EXPLORE
Jurnal Sistem Informasi dan Telematika
(Telekomunikasi, Multimedia dan Informatika)

# Analisis Kepatuhan Keamanan Aplikasi E-Goverment Tingkat Daerah sebagai Penunjang New Normal

**Sarah Ahya Khairunisa, Ana Mardiyah, Eva Agustine, Nur Aini Rakhmawati**
Jurusan Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Jawa Timur, Indonesia
srhahyanisa@gmail.com, anamardiyah@gmail.com, evaagustine11@gmail.com, nur.aini@is.its.ac.id

**Abstract-** The era of *e-government* demands that Regional Governments develop internet-based systems and applications, especially during the COVID-19 pandemic which limits the movement of the citizen, it requires many applications that can connect the government and society. Several applications were developed to provide actual data on COVID-19 in each region, as well as to help people adapt to new habits in the pandemic, such as health applications, e-attendance, e-market, and e-library. In this paper, an analysis of the security feasibility of regional *e-government* applications will be carried out by correlating the number of downloads and ratings with application security, elaborating application access and its compliance with UU ITE, and evaluating the compliance of privacy policies with Google policies. From observations made on 20 sample applications, it was found that all of them have dangerous permissions, but 55% of them have not followed the privacy policy regulated by Google. Another finding is that all application samples have met the provisions of the UU ITE Article 26 paragraph 1 regarding the approval of requests for personal data, and the number of downloads and ratings cannot be used as benchmarks in assessing application security.

**Keywords: Covid-19, Privacy Policy, Regional Government Applications, Security**

**Abstrak-** Era *e-government* menuntut Pemerintah Daerah untuk mengembangkan sistem dan aplikasi yang berbasis internet, terutama disaat pandemi COVID-19 yang membatasi ruang gerak masyarakat dibutuhkan banyak aplikasi yang dapat menjembatani pemerintah dan masyarakat. Beberapa aplikasi dikembangkan untuk memberikan data aktual COVID-19 di setiap daerah, serta membantu masyarakat untuk beradaptasi pada kebiasaan baru di pandemi, seperti aplikasi kesehatan, e-attendance, e-market, dan e-library. Pada penelitian ini akan dilakukan analisis kelayakan keamanan aplikasi *e-government* tingkat daerah dengan menghubungkan jumlah unduhan dan rating dengan level perlindungan izin aplikasi, menjabarkan akses aplikasi dan kesesuaiannya dengan UU ITE, serta mengevaluasi kesesuaian privacy policy dengan kebijakan Google. Dari observasi yang dilakukan pada 20 sampel aplikasi, didapati bahwa semua memiliki dangerous permissions, tetapi 55% diantaranya belum mengikuti kebijakan privacy policy yang diatur oleh Google. Penemuan lain yang didapatkan adalah bahwa semua sampel aplikasi telah sesuai dengan ketentuan UU ITE Pasal 26 ayat 1 mengenai persetujuan permintaan data pribadi, serta jumlah unduhan dan rating tidak bisa dijadikan tolok ukur dalam menilai keamanan aplikasi.

**Kata Kunci: Aplikasi Pemerintah Daerah, Covid-19, Keamanan, Privacy Policy**

## 1. Pendahuluan

Kinerja *e-government* di Indonesia jika dibandingkan dengan negara lain, ditambah pemahaman masyarakat Indonesia terhadap penggunaan ponsel pintar, memiliki potensi pertumbuhan yang masih luas. Survey [1] yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJ II) dan Badan Pusat Statistik (BPS) mengungkapkan jumlah pengguna Internet di Indonesia pada tahun 2019-2020 Q2 mencapai 196,71 juta orang, yang menunjukkan bahwa penetrasi pengguna internet di Indonesia mencapai 73,7% dari 266,91 juta jiwa penduduk Indonesia.

Artikel [2] menyatakan bahwa *e-government* memiliki tujuan yakni membuat interaksi yang terjadi antara pemerintah dengan masyarakat (G2C), pemerintah dengan industri bisnis (G2B), pemerintah dengan karyawannya (G2E), dan antar pemerintahan (G2G) semakin dekat, transparan, dan tidak membebani berbagai pihak dari segi material. Kemudian berdasarkan artikel [3] dijelaskan bahwa implementasi *e-government* terbagi

menjadi 4 (empat) fase, dimana masing-masing tidak harus dilakukan secara berurutan, namun tetap mengacu pada tujuan dari *e-government* sekaligus perkembangannya. Keempat jenis tersebut adalah *presence*, *interaction*, *transaction*, dan *transformation*. Salah satu fase yakni *transaction* diimplementasikan dalam bentuk aplikasi e-government.

Dalam implementasi aplikasi *e-government* tingkat daerah, terdapat peraturan yang harus diperhatikan, salah satunya perlindungan data pribadi pengguna pada UU No 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (ITE) Pasal 26. UU ITE Pasal 26 ayat 1 mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan pemilik data bersangkutan [4].

Kemudian dengan dilakukannya publikasi aplikasi *e-government* tingkat daerah di platform Google Play Store, masing-masing dari setiap aplikasi harus mematuhi Panduan *Privacy Policy* dari Google, dimana panduan ini menjelaskan ekspektasi minimum Google tentang apa yang harus disertakan dalam *Privacy Policy* setiap aplikasi [5]. *Privacy Policy* membantu pengguna memahami tindakan spesifik dari aplikasi yakni data yang aplikasi kumpulkan, alasan aplikasi mengumpulkannya, dan apa yang aplikasi lakukan dengan data tersebut.

*Privacy Policy* yang dibuat oleh para pengembang aplikasi, tidak terkecuali *e-government* tingkat daerah, harus mempertimbangkan semua cara agar pengguna dapat berinteraksi dengan layanan aplikasi, terutama dalam pengumpulan dan penggunaan data pengguna yang dimasukkan ke layanan aplikasi. Pertimbangan tersebut harus komprehensif, akurat, dan mudah dipahami oleh pengguna. *Privacy Policy* harus secara komprehensif dan akurat mengungkapkan semua praktik privasi aplikasi. Tindakan dan *Privacy Policy* juga harus mematuhi semua hukum dan peraturan yang berlaku, dan oleh karena itu setiap *e-government* perlu menyertakan informasi tambahan berdasarkan undang-undang dan peraturan yang berlaku [5].

Urgensi mengenai perlindungan data pribadi semakin tinggi terutama disaat pandemi COVID-19. Salah satu penelitian di UK [6] menunjukkan bahwa laporan kejahatan yang berhubungan dengan penipuan online meningkat selama pandemi COVID-19 ini. Aktivitas masyarakat yang berpindah dari offline ke online untuk mengantisipasi bahaya pandemi juga membuat peluang kejahatan online semakin besar.

Developer dapat menerapkan proteksi privasi data pengguna dengan memperhatikan beberapa hal pada saat mengembangkan aplikasi, yakni pada akses yang dibutuhkan oleh fitur yang dimiliki aplikasi. Suatu aplikasi harus meminta izin untuk mengakses data pribadi pengguna (seperti kontak dan SMS), serta fitur sistem tertentu (seperti kamera dan internet). Bergantung pada fiturnya, sistem mungkin memberikan izin secara otomatis atau mungkin meminta persetujuan pengguna untuk menyetujui permintaan.

Dalam aplikasi untuk android, izin dibagi menjadi beberapa tingkat perlindungan yang memengaruhi apakah aplikasi perlu melakukan permintaan izin kepada pengguna pada fitur tertentu [7]. Izin tersebut diantaranya Izin Normal *(Normal Permission)*, Izin Tanda Tangan (Signature Permission), dan Izin Berbahaya *(Dangerous Permission)*.

Dari aturan dan kebijakan yang telah disebutkan serta urgensi yang diberikan dari keadaan saat ini, telah ditegaskan bahwa keamanan data pribadi merupakan hal yang sangat penting, dan oleh karena itu untuk setiap produk atau jasa yang memerlukan data pribadi pengguna, terutama pada lingkup *e-government*, harus mengutamakan aspek persetujuan pengguna.

## 2. Dasar Teori

### A. Penelitian Terdahulu

Beberapa penelitian dan artikel terdahulu telah membahas topik seputar keamanan aplikasi e-government, salah satunya artikel [2] yang membahas pemodelan defense in depth untuk menganalisis data Sistem Database Pemasyarakatan. Defense in Depth sendiri adalah konsep keamanan teknologi informasi yang memerlukan penerapan lapisan keamanan untuk mempertahankan keamanan sistem informasi e-government. Pemodelan ini dapat mendeteksi serangan, melakukan respon terhadap serangan dan menyediakan lapisan pertahanan. Hasil yang diperoleh berupa evaluasi keamanan data pada SDP dengan menguraikan data menjadi enam lapisan sesuai dengan struktur model. Penulis artikel memberikan kesimpulan bahwa kerentanan keamanan suatu informasi, selain disebabkan karena faktor teknikalitas seperti lemahnya pengamanan fisik jaringan, juga disebabkan karena kurangnya security awareness dari sumber daya manusia. Selain itu, penelitian ini masih sebatas pada analisis keamanan database penyimpanan data, bukan pada aplikasi yang menggunakan informasi tersebut.

Terdapat artikel lain [8] yang melakukan penilaian untuk mengetahui tingkat reliabilitas dan konsistensi aplikasi dengan membandingkan konten pada aplikasi dengan variabel beserta indikator penilaiannya. Variabel tersebut kemudian diberi bobot (identitas lembaga, konten, fitur, partisipasi masyarakat, kegunaan, layanan, aktivitas media sosial, dan keamanan) agar dapat menghitung skor akhir. Berdasarkan hasil yang diperoleh pada penelitian, yakni bahwasannya kelayakan aplikasi dalam mendukung fasilitas layanan publik termasuk sangat baik, penulis menilai adanya beberapa hal yang luput dari penelitian, terutama dari sisi penilaian keamanan. Indikator penilaian di variabel keamanan terbilang terlalu umum, yakni hanya berfokus pada penggunaan username dan password, dan bobot yang diberikan di variabel keamanan juga termasuk sedikit, yakni hanya 5% dari keseluruhan.

### B. Tujuan Penelitian

Tujuan yang ingin dicapai dari pembuatan artikel ini dapat diuraikan dalam poin poin berikut:

1. Menganalisis aplikasi *e-government* Tingkat Daerah yang menunjang hidup masyarakat saat New Normal dari

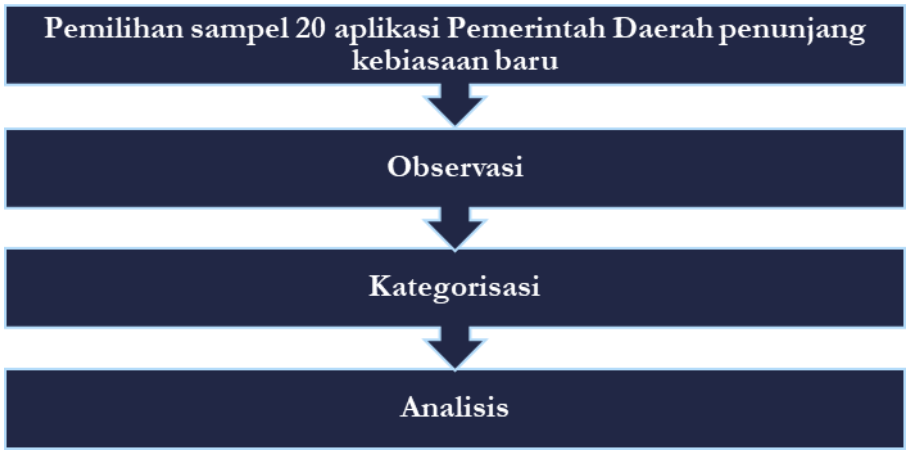
level perlindungan izin, data pribadi yang diminta oleh aplikasi, dan kesesuaiannya dengan UU ITE.
2. Menganalisis hubungan jumlah unduhan dan rating pada aplikasi *e-government* Tingkat Daerah yang menunjang hidup masyarakat saat New Normal dengan keamanan aplikasi.
3. Menganalisis kesesuaian *Privacy Policy* yang tercantum pada aplikasi *e-government* Tingkat Daerah yang menunjang hidup masyarakat saat New Normal dengan Kebijakan Google.

## 3. Metodologi

Metode utama yang dilakukan pada penelitian ini yakni dengan melakukan observasi data analitik pada sampel aplikasi *e-government* Tingkat Daerah untuk selanjutnya dilakukan kategorisasi dan analisis.

### A. Tahapan Pengerjaan

Dalam menjawab rumusan masalah yang diajukan, penulis melakukan beberapa langkah pengerjaan penelitian




**Gambar 1.** Tahapan Pengerjaan Penelitian

Penjelasan lebih detail mengenai masing-masing poin dalam Gambar 1 akan dijelaskan pada sub-bab selanjutnya.

### B. Pemilihan sampel 20 aplikasi Pemerintah Daerah penunjang New Normal

Pada saat melakukan penelitian, penulis tidak menemukan data yang memberikan jumlah konkrit aplikasi *e-government* di Indonesia. Oleh karena itu, penulis mengambil nilai populasi sebanyak 548 yang merupakan jumlah kalkulasi dari Kota, Kabupaten, dan Provinsi di Indonesia. Angka tersebut menjadi dasar dalam menghitung nilai sampel observasi dengan rumus *Slovin* [9]. Berikut adalah rumus *Slovin*.

$$n = \frac{N}{1 + Ne^2}$$

Nilai N adalah populasi (548), sementara nilai e atau *margin of error* yang penulis ambil sebesar 20%. Penulis melakukan perhitungan yang tertulis seperti di bawah ini:

$$n = \frac{548}{(1 + 548\ x\ 0.2^2)}$$
$$n = 23.9 = 24\ sampel$$

N = 548 ; e = 20% = 0.2

Berdasarkan perhitungan rumus *Slovian*, didapatkan sampel sebanyak 24. Namun, pada tanggal saat dilakukan observasi, ternyata tidak semua pemerintah daerah memiliki fasilitas yang mendukung untuk mengembangkan aplikasi *e-government* penunjang *new normal*. Oleh karena itu, penulis memutuskan untuk mengurangi sampel menjadi 20 aplikasi Android yang tersedia pada *Google Play Store*. Aplikasi-aplikasi tersebut tersebar pada berbagai bidang diantaranya kesehatan, *e-attendance,* penyedia data statistik COVID-19*, e-library* dan *e-market,* serta terhitung terakhir merilis *update* pada tahun 2019 sampai 2020. Pencarian aplikasi pada *Google Play Store* dengan memasukkan *keyword* beberapa nama daerah di Indonesia dan "COVID-19" secara acak pada *Google Play Store.*

### C. Observasi

Kemudian dilakukan observasi dengan mengidentifikasi poin-poin seperti nama *developer,* jumlah *download, rating,* akses, data pribadi yang diminta aplikasi dan keberadaan *Privacy Policy*. Berikut adalah daftar seluruh aplikasi Pemerintah Daerah yang akan dianalisis:

**Tabel 1** Daftar Aplikasi *E-government* Tingkat Daerah

| No | Nama Aplikasi | Jumlah Unduhan | *Rating* | *Developer* | Diakses pada |
|---|---|---|---|---|---|
| **1** | JAKI – Jakarta Kini | 500.000+ | 3,4 | Pemerintah Provinsi DKI Jakarta | Agustus 2020 |
| **2** | e-Health Surabaya | 100.000+ | 4,1 | eHealth Surabaya | Agustus 2020 |
| **3** | PIKOBAR Jawa Barat | 500.000+ | 4,2 | Pemerintah Provinsi Jawa Barat | Agustus 2020 |
| **4** | KMOB JABAR | 10.000+ | 1,9 | Pemerintah Provinsi Jawa Barat | Agustus 2020 |
| **5** | Ambulan Hebat Semarang | 1.000+ | 4,8 | Dinas Kesehatan Kota Semarang | Agustus 2020 |
| **6** | SI D'nOK – Dukcapil Kota Semarang | 10.000+ | 2,3 | Pemerintah Kota Semarang | Agustus 2020 |
| **7** | SiABA | 5.000+ | 3,7 | Diskominfo Kabupaten Magelang | September 2020 |
| **8** | Cek Presensi | 1.000+ | 4,8 | Pemkab Rembang | September 2020 |
| **9** | Presensi Sidoarjo | 5.000+ | 3,4 | Pemerintah Kabupaten Sidoarjo | September 2020 |
| **10** | e-Pasar Malang | 1.000+ | 5 | indieTown | September 2020 |
| **11** | e-Absensi | 1.000+ | 4,7 | Pemkab Pirang | September 2020 |
| **12** | E-PERPUS BANJARMASIN | 1.000+ | 4,4 | BKPSDM KAB. LUWU TIMUR | September 2020 |
| **13** | PaPa Sulbar | 1.000+ | 4,6 | Pemerintah Provinsi Sulawesi Barat | Agustus 2020 |
| **14** | E-Absensi ASN Sumut | 10.000+ | 4,2 | Diskominfo Sumatera Utara | September 2020 |
| **15** | Absensi ASN Langkat | 1.000+ | 4,5 | Diskominfo Kab. Langkat | September 2020 |
| **16** | Absensi Online Aceh | 5.000+ | 3.8 | Dinas Komunikasi Informatika dan Persandian Aceh | September 2020 |
| **17** | Absensi Online Sumbar | 5.000+ | 4.4 | Diskominfo Sumbar | September 2020 |
| **18** | Absensi Pemprov Bali | 1.000+ | 2.8 | Diskominfos Provinsi Bali | September 2020 |
| **19** | Absensi Sampang | 1.000+ | 3.6 | BKPSDM Kabupaten Sampang | September 2020 |
| **20** | iJogja | 10.000+ | 4,1 | DPAD Daerah Istimewa Yogyakarta | September 2020 |

Dari Tabel 1 dapat dilihat bahwa aplikasi Pemerintah Daerah yang menjadi sampel tersebar di pulau Jawa, Bali, Sulawesi, Kalimantan sampai Sumatera.

## D. Kategorisasi

Kategorisasi yang dimaksud pada Gambar 1 yakni kategorisasi terhadap akses izin yang diminta oleh aplikasi, berdasarkan pada level perlindungan izin Ada tiga tingkat perlindungan izin yang ditetapkan oleh

Google [7], yang pertama Izin Normal (Normal Permissions), di mana aplikasi perlu mengakses data atau sumber daya di luar sandbox aplikasi, tetapi hanya memberikan sedikit risiko terhadap privasi pengguna atau pengoperasian aplikasi lainnya. Kedua adalah Izin Tanda Tangan (Signature Permissions), dimana sistem memberikan izin aplikasi ini pada waktu penginstalan, tetapi hanya jika aplikasi yang mencoba menggunakan izin ditandatangani oleh sertifikat yang sama dengan aplikasi yang menetapkan izin tersebut. Ketiga adalah Izin Berbahaya (Dangerous Permissions), dimana aplikasi menginginkan data yang melibatkan informasi pribadi pengguna, atau berpotensi memengaruhi data yang disimpan pengguna atau pengoperasian aplikasi lainnya.

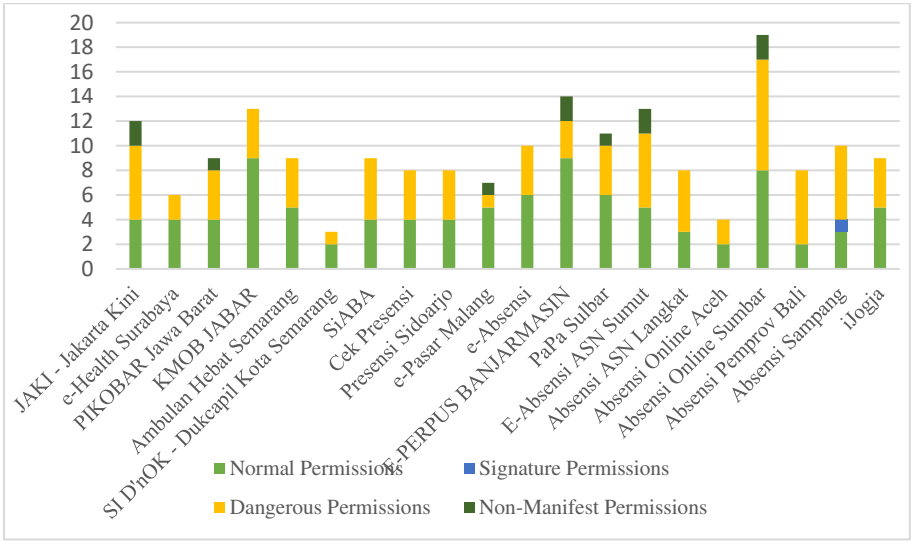
### E. Analisis

Setelah dilakukan kategorisasi, selanjutnya dilakukan analisis terhadap level perlindungan izin aplikasi daerah dan data pribadi yang diminta pada aplikasi, analisis hubungan hasil level perlindungan izin dengan jumlah unduhan dan rating serta regulasi hukum perlindungan data pribadi yang berlaku. Selain itu, juga dianalisis mengenai kepatuhan *Privacy Policy* aplikasi sampel.

## 4. Hasil dan Pembahasan

Pada bagian ini akan dipaparkan hasil observasi yang akan dianalisis kesesuaian dan hubungannya dengan regulasi hukum yang berlaku. Untuk analisis lebih detail dapat dilihat melalui Zenodo [10].

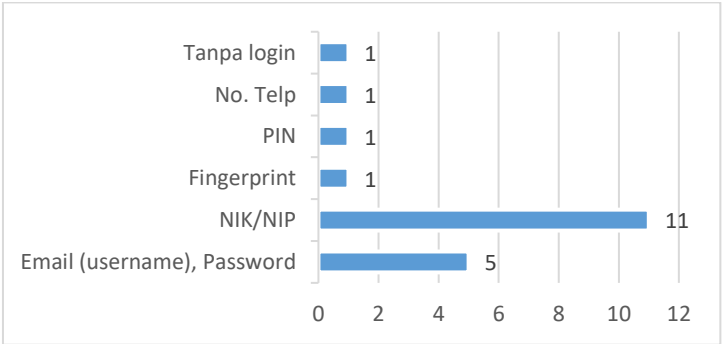
### A. Analisis level perlindungan izin dan data pribadi yang diminta oleh aplikasi Pemerintah Daerah




**Gambar 2.** Jumlah Level Perizinan Berdasarkan Setiap Aplikasi

Dari gambar 2. dapat diketahui 7 dari 20 aplikasi memiliki jumlah *dangerous permissions* yang lebih banyak dari permissions lainnya. Sisa dari aplikasi yang dianalisis memiliki jumlah *normal permisssions* lebih banyak serta *dangerous* dan *normal permissions* yang sama banyak. Sehingga, dapat disimpulkan bahwa seluruh sampel aplikasi memerlukan *dangerous permissions* yang meminta data pribadi pengguna.

Sementara itu, mekanisme validasi pengguna aplikasi dapat dilihat saat meminta pengguna untuk *login* atau *sign in*.




**Gambar 3.** Data untuk login pada seluruh aplikasi

Berdasarkan gambar 3. Dapat dilihat bahwa terdapat 13 aplikasi yang membutuhkan NIK, NIP, PIN, dan *Fingerprint* untuk melakukan login, aplikasi tersebut adalah aplikasi absensi dan kesehatan yang memerlukan data yang valid untuk menjadi bukti tentang keabsahan pengguna yang mengakses. Sementara 5 aplikasi yang membutuhkan *email* serta *password* merupakan aplikasi yang menyasar seluruh masyarakat seperti *e-library,* e-market, dan penyedia data COVID. Sehingga, dapat disimpulkan sebagian besar sampel aplikasi telah menerapkan mekanisme validasi pengguna yang kredibel.

### B. Analisis hubungan antara level perlindungan izin dengan jumlah unduhan dan rating

Dari hasil observasi dari segi jumlah unduhan, rating, dan jumlah level perizinan setiap aplikasi yang ditunjukkan pada tabel 2, diperoleh hasil yang beragam.

**Tabel 2** Perbandingan Jumlah Setiap Level Perizinan dengan Jumlah Unduhan

| Berdasarkan jumlah unduhan | *Normal* | *Signature* | *Dangerous* | *Non-Manifest* |
|---|---|---|---|---|
| **Tertinggi (500.000+)** | | | | |
| JAKI (Jakarta Kini) | 4 | 0 | 6 | 2 |
| PIKOBAR | 4 | 0 | 4 | 1 |
| **Terendah (1.000+)** | | | | |
| Ambulan Hebat Semarang | 5 | 0 | 4 | 0 |
| Cek Presensi | 4 | 0 | 4 | 0 |
| e-Pasar Malang | 5 | 0 | 1 | 1 |
| e-Absensi | 6 | 0 | 4 | 0 |
| e-Perpus Banjarmasin | 9 | 0 | 3 | 2 |
| PaPa Sulbar | 6 | 0 | 4 | 1 |
| Absensi ASN Langkat | 3 | 0 | 5 | 0 |
| Absensi Pemprov Bali | 2 | 0 | 6 | 0 |
| Absensi Sampang | 3 | 1 | 6 | 0 |

Setelah dilakukan analisis hubungan jumlah unduhan dengan tingkat keamanan suatu aplikasi, yakni dari jumlah setiap level perizinan pada setiap aplikasi, ditemukan bahwa jumlah unduhan **tidak bisa dijadikan tolok ukur** dalam menilai tingkat keamanan suatu aplikasi karena tidak ditemukannya kecenderungan pola. Seperti pada tabel 2. aplikasi dengan jumlah unduhan tertinggi dan terendah seperti JAKI dan Absensi Sampang memiliki jumlah level perizinan berbahaya yang sama sebanyak 6.

Kemudian, berikut adalah jumlah level perizinan pada aplikasi yang memiliki rating tertinggi dan terendah.

**Tabel 3** Perbandingan Jumlah Setiap Level Perizinan dengan Nilai Rating Tertinggi dan Terendah

| Berdasarkan nilai rating | *Normal* | *Signature* | *Dangerous* | *Non-Manifest* |
|---|---|---|---|---|
| **Tertinggi (5.0)** | | | | |
| e-Pasar Malang | 5 | 0 | 1 | 1 |
| **Terendah (1.9)** | | | | |
| KMOB Jabar | 9 | 0 | 4 | 0 |

Setelah dilakukan analisis hubungan nilai rating dengan tingkat keamanan suatu aplikasi, yakni dari jumlah setiap level perizinan pada setiap aplikasi, ditemukan bahwa nilai rating **tidak bisa dijadikan tolok ukur** dalam menilai tingkat keamanan suatu aplikasi. *Rating* suatu aplikasi kebanyakan diberikan oleh pengguna untuk menilai performa aplikasi secara umum, sehingga tidak ditemukannya dasar yang konkrit dalam menganalisis hubungan nilai rating dengan tingkat keamanan aplikasi.

Salah satu aplikasi yang ditunjukkan yakni aplikasi Absensi Online Sumbar memiliki jumlah akses izin aplikasi tertinggi sebanyak 19. Bila dilihat dari jumlah unduhan dan rating yang dimiliki, aplikasi ini memiliki 5.000+ unduhan dengan rating sebesar 4.4. Kemudian pada saat dilakukan observasi lebih lanjut di*review* yang diberikan oleh pengguna, hampir tidak ada yang mencantumkan penilaian keamanan aplikasi, dan lebih memfokuskan kepada fungsional aplikasi secara general. Hal ini menunjukkan bahwa informasi yang tercantum di *PlayStore* mengenai akses izin yang diminta aplikasi, serta upaya diri dari ancaman penyalahgunaan data pribadi, masih terbilang luput dari perhatian masyarakat saat menggunakan aplikasi.

### C. Analisis kesesuaian antara level perlindungan izin dengan regulasi hukum perlindungan data pribadi

Jika dikaitkan dengan pasal 26 UU ITE ayat 1, sebuah aplikasi yang memiliki level perlindungan izin *dangerous permission* wajib meminta persetujuan dari pengguna karena *permission* tersebut meminta data pribadi. Setelah dilakukan analisis, ternyata *Google* telah menetapkan keharusan sebuah aplikasi meminta persetujuan dari pengguna jika pengembang aplikasi menggunakan versi Android 6.0 atau lebih tinggi, dan melibatkan *dangerous permission* untuk berjalannya aplikasi. Permintaan persetujuan dari pengguna ini dilakukan dengan menambahkan <*uses-permission*> pada *application manifest*. Pada 20 aplikasi yang telah dianalisis, seluruh aplikasi yang melibatkan *dangerous permission* telah meminta persetujuan akses dari pengguna.


**Gambar 4.** Contoh Aplikasi SI D'nok Meminta Izin Untuk Dangerous Permission

Sehingga, dapat disimpulkan bahwa level perlindungan izin khususnya *dangerous permission* seluruh aplikasi telah sesuai dengan regulasi hukum perlindungan data pribadi yang berlaku, yakni UU ITE pasal 26 ayat 1.

### D. Analisis kepatuhan *Privacy Policy* pada sampel aplikasi

Ketersediaan *Privacy Policy* pada setiap aplikasi Android yang diluncurkan pada *Google Play Store* merupakan sebuah kewajiban bagi *developer* karena telah menyetujui *Google Play Store Distribution Agreement*. Hal ini tidak terkecuali bagi aplikasi milik Pemerintah Daerah Indonesia.

**Tabel 4** Ketersediaan *Privacy Policy* pada aplikasi sampel

| No | Nama Aplikasi | Privacy Policy | | |
|---|---|---|---|---|
| | | Google Play Developer | Dalam Aplikasi | Relevansi |
| 1 | JAKI – Jakarta Kini | Ada | Ada | Relevan |
| 2 | e-Health Surabaya | Tidak | Tidak dapat diketahui* | Tidak dapat diketahui |
| 3 | PIKOBAR Jawa Barat | Ada | Ada | Relevan |
| 4 | KMOB JABAR | Ada | Tidak dapat diketahui* | Relevan |
| 5 | Ambulan Hebat Semarang | Ada | Tidak | Tidak Relevan |
| 6 | SI D'nOK – Dukcapil Kota Semarang | Tidak | Tidak | Tidak dapat diketahui |
| 7 | SiABA | Ada | Tidak dapat diketahui* | Relevan |
| 8 | Cek Presensi | Ada | Tidak dapat diketahui* | Tidak Relevan |
| 9 | Presensi Sidoarjo | Ada | Tidak dapat diketahui* | Tidak Relevan |
| 10 | e-Pasar Malang | Ada | Ada | Relevan |
| 11 | e-Absensi | Tidak | Tidak dapat diketahui* | Tidak dapat diketahui |
| 12 | E-PERPUS BANJARMASIN | Ada | Ada | Relevan |
| 13 | PaPa Sulbar | Ada | Tidak | Tidak Relevan |
| 14 | E-Absensi ASN Sumut | Ada | Tidak dapat diketahui* | Tidak Relevan |

| | | | | |
|---|---|---|---|---|
| **15** | Absensi ASN Langkat | Ada | Tidak dapat diketahui* | Tidak Relevan |
| **16** | Absensi Online Aceh | Ada | Tidak dapat diketahui* | Tidak Relevan |
| **17** | Absensi Online Sumbar | Ada | Tidak dapat diketahui* | Relevan |
| **18** | Absensi Pemprov Bali | Ada | Tidak dapat diketahui* | Relevan |
| **19** | Absensi Sampang | Ada | Tidak dapat diketahui* | Tidak Relevan |
| **20** | iJogja | Ada | Ada | Relevan |

Tidak dapat diketahui* akibat aplikasi memerlukan nomor identitas tertentu untuk login yang tidak penulis ketahui

Dari tabel 4. dapat dilihat bahwa terdapat 17 dari 20 aplikasi yang mencantumkan *Privacy Policy* pada situs *Google Play Developer,* tapi pada faktanya terdapat 8 dari 17 aplikasi tersebut memberikan *Privacy Policy* yang tidak relevan. Dimana link *Privacy Policy* yang tersebut menuju ke website daerah masing-masing aplikasi, bukan berisi sebuah penjelasan komprehensif mengenai informasi penggunaan pribadi yang diminta maupun bagaimana kebijakannya. Sementara itu, terdapat 3 dari 20 aplikasi yang tidak mencantumkan *Privacy Policy* sama sekali.

Sehingga jika disimpulkan, terdapat 11 dari 20 aplikasi sampel yang masih belum mematuhi *Privacy Policy* dengan benar**.** Hal ini mencerminkan bahwa sebagian besar aplikasi Pemerintah Daerah yang menjadi sampel mengesampingkan kewajiban pemberian *Privacy Policy* yang sesuai dengan ketentuan, dan keamanan data pribadi pada aplikasi belum terjamin sepenuhnya. Padahal seperti yang telah dituliskan diatas, *Privacy Policy* telah diatur pada *Google Play Store Distribution Agreement* dan ditujukan untuk mencegah adanya penyalahgunaan data pribadi pengguna.

Dari hasil yang didapat setelah dilakukan pembahasan ditemukan banyak perbedaan dengan penilitian terdahulu, persamaan yang dapat ditemukan dengan penelitian hanya pada objek penelitian, yakni Keamanan dan *E-Government,* sementara metodologi yang digunakan sangat berbeda [2]. Penulis memfokuskan pada observasi aplikasi sampel diantaranya permintaan akses, data pribadi, unduhan, rating dan *Privacy Policy*. Persamaan dengan penelitian lain adalah salah satu indikator penilaian keamanan, yakni sama-sama menganalisis apakah ada mekanisme validasi pengguna [8]. Sementara itu, perbedaan terdapat pada indikator penilaian keamanan yang lain, yakni penggunaan permintaan akses, regulasi hukum yang berlaku di Indonesia, dan kebijakan *Privacy Policy*.

## 5. Kesimpulan

Berdasarkan hasil analisis hubungan level perlindungan izin dan data pribadi yang diminta oleh aplikasi Pemerintah Daerah bahwa seluruh sampel aplikasi membutuhkan *dangerous permissions* untuk meminta data pribadi pengguna, serta telah menetapkan mekanisme validasi pengguna yang kredibel, dibuktikan ketika pengguna *login* atau *sign in* memerlukan NIK, NIP, PIN, dan *Fingerprint*. Sedangkan hasil analisis hubungan *level* perlindungan izin dengan jumlah unduhan dan rating tidak menghasilkan bukti secara empiris, yang membuktikan bahwa jumlah unduhan dan nilai rating aplikasi tidak bisa dijadikan tolok ukur dalam mengetahui tingkat keamanan aplikasi.

Dari hasil analisis kesesuaian aplikasi dengan Hukum Perlindungan Data Pribadi di Indonesia, dapat dinyatakan bahwa semua sampel aplikasi telah sesuai dengan poin pada Pasal 26 UU ITE Ayat 1, yakni tentang persetujuan saat meminta data pribadi pengguna. Sementara itu, berdasarkan hasil analisis kepatuhan *Privacy Policy,* 55% dari sampel aplikasi masih tidak relevan dengan kebijakan *Google Play Store Distribution Agreement.*

**Saran**

Penelitian ini masih menilai aspek keamanan dari sisi luar aplikasi selama diakses oleh pengguna. Saran untuk penelitian selanjutnya dapat menambah penilaian aspek keamanan dari sisi teknikal, yang bisa menunjukkan penilaian lebih komprehensif, seperti *sandbox* aplikasi android dan enkripsi aplikasi. Kemudian, ruang lingkup pembahasan bisa diperluas lagi seperti ditambahkan sumber lain sebagai acuan penilaian aspek keamanan, contohnya Sistem Pemerintahan Berbasis Elektronik.

## 6. Daftar Pustaka


[1] A. W. Irawan, A. Yusufianto, D. Agustina, and R. Dean, "Laporan Survei Internet Apjii 2019-2020 (Q2)," vol. 2020, p. 15, 2020.

[2] F. Novianto, "Evaluasi Keamanan Informasi *E-government* Evaluation of *E-government* Information Security Using the Defense in Depth Model," vol. 3, no. 1, pp. 14–19, 2020.

[3] F. Makoza, "The level of *e-government* implementation: Case of Malawi," *Int. Bus. Concepts, Methodol. Tools, Appl.*, vol. 11, no. 2, pp. 880–895, 2016, doi: 10.4018/978-1-4666-9814-7.ch041.

[4] R. Indonesia, "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *UU No. 19 tahun 2016*, no. 1, pp. 1–31, 2016.

[5] Google, "Privacy Policy Guidance | Actions on Google | Google Developers," 2019. https://developers.google.com/actions/policies/privacy-policy-guide (accessed Sep. 06, 2020).

[6] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño, "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK," *Eur. Soc.*, vol. 0, no. 0, pp. 1–13, 2020, doi: 10.1080/14616696.2020.1804973.

[7] Google, "Permissions Overview | Android

Developers," *2015*. https://developer.android.com/guide/topics/permissions/overview (accessed Aug. 10, 2020).

[8] R. Ramadhani, E. P. Purnomo, and ..., "*E-government* Assessment pada Kualitias Aplikasi Jogja Smart Service (JSS) di Kota Yogyakarta," *J. Pemerintah. dan* …, vol. 5, no. 2, pp. 58–62, 2020, [Online]. Available: http://ejournal.uigm.ac.id/index.php/PDP/article/view/1031.

[9] Ansar, A. Lukum, Arifin, and Y. J. Dengo, "The Influence of School Culture on The Performance of High School English Teachers in Gorontalo Province," *Int. J. Educ. Res.*, vol. 5, no. 10, pp. 35–48, 2017.

[10] S. A. Khairunisa, "Data Observasi Analisis Privacy Policy Aplikasi *E-government* Tingkat Daerah [Data set]," 2020. http://doi.org/10.5281/zenodo.4160433 (accessed Oct. 30, 2020).