JURNAL HUKUM "DE'RECHTSSTAAT"
DIKELOLA OLEH FAKULTAS HUKUM UNIVERSITAS DJUANDA BOGOR P-ISSN 2549-9874 E-ISSN 2442-5303
jurnal.hukum@unida.ac.id

"Effectiveness Of The Ministry Of Communication And Information In Handling The Misuse Of Personal Data"

Ira Riswanih[1], Nurwati[2], M. Rendi Aridhayandi[3]

[1]Faculty Of Law, Djuanda University, Indonesia
[2]Faculty Of Law, Djuanda University, Indonesia
[3]Faculty Of Law, Djuanda University, Indonesia

Special Issue
(February, 2025)
e-ISSN 2716-5191

ARTICLE INFO

Article history:
Received: 22 Januari 2025
Revised version received: 12 Februari 2025
Accepted: 28 Februari 2025
Available online: 28 Februari 2025

Keywords:
cyber crime, Remove cyber crime, Personal Data, Cyber Security, Government

How to Cite:
Ira Riswanih, Nurwati, M. Rendi Aridhayandi. 2025. "Effectiveness Of The Ministry Of Communication And Information In Handling The Misuse Of Personal Data" *Jurnal Hukum DE'RECHTSSTAAT*

Corresponding Author:
Name: Ira Riswanih
Email: Irariswanih@gmail.com

ABSTRAK

Kementerian Komunikasi dan Informatika (KOMINFO) memiliki peran penting dalam penanganan fenomena kejahatan dunia maya, khususnya penyalahgunaan data pribadi. Total dugaan kasus pelanggaran perlindungan data pribadi sejak tahun 2019 hingga 14 Mei 2024 mencapai 124 kasus. Pelanggaran terbanyak adalah kebocoran data, yakni sebanyak 111 kasus. Tujuan dari penelitian ini adalah untuk mengetahui seberapa efektif Kementerian Komunikasi dan Informatika dalam menangani tindak pidana siber terkait penyalahgunaan data pribadi. Penelitian ini menggunakan pendekatan hukum normatif. Penelitian ini berfokus pada analisis peraturan perundang-undangan terkait UU ITE dan UU PDP. Penelitian ini menunjukkan temuan bahwa terdapat kesenjangan yang cukup parah yang dapat dialami oleh Kementerian Komunikasi dan Informatika dalam menjalankan uraian tugas terkait perlindungan data pribadi. Kesenjangan tersebut tidak hanya berasal dari luar tetapi juga dari dalam Kementerian Komunikasi dan Informatika itu sendiri. Sehingga apabila gap tersebut tidak segera ditutup dan diperbaiki, maka akan berdampak pada program-program Kementerian Komunikasi dan Informatika, lembaga lain, maupun masyarakat luas. Fokus penelitian ini akan dibatasi pada banyaknya perubahan yang terjadi di Kementerian Komunikasi dan Informatika itu sendiri. Penelitian ini relevan dengan konteks hukum dan kebijakan, khususnya terkait dengan perlindungan data pribadi. Dengan menganalisis kebijakan perlindungan data pribadi ini, diharapkan dapat memberikan masukan yang bermanfaat bagi para pembuat kebijakan, khususnya bagi Kementerian

Komunikasi dan Informatika dalam memperbaiki gap-gap yang terjadi sebelumnya agar tidak terjadi lagi di kemudian hari.

ABSTRACT

The Ministry of Communication and Informatics (KOMINFO) has an important role in handling the phenomenon of cybercrime, especially misuse of personal data. The total number of alleged cases of violations of personal data protection from 2019 to May 14, 2024 reached 124 cases. The most violations were data leaks, which were 111 cases. The purpose of this study is to determine how effective the Ministry of Communication and Informatics is in handling cybercrimes related to misuse of personal data. This study uses a normative legal approach. This study focuses on the analysis of laws and regulations related to the ITE Law and the PDP Law. This study shows findings that there is a fairly severe gap that can be experienced by the Ministry of Communication and Informatics in carrying out the job description related to personal data protection. This gap does not only come from outside but also from within the Ministry of Communication and Informatics itself. So if this gap is not immediately closed and fixed, it will have an impact on the programs of the Ministry of Communication and Informatics, other institutions, and the wider community. The focus of this study will be limited to the many changes that have occurred in the Ministry of Communication and Informatics itself. This research is relevant to the legal and policy context, especially related to personal data protection. By analyzing this personal data protection policy, it is expected to provide useful input for policy makers, especially for the Ministry of Communication and Informatics in fixing the gaps that occurred previously so that they do not happen again in the future.

1. Introduction

Recently, there was a phenomenon of cybercrime related to the misuse of personal data of the public experienced by a state institution, namely the Ministry of Communication and Informatics (KOMINFO), because of this phenomenon, several activities in other institutions experienced delays in their work processes, and the public was also affected.

In the increasingly advanced digital era, personal data protection is one of the most influential forms of cybercrime. The Ministry of Communication and Informatics (KOMINFO) has an important role in dealing with cybercrime.[1] In addition, globalization and the development of information technology have accelerated the emergence of cybercrime, which makes handling this problem increasingly complex. Regarding law and social engineering, law can function to control society and can also be a means to make changes in society. the argument that is always put forward is that society is always changing, nothing is static.[2] So that the PDP Law and the ITE Law were formed because of an urgent need for society, the nation and the Republic of Indonesia today and in the future so that they can be competitive in the global era.[3]

[1] http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/63). Diakses pada tanggal 25 November 2024
[2] Dwidja Priyatno, M. Rendi Aridhayandi, Jurnal Mimbar Justitia, Vol. II No. 02 Edisi Juli-Desember 2016, Hlm 886
[3] Nurwati,, Hukum Teknologi Informasi dan Komunikasi, KBM Indonesia. 2024. Hlm 5.

However, global threats, technological advances and information are not only aimed at attacking government agencies and the military. However, it can also threaten all aspects of human life, such as the economy, politics, culture, and security of a country.[4] According to data from the Ministry of Communication and Information, the number of cases of alleged violations of personal data protection handled tends to increase. The total number of cases of alleged violations of personal data protection from 2019 to May 14, 2024 reached 124 cases. Of the 124 cases, the majority of the types of violations were in the form of personal data leaks, namely 111 cases.[5] Banyak kasus kriminal yang terjadi di daerah Jabodetabek dengan beragam jenis, diantaranya pembunuhan, pemerkosaan, perampokan, pembegalan, pengeroyokan, pencurian, copet, sampai pada yang paling ringan seperti bully. Sebagaimana diungkapan oleh Polda Metro Jaya bahwa terdapat kurang labih 199 kasus yang terjadi Terdapat 199 kasus kejahatan jalanan di wilayah DKI Jakarta, Depok, Tangerang, Tangerang Selatan, dan Bekasi dalam kurun waktu sebulan terakhir,[6] Kondisi ini menunjukkan bahwa tingkat kejahatan di Jabodetabek masih sangat banyak, sehingga harus ada upaya untuk mencegah atau meminimalisir dan menekan angka kriminal.

Meskipun sudah ada regulasi dan aparat kepolisian yang bertugas menjaga keamanan dan keteriban, namun gangguan terhadap keamanan dan ketertiban terus terjadi. terlebih lagi dengan semakin meningkatnya kualitas serta kuantitas kejahatan saat ini.[7] Maka perlu adanya peran pemerintah daerah dalam menyukapi persoalan hukum yang selalu terjadi. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.[8]

Recently, a cyber attack also occurred on the government's telecommunications industry website. This indicates the government's unpreparedness, either in managing large amounts of data or facing a cyber crisis. According to the head of the National Cyber and Crypto Agency "(BSSN), the PDN server was hit by a ransomware attack that locked important data and could not be accessed, the main problem is governance and data not being backed up by KEKOMINFO, and only 2% of data in the Temporary National Data Center (PDNS) is backed up by KEKOMINFO. This statement raises a big question mark as to why the ministry level does not have adequate data backup and security. Not only that, but other questions about institutional relations between ministries also become new questions.

Based on the research background above, the main research problems are as follows:

1. How is the level of effectiveness of the Ministry of Communication and Informatics (KOMINFO) in protecting personal data?
2. How is the institutional relationship between the Ministry of Communication and Information (KOMINFO) and other institutions?

---

[4] Ineu Rahmawati, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense, Jurnal Pertahanan dan Bela Negara, Volume 7 No. 2, Agustus 2017, Hlm. 52.

[5] https://www.kompas.id/baca/ekonomi/2024/06/03/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024 diakses tanggal 25 November 2024

[6] (Https://Megapolitan.Kompas.Com/Read/2023/02/16/18212261/Polda-Metro-Jaya-Ungkap-199-Kasus-Begal-Hingga-Pencurian-Di-Jakarta-Dan)

[7] Karimah Tauhid And ; | Gautama, "Analisis Hukum Dampak Peresmian Daerah Otonomi Baru (DOB) Dalam Penanggulangan Kelompok Kriminal Bersenjata (KKB) Guna Mewujudkan Kamtibmas Di Papua," Vol. 3, 2024.

[8] M Rendi Aridhayandi, "PERAN PEMERINTAH DAERAH TERHADAP KETERSEDIAAN AIR MINUM UNTUK KONSUMEN MELALUI PERUSAHAAN DAERAH AIR MINUM," Vol. 3, 2024.

2. Method

This study uses a normative legal approach, namely law is understood as a norm, rule, principle or dogma, a normative legal approach is also called a doctrinal approach or normative legal research. This study focuses on the analysis of laws and regulations related to the ITE Law and the PDP Law. This analysis also focuses on the role of the Ministry of Communication and Information in protecting people's personal data. This type of normative research uses qualitative analysis, namely by analyzing data in the form of concepts, opinions, and opinions obtained from library research, then processed, generalized, and analyzed to answer the problem, then conclusions are drawn regarding the effectiveness of the Ministry of Communication and Information (KOMINFO) in handling cybercrime related to misuse of personal data.

3. Results and Discussion

3.1. Effectiveness Of The Ministry Of Communication And Information (KOMINFO) In Personal Data Protection

In today's digital era, there are many crimes that exploit personal data so it needs to be protected. Weak data protection in Indonesia has resulted in rampant data leaks. This is evidenced by the frequent occurrence of cybercrime cases, such as hacking and social media break-ins that lead to personal data violations, extortion, and online fraud. Even hacking cases occurred at the Ministry of Communication and Information. The government is aware of the need for a number of regulations on personal data protection. In fact, there are already a number of personal data protection regulations that have been formed by the government, one of which is Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), but so far it has not been optimal in terms of its implementation.

In this case, the Ministry of Communication and Information (Kominfo) has taken steps to address cybercrime and personal data violations, including cases of data leaks that occurred at the National Data Center. The following is an assessment of the effectiveness of the Ministry of Communication and Information (KOMINFO) in addressing this problem:

1. Response to Data Breach Incidents :
    a) Response Speed: The Ministry of Communication and Informatics has demonstrated a rapid response to data breach incidents, including conducting investigations and blocking access to sites that disseminate leaked data.
    b) Transparency: The Ministry strives to provide clear information to the public regarding the steps taken following an incident, although this information is sometimes considered inadequate.
2. Policy and Regulation
    a) Implementation of Regulations: The Ministry of Communication and Informatics has issued regulations related to personal data protection, such as the Personal Data Protection Law. However, implementation and enforcement remain challenges.

b) Development of Cybersecurity Policy: The Ministry has attempted to develop a cybersecurity policy, but there needs to be more emphasis on implementing and monitoring the policy.

3. Security Infrastructure
   a) Investment in Technology: Despite efforts to improve security infrastructure, data breach cases show that there are still weaknesses in the system that need to be fixed.
   b) Security Audits and Assessments: The Ministry needs to conduct regular security audits to identify and address potential security gaps.

4. Education and Awareness
   a) Training Programs: The Ministry of Communication and Information needs to improve cyber training and awareness programs for employees and the public to prevent misuse of personal data.
   b) Public Awareness Campaigns: Increase campaigns to raise public awareness about the importance of personal data protection and how to protect their information.
5. Collaboration with Other Parties
   a) Collaboration with Law Enforcement: The Ministry needs to strengthen cooperation with law enforcement agencies and the private sector to deal with cybercrime more effectively.
   b) Participation in International Forums: Participate in international forums on cybersecurity to share knowledge and best practices.

From several assessments that have been presented, many efforts have been made by the Ministry of Communication and Informatics, but these efforts are still not optimal due to several factors. and there are still several things that need to be improved and maximized.

3.2. The Institutional Relationship Between The Ministry Of Communication And Information (KOMINFO) And Other Institutions

The Ministry of Communication and Informatics (KOMINFO) has institutional relations with various institutions, both at the national and regional levels. The following are some institutions that have institutional relations with KOMINFO:

1. Ministries and State Institutions

   KOMINFO coordinates with various ministries and state institutions, including:
   a) Ministry of Education and Culture: In the development of information technology for education.
   b) Ministry of Home Affairs: For the management of information and communication at the regional government level.
   c) Ministry of Law and Human Rights: In terms of regulation and law enforcement related to communication and information.
2. Public Relations Coordination Agency (Bakohumas)

Bakohumas is a non-structural institution that functions as a forum for coordination and cooperation between units in ministries and government institutions in the field of public relations.

3. Law Enforcement Institutions

   KOMINFO collaborates with law enforcement agencies such as:

   a) Polri: In handling cybercrime and violations of the law in cyberspace.
   b) Prosecutor's Office: For law enforcement related to violations in the field of communication and informatics.

4. Research and Development Agency

   KOMINFO collaborates with research institutions such as:

   Information and Communication Technology Research and Development Agency (BPPTIK) In developing technology and innovation in the field of communication and informatics.

5. Regional Government

   KOMINFO establishes relationships with regional governments to:

   a) Policy Implementation: Implement communication and informatics policies that are in accordance with regional needs.
   b) Infrastructure Development: Improve communication infrastructure in the regions.

6. Non-Governmental Organizations (NGOs)

   KOMINFO collaborates with NGOs to:

   a) Increasing Public Awareness: Increasing public awareness of the importance of good communication and information.
   b) Public Participation: Encouraging public participation in developing communication and informatics policies.

With these institutional relations, more or less everything that happens in the Ministry of Communication and Informatics will have an impact on other institutions, and vice versa. It is hoped that these institutional relations will remain harmonious so that the expected synergy can run optimally.

4. Conclusion

The Ministry of Communication and Informatics (KOMINFO) has taken significant steps to address the challenges of cybercrime and data breaches. However, the effectiveness of these efforts can still be improved through several key strategies, including strengthening more comprehensive regulations, increasing investment in cybersecurity infrastructure, and developing broader education and awareness programs among the public.

The data breach case that occurred at the National Data Center highlights the need for a more proactive and collaborative approach between KOMINFO, the private sector, and civil society. Protecting personal data is not only the responsibility of the government, but is a

collective challenge that requires commitment and cooperation from all parties. The Ministry of Communication and Informatics (KOMINFO) plays a strategic role through broad and multidimensional institutional relationships with various entities, including ministries, law enforcement agencies, local governments, and community organizations. This collaboration not only strengthens synergy in developing communication and informatics policies, but also increases responsiveness to the challenges and dynamics that arise in the digital era. Through effective collaboration, KOMINFO can ensure more adaptive and inclusive policy implementation, and encourage active community participation in the decision-making process. Thus, this institutional relationship is key to achieving effectiveness and sustainability in the management of communications and informatics in Indonesia, while maintaining the security and protection of people's personal data

References

Dwidja Priyatno, M. Rendi Aridhayandi, Jurnal Mimbar Justitia, Vol. II No. 02 Edisi Juli-Desember 2016.

Gautama, "Analisis Hukum Dampak Peresmian Daerah Otonomi Baru (DOB) Dalam Penanggulangan Kelompok Kriminal Bersenjata (KKB) Guna Mewujudkan Kamtibmas Di Papua," Vol. 3, 2024

Ineu Rahmawati, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense, Jurnal Pertahanan dan Bela Negara, Volume 7 No. 2, Agustus 2017.

M Rendi Aridhayandi, "PERAN PEMERINTAH DAERAH TERHADAP KETERSEDIAAN AIR MINUM UNTUK KONSUMEN MELALUI PERUSAHAAN DAERAH AIR MINUM," Vol. 3, 2024.

Nurwati, Hukum Teknologi Informasi dan Komunikasi, KBM Indonesia. 2024.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/63). Diakses pada tanggal 25 November 2024.

https://www.kompas.id/baca/ekonomi/2024/06/03/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024 diakses tanggal 25 November 2024.