big data sets from volume, variety, velociy, variability, and veracity[32]. Thus, consists of complex and voluminious set of capturing data, processing system, analyzing, storing and updating information privacy[33]. In the previous discussion, biometric data obtained from processed fingerprint scan, iris/retinal scan, digital signature, face/face shape

[27] *Ibid.*

[28] INTERPOL, '*Databases*' <https://www.interpol.int/INTERPOL-expertise/Databases>.

[29] *Ibid.*

[30] Interview with Nina Naramurti, International Communication Division of Indonesia's Interpol NCB Secretariat, International Relations Division of Indonesia National Police, Jakarta, 15 August 2017.

[31] *Ibid.*

[32] Martin Hilbert, 'Big Data for Development: A Review of Promises and Challenges' (2016) 34 (1) *Development Policy Review* 135-174.

[33] Danah Boyd and Kate Crawford, 'Six Provocations for Big Data: A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society' (2011). <https://ssrn.com/abstract=1926431> or <http://dx.doi.org/10.2139/ssrn.1926431>

recognition, dental shape, and voice recognition. Also it requires set of technique and technology to reveal certain information such as processing, analyzing and storing. Thus it can be drawn that biometric data meets the criteria of big data.

The debate around big data is that it presents various advantages also disadvantages. In terms of business sector, big data can be used to identify customer's behaviour in the dimension of Internet of Thing (IOT). While in terms of preventing and combating crime as dicussed previously, big data can be used to help preventing and combating crime especially pre-crime activity likewise in INP's Sisinfo. While the disdvantages may vary because of the collection process may occurs constantly and unseen, the system creates new authority (artificial agent) and the result of processing data becomes unreliable since individual may change their physical appearance. As a result, it is a potential threat for personal information authenticity.

In terms of privacy, it defines as the control over personal information[34] yet to decide or to disclose personal information in this matter includes any information that identifies a person such as (1) name, address, email address, phone number, (2) race, nationality, ethnicity, origin, color, religious or political beliefs or associations, (3) age, sex, sexual orientation, marital status, family status, (4) identifying number, code, symbol, (5) finger prints, blood type, inherited characteristics, (6) health care history including information on physical/mental disability, (7) educational, financial, criminal, employment history, (8) others' opinion about the individual, and (9) personal views except those about other individuals.[35] Furthermore, many legal scholars articulates privacy as the control and claim of individual to communicate their pesonal information with others.[36]As a result, the legal perspective on privacy is determined by the control of individual to maintain his personal information from collecting, processing, sharing, retaining or even manipulating data.

As discussed previously, biometric data that obtained from processed fingerprint scan, iris/retinal scan, digital signature, face/face shape recognition, dental shape, and voice recognition has resulted in different perspective, challenging traditional value and some its significant contribution to the society's need on safety and security. As a new technology, biometric data required of personal information that processed in certain way. The process is undeniably collides with individual rights since it is reduce certain rights and freedom of individual. For example, iris scanners that considered as the most reliable biometric yet expensive. It is painless and can be carried out without the subject even noticing[37]. Thus, this circumstance explains the system and technology challenge toward citizen's privacy.[38]

The use of biometric data entails discussion concerning personal integrity, autonomy and identity.[39] Regarding to the complexity activity on sharing and exchanging biometric data, the foremost impacted aspect is individual as the subject data itself. Thus, individual as the main

[34] Sheri B. Pan, 'Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze' (2016) 30(1) *Harvard Law Journal & Technology*.

[35] Bryan A. Gardner, *Black's Law Dictionary* (West Group, 8th Ed, 2004).

[36] note 34, 241

[37] Darcie Sherman, 'Biometric Technology: the Impact on Privacy', (2005) 1 (1) *Comparative Research in Law & Political Economy* CLPE Research Paper.

[38] *Ibid*.

[39] Nancy Yue Liu,*Bio-Privacy: Privacy Regulations and the Challenge of Biometric* (Routledge, 2013)

object of sharing and exchanging activity is facing privacy issue, and post 9/11 makes it more debatable since privacy has been considered as obstacle to security.[40]At least there are three main challenges to privacy on sharing and exchanging biometric data. First, the needs to provide security against FTF without infringing citizen's privacy and its relation to the absence of individual consent; second is a new generation of collective rights as a result of big data and technological change; third, the emergence of artificial agent as a result of the surveillance system.

The need to provide security against FTF without infringing citizen's privacy is closely related to individual consent. The collection of personal information must be done fairly, legally and under the knowledge of subject of data or individuals concerned. It is found that the authority has not fully implemented this principle. As previously dicussed, the collection process through three different authority in different sectors may have different treatment. Those respect authorities, however, have different standard in processing data due to their resources and internal regulation. Although processed in three different authorities, there should be one common issue in giving prior information and notification to the data subject. In this case, it may be conducted by providing short information on the register form. Thus, the information at least contains the subject data's content during eights phases, collecting, processing and analyzing, retaining and storing, acessing, disclosure phase and destruction.

Biometric data ownership is merely related to the ethical concerns.[41] For this reason, biometric data ownership should be understood as subject data's authority to control or in this case to authentify their biometric data. Hence, the process of collecting, analyzing, storing and retaining that involves data contollers should remain limited. However, technology makes it impossible since the system has its own way to process biometric data and it does not under possession of biometric data owner. Further, the debate remains on how biometric data owner should able to control their personal information, and how far the authorities remain to limit their control over biometric data owner. Therefore without clear legal provision, there will be no sufficient legal arguments for subject data to claim in such ownership rights. While in the issue of technology development, the subject data may be granted by more control over their data due to its complexcity process. Yet, in this case, the INTERPOL National Central Bureau (NCB) for Indonesia does not have its own database system, but has a resourece sharing pattern with INP's PUSINAFIS. There is should be clear information given to biometric data ownership over the existence of the database as well.

Big data allows government to improve public sector administration and assists global organization in analyzing information to develop strategic planning.[42] Biometric data as the result of applied technology on biometric process has consequence in the emergence of the artificial agents. Artificial

[40] Hansen M., Raguse M., Storf K., Zwingelberg H. Delegation for Privacy Management from Womb to Tomb – A European Perspective in Bezzi M., Duquenoy P., Fischer-Hübner S., Hansen M., Zhang G. (eds) *Privacy and Identity Management for Life Privacy and Identity* (IFIP Advances in Information and Communication, 2009).

[41] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, (Springer, 2013)

[42] Tene, Omer and Polonetsky, Jules, Big Data for All: Privacy and User Control in the Age of Analytics (2013) 239 *Northwestern Journal of Technology and Intellectual Property* <https://ssrn.com/abstract=2149364>.

agents in this case is the the end user of the system and liable for any illicit treatment of personal[43]. Thus, it is needed certain standart in order to distinguish such liablity in the biometric data processing since the presence of artificial agents may harm privacy in three ways: over and inacurrate personalization, violation due to process and discrimination. Over and inacurrate personalization may caused by the system that allowed to display images to identify fugitives, missing persons and persons of interest. Yet, there's always changing on physical appereance of individual. Violation occurs when there is an absence of data protection principles for acquisitioning such data.

Thus, the legal mechanism to ensure privacy is a set of regulation on data protection.[44] As a fundamental right, the right to privacy has been recognized in international and regional human rights conventions among others the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and European Commission on Human Rights (ECHR). Other than that, one of the main international instruments on privacy and data protection is the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981. Though this convention only adopted by European countries, non-European countries is allowed to take accession process. Moreover, Directive 45/46/EC also known as the EU Data Protection Directive also ensures effective privacy protection in order to cope with new development on technology. This also strengthened by the implementation on the General Data Protection Regulation (GDPR) by May 25, 2018. The GDPR will introduce a new concept on accountability that requires data controller to be more responsible and able to demonstrate compliance based on data protection principles.[45] Beside that, there are also strengthening over data subject rights including right to access, breach notification, right to be forgotten, introducing data portability and privacy by design.[46]

Indeed privacy as a fundamental right should be protected; however the way of life influences the practice of the privacy itself. Though in western countries privacy may entitled as important issue, it may have lesser importance in other area or culture. As a result, there are some obstacles both in national and international level.

In international level there is different implementation on data protection among INTERPOL member countries. The implementation depends on government approach to govern such issue. In cyber-libertarian perspective, the approach is considered as self-regulation approach or in the other words is negating government existance, but in its development, this approach is questionable because the presence of the government will influence the decision making and on the technical provision of physical infrastructure of the data protection.[47] Meanwhile in the perspective of cyber-paternalism, the government is the single actor (state-centris) in regulating and managing technical provision of physical infrastructure of data protection.[48] Thus it caused imbalance power

[43] Samir Chopra and Laurence White, *A Legal Theory for Autonomous Artificial Agents* (University of Michigan Press, 2011) 73.

[44] Jovan Kurbalija, *An Introduction to Internet Governance* (Diplo Foundation, 6th ed, 2014)

[45] GDPR, 'GDPR Key Changes',eugdpr (online) <https://www.eugdpr.org/>

[46] *Ibid*.

[47] Kristen E.Eichensehr, 'The Cyber-Law of Nations' (2014) 103 *The Georgeton Law Journal* 317.

[48] M. Fromkin, *Lesson learned too well: The Evolution of Internet Regulation*, Technical Report, CDT Fellows Focus Series (2011).

between citizen and government, also creates polarization of western and eastern countries influences.[49]This debate requires maturity of governance since implementation and enforcefement between and amongst INTERPOL member states is facing different cultural demography, historical legal system, legislative influences, and political enthusiasm.

In national level, regulations relating to data protection are scattered in some areas such as immigration, banking and finance, population and administration, information and electronic transaction that ruled based on sectoral problems. The existing legal framework concerning data protection refers mainly to the ministerial level instrument enacted by the Ministry of Communication and Information Number 20 Year 2016. Departmental regulation is basically a delegated or secondary legislation which get its validity from two situations; *firstly*, it is delegated clearly by the primary legislation to rule further procedural detail or *secondly*, it is to accommodate discretion in response to public service in the context of conducting administrative power.[50] Secondary legislation is used to take the aim of primary legislation further. It is mainly aiming to introduce technical or detailed provisions necessary for the implementation of primary legislation or to introduce administrative arrangements necessary for primary legislation. Moreover, secondary legislation or administrative rules is not to introduce new law. Therefore, these instruments are undeniably inevitable to set up a strong national legal policy regarding data protection. The advantage of this administrative instrument is temporary. It may somehow fill the need to a more responsive rule to address sectoral problems as secondary legislation does not require to pass parliament deliberative. Thus, legislations even though provide maximum protection it necessarily agreed by legislators make it slower to take effect.

The idea to tie up data protection principles in a draft bill has been passed through the legislative process since 2016. The draft bill accommodated four purposes; to protect and to fulfil citizens' rights on data privacy; to ensure government, business and community organization provide good service for the public; to support the development of industries, technology, information and communication; also, to promote domestic industries competitiveness.[51] However, it has not yet take the law-maker attention to even list the bill on the national legislative priority program.

The legislative challenge regarding data protection in Indonesia is seemingly go to different directions. Euphoria of digitalized era does not emerge the need to protect private data but to bring out details publicly. Culturally, many people still communicate through digitalized media as honest as they do in actual relations, so they tend to open their private information through this communication without cautions. These groups of people put trust to the information provided by the media more than before which make them easily affected by hoaxes. In many cases there are attempts

[49] *Ibid*.

[50] Jimly Asshiddiqie, *Perihal Undang-Undang* (Rajawali Pers, 2010).

[51] Shinta Dewi, Nilai Komersial dalam Data Pribadi dan Konsep Perlindungannya, Makalah, 2015 cited in Anggara et al, Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia 2015, <http://icjr.or.id/data/wp-content/uploads/2015/11/paper-3-final-Menyeimbangkan-Hak.pdf> accessed on December 2016.

to use ambiguous tread as political commodities that benefits some groups.[52] Information technology experts have also underlined the danger of the massive dispersion of racial hoaxes to create chaos and horizontal conflict that apparently escalating public distrust to the government. This tension draw legislator attention to muffle the flame rather than to finish the task to legislate on the theme that emerge rights to privacy and the protection on the use of private data. This fact in turn influences the progress of the initiation of further legal framework for data protection in Indonesia.

Implementation of 'Bali Resolution' as well as Challenges and Obstacles in Biometric Data Collection, Storage and Sharing with Respect to Personal Data Protection

With respect to 'Bali Resolution' 2016, this study found that Bali Resolution 2016 has not been fully implemented to date. INTERPOL NCB for Indonesia is currently developing a system for sharing biometric data, and coordinating with government agencies, especially Immigration Agency and the relevant unit in Indonesia National Police, namely the Centre of Automatic Fingerprint Identification System (known as Pusinafis). To date, INTERPOL NCB for Indonesia has not had its own dedicated database system because the currently available system is only the biometric database system in the INP's Centre of Automatic Fingerprint Identification System (Pusinafis). Therefore, in relation to FTFs prevention and biometric data sharing, the current practice is that whenever there is a request from INTERPOL for data or information on terrorists involving Indonesian citizens, NCB Indonesia will coordinate with INP's Pusinafis, Densus 88 (Indonesian Special Forces Counter-Terrorism Squad), Directorate General of Immigration and the Ministry of Home Affairs to obtain biometric data (with the data shared being limited to names, photos and fingerprints) as comparative data.[53]

Each member country may have a biometric system with various purposes such as to reduce the cost of immigration services, reduce cases of identity fraud, prevent illegal immigrants and help counter terrorism. Generally, countries participating in 'Bali Resolution' have used (proposed to use) biometric recognition systems for various purposes, among others, travel-related purposes, immigration, citizen ID cards or national identification documents (passports, national identity cards, or both), criminal investigations, social security identification and disaster relief systems.

In the collection and storing processes which are then followed by the establishment of biometric databases, there are challenges frequently encountered in the efforts to protect the confidentiality of personal data[54] and there is an ethical aspect mainly related to some matters, such as who are authorized to access the data, the integrity of data contained in the central database system, data protection for third parties, discrimination issues, data storage restrictions and use of

[52] BBC Indonesia, 'Kasus Saracen: Pesan kebencian dan hoax di media social 'memang terorganisir', bbc (online) 24 August 2017 <http://www.bbc.com/indonesia/trensosial-41022914>.

[53] See the development of a pilot project on sharing intelligence INTERPOL, 'Terrorism intelligence shared via INTERPOL's Project Kalkan strengthens global 'early warning system'', Interpol (online) 10 July 2017 <https://www.interpol.int/News-and-media/News/2017/N2017-090>.

[54] Personal data constitute certain data of individuals that are stored and maintained, and the integrity and confidentiality of which is kept and protected.

data for crime prevention as well as its impact on privacy. At the international level, there are more significant challenges with respect to legal and privacy issues considering the fact that the impact on data protection and privacy can affect a far greater number of individuals compared to the number of individuals listed in the national database. In addition, not all countries are fully committed to privacy right protection as contained in a number of different treaties and agreements.

In this research, it was found that with respect to the use of biometrics to support the law enforcement process, and the efforts to fight against crimes and terrorism, the INP's Centre of Automatic Fingerprint Identification System (Pusinafis) plays a central role. Besides having its own biometric database, Pusinafis is also authorized to access data in the database center of Directorate General of Population and Civil Registration of the Ministry of Home Affairs. Demographic data that have been accessed from the data center of the Ministry of Home Affairs can be used to develop and can be added to the fingerprint database stored in the Pusinafis of INP's Criminal Investigation Agency.

Based on the Regulation of the Minister of Home Affairs No. 25 of 2011, access is only granted to data managers/operators who meet certain criteria, and the access is granted upon approval from the Minister/Governor/Regent/ Mayor only.[55] The data operators, managers and administrator are bound by the laws and professional codes of ethics. Therefore, each officer is required to act professionally when performing their duties and uphold the oath of office.[56] In respect of the data storage, biometric data that have been collected and stored in the database system of Pusinafis will be stored permanently or in other words there is no specific time frame or expiration period for the biometric data stored and there are no methods or rules for the deletion or change of data.[57]

When biometric data are collected (for example in the process of fingerprint recording), there are generally no mechanism or procedures or notification served to the bearers with respect to the use of their biometric data, as well as their rights and obligations over their recorded biometric data.[58] Generally, what these bearers know is that their biometric data collected in the process of making electronic Resident's ID Cards, e-Passports and Certificates of Police Record will be used only for administrative purposes.[59] So far, the biometric data stored in the database of Pusinafis by the law enforcement officers are only used as comparative data. There has not been any follow-up in the form data processing, for example big data processing for crime prediction or other types of data processing.[60] The data sharing agreement between the Directorate General of Population and Civil Registration of the Ministry of Home Affairs and the INP's Criminal Investigation Agency, has provided a clear framework with respect to the type of data to be shared and when the data sharing will be done.[61]

[55] See Articles 27-32, 36 of the Regulation of the Ministry of Home Affairs Number 25 of 2011.
[56] Interview with Nurul Tristiati, INP's Pusinafis, Jakarta, 16 August 2017
[57] *Ibid.*
[58] *Ibid.*
[59] *Ibid.*
[60] *Ibid.*
[61] See discussion point 3. Biometric Data Sharing at the National Level

However, there has not been any mechanism on data retention.[62]

The above discussion shows that in the collection, recording and storage of biometric data there are still a number of issues that indicate weaknesses in the protection of personal data, and there are indications of violations. This is mainly due to the fact that personal data protection is not clearly regulated or has not been formally regulated.

In general, there are at least a number of challenges in biometric data or information sharing, which among others include different regulations in each member country of ICPO-INTERPOL, ethical issues and unintegrated systems. In addition, a number of factors such as differences in standards, technical equipment, biometric technology capabilities possessed by each member country, as well as differences in policies and regulations in each member country primarily with respect to data protection and privacy, have become a particular challenge in the implementation of Bali Resolution.[63] In the efforts to identify, gather, store and share biometric information, there are certainly gaps from both in the technical and legal aspects.

Different regulations applied by each ICPO-INTERPOL member country, for example, privacy protection systems of member country data, including methods of access and correction to personal information held by government agencies seem to vary greatly. This data privacy protection system may also be operated within the framework of different regional and international privacy principles such as the United Nations Guidelines for the Regulation of Computerized Personal Data Files,[64] EU General Data Protection Regulation,[65] OECD Guidelines on the Protection of Privacy and Transborders Flows of Personal Data.[66] In addition, ICPO-INTERPOL member countries may also have international obligations including non-refoulment obligations under the Universal Declaration of Human Rights,[67] and where applicable, the Refugee Conventions,[68] the International Covenant on Civil and Political Rights,[69] Convention against Torture,[70] and the United Nations Convention against Transnational Organized Crime.[71]

---

[62] William C. Buhrow, *Biometrics in Support of Military Operations: Lessons from the Battlefield* (CRC Press Taylor & Francis Group, 2017).

[63] See note 9.

[64] Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 on 14 December 1990 <http://www.refworld.org/pdfid/3ddcafaac.pdf>.

[65] European Commission, 'Data protection Rules for the protection of personal data inside and outside the EU' <http://ec.europa.eu/justice/data-protection/index_en.htm>.

[66] OECD, 'The OECD Privacy Guidelines' <http://www.oecd.org/sti/ieconomy/49710223.pdf>

[67] Universal Declaration of Human Rights <http://www.un.org/en/universal-declaration-human-rights/>.

[68] The 1951 Convention Relating to the Status of Refugees; the 1967 Protocol Relating to the Status of Refugees; Resolution 2198 (XXI) adopted by the United Nations General Assembly available at <http://www.unhcr.org/protection/basic/3b66c2aa10/convention-protocol-relating-status-refugees.html>.

[69] International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx >.

[70] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, adopted and opened for signature, ratification and accession by General Assembly resolution 39/46 of 10 December 1984 entry into force 26 June 1987, in accordance with article 27 (1) <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CAT.aspx >.

[71] The United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, <

In addition to legal variables that may vary among member countries, there may also be an overlap among the multilateral mechanisms that have existed before the adoption of Bali Resolution, for example Eurodac (the EU's multinational biometric data sharing mechanism),[72] Five Country Conference (FCC),[73] INTERPOL I-24/7 communication system and Automated Fingerprint Identification System (AFIS),[74] Agreement on Information Exchange and Establishment of Communication among some ASEAN countries,[75] UNODC Voluntary Reporting System on Migrant Smuggling and Related Conduct (VRS-MSRC) as well as informal and ad-hoc arrangements among countries.[76]

Biometric data sharing agreements have been established through, among others, Five Countries Conference (FCC), which involved the United Kingdom, the United States, Canada, Australia and New Zealand.[77] These countries have agreed to share biometric data collected from visa applications, and other immigration-related data collected from prospective immigrants to be used to jointly combat illegal immigration under High Value Data Sharing (HVDS) Protocol.[78]

This data sharing primarily aims to enhance security and monitor criminal activities in FCC countries and to track suspected terrorists and criminals who are fleeing or intend to avoid legal action.[79] However, the request to share such biometric data must first meet certain requirements such as being able to provide evidence that the individual has traveled from an FCC country or has previously been arrested in one of the FCC countries before such can be submitted to another member country.[80]

Furthermore, it is important to note that no information is shared about the individual concerned unless there is a match of information in terms of the individual's fingerprint.[81] HVDS has also explained the important procedures each country should follow to ensure a safe information sharing process.[82] One of these guidelines instructs the FCC countries to safely delete the data that they have obtained within a certain period of time.[83] Furthermore, an example of biometric data sharing that has been conducted bilaterally is between the United Kingdom and Ireland through a Memorandum of Understanding to enhance their ability to detect illegal immigrants in common travel area within the jurisdiction of

https://www.unodc.org/unodc/en/treaties/CTOC/ >

[72] European Commission, 'Identification of applicants (EURODAC)' <https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en>.

[73] Home Office, 'Biometric data-sharing process (Five Country Conference (FCC) data-sharing process)' 2016, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557896/biometric-data-sharing-v7.0.pdf>

[74] note 24.

[75] Agreement on Information Exchange And Establishment of Communication Procedures <http://www.asean.org/storage/images/archive/17346.pdf>

[76] UNODC, Voluntary Reporting System on Migrant Smuggling and Related Conduct (VRS-MSRC): VRS-MSRC launched in 2013, UNODC (online) <https://www.unodc.org/southeastasiaandpacific/en/vrs-msrc.html; https://www.unodc.org/southeastasiaandpacific/en/2013/07/vrs-launch/story.html>.

[77] Home Office, 'Biometric data-sharing process (Five Country Conference (FCC) data-sharing process)' (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557896/biometric-data-sharing-v7.0.pdf

[78] *Ibid.*

[79] *Ibid.*

[80] *Ibid.*

[81] *Ibid.*

[82] *Ibid.*

[83] *Ibid.*

both countries and also the Isle of Man and the Channel Islands.[84] The MOU allows the UK and Ireland to share and exchange biometric data and information, which will be used to make immigration-related decisions.[85]

Particularly in the context of Indonesia, the most obvious obstacles and challenges are the lack of regulations on personal data protection, and the fact that the biometric data system is relatively new and the databases have not been fully developed, which may lead to possibilities of violations against personal data protection when Indonesia attempts to fulfill its obligations as a member country of ICPO-INTERPOL to share existing biometric data.

Technically speaking, the obstacles and challenges can be seen from the fact that the automatic fingerprint identification system is still centered in the INP's headquarters as the holder and manager of biometric databases to support the law enforcement throughout Indonesia. The Indonesia National Police's Centre of Automatic Fingerprint Identification System (Pusinafis) still has structural barriers in its organization (INP's internal bureaucracy). The structural barriers of this organization seemed to have weakened Pusinafis-related communications between INP's headquarters and police offices at the local level (Sectoral Police, Municipal/Regency Police, Provincial Police). For example, during the process of fingerprint recording through the process of producing Certificates of Police Record at the local police office (Sectoral Police, Municipal/Regency Police, Provincial Police), Pusinafis has no authority to directly direct or instruct local officers to promptly report or upload the recorded data to the central database of Pusinafis. As an illustration, if in a day there are 100 Certificates of Police Record applicants whose fingerprints are recorded at a Municipal/Regency Police, Pusinafis cannot control or ensure that all of the biometric data recorded on the same day are entirely reported or uploaded to the central database system (Pusinafis) by the officers who recorded the said fingerprints at the Municipal/Regency Police. In addition, the telecommunication network is still inadequate, especially in the Sectoral Police and Municipal/Regency Police levels. This is one of the barriers in the collection, recording, storage and sharing of biometric data.

IV. CONCLUSIONS AND SUGGESTIONS

Bali Resolution encourages each member country of ICPO-INTERPOL to systematically collect and store biometric information that is an integral part of the effort to share terrorist profile data that has been done through the ICPO-INTERPOL's channel. The focus of systematic collection and storage of biometric information is the unique identifiable attributes, which include fingerprints and DNA profiles.

In Indonesia, the collecting, recording and storing biometric data are through three doors or processes, i.e.: 1) the process of making electronic Resident's ID Cards under the coordination and supervision of the Ministry of Home Affairs (Directorate General of Population and Civil Registration); 2) the process of making e-Passports under the coordination and supervision of the Ministry of Law and

[84] Seamus Eagan, 'UK and Ireland to share biometric data to fight illegal immigration' Secure Id News (online) 20 December 2011 <https://www.secureidnews.com/news-item/uk-and-ireland-to-share-biometric-data-to-fight-illegal-immigration/>.

[85] *Ibid.*

Human Rights (Directorate General of Immigration); 3) the process of making Certificates of Police Records under the coordination and supervision of INP (Centre of Automatic Fingerprint Identification System of INP's Criminal Investigation Agency). Of the three doors, the largest amount of biometric data is collected through the making of Resident's ID Cards.

One of the functions of biometric data is to support law enforcement and crime prevention processes, as set forth in Article 58 paragraph 4 of Law No. 24 of 2013 on Amendment to Law Number 23 of 2006 on Population Administration, which regulates the utilization of the population data collected from electronic Resident's ID Cards. Thus, in accordance with the mandate of Law, the Ministry of Home Affairs and INP have signed a memorandum of understanding (MoU) on the utilization of electronic Resident's ID Card data. This agreement has provided a framework and guidelines for instituting biometric data sharing mechanisms between the two institutions to improve the effectiveness of law enforcement and crime prevention functions.

The scope of this cooperation covers the utilization of electronic Resident's ID Card data, National Identification Number (NIK) and Population Data. Through this cooperation, the Ministry of Home Affairs as the owner of the database basically grants authorization to INP to access the population data including fingerprint data, but this right to access is only granted to officers in charge as data managers in INP (in this case Pusinafis or INP's Centre of Automatic Fingerprint Identification System). Meanwhile, the passport biometric database system has not been fully developed, and thus, it has not been able to provide an optimum support in law enforcement and crime prevention processes since the old users' data have not been included in the biometric database.

With respect to the 2016 Bali Resolution, this study found that the 2016 Bali Resolution has not been fully implemented. NCB Indonesia is currently building a system related to biometric data sharing and coordinating with government agencies, especially Immigration Agency and the relevant unit in INP namely the Centre of Automatic Fingerprint Identification System (Pusinafis). To date, INTERPOL NCB for Indonesia has not had its own dedicated database system because the currently available system is only the biometric database system in the INP's Pusinafis. Therefore, in relation to a defense against FTFs and biometric data sharing, the current practice is that whenever there is a request from INTERPOL for data or information on terrorists involving Indonesian citizens, NCB Indonesia will coordinate with INP's Pusinafis, Densus 88 (Indonesian Special Forces Counter-Terrorism Squad), Directorate General of Immigration and the Ministry of Home Affairs to obtain biometric data (with the data shared being limited to names, photos and fingerprints) as comparative data.

In general, there are a number of challenges in biometric data or information sharing, which cover, among others a variety of regulations binding each member country of ICPO-INTERPOL, ethical issues and unintegrated systems. In addition, there are also other challenges such as differences in standards, technical equipment, biometric technology skills possessed by each member country, as well as differences in policies and regulations in each member country

primarily with respect to data protection and privacy.

In the biometric data collection, recording and exchange or sharing, there are indications of violations of personal data protection and privacy, owing to, among others lack of regulations on data retention, consent, processing, notification and disclosure mechanism. Meanwhile, the most obvious obstacles and challenges are the absence of regulations on personal data protection and privacy, in addition to the fact that the biometric data system is still relatively new and the database has not been fully developed. While discrimination is occurring when there is innacurate personalization that cause different treatment over biometric data owner, the result of this study found that the system has been not fully implemented, the potential threat over artificial agents should be noticed more by the authority to be diminished in the future in analysing and developing strategic plan against FTF.

This seems to have led to cases of violations when Indonesia attempts to fulfill its obligations as a member country of ICPO-INTERPOL to share existing biometric data. Therefore, laws and regulations related to the personal data protection becomes an urgent need to be addressed immediately.

The INP's Centre of Automatic Fingerprint Identification System (Pusinafis) has a central role as a holder and manager of biometric databases to support law enforcement throughout Indonesia. Thus, INP needs to improve the efficiency of its internal bureaucracy efficiency to facilitate the work of Pusinafis in the process of recording, storing and utilizing biometric data.

The biometric data recorded, collected and stored are big data, but to date, in the law enforcement and crime prevention processes, these big data are only used as comparative data. In fact, the big data have a great potential to be processed and analyzed, such as to support crime prediction analysis. However, the innovation ethics, in this case the protection of citizens' personal data remains of paramount importance and must be guaranteed by laws.

REFERENCES

Book

Asshiddiqie, Jimly, *Perihal Undang-Undang* (Rajawali Pers, 2010).

Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Toward Harmonized Data Protection Principles for Information Exchange at EU-Level* (Springer, 2012)

Buhrow, C. William, *Biometrics in Support of Military Operations: Lessons from the Battlefield* (CRC Press Taylor & Francis Group, 2017)

Gardner, A, Bryan, *Black's Law Dictionary* (West Group, 8th Ed, 2004)

Chalk, Peter, et.al, *The Evolving Terrorism in South East Asia* (RAND Corporation, 2009)

Chopra, Samir and Laurence White, *A Legal Theory for Autonomous Artificial Agents* (University of Michigan Press, 2011)

Deflem, Mathieu and Samantha Hauptman, 'Policing International Terrorism' in Francis Pakes (ed.), *Globalisation and the Challenge to Criminology* (Routledge, 2013)

Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer, 2013)

Kurbalija, Jovan, *An Introduction to Internet Governance* (Diplo Foundation, 6th ed, 2014)

Kumar, Ajay Zhang, David (Eds), *Ethics and Policy of Biometric* (Springer, 2010)

Ratcliffe, JH, *Intelligence-Led Policing* (Willan publishing, 2008)

Woodward, D, Jr, *Facing Up to Terrorism* (RAND Publication, 2001)

Yue Liu, Nancy, *Bio-Privacy: Privacy Regulations and the Challenge of Biometric* (Routledge, 2013)

Journal Articles

Crelinsten, Ronald, 'Perspectives on Counterterrorism: From Stovepipes to a Compehensive Approach' (2014) 1 *Perspectives on Terrorism* 8

Eichensehr, E. Kristen, 'The Cyber-Law of Nations' (2014) 103 *The Georgeton Law Journal* 317.

Hornung, Gerrit, Monika Desoi and Mattihias Pocs, 'Biometric System in Future Scenarios—Legal Issues and Challenges' (2016) Protection of Privacy in Biometric Data, IEEE Access

Hilbert, Martin, 'Big Data for Development: A Review of Promises and Challenges' (2016) 1 *Development Policy Review* 34

Liu, Yue, 'Identifying Legal Concerns in the Biometric Context' (2008) 1 Journal of International Commercial Law and Technology 3

Madensen, D, Tamara, 'Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective' (2007) 1 Policing: An International Journal of Police Strategies & Management 30

Morris R, Victor, 'Identity and Biometrics Enabled Intelligence (BEI) Sharing for Transnational Threat Actors' (2016) Small Wars Journal

Pan, Sheri, B, 'Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze' (2016) 1 *Harvard Law Journal & Technology* 30

Tene, Omer and Polonetsky, Jules, Big Data for All: Privacy and User Control in the Age of Analytics (2013) *Northwestern Journal of Technology and Intellectual Property* 239

Rahmaniar, Mirna , Lucky Endrawati and Milda Istiqomah, 'Analisis Yuridis Data Kependudukan Kartu Tanda Penduduk Elektronik Untuk Penyidikan Tindak Pidana (Juridical Analysis of Population Data on Electronic Identity Cards for Criminal Investigation)' (2014) Jurnal Hukum Fakultas Hukum Unversitas Brawijaya <http://hukum.studentjournal.ub.ac.id/index.php/hukum/issue/view/31>

Website

European Commission, 'Data protection Rules for the protection of personal data inside and outside the EU' <http://ec.europa.eu/justice/data-protection/index_en.htm>

European Commission, 'Identification of applicants (EURODAC)' <https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en>

Fromkin,M, *Lesson learned too well: The Evolution of Internet Regulation*, cdt (online) <https://cdt.org/blog/lessons-

learned-too-well-the-evolution-of-internet-regulation/>

GDPR, 'GDPR Key Changes',eugdpr (online) <https://www.eugdpr.org/>

INTERPOL, '*Foreign Terrorist Fighters,*' <https://www.INTERPOL.int/Crime-areas/Terrorism/Foreign-terrorist-fighters>

INTERPOL, 'Practical Guidelines: Sharing Information with Law Enforcement,' < file:///C:/Users/parip/Downloads/Practical%20Guidelines%20for%20sharing%20Information%20with%20Law%20Enforcement%20v2017.pdf>

INTERPOL, '*Data Exchange*' <https://www.interpol.int/INTERPOL-expertise/Data-exchange>

INTERPOL, '*Databases*' <https://www.interpol.int/INTERPOL-expertise/Databases>

Kementerian Dalam Negeri RI, 'Apa dan Mengapa E-KTP (What e-ID Cards Are and Reasons (for their use))', e-ktp (online), 20 June 2011 <http://www.e-ktp.com/2011/06/hello-world/>

Reports

'Roundtable on Biometric Data Sharing for Identity Verification: Introduction To The Regional Data Sharing Initiative,' Baliprocess.net (online), October 2014 <http://www.baliprocess.net/UserFiles/baliprocess/File/Discussion%20Paper%20on%20Biometric%20Data%20Sharing.pdf>

OECD, 'The OECD Privacy Guidelines' <http://www.oecd.org/sti/ieconomy/49710223.pdf>

Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 on 14 December 1990 <http://www.refworld.org/pdfid/3ddcafaac.pdf>

Home Office, 'Biometric data-sharing process (Five Country Conference (FCC) data-sharing process)' 2016, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557896/biometric-data-sharing-v7.0.pdf>

Agreement on Information Exchange And Establishment of Communication Procedures <http://www.asean.org/storage/images/archive/17346.pdf>

European Union Committee, 'House of Lords European Union Committee Europol: Coordinating the Fight Against Serious and Organised Crime : Report with Evidence', 29th Report of Session 2007–08, < https://publications.parliament.uk/pa/ld200708/ldselect/ldeucom/183/183.pdf>

Buskey, Carlos, Delano, *How Face Recognition Will Be Used to Counter Terrorism*, Biometrics Report (2001), http://csis.pace.edu/ctappert/dps/d860-01/options/carlos.pdf >

Conference Paper

Boyd, Dana and Kate Crawford, 'Six Provocations for Big Data: A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society' (2011). <https://ssrn.com/abstract=1926431> or <http://dx.doi.org/10.2139/ssrn.1926431>

Sherman, Darcie, 'Biometric Technology: the Impact on Privacy', *Comparative Research in Law & Political Economy* (2005) 1 (1)CLPE Research Paper.

Hansen M, Raguse M. and Storf K., Zwingelberg H. (2010) Delegation for

Privacy Management from Womb to Tomb – A European Perspective in Bezzi M., Duquenoy P., Fischer-Hübner S., Hansen M., Zhang G. (eds) *Privacy and Identity Management for Life Privacy and Identity* (IFIP Advances in Information and Communication, 2009)

Shinta Dewi, Nilai Komersial dalam Data Pribadi dan Konsep Perlindungannya, Makalah, 2015 cited in Anggara et al, Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia 2015, <http://icjr.or.id /data/wp-ontent/uploads/2015/11/paper-3-final-Menyeimbangkan-Hak.pdf>

International Treaties And Legislations

Universal Declaration of Human Rights <http://www.un.org/en/universal-declaration-human-rights/>.

The 1951 Convention Relating to the Status of Refugees; the 1967 Protocol Relating to the Status of Refugees; Resolution 2198 (XXI) adopted by the United Nations General Assembly available at <http://www.unhcr.org/protection/basic/3b66c2aa10/convention-protocol-relating-status-refugees.html>

International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49 <http://www.ohchr.org/en /professionalinterest/pages/ccpr.aspx>

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, adopted and opened for signature, ratification and accession by General Assembly resolution 39/46 of 10 December 1984 entry into force 26 June 1987 <http://www.ohchr.org/EN /ProfessionalInterest/Pages/CAT.aspx >.

The United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, < https://www.unodc.org/unodc/en/treaties/CTOC/ >

Newspaper

Bramantoro, Toni, 'Koordinasi Antar Negara Adalah Kunci Untuk Mencegah Aksi Foreign Terrorist Fighter', Tribunnews (online), 11 August 2016 <https://www.tribunnews.com/nasional/2016/08/11/koordinasi-antar-negara-kunci-untuk-mencegah-foreign-terrorist-fighter>

Lee, Justin, 'INTERPOL says Lack of Biometric Data on Terrorists a Security Vulnebaribility', Biometricupdate (online), 10 November 2016 <http://www.biometricupdate.com/201611/INTERPOL-says-lack-of-biometric-data-on-terrorists-a-security-vulnerability

Paripurna, Amira, 'Time to Improve Info Sharing and Law,' Jakarta Post (online) 28 January 2016 < http://www.thejakartapost.com/news/2016/01/28/time-improve-info-sharing-and-law.html >

Saifulloh, Muhammad, 'BNPT Pimpin Negara ASEAN Bahas Foreign Terrorist Fighter', Okezone (online), 11 August 2016, <http://news.okezone.com/read /2016/08/11/337/1460830/bnpt-

pimpin-negara-asean-bahas-foreign-terrorist-fighter>

BBC Indonesia, 'Kasus Saracen: Pesan kebencian dan hoax di media social 'memang terorganisir', BBC (online) 24 August 2017 <http://www.bbc.com/indonesia/trensosial-41022914>

National Legsilations

Undang-undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Tambahan Lembaran Negara Republik Indonesia Nomor 4674)

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Tambahan Lembaran Negara Republik Indonesia Nomor 4843)

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Tambahan Lembaran Negara Republik Indonesia Nomor 5952)

Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Tambahan Lembaran Negara Republik Indonesia Nomor 4846)

Peraturan Pemerintah No 82 Tahun 2012 tentang Penyelenggaran Sistem Transaksi Elektronik (Tambahan Lembaran Negara Republik Indonesia Nomor 5348)