TANTANGAN *SECURITY* DAN KEHANDALAN SISTEM DALAM APLIKASI BERGERAK

Yusuf Amrozi[a], Khoirun Nadiya[b], Laylatul Rahmah[c], Ni'matus Shofiyah[d], dan One Thowimma[e]

[abcde]*Program Studi Sistem Informasi, Universitas Islam Negeri Sunan Ampel, Surabaya.*

[a]yusuf.amrozi@uinsby.ac.id, [b]09020620029@student.uinsby.ac.id,
[c]09040620054@student.uinsby.ac.id, [d]09040620054@student.uinsby.ac.id,
[e]H76219031@student.uinsby.ac.id

ABSTRAK

Penelitian ini bertujuan untuk mendeskripsikan tantangan aplikasi perangkat bergerak dan kehandalan sistem tentang kasus kejahatan dunia mayayang terjadi di Indonesia, serta penerapan keamanan internet dalam bisnis. Dengan demikianpengguna dapat memahami dengan benar keuntungan dan kerugian dalam menggunakan suatu teknologi. Metode penelitian yang digunakan adalah metode kualitatif, dimana penelitian bersifat deskriptif dan cenderung menggunakan analisis. Proses penelitian dimulai dari menyusun asumsi dasar dan rancangan kerangka yang akan digunakan dalam penelitian. Dengan mengkaji referensi dari jurnal-jurnal yang tersedia, hasil penelitian menunjukkan tentang perbedaan aplikasi bergerak dengan *website mobile*, tantangan *security* tentang kasus kejahatan siberdi Indonesia, peranan kemanan siber dalam dunia bisnis, dan juga cara meningkatkan keamanan siber agar terhindar dari bahaya kejahatan siber.

Katakunci:*Aplikasi bergerak, tantangan security, kejahatan siber*

ABSTRACT

The study aims to describe the challenges of mobile device applications and system reliability regarding virtual crimes occurring in Indonesia, as well as the implementation of Internet security in business. Thus the user can correctly understand the advantages and disadvantages of using a technology. The research methods used are qualitative methods, where research is descriptive and tends to use analysis. The research process begins with formulating the basic assumptions and skeletal design to be used in the study. By reviewing references from available journals, research shows how different mobile apps differ from mobile websites, security challenges to cybercrime in Indonesia, the role of cybersecurity in the business world, and also how to increase cybersecurity to avoid the dangers of cybercrime.

Keywords:*Mobile application, cyber security, cybercrime*

1. PENDAHULUAN

Teknologi mengalami perkembangan yang sangat signifikan dalam beberapa tahun terakhir. Perkembangan teknologi berbanding lurus dengan kebutuhan manusia yang semakin meningkat. Salah satu teknologi yang berkembang sangat pesat adalah teknologi informasi dan telekomunikasi. Teknologi informasi mempunyai peran yang besar dalam penyebaran suatu informasi yang akurat, terbaru dan dapat dipercaya guna membantu dalam pengambilan suatu keputusan. Untuk menghasilkan informasi yang diperlukan, suatu organisasi

membutuhkan teknologi informasi dalam pengolahan data.

Dengan berkembangnya teknologi informasi berupa cloud, drive dan lainnya memudahkan seorang pengguna dalam mengakses data atau informasi dimanapun dia berada. Namun, sistem ini masih memerlukan konektivitas antara satu dengan yang lain, entah berupa perangkat keras maupun perangkat lunak. Dalam hal ini muncul sesuatu hal yang baru yaitu jaringan internet. Meluasnya internet memudahkan pengguna dalam mengakses data tanpa menyambungkan satu perangkat dengan perangkat yang lainnya.

Pertumbuhan internet dalam seluruh bidang kehidupan manusia membuat teknologi telekomunikasi juga berkembang tak kalah cepat. Dimana dalam waktu yang singkat model bisnisnya dapat berubah. Perubahan ini disesuaikan dengan inovasi atau teknologi baru yang dibutuhkan masyarakat sebagai target pasar.

Perkembanganteknologi telekomunikasi yang sangat pesat di buktikan dengan pengguna internet di Indonesia yang semakin meningkat tiap tahunnya. Dilansir dari kominfo.go.id melalui survei Asosiasi Penyelenggara Jasa Internet di Indonesia (APJII) menghasilkan data sebagai berikut, Sekretaris Jenderal APJII Henri Kasyfi Soemartono menjelaskan pengguna internet di Indonesia pada tahun 2019-2020 berjumlah 73,7 persen, naik sekitar 8,9 persen dari tahun 2018 yang berjumlah 64,8 persen.

Menurut Sekretaris Jenderal APJII, jumlah populasi di Indonesia tahun 2019 adalah 266.911.900 juta, sehingga pengguna internet di Indonesia diperkirakan mencapai 196,7 juta. Jumlah tersebut naik sekitar 25,5 juta dari tahun 2019 yang berjumlah 171 juta pengguna. Pandemi Covid-19 sendiri juga memberikan efek yang besar untuk peningkatan penggunaan internet di Indonesia yang disebabkan oleh imbauan pemerintah untuk bekerja dari rumah, belajar dari rumah dan beribadah di rumah.

Bukan hanya penggunaan internet yang semakin meningkat, kejahatan di internet juga sangat tinggi. Dilansir dari CNN Indonesia, FBI (*Federal Bureau of Investigation*) menyatakan kejahatan dunia maya meningkat sebanyak 300 perse sejak awal pandemi Covid-19. FBI mengatakan menerima pengaduan keamanan *cyber* setiap harinya sekitar kurang lebih 3000 sampai 4000, naik rata-rata 1000 pengaduan per hari sebelum pandemi.

Melansir dari “The Star”, aktivitas peretasan terhadap perusahaan di Amerika Serikat dan negara lain meningkat lebih dari dua kali lipat. Penelitian mengatakan pencuri digital mengambil keuntungan dari keamanan yang dilemahkan sebab

kebijakan kerja dari rumah. Perusahaan perangkat lunak dan keamanan Vmware Carbon Black mengatakan bahwa serangan *ransomware* yang dipantaunya melonjak 148 persen pada bulan Maret 2020.

Dengan berkembangnya teknologi informasi, pengguna juga harus memahami bahwa ada lebih dari satu jenis metode serangan, yang dapat merusak suatu sistem. Banyak kejahatan yang masuk ke dalam sistem datebase perusahaan. Kejahatan sistem tersebut juga biasanya melakukan pencurian data yang tersimpan didalam sistem database perusahaan. Oleh karena itu, sangat dibutuhkannya benteng pertahanan. Hal ini perlu dipahami oleh para pembisnis dan yang paling utama orang yang mengelola data pribadi pengguna atau pelanggan. Agar data-data yang dikelola tetap aman dan sampai ke tujuan dengan selamat, semakin diperlukannya suatu proteksi sebagai benteng yang melindungi data atau informasi dari kejahatan secara ilegal.Penulisan artikel ini bertujuan untuk mendeskripsikan pengertian aplikasi perangkat begerak dan tantangan *security* dalam kehandalan sistem tentang *cybercrime* yang terjadi di Indonesia sehingga kita dapat menangani masalah tersebut jika terjadi dikemudian hari. Serta dapat dimanfatkan dalam hal integrasi keilmuwan di berbagai bidang yang diperlukan seperti, penerapan sistem *security* dalam sebuah bisnis ataupun untuk melindungi dari kejahatan sosial.

2. METODE PENELITIAN

Pendekatan dalam metode penelitian ini terdiri atas dua bagian, pertama adalah pendekatan penelitian perkembangan berguna untuk metode penelitian yang sifatnya menyelidiki pola dan pertumbuhan dan penelitian deskriptif. Disusun secara sistematis, akurat dan faktual untuk mendeskripsikan variabel yang diteliti.

Oleh karena itu, dengan menggunakan dua bagian pendekatan maka penelitian ini menggunakan metode kualitatif, karena bersifat deskriptif dan cenderung menggunakan analisis. Maka dengan demikian, proses penelitian kualitatif dimulai dengan menyusun asumsi dasar dan kerangka berfikir yang digunakan dalam penelitian.

3. HASIL DAN PEMBAHASAN

Perkembangan aplikasi bergerak atau biasa disebut dengan teknologi perangkat bergerak, diawali dengan teknologi komunikasi yaitu teknologi telepon seluler. Pada awalnya ponsel hanya memiliki fasilitas telepon dan *Short Messages Service* (SMS) yang berfungsi untuk alat komunikasi. Dengan dua fasilitas tersebut, penguna bisa melakukan komunikasi

dengan pengguna lain dimanapun berada selama masih berada di dalam cangkupan layanan.

Seiring berjalannya waktu dan semakin berkembangnya teknologi informasi, ponsel dilengkapi dengan berbagai perangkat keras berupa prosesor, memori, dan kamera yang lebih baik. Tidak hanya itu, ponsel juga dilengkapi dengan aplikasi lain yang dapat ditambahkan sendiri oleh penggunanya. Dari sinilah mulai terjadi konvergurasi teknologi yaitu perpaduan antara teknologi informasi, komunikasi dan juga hiburan dari yang awalnya hanya sebagai alat komunikasi.

Aplikasi bergerak secara umum dapat dibedakan menjadi 2 macam, yang pertama yaitu aplikasi bergerak yang bersifat *native (Native Mobile Application)*. Aplikasi bergerak mampu mengambil data baik secara langsung *(online)* dari internet atau mengunduhnya dahulu, kemudian digunakan secara *offline.* Aplikasi bergerak dijalankan di atas sistem operasi atau *platform* yang beragam seperti *iOS, Blackberry, Android, Windows,* dan lain-lain. Beberapa *platform* tersebut juga memiliki versi yang beragam, misalnya dalam android 4.4 Kitkat, 5.0 Lollipop, 6.0 Marshmallow, 7.0 Nougat sampai pada Android terbaru, yaitu Android 10.

Yang kedua, aplikasi bergerak yang berbasis web *(Web-based Mobile Application)*. Aplikasi bergerak dengan basis web biasanya berupa situs web bergerak *(Mobile Website)*, yaitu situs web yang dirancang khusus agar mudah diakses melalui perangkat bergerak. Situs web ini berupa halaman-halaman web yang ditulis menggunakan HTML dan diakses melalui internet. Aplikasi bergerak dan *mobile website* memiliki keunggulan masing-masing. Penyedia jasa informasi bisa memilih untuk mengimplementasikan salah satu atau keduanya agar saling melengkapi.

Tabel 1 perbedaan antara Aplikasi bergerak dengan *Mobile Website*

Kriteria	Aplikasi Bergerak	*Mobile Website*
Ketersediaan	Sebelum digunakan aplikasi harus diunduh dari penyedia aplikasi.	Langsung bisa diakses dengan syarat tersedia layanan internet dan aplikasi browser.
Kompatibilitas	Aplikasi harus dibuat untuk masing-maing *platform.*	sekali buat bisa langsung diakses dengan perangkat dari berbagai *platform.*
Pembaharuan	*Upgrade* dan *update* harus diberitahukan kepada *user,* agar mengunduh ulang sesuai dengan *platform* nya.	Dapat di *update* dengan mudah tanpa memberitahu pengguna.
Pemakaian bersama	Pengguna lain harus mengunduh	Pengguna dapat memberitahukan kepada *user*

	sendiri sesuai *platform* nya.	lain melalui sebuah *link*.
Jangkauan	Terbatas pada perangkat yang *platform* dan tipenya sama dengan aplikasi yang dibuat.	Dapat menjangkau semua perangkat bergerak yang telah dilengkapi aplikasi *browser*.
Waktu dan biaya	Waktu pengembangan nya lebih lama.	Watu pengembangan n-anya lebih singkat dan murah.
Interaktifi-tas	Lebih interaktif.	Kurang interaktif.
Personalis a-si	Mudah disesuaikan, dikustomisasi, dan dipersonalisasi sesuai dengan status *user*.	Lebih bersifat umum, sulit disesuaikan dengan status *user*.
Koneksi	Tidak terlalu menuntut menggunakan internet, bisa di operasikan secara *offline*.	Selalu membutuhkan sambungan internet.
Fungsiona-litas	Mampu memanfaatkan secara penuh fitur perangkat seperti kamera, GPS, kompas dll.	Kemampuan menggunakan fitur perangkat terbatas dan kurang efektif.
Komplesit-as	Mampu mengolah data seperti perhitungan kompleks, menampilkan grafik dan laporan.	Lebih cocok untuk menampilkan informasi tekstual yang tidak memerlukan perhitungan kompleks.

Peningkatan penggunaan internet di era modern saat ini tak luput dari dampak negatif yang membuntutinya. Setelah mengetahui perkembangan aplikasi perangkat bergerak yang sangat pesat sudah semestinya kita juga memahami bahwa ada banyak tantangan dan kejahatan yang dapat menimpa kita kapan saja, salah satunya adalah maraknya kejadian peretasan data-data perusahaan atau bahkan data negara yang disebabkan oleh hacker yang menyusup ke dalam sistem pengamanan.

Aktivitas kejahatan dengan komputer atau jaringan komputer terutama pada sistem aplikasi bergerak sudah marak dilakukan di era teknologi saat ini. Menurut (Fitriani & Pakpahan, 2020) pengertian cybercrime merupakan setiap aktivitas seseorang atau kelompok, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan dan komputer sebagai sasarannya. Banyak pola dan cara yang dilakukan oleh para pelaku *cybercrime* untuk merusak atau membobol sistem keamanan dari sebuah aplikasi. Beberapa pelaku *cybercrime* merupakan tindakan yang terorganisir dan memiliki tujuan yang menguntungkan pihak mereka.

Insiden *Cyber*sendirimerupakan kejadian yang dapat mengganggu berjalannya sistem elektronik seperti serangan virus, pencurian data, informasi

pribadi, hak kekayaan intelektuan perusahaan, *web defacement* dan gangguan akses terhadap layanan elektronik.

Indonesia termasuk ke dalam salah satu negara dengan *cyber-security* yang lemah. Pada tahun 2014 perusahaan *monitoring internet*Akamai mengungkap bahwa kejahatan internet di Indonesia meningkat bahkan sampai dua kali lipat. Angka ini menempatkan Indonesia di posisi pertama negara yang berpotensi menjadi target *hacker* menggantikan Tiongkok.

Sedangkan pada tahun 2020 di saat terjadi pandemi COVID-19, peningkatan jumlah *cyber crime* mencapai empat kali lipat dibandingkan dengan tahun 2019. Pusat Operasi Keamanan Siber (Pusopskamsina) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 terjadi pada 1 Januari hingga 12 April. Jumlah serangan sempat menurun secara signifikan saat diberlakukannya *Work From Home* (WFH). Serangan siber ini memanfaatkan isu terkait dengan COVID-19. Dikutip dari bbsn.go.id, jenis serangan yang paling banyak adalah *trojan activity* sebanyak 56%, *information gathering* (pengumpulan informasi) sebanyak 43%, dan yang terakhir adalah *web application attack* sejumlah 1%.

Dengan adanya data ini sudah seharusnya Indonesia semakin memperbaiki dan meningkatkan keamanan dalam dunia maya dengan *cyber security*, karena tingkat kejahatan *cyber* yang semakin meningkat dari waktu ke waktu. Penanganan kejahatan di dunia maya dengan kejahatan di dunia nyata tentu saja berbeda. Dalam menangani kejahatan di dunia maya, diperlukan pemikiran yang kritis dan komperehensif.

Pemanfaatan dalam teknologi sudah dapat di rasakan dalam berbagai bidang seperti pertanian, perternakan, sosial, ekonomi yang pasti berdampak banyak kepada masyarakat. Tak luput dari itu sebagai masyarakat yang tinggal di daerah perkotaan yang tak lepas dengan teknologi juga mendapat manfaat yang dalam berbisnis seperti memanfaatkan model keamanan yang di kembangkan untuk bagian keamanan teknologi informasi. Konsep keamanan tersebut biasanya yang disebut dengan “CIA Triad” atau yang biasa kita kenal dengan *confidentiality* (kerahasiaan)**,** *integrity*(integritas),dan*availability* (ketersediaan) informasi**,** konsep ini biasanya yang di gunakan dalam mengantisipasi terjadinya cyber crime.

Confidentiality (kerahasiaan) yakni biasanya usaha yang dilakukan suatu perusahaan dalam menyimpan data agar dapat merahasia data tersebut sehingga data tersebut dapat dikontrol oleh perusahaan sehingga tidak terjadi

kebocoran data yang merugikan berbagai pihak yang terkait. *confidentiality* biasanya dilakukan dengan mengaktifkan 2 faktor autentifikasi atau *two factor authentication*(2FA). Seperti namanya 2 faktor autentifikas terdiri dari dua tahap, tahap pertama sebelum mengakses data dengan memasukkan password yang telah di buat selanjutnya masuk pada tahap kedua yakni dengan memasukkan kode khusus yang dikirimkan kepada perangkat atau email yang di daftarkan dalam data yang akan di akses tersebut. Dengan adanya pemanfaat teknologi ini membuat data anda menjadi lebih aman dari pada hanya memasukkan password saja dalam mengakses data tersebut.

Selanjutnya ada *integrity* (integritas), yakni biasanya cara untuk memberikan data yang akurat, konsisten dan terpercaya. Biasanya ini di gunakan oleh perusahaan yang berkembang di bidang bisnis toko online yang harus memberikan informasi terkait produk yang jelas agar para pelanggan percaya akan integritas toko online. Ada beberapa cara yang dapat di gunakan dalam menjaga integritas seperti enskripsi, tanda tangan digital dan *certificate authority* (CA), beberapa cara tersebut berguna untuk verivikasi identitas pengguna situs website yang digunakan

Selain *confidentiality* dan *integrity* ada juga *availability* (kesediaan), maksudnya dalam bisnis kita harus menyediakan ketersedianya sistem yang data serta aplikasinya yang dapat diakses kapan pun dan dimanapun oleh pelanggan. Jika tidak ada *availability* maka akan mempegaruhi kepecayaan terhadap perusahaan tersebut karena tidak dapat mengakses data dimana pun dan kapan pun.

Setelah mengetahui konsep keamanan teknologi informasi, kini seharusnya para pebisnis ataupun para pemimpin perusahaan harus memikirkan serta memiliki dengan tepat, akurat serta terperinci dalam mengatur bisnis yang di jalankan, jika tidak akan cukup berisiko apabila tidak memikirkan serta memiliki cibersecurity yang tepat.

Pertama, risiko sebagai individu jika anda sebagai owner atau orang kepercayaan dalam suatu bisnis tersebut yakni anda akan berpotensi kehilangan data informasi pribadi anda yang penting karena data anda tidak mengakses serta atau mengendalikan data pribadi anda sendiri.

Kedua, risiko dalam hal finansial, biasanya yang terjadi seperti hilangnya uang yang ada dalam rekening bank user, hal ini sangat mempengaruhi kepercayaan konsumen terhadap bisnis anda karena sistem keamanan yang anda gunakan mengalami kebocoran data yang berarti sistem pertahanan keamanan data dalam

bisnis anda lemah sehingga dapat di hack oleh hacker.

Ketiga, risiko sebgai orang yang bekerja sebagai profesional,anda akan dipecat dan dapat di tuntut untuk masuk dalam penjara karena seorang hacker dapat meretas data user dan dipergunakan hal yang merugikan pelanggan.

Keempat, resiko yang dialami oleh perusahaan juga berakibat fatal jika hal ini terjadi karena perusahan yang telah berpartner akan tidak saling percaya lagi sehingga kedepannya tidak dapat berkerja sama lagi dalam berbisnis.

Banyak tantangan-tantangan yang dihadapi selama menggunakan teknologi informasi terutama pada sistem keamanannya. Untuk melindungi berbagai macam aktivitas *cybercrime*, ada berbagai cara peningkatan *cyber security* pada sebuah sistem aplikasi yang dapat diterapkan sebagaimana dikutip dalam (Hius, Saputra, & Nasution, 2014) , diantaranya yaitu :

a. Peningkatan standar pengamanan sistem jaringan komputer nasional sesuai dengan standar internasional.Salah satu cara paling mudah adalah dengan tetap menjaga keamanan sistem komputer maupun perangkat lunak dengan melakukan update-update secara berkala dan sesuai dengan standar internasional. Hal tersebut ditujukan untuk menutup celah keamanan yang ada pada sistem agar para pelaku *cybercrime* tidak dapat mencuri informasi-informasi penting yang terdapat pada sistem aplikasi.

b. Perkuat *password* pada setiap akun yang dimiliki dengan menggunakan berbagai kombinasi huruf, angka atau simbol. Dengan kombinasi password yang kuat akan meminimalisir pelaku *cybercrime* untuk melakukan pembobolan.

c. Install perangkat lunak antivirus.Perangkat lunak antivirus dapat digunakan untuk mencegah, mendeteksi dan menghilangkan berbagai *malware* seperti, *hijackers, virus, worms, spyware* dan lain sebagainya. Gunakan antivirus yang up-to-date agar dapat mendeteksi berbagai malware baru.

d. Sebaiknya data-data yang tersimpan pada sistem komputer atau perangkat lunak dapat diback up secara berkala agar data-data tersebut tetap aman apabila suatu saat terjadi pencurian data atau adanya kesalahan pada sistem. Melakukan backup data dapat dilakukan dengan penyimpanan awan *"Cloud"* atau dengan hard disk.

e. Melakukan penegakan hukum pidana pelaku *cybercrime*.Penegakan hukum tentang *cybercrime* terutama di Indonesia sangatlah dipengaruhioleh lima faktor yaitu Undang-Undang, mentalitas aparat penegak hukum, perilakumasyarakat, sarana dan kultur. Semua undang-undang

hukum pidana dijabarkan pada Kitab Undang-undang Hukum Pidana (KUHP) salah satunya tentang tindak kejahatan *cybercrime*. Dengan keterlibatan pihak pemerintahan dan kepolisian dalam mengangani *cybercrime* diharpkan para pelaku kejahatan *cybercrime* dapat diadili sesuai pasal yang berlaku.

Upaya lain yang dapat dilakukan untuk mencegah *cybercrime* terutama pada sistem aplikasi bidang bisnis adalah dengan melakukan kerjasama dengan pihak ketiga seperti konsultan keamanan sistem teknologi informasi untuk mencegah *cybercrime*. Konsultan TI akan melakukan beberapa evaluasi mengenai seberapa aman sistem aplikasi yang digunakan, memberitahu letak-letak kelemahan keamanan sistem dan menentukan solusinya (Supanto, 2016).

4. KESIMPULAN

Berdasarkan kajian yang telah dipaparkan diatas, dapat disimpulkan bahwa pada perkembangan teknologi pada aplikasi bergerak atau biasa disebut dengan teknologi perangkat bergerak diiringi dengan berbabagai tantangan dan risiko, terutama risiko *cybercrime*. Untuk meminimalisir tindak kejahahatan tersebut maka harus ditingkatkan kekuatan *cyber security* pada sistem aplikasi yang digunakan. Upaya peningkatan *cyber security* pada sebuah sistem aplikasi dapat meningkatkan keamanan sistem dari berbagai tindakan *cybercrime* seperti, *hijackers, spyware, virus* dan lain sebagainya. Pihak penegak hukum juga memberikan hukum pidana kepada para pelaku *cybercrime* sesuai dengan pasal yang berlaku.

DAFTAR PUSTAKA

[1] Alvin Yudistriansyah. (2019). Evaluasi Maturity Level Keamanan dan Rekomendasi Perbaikan Keamanan Internet of Things (IOT) PT XYZ Berdasarkan Kerangka Kerja IOT Security Maturity Model. Universitas Indonesia. 1-2.

[2] Budi Rahardjo. (2014). Keamanan Perangkat Lunak. PT Insan Indensia. 7-8.

[3] Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. CAKRAWALA: Jurnal Humaniora Bina Sarana Informatika, 20(1).

[4] Hius, J. J., Saputra, J., & Nasution, A. (2014). Mengenal dan Mengantisipasi Kegiatan Cybercrime pada Aktifitas Online Sehari-Hari dalam Pendidikan, Pemerintahan dan Industri dan Aspek Hukum yang Berlaku. Prosiding SNIKOM, 1(1), 1–9.

[5] Irwan Padli Nasution, M. (2008). Urgensi Keamanan Pada Sistem Informasi. Jurnal Iqra' Volume 02 Nomor 02. 41-43.

[6] Joko Nugroho, Y. (2014). Pemanfaatan Teknologi Bergerak Pada Layanan Perpustakaan. E-Journal Universitas Sanata Dharma. 77-79.

[7] Supanto. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy. Yustisia Jurnal Hukum, 5(1), 52–70.

[8] Ilham Bagus. Cyber Security : Panduan

Lengkap dan Penerapannya. https://niagahoster.co.id. Diakses pada tanggal 2 Juni 2021.

[9] Putri Zakia Salsabila. Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi. https://amp.kompas.com. Diakses pada tanggal 9 Mei 2021.