JURNAL PENGABDIAN MASYARAKAT KHATULISTIWA
http://jurnal.stkippersada.ac.id/jurnal/index.php/JPMK
e-ISSN 2560-5300

UPAYA PENCEGAHAN TERJADINYA PENCURIAN DATA PADA E-KTP BAGI PENDUDUK PADA DINAS KEPENDUDUKAN DAN PENCATATAN SIPIL KOTA MEDAN

Adelika[1], & Nurbaiti[2]
[1,2]Fakultas Ekonomi dan Bisnis Islam, UIN Sumatera Utara
Fakultas Ekonomi dan Bisnis Islam, UIN Sumatera Utara
Email : adelika002@gmail.com , nurbaiti@uinsu.ac.id

ABSTRACT: *This journal discusses efforts to prevent data theft on citizens' E-KTPs stored at the Medan City Population and Civil Registration Service. Theft of personal data is a serious problem in this digital era, especially when it involves sensitive population identity data such as E-KTP. In this context, this research aims to analyze the risk of E-KTP data theft and identify preventive efforts that can be carried out by the Medan City Population and Civil Registration Service. This research uses case study methods and interviews with relevant officers to collect data. The research results show that the risk of E-KTP data theft can be identified through security gaps in the data storage and processing system. Therefore, some of the proposed preventive measures include increasing physical and cyber security, training relevant staff, and improving data access procedures. This research contributes to better understanding the problem of data theft on E-KTPs and provides practical guidance for the Medan City Population and Civil Registration Service and similar agencies in maintaining the security of population data.*

Keywords *: E-KTP, Data Theft, Data Security, Digital Security, Population and Civil Registration Service Medan City*

ABSTRAK: Jurnal ini membahas tentang upaya pencegahan pencurian data pada E-KTP warga yang disimpan di Dinas Kependudukan dan Pencatatan Sipil Kota Medan. Pencurian data pribadi menjadi permasalahan serius di era digital ini, apalagi jika menyangkut data identitas kependudukan yang sensitif seperti E-KTP. Dalam konteks tersebut, penelitian ini bertujuan untuk menganalisis risiko pencurian data E-KTP dan mengidentifikasi upaya preventif yang dapat dilakukan oleh Dinas Kependudukan dan Pencatatan Sipil Kota Medan. Penelitian ini menggunakan metode studi kasus dan wawancara dengan petugas terkait untuk mengumpulkan data. Hasil penelitian menunjukkan bahwa risiko pencurian data E-KTP dapat diidentifikasi melalui celah keamanan pada sistem penyimpanan dan pengolahan data. Oleh karena itu, beberapa langkah pencegahan yang diusulkan antara lain meningkatkan keamanan fisik dan siber, melatih staf terkait, dan meningkatkan prosedur akses data. Penelitian ini memberikan kontribusi untuk lebih memahami masalah pencurian data pada E-KTP dan memberikan panduan praktis bagi Dinas Kependudukan dan Pencatatan Sipil Kota Medan dan instansi sejenis dalam menjaga keamanan data kependudukan.

Kata Kunci *: E-KTP, Pencurian Data, Keamanan Data, Keamanan Digital, Dinas Kependudukan dan Pencatatan Sipil Kota Medan*

PENDAHULUAN

Fenomena globalisasi telah mengawali zaman perkembangan teknologi informasi dan komunikasi, yang merambah dari negara maju hingga ke negara berkembang di seluruh dunia. Kemajuan teknologi ini telah meresap ke berbagai sektor kehidupan dan kini menjadi

ciri khas dari peradaban global saat ini. Dampaknya merata secara global, mengubah perilaku sosial dan merombak budaya dengan cepat. Perubahan ini membentuk dunia yang terlihat tidak memiliki batas, dengan transformasi sosial yang terjadi begitu cepat. Kecepatan pertumbuhan teknologi informasi dan komunikasi telah menjadi salah satu indikator utama kemajuan suatu bangsa.

Informasi memiliki peran yang sangat penting dalam pertumbuhan ekonomi, baik di negara maju maupun negara berkembang. (DEWI, 2009). Manajemen data pribadi, yang sebelumnya menjadi tugas pemerintah dan perusahaan swasta, menghadapi risiko yang lebih tinggi di era komputer saat ini. Ancaman terhadap privasi individu dan potensi kehilangan data karena kelalaian atau bocornya informasi menjadi semakin besar. (Marret, 2002). Zaman digital telah mengakibatkan peningkatan besar dalam jumlah data pribadi yang dihasilkan, disimpan, dan dipindahkan melalui komputer, perangkat mobile, jaringan broadband, situs web, dan media online.(Shilling, 2011). Dengan terus berkembangnya teknologi, privasi dan keamanan informasi pribadi menjadi semakin rawan. Dalam bidang hukum telematika, istilah "data" mengacu pada representasi formal dari konsep, fakta, atau instruksi. Secara keseluruhan, data adalah pernyataan yang dapat diwakili dalam berbagai bentuk. Asal kata "data" berasal dari bahasa Latin "datum," yang berarti "sesuatu yang diberikan." (Purwanto, 2007). Data mencakup segala informasi yang diproses secara otomatis sesuai dengan instruksi yang diberikan, dan informasi tersebut disimpan dengan maksud untuk diproses lebih lanjut. Informasi ini melibatkan catatan kesehatan, aktivitas sosial, pendidikan, atau disimpan dalam sistem penyimpanan yang relevan. Di Indonesia, seringkali terjadi kebocoran data pribadi. Informasi pribadi dapat terungkap melalui pertukaran data antar pusat kartu kredit, pengungkapan kepada pihak ketiga, seperti transaksi pemilik kartu kredit, atau transaksi antar bank. Kebocoran ini dapat terjadi melalui sistem umum atau melalui perantara, baik itu individu maupun perusahaan yang mengumpulkan dan berdagang data pelanggan. Ancaman penyalahgunaan data pribadi di Indonesia semakin meningkatkan kekhawatiran, terutama sejak pemerintah meluncurkan program Kartu Tanda Penduduk elektronik (E-KTP) dan merencanakan pembangunan Indonesia Automatic Fingerprints Identification System (INAFIS). Meskipun rencana INAFIS dibatalkan karena dianggap bertentangan dengan program E-KTP, kekhawatiran akan privasi tetap tinggi. Pengumpulan data pribadi tidak hanya dilakukan oleh pemerintah, tetapi juga oleh entitas swasta seperti bank dan penyedia layanan telekomunikasi. Beberapa waktu lalu, masyarakat dihebohkan oleh dugaan kebocoran data pelanggan telepon seluler, menyoroti risiko penyalahgunaan data pribadi.

Program E-KTP, yang dimulai pada awal tahun 2011, adalah bagian dari upaya pemerintah untuk menerapkan Nomor Induk Kependudukan (NIK). Tujuannya adalah menciptakan identitas tunggal seumur hidup untuk setiap penduduk, yang diwakili melalui satu kartu identitas yang mencakup NIK.

METODE PELAKSANAAN

Penelitian ini mengadopsi metode penelitian kualitatif yang berfokus pada pengamatan mendalam di Dinas Kependudukan dan Pencatatan Sipil Kota Medan, sambil menganalisis beberapa artikel yang membahas insiden kebocoran data. Pendekatan penelitian ini melibatkan analisis hukum dan studi kasus.(S, 2018). (UU ITE). Informasi diperoleh melalui penyelidikan literatur, perundang-undangan, dan pengumpulan data elektronik yang terkait dengan topik penelitian. Pendekatan analisis yang diterapkan adalah kualitatif, yang melibatkan eksplorasi mendalam data dan penafsiran oleh peneliti untuk mencapai kesimpulan yang diinginkan.(Mandasari Yasmirah Saragih, 2018). Bahan hukum yang telah diatur dengan sistematis kemudian dievaluasi dengan metode analisis kualitatif.

HASIL DAN PEMBAHASAN

Tingkat ketidakaturan dalam penggunaan data pribadi dan upaya mengatasi pencurian data pribadi di era ekonomi digital semakin meningkat. Oleh karena itu, situasi seperti ini membutuhkan kebijakan yang cermat dalam pembentukan undang-undang yang spesifik untuk melindungi data pribadi setiap individu. Selain itu, strategi efektif diperlukan untuk menghadapi masalah ini, termasuk tindakan hukum dan non-hukum yang berfungsi sebagai bentuk perlindungan, sehingga perkembangan ekonomi digital dapat berjalan dengan lancar. Namun, upaya perlindungan data pribadi di Indonesia masih terbatas oleh instrumen hukum yang kurang spesifik dan terfragmentasi, sehingga belum cukup untuk mendorong perkembangan ekonomi digital di negara ini.

Dalam paragraf keempat Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, ditegaskan bahwa Pemerintah Negara Indonesia bertanggung jawab secara konstitusional untuk melindungi semua warga dan keturunan Indonesia, serta meningkatkan kesejahteraan umum, memberikan pendidikan kepada penduduk, dan mendukung perdamaian global berdasarkan kebebasan, perdamaian abadi, dan keadilan sosial. Dalam konteks perkembangan teknologi informasi dan komunikasi, misi negara ini diwujudkan melalui upaya perlindungan data pribadi setiap warga negara Indonesia dari potensi ancaman. Dengan demikian, dapat disimpulkan bahwa Konstitusi Republik Indonesia Tahun 1945 memberikan panduan dalam melawan pencurian data pribadi dan melindungi kepemilikan pribadi dari upaya peretasan atau pencurian data individu melalui media elektronik.

Banyaknya orang yang menggunakan media elektronik sebagai alat komunikasi telah meningkatkan risiko pelanggaran privasi, terutama dalam bentuk penyalahgunaan seperti pencurian data pribadi atau peretasan. Hal ini dipicu oleh kebiasaan masyarakat yang sering membagi informasi pribadi. Sebagai contoh, di media elektronik seperti telepon seluler, pengguna diharuskan memberikan data pribadi sebelum dapat menggunakan kartu telepon seluler. Di platform internet, pada setiap profil jejaring sosial seperti Facebook, Twitter, Friendster, Myspace, dan sejenisnya, individu sering mempublikasikan informasi pribadi mereka secara rinci dan terbuka. Informasi pribadi seperti tanggal lahir, nomor telepon, alamat tinggal, foto pribadi, dan lainnya, baik disengaja maupun tidak, dapat dengan mudah tersebar karena internet bersifat terbuka dan bebas, memungkinkan data ini berpindah dari satu tempat ke tempat lain tanpa pengawasan yang ketat. Banyak masalah yang timbul, baik di Indonesia maupun secara global, berkaitan dengan penyalahgunaan data pribadi. Contoh kasus yang telah dijelaskan di atas hanya merupakan sebagian kecil dari ribuan kasus serupa yang terjadi terkait dengan pelanggaran privasi data.

Di Indonesia, penanganan kasus pencurian data pribadi saat ini diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Menurut UU ITE, tindakan penanganan pencurian data pribadi melibatkan penghapusan, yang dilakukan berdasarkan putusan pengadilan atas permintaan pemilik data. Sementara itu, dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, kebijakan terkait penyalahgunaan data pribadi diatur dalam Pasal 15, Pasal 16, dan Pasal 17. Menurut peraturan tersebut, penanganan pencurian data pribadi melibatkan penghapusan, yang terdiri dari dua jenis, yaitu hak untuk dihapus (right to erasure) dan hak untuk dihapus dari mesin pencari (right to delisting). Penghapusan ini dilakukan sesuai dengan keputusan pengadilan terkait informasi dan/atau dokumen elektronik.

Dalam situasi ini, Dinas Kependudukan dan Pencatatan Sipil Kota Medan sedang berupaya keras untuk menghindari kebocoran data, sesuai dengan kekhawatiran penduduk Kota Medan. Ika, salah satu warga, mengungkapkan kekhawatirannya tentang keamanan data pribadinya yang disimpan secara digital melalui bimbingan dan arahan dari Pak Rudi, Kepala Bidang Divisi Kartu Tanda Penduduk (KTP). Pak Rudi memastikan bahwa E-KTP dirancang untuk memberikan kemudahan akses kepada penduduk tanpa kesulitan, sambil menjamin bahwa data disimpan dengan aman dan privasi terjaga. Banyaknya kekhawatiran para penduduk mengenai data yang disimpan secara digital membuat Dinas Kependudukan dan Pencatatan Sipil Kota Medan mensosialisasikan dan memberikan bimbingan serta arahan kepada para Penduduk agar

melakukan upaya-upaya pencegahan terhadap kebocoran Data.

Adapun Faktor penyebab kebocoran data E-KTP yaitu :

1. **Human Error**

Telah menjadi pengetahuan umum bahwa sebagian besar insiden kebocoran data disebabkan oleh kesalahan manusia. Human error merujuk pada kesalahan atau tindakan yang dilakukan oleh individu manusia yang mengakibatkan data pribadi dari E-KTP bocor atau terungkap kepada pihak yang tidak berwenang. Contoh-contoh kesalahan manusia dalam kasus kebocoran data E-KTP melibatkan kelalaian dalam pengelolaan data, kurangnya pelatihan dan kesadaran, serta pengabaian terhadap protokol keamanan.

2. **Terserang Malware**

Malware, singkatan dari Malicious Software, adalah program yang dibuat khusus untuk merusak sistem komputer dengan cara menyusup. Penyusupan ini dapat terjadi melalui email, unduhan dari internet, atau program yang terinfeksi. Malware dapat mengakibatkan kerusakan pada sistem komputer dan memungkinkan pencurian informasi. Contoh malware meliputi virus, spyware, ransomware, dan jenis lainnya.

3. **Kelemahan Keamanan Sistem**

Kerentanan dalam sistem keamanan merujuk pada celah atau titik lemah dalam infrastruktur teknologi serta perangkat lunak yang digunakan untuk mengelola, menyimpan, atau mengakses data E-KTP. Celah ini dapat dimanfaatkan oleh pihak yang tidak sah untuk mengakses atau mencuri data E-KTP secara ilegal. Kelemahan keamanan sistem ini dapat muncul karena berbagai alasan, termasuk desain yang tidak optimal, kurangnya pemeliharaan, penundaan dalam pembaruan perangkat lunak, atau pelaksanaan kebijakan keamanan yang tidak hati-hati.

4. **Insider Threats**

Ancaman insider merujuk pada risiko yang berasal dari individu atau entitas yang memiliki akses internal atau kedekatan dengan sistem, data, atau informasi terkait E-KTP. Mereka, dengan sengaja atau tidak sengaja, melakukan tindakan yang merugikan dengan mengungkapkan, mencuri, atau menyalahgunakan data tersebut. Insider threats dapat muncul dari dalam organisasi yang mengelola data E-KTP, melibatkan karyawan, kontraktor, atau pihak lain yang memiliki keterbatasan akses ke sistem atau data.

5. **Kurangnya Kesadaran Keamanan**

Individu atau pihak yang mengurus atau bisa mengakses data E-KTP mungkin tidak memahami atau tidak memperhatikan secara memadai pentingnya menjaga kerahasiaan informasi pribadi yang ada dalam E-KTP. Hal ini bisa mengakibatkan tindakan atau keputusan yang pada akhirnya bisa menyebabkan kebocoran atau penyingkapan data E-KTP kepada pihak yang tidak berhak.

Dampak Serius dari Kasus Pembocoran Data E-KTP

Pelanggaran keamanan pada data E-KTP (Kartu Tanda Penduduk elektronik) bisa berdampak serius pada individu dan masyarakat secara keseluruhan. Berikut adalah beberapa konsekuensi yang mungkin timbul karena pelanggaran tersebut.:

1. **Penipuan Identitas**

   Dengan mendapatkan akses ke informasi pribadi seperti nomor KTP dan tanggal lahir, individu yang tidak bertanggung jawab dapat melakukan penipuan identitas. Mereka dapat memanfaatkan informasi ini untuk membuat rekening palsu, mengajukan pinjaman, atau terlibat dalam aktivitas kriminal lainnya.

2. **Pencurian Identitas**

Informasi pribadi yang ada dalam E-KTP, termasuk nama, alamat, nomor KTP, dan foto, bisa dimanfaatkan oleh individu yang tidak bertanggung jawab untuk mencuri identitas. Hal ini bisa mengakibatkan penyalahgunaan, seperti membuka rekening bank palsu, mengajukan pinjaman tanpa izin, atau terlibat dalam tindakan kriminal lainnya atas nama korban.

3. **Privasi yang Terancam**

Dalam era di mana masyarakat semakin terkoneksi secara digital, menjaga privasi individu menjadi sangat krusial. Kebocoran data E-KTP dapat membahayakan privasi individu. Pemanfaatan informasi pribadi dengan tidak semestinya dapat menyebabkan hilangnya kendali atas informasi yang seharusnya bersifat rahasia.

4. **Penipuan Keuangan**

Penjahat yang berhasil mengakses data E-KTP dapat menggunakan informasi tersebut untuk menyamar sebagai pemilik asli dan melakukan penipuan keuangan atau transaksi ilegal. Selain itu, ketika data KTP bocor, ada risiko penyalahgunaan dalam mengajukan pinjol atau pinjaman online di aplikasi atau layanan dengan sistem keamanan yang tidak memadai. Mereka dapat memanfaatkan informasi tersebut untuk masuk ke akun bank, melakukan pembelian online, atau meretas akun-akun penting milik korban.

5. **Ancaman Keamanan Nasional**

Ancaman terhadap keamanan nasional dalam situasi kebocoran data E-KTP merujuk pada potensi risiko terhadap stabilitas dan keamanan suatu negara akibat informasi yang sangat sensitif dan penting dalam E-KTP jatuh ke tangan yang salah. Dampak dari ancaman ini bisa sangat meluas dan serius, termasuk penggunaan data untuk kegiatan kriminal dan terorisme, pembuatan identitas palsu untuk spionase, penurunan kepercayaan terhadap pemerintah, dan berbagai dampak negatif lainnya.

Perlindungan agar Tidak Terjadi Bocornya Data E-KTP

Melindungi data E-KTP dari kebocoran merupakan langkah yang sangat krusial untuk menjaga privasi dan keamanan individu serta menghindari potensi risiko terhadap keamanan nasional. Di bawah ini disajikan beberapa langkah perlindungan yang bisa diambil:

1. **Mengganti Kata Sandi Secara Berkala**

Merubah kata sandi secara rutin adalah tindakan yang sangat penting untuk menjaga keamanan data dan informasi pribadi secara keseluruhan, terutama dalam sistem informasi yang terhubung dengan data E-KTP. Jika sistem atau aplikasi menggunakan data E-KTP, pastikan bahwa kata sandi yang digunakan memiliki kekuatan yang memadai dan telah dienkripsi. Selain itu, pastikan bahwa akses tersebut hanya diberikan kepada individu atau entitas yang memerlukan dan berwenang.

2. **Berhati-hati dalam Menggunakan Aplikasi E-Commerce**

Saat menggunakan aplikasi e-commerce atau media sosial, penting bagi kita untuk bersikap selektif dan berhati-hati ketika memberikan informasi pribadi. Kita harus mempertimbangkan apakah data pribadi yang diberikan kepada aplikasi tersebut memiliki potensi risiko atau tidak.

1. **Hindari Mengunggah Foto KTP Sembarangan**

Hindari mengunggah foto KTP atau data pribadi dengan tidak hati-hati. Sampaikan informasi pribadi hanya kepada pihak yang sah dan terpercaya, seperti instansi pemerintah atau layanan yang sudah diverifikasi secara resmi.

Melakukan tindakan pencegahan terhadap kebocoran data penduduk dalam sistem Dinas Kependudukan dan Pencatatan Sipil Kota Medan adalah langkah krusial untuk melindungi privasi dan keamanan informasi warga. Berbagai langkah dapat diambil untuk menghindari kebocoran data penduduk:

1. Perlindungan Data: Informasi yang bersifat sensitif seperti nomor KTP dan data pribadi lainnya perlu dienkripsi dengan cermat ketika disimpan dan saat dipindahkan antar sistem.

2. Pembatasan Akses: Hanya individu yang memiliki izin yang diizinkan untuk mengakses informasi penduduk. Ini dapat dicapai melalui penerapan sistem otentikasi yang kuat dan pengaturan hak akses yang tepat.

3. Pemantauan Aktivitas : Melakukan pemantauan terhadap aktivitas yang mencurigakan atau akses yang tidak sah ke sistem. Ini bisa melibatkan sistem deteksi intrusi dan pemantauan log.

4. Pelatihan Karyawan : Karyawan yang mengakses sistem harus diberikan pelatihan tentang pentingnya menjaga kerahasiaan data dan praktik keamanan yang tepat.

5. Kebijakan Keamanan : Menyusun kebijakan keamanan data yang jelas dan mengikuti standar keamanan yang berlaku, seperti ISO 27001.

6. Pembaruan Perangkat Lunak : Memastikan bahwa semua perangkat lunak yang digunakan dalam sistem finas kependudukan selalu diperbarui dengan patch keamanan terbaru.

7. Audit Keamanan : Melakukan audit keamanan secara berkala untuk mengidentifikasi potensi kerentanannya dan mengambil tindakan korektif.

8. Pentingnya Privasi : Menekankan pentingnya menjaga privasi data penduduk kepada semua pihak yang terlibat dalam pengelolaan data.

9. Backup Data : Melakukan backup data secara teratur agar data tetap tersedia jika terjadi insiden keamanan.

10. Kerjasama Dengan Otoritas : Bekerjasama dengan otoritas keamanan data dan regulator untuk memastikan kepatuhan dengan peraturan perlindungan data yang berlaku.

11. Respon Krisis : Mempersiapkan rencana respons krisis untuk menghadapi insiden keamanan data jika terjadi.

12. Penghapusan Data yang Tidak Diperlukan : Menghapus data yang sudah tidak diperlukan atau perlu secara berkala untuk mengurangi potensi risiko keamanan.

Semua upaya ini harus terus diawasi dan diperbarui sesuai dengan perkembangan teknologi dan ancaman keamanan yang mungkin muncul. Upaya ini penting untuk menjaga kepercayaan warga terhadap sistem finas kependudukan dan menjaga data penduduk tetap aman.

SIMPULAN

Bahwa perlu adanya langkah-langkah yang diterapkan untuk melindungi data penduduk dalam sistem E-KTP di Kota Medan agar terhindar dari pencurian data yang berpotensi merugikan masyarakat dan institusi terkait. perlindungan data penduduk dalam sistem E-KTP di Dinas Kependudukan dan Pencatatan Sipil Kota Medan merupakan suatu keharusan, dengan diperlukannya berbagai tindakan preventif dan pengamanan data yang efektif guna mencegah insiden pencurian data yang dapat berdampak merugikan masyarakat serta institusi yang bertanggung jawab atas informasi tersebut.

Adapun upaya pencegahan yang dilakukan oleh Dinas Kependudukan dan Pencatatan Sipil Kota Medan yaitu dengan cara mensosialisasikan serta memberikan bimbingan dan arahan kepada Penduduk agar selalu berhati-hati dan data tetap aman.

DAFTAR RUJUKAN

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. Padjadjaran Law Review, 9.

Dewi, S. (2009). Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional. Bandung: Widya Padjajaran.

Marrett, P. (2002). Information Law in Practice : 2nd Edition. Cornwall: MPG Books Ltd.

Shilling, C. G. (2011). Privacy and Data Security : New Challenges of The Digital Age. New Hampshire Bar Journal, 13

Purwanto. (2007). Penelitian Tentang Perlindungan Hukum Data Digital. Jakarta: Badan Pembinaan Hukum Nasional.

Laurensius Arliman S. (2018). Peranan Metodologi Penelitian Hukum di Dalam Perkembangan Ilmu Hukum di Indonesia. Soumatera Law Review

Yasmirah Mandasari Saragih, Teguh Prasetyo, J. H. (2018). Analisis Yuridis Kewenangan Komisi Pemberantasan Korupsi Sebagai Penuntut Pelaku Tindak Pidana Korupsi. Unifikasi : Jurnal Ilmu Hukum, 5

Richardus Eko Indrajit. "Fenomena Kebocoran Data; Mencari Sumber Penyebab Dan Akar Permasalahannya,." Folder.Idsirtii.or.Id

Satrio, M. B., & Widiatno, M. W. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). JCA of Law, 1

Natha, K. D. R., Budiartha, N. P., & Astiti, N. G. K. S. (2022). Perlindungan Hukum atas Kebocoran Data Pribadi Konsumen pada Perdagangan Elektronik Lokapasar (Marketplace). Jurnal Preferensi Hukum, 3, 143-148.