SABER: Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi
Vol. 2, No. 4 Oktober 2024
e-ISSN: 3025-342X; p-ISSN: 3025-2776, Hal 12-22
DOI: https://doi.org/10.59841/saber.v2i3.1626
Available online at: https://jurnal.stikes-ibnusina.ac.id/index.php/SABER

Analisis Pembuktian Isu Pengambilalihan Akun oleh Pihak Ketiga Aplikasi Zenly Melalui Pemberlakuan UU Perlindungan Data Pribadi

Velycia Debora Gloria
Fakultas Ilmu Komunikasi, Universitas Padjadjaran, Jatinangor, Indonesia
Email: Velycia20001@mail.unpad.ac.id

Abstract*. The era of technological development is accompanied by the ease of obtaining information, digital things need to be considered for their sustainability. The presence of the PAPA concept (Privacy, Accuracy, Property, Accessibility) helps to make companies and applications aware of maintaining information and carrying out digital responsibilities. Privacy is a dimension that focuses on protecting personal data. The social map application is a platform that makes it easy for users to share and find out the location of friends and family. With a total of 35 million monthly active users, the level of data security is increasingly vulnerable because many new users register their personal data into user data. Although only diagnosing cases of account takeovers, of course, action and literacy education are needed because the company is fully responsible. The analysis tool used in qualitative research is Mitmproxy. The Zenly application is the object of this study. The results of the study are proven diagnoses that account takeovers can occur due to low levels of security, thus violating the ITE Law article 26.*

Keywords: *Privacy, Zenly, Account Takeovers, Security Issues.*

Abstrak. Era perkembangan teknologi diiringi oleh kemudahan mendapat informasi, hal-hal digital perlu diperhatikan keberlangsungannya. Hadirnya konsep PAPA (*Privacy*, *Accuracy*, *Property*, *Accessibility*) membantu menyadarkan perusahaan dan aplikasi untuk menjaga informasi dan melakukan tanggung jawab digital. Privasi menjadi dimensi yang berfokus pada perlindungan data pribadi. Aplikasi *social maps* merupakan sebuah *platform* memudahkan pengguna untuk berbagi dan mengetahui lokasi teman dan keluarga. Dengan total 35 juta pengguna aktif bulanan menjadikan tingkat keamanan data semakin rentan karena banyak pengguna baru yang mendaftarkan data pribadinya ke dalam data pengguna. Meski hanya diagnosa kasus *account takeover* tentu diperlukan penindakan serta edukasi literasi karena perusahaan yang bertanggung jawab sepenuhnya. Alat analisis yang digunakan dalam penelitian kualitatif adalah Mitmproxy. Aplikasi Zenly menjadi objek dalam penelitian ini. Hasil dari penelitian adalah terbuktinya diagnosa bahwa bisa terjadi *account takeover* akibat tingkat keamanan yang rendah sehingga melanggar UU ITE pasal 26.

Kata Kunci : Privacy, Zenly, Account Takeover, Security Issue.

1. LATAR BELAKANG

Pada zaman keterbukaan informasi ini, data dapat dengan mudah dan cepat berkembang di masyarakat tanpa adanya batasan. Melihat ini, Richard Mason (1986) berniat untuk melihat etika dalam ranahan penggunaan informasi. Menurutnya ada empat dimensi yang bisa diukur yaitu, ***privacy, accuracy, property,*** **dan** ***accessibility*** yang disingkat dengan PAPA. Privasi tidak bisa diganggu oleh orang lain bahkan negara sekalipun karena seluruh individu memiliki hak atas perlindungan diri pribadi. Privasi sendiri bersifat lebih sensitif yang berkaitan dengan bagaimana cara melindungi harkat dan martabat sebagai seorang individu. Hal ini menggambarkan bagaimana cara manusia melindungi dirinya sendiri dengan membuat batas-batas tentang siapa saja yang bisa mendapat akses terkait dengan diri kita.

Konsep privasi seiring berjalannya waktu memang memiliki definisi yang beragam, bergantung kepada sisi mana yang ingin dilihat. Dulu kita mengenal bahwa privasi

Received: Juni 25, 2024; Revised: Juli 10, 2024; Accepted: Juli 27, 2024; Online Available: Juli 31, 2024;

dilindungi oleh hukum yang didukung oleh konsep John Locke. Saat ini privasi individu juga turut dilindungi baik dari norma-norma budaya, etika, dan praktik profesional agar arus informasi akan individu semakin terkontrol.

Privasi memiliki hubungan erat dengan konsep ruang personal dan teritorialitas. Ruang personal sendiri merupakan kondisi dimana sebuah ruang yang selalu melekat pada diri individu dan akan merasa terganggu bila ruangan tersebut diintervensi oleh orang lain. Sedangkan ruangan yang dapat dimasuki orang lain disebut ruang interpersonal. Memasuki era digital saat ini kondisi privasi yang selama ini dipertahankan mulai bergeser karena perpindahan posisi privasi yang semakin berada dibawah pengawasan era digital. Hal ini terjadi akibat segala jenis komunikasi menjadi lebih canggih, bersifat global, dan bernilai komersial yang membuat mulai hilangnya kontrol atas informasi pribadi seseorang.

Era globalisasi erat hubungannya dengan anak muda atau generasi Z yang lahir di tahun 1997 hingga 2012, disini teknologi dan internet berkembang dengan pesat sehingga mudah dijangkau. Dimasa inilah posisi privasi anak dirasakan semakin rentan, dengan 3 alasan utama yaitu; (1) Mereka kerap kali menjadi pionir dalam rangka eksperimen dan eksplorasi *platform*, layanan, konten digital terbaru. Menjadi kelompok pertama yang menghadapi risiko, sebelum generasi sebelumnya melakukan strategi untuk pencegahan *error* yang ada, (2) Kurang kritis dalam menghadapi risiko baik sekarang maupun dimasa depan akibat penggunaan teknologi digital yang kurang pengalaman. Melihat mereka rentan akan kondisi kesehatan mental, fisik, sosial, maupun ekonomi yang menjadi tantangan untuk meningkatkan literasi media pada anak muda. (3) Hak dan kebutuhan anak yang belum maksimal disediakan lingkungan digital. Konsep *safety and privacy* yang harus ditingkatkan untuk bisa melindungi data pengguna, terutama anak agar informasi yang ada terlindungi. Hal ini juga disampaikan oleh Council of Europe (2018) mengenai pedoman untuk melindungi, menghormati, dan memenuhi hak seorang anak di lingkungan digital sehingga privasi dan perlindungan pada data pribadi muncul sebagai perhatian utama.

Menurut Nissenbaum (2010: 3) sendiri privasi tidak sekedar lagi membahas hak atas kerahasiaan atau kontrol saja, tetapi bagaimana informasi pribadi mengalir di lingkungan digital. Ini menanamkan bahwa privasi bersifat relasional dan kontekstual. Menurut UNICEF, privasi anak dan kebebasan berekspresi yang dipengaruhi oleh teknologi bisa dibedakan menjadi– privasi fisik, komunikasi, informasi, dan keputusan (UNICEF 2018). Privasi fisik dapat dikatakan melanggar bila dalam penggunaan teknologi terdapat pelacakan, pemantauan, atau siaran langsung yang mengekspos gambar, aktivitas, atau

lokasi seorang anak. Sedangkan untuk privasi komunikasi dikaitkan oleh akses ke postingan dan pesan yang tidak diinginkan oleh penerima. Ancaman privasi informasi dapat terjadi pada pengumpulan, penyimpanan, dan pemrosesan data pribadi pada anak yang tidak mendapatkan *consent* dari pihak yang bersangkutan. Terakhir ada gangguan privasi keputusan yang dikaitkan dengan pembatasan atas akses pada informasi sehingga membatasi pengambilan keputusan.

Berdasarkan riset yang dilakukan oleh Pew Research Center, anak muda sekarang lebih sering memberikan informasi mengenai dirinya melalui media sosial. Sebuah tren yang kemungkinan dipengaruhi oleh evolusi *platform digital* memungkinkan adanya kerugian pencurian data pribadi, hal ini didukung oleh fakta lainnya bahwa Gen Z tidak terlalu peduli mengenai pihak ketiga– Cloud Platform, Bug, Maps– yang mengakses data mereka dan hanya 9% yang mengkhawatirkan hal ini. 91% remaja lainnya mungkin tidak memiliki informasi yang cukup dengan akibat yang terjadi jika informasinya digunakan oleh pihak ketiga. Hal ini membawa generasi Z banyak menganggap bahwa privasi– terutama dalam hal ini privasi fisik yang– menjadi hal yang biasa saja karena kurangnya kesadaran dalam etika penggunaan sosial. Mereka cenderung memberikan informasi yang menyangkut dirinya pada media sosial sehingga sulit untuk mengontrol siapa saja yang dapat mengaksesnya karena terlalu luas dan bebasnya media ini. Kelengahan ini diikuti oleh munculnya berbagai aplikasi yang secara tidak kita sadari melanggar privasi pribadi namun tertutup karena cukup membantu dan menghibur kita, salah satunya yaitu Zenly.

Zenly atau beberapa negara mengenalnya sebagai “Popsicle” beberapa tahun belakangan menduduki kursi popularitas untuk sebuah aplikasi *geolocation*. Zenly memberikan akses pada penggunanya untuk membagikan lokasi mereka selama 24 jam – setiap saat dan dimanapun. Di Singapura sendiri, aplikasi ini ramai digunakan oleh anak-anak dari *primary* hingga *secondary,* menurut penuturan James– narasumber TODAY– bahwa aplikasi ini cukup populer di sekolahnya, bahkan setengah murid kelasnya menggunakan Zenly untuk melihat posisi temannya ketika telat masuk kelas. Sekilas memang aplikasi ini cukup bermanfaat namun tanpa disadari Zenly menjadi sarana oknum tidak bertanggung jawab untuk mendobrak privasi penggunanya. Oleh karenanya peneliti tertarik untuk melihat Zenly *privacy concern* untuk membantu mengurangi kekhawatiran pengguna aplikasi.

2. METODE PENELITIAN

Penelitian ini dilaksanakan dengan menggunakan pendekatan penelitian kualitatif. Gunawan *et al.* (2023) menjelaskan bahwa penelitian kualitatif dilaksanakan untuk memahami fenomena berdasarkan perspektif manusia yang sedang diteliti secara menyeluruh. Dalam penelitian kualitatif, peneliti memiliki peranan yang sangat penting dalam setiap prosesnya dari mulai mengumpulkan, memahami, hingga menafsirkan data dari fenomena yang ingin diamati. Penelitian ini menggunakan metode deskriptif kualitatif dimana peneliti akan mendeskripsikan dan menggambarkan fenomena dengan lengkap, rinci, dan mendalam (Nugrahani, 2014). Kualitatif deskriptif memiliki tujuan untuk mendeskripsikan atau menggambarkan fenomena dengan apa adanya.

3. HASIL DAN PEMBAHASAN

A. Zenly

Zenly merupakan aplikasi yang masuk kedalam kategori *social networking* dengan *geolocation tracking*, aplikasi ini cukup populer dikalangan anak muda hampir seluruh dunia. Zenly menyediakan kemudahan untuk teman maupun keluarga melacak lokasi satu sama lain secara *real time* hanya dengan tap foto profil seseorang. Ikut meramaikan bidang *geolocation*, *social network,* hingga *messaging and utility*, Zenly berhasil mengepakkan sayapnya dengan target utama kalangan remaja hingga mencapai 1 juta pengguna terdaftar. Awalnya, aplikasi ini dikembangkan oleh perusahaan asal Perancis yang kemudian diakuisisi oleh Snap Inc – perusahaan Snapchat pada tahun 2017 kemarin. Tujuan bergabungnya pada Snapchat ini berlandaskan bahwa perkembangan Zenly yang sudah semakin besar skalanya dan butuh lebih banyak pengawasan dan dukungan dari profesional. Melihat dari fungsinya, peneliti membaginya kedalam dua kategori yang berbeda yaitu media sosial dan fungsi berbagi lokasi.

B. Zenly Reputation

Zenly hadir dari sebuah aplikasi kecil yang berevolusi menjadi media sosial raksasa dengan pengguna aktif mencapai total 35 juta perbulannya. Aplikasi ini bukan *messaging app*, *social network,* bahkan *utility,* namun sesuatu yang berdiri di tengah tengah dengan keinginan membuat aplikasi peta sosial definitif yang menjadi pendobrak inovasi baru dalam media sosial.

Persaingan sengit untuk sebuah developer aplikasi dimana rata-rata orang memasang 60-90 aplikasi pada ponselnya dan hanya 30 saja yang digunakannya, sedangkan ada 9 aplikasi baru yang berhasil diluncurkan. Zenly tentu saja sadar akan kondisi ini, maka dari itu untuk mendapatkan perhatian pengguna maka kolaborasi dengan BPO pun dilakukan untuk memberikan akses mudah dalam bahasa, terutama bahasa di Asia yang memang sulit untuk diterjemahkan. Kerja keras Zenly membuahkan hasil jika dilihat dari matriks, aplikasi ini semakin lebih baik dari sebelumnya. Menurut data.ai sendiri pada Maret 2022, Zenly masuk ke dalam urutan 10 *most-downloaded social app globally*. Aplikasi ini sangat populer di Jepang, Asia Tenggara, dan Eropa Timur, bahkan sudah memasuki Brasil dan India.

C. Zenly User Datas

Zenly sebagai aplikasi *tracking location* mengizinkan penggunanya untuk melihat lokasi teman atau keluarga setiap saat, menampilkan persentase baterai ponsel, hingga kecepatan gerak seseorang. Kemudahan yang diberikan sungguh mengkhawatirkan karena Zenly secara otomatis dapat mendeteksi rumah, tempat kerja, sekolah dan memperhitungkan kegiatan rutinitas para penggunanya. Semua informasi ini akan ditampilkan dengan ikon kecil yang dilampirkan di sebelah profil para pengguna.

Memang pada awalnya hanya berfokus pada teman-teman dekat saja, namun dengan kemudahan *add friend* melalui kontak pada ponsel menjadi berbahaya karena lebih mudah untuk menambah dan menerima permintaan pertemanan walaupun dari orang asing. Apakah para *user* merasa aman dengan mengungkapkan lokasi mereka secara jelas selama 24 jam? Bagaimana Zenly mengelola seluruh data penggunanya?

Keresahan beberapa pihak juga dipahami oleh Zenly yang merasa bahwa privasi itu sesuatu yang penting, terutama dalam hal berbagi lokasi yang cukup sensitif. Zenly membantu penggunanya dengan menyediakan fitur visibilitas dan kontrol penuh atas apa saja yang ingin dibagikan dan dilihat oleh orang lain. Data sendiri bersifat pribadi dan itu akan disimpan oleh Zenly selama pengguna akun aktif menggunakan aplikasi, namun ada untuk pengguna tidak aktif sebagian besar data disembunyikan dan sebagian lainnya digunakan untuk kebutuhan penelitian.

Berdasarkan privacy & policy Zenly sendiri Ada beberapa kategori informasi yang dikumpulkan oleh Zenly sebagai upaya untuk tetap transparan.

- Informasi yang pengguna berikan

Berisi informasi umum seperti nama pengguna, nama tampilan, dan nomor telepon, lokasi, dan fitur komunikasi. Seluruh informasi ini akan dihapus jika akun terdeteksi tidak digunakan selama 1 tahun dan juga bila ada permintaan khusus.

- Informasi yang didapatkan saat menggunakan aplikasi Zenly

  Data seperti informasi terkait penggunaan aplikasi, analisis statistik, informasi yang dihimpun dari aktivitas pengguna – tempat yang dikunjungi, dan otentikasi dan informasi sesi. Seluruh data yang terkumpul akan dihapus dengan keadaan akun yang sudah tidak aktif minimal satu tahun, serta ada data yang dianonimkan oleh Zenly.

- Informasi yang didapatkan dari pihak ketiga

  Pihak ketiga dari Zenly sendiri sudah melakukan perjanjian untuk melindungi data pribadi pengguna aplikasi. Beberapa tipe *third parties* yaitu cloud, bug, maps, analytic, dan internal software dimana Zenly membagikan data sesuai dengan porsi pekerjaan masing-masing.

Zenly secara sadar mengetahui bahwa data merupakan suatu yang harus dijaga dengan benar, dengan itu aplikasi ini hanya meminta data sesuai kebutuhan saja dan seluruh data akan disimpan selama pengguna aktif menggunakan Zenly. Untuk akun yang sudah tidak dioperasikan selama satu tahun, sebagian data mereka akan dihapus dan beberapa informasi akan dianonimkan guna keperluan internal dalam membuat statistik dan penelitian.

D. Account Takeover by Friend Request

Menurut privacy policy milik Zenly. "*Zenly is an app that makes it fun and easy to know that your friends and family are up to and keep memories of your real life interactions. With Zenly, you can keep up with the people you care about the most, both near and far, create a personal diary of where you've been or publicly showcase the places you've visited.*"

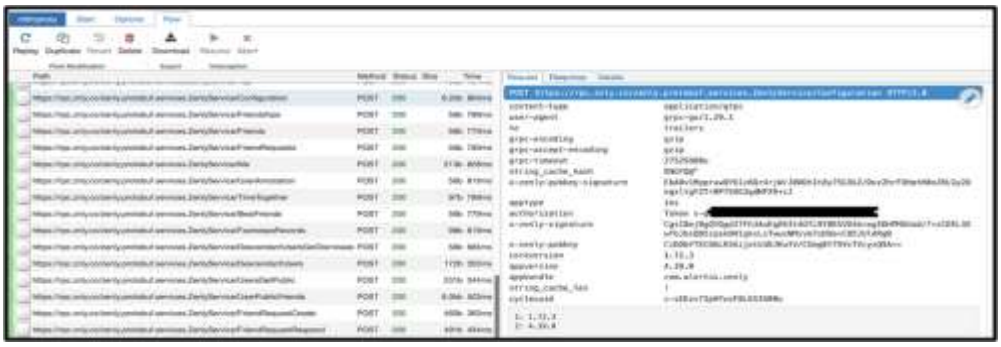
Setelah membaca kebijakan privasi mereka dan merasakan langsung semua fitur dan kemudahan dari aplikasi ini, peneliti bisa mendiagnosis bahwa adanya kerentanan eksposur data pengguna sehingga rentan terjadi *account takeover* yang berpotensi mengancam keamanan Zenly's *users*. Diagnosa ini terjadi ketika permintaan pertemanan dikirimkan kepada pengguna, Zenly akan mengizinkan akses ke nomor telepon pengguna terlepas apakah permintaan diterima ataupun tidak sehingga untuk melancarkan aksinya, oknum cukup mengetahui nama akun mereka dan ini dipermudah karena Zenly juga memperlihatkan daftar lengkap teman pengguna. Artinya pelaku cukup mengikuti *mutual friends* dari salah satu pengguna Zenly.

Sumber. checkmarx.com

Gambar 1. Zenly Statements

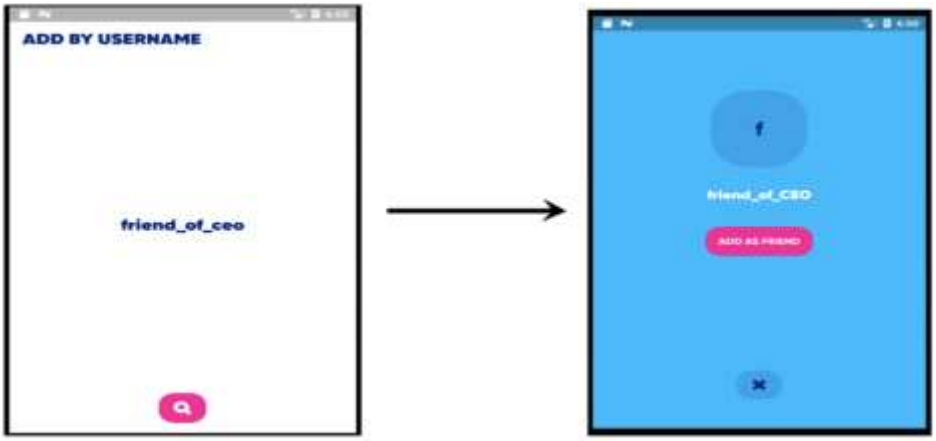
Berdasarkan dokumentasi diatas, dapat terlihat bahwa nomor telepon pengguna tidak mungkin diambil kecuali pengguna sudah saling berteman.

Berikut adalah bukti proses bagaimana seorang bisa melakukan Account Takeover pada akun Zenly dengan tools Mitmproxy :



Sumber. checkmarx.com

Gambar 2. Tampilan Mitmproxy



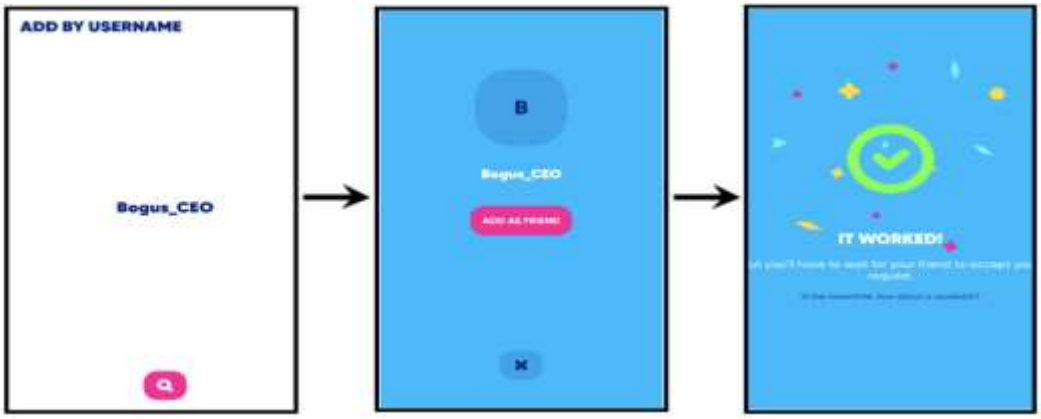
Sumber. checkmarx.com

Gambar 3. Step pertama proses *account takeover*

Langkah awal bisa dengan memanfaatkan fitur "Add by Username", dimulai dengan mencari nama pengguna yang kita kenal. Tools Mitmproxy bisa membantu untuk melihat aktivitas selama penggunaan Zenly berlangsung.

Sumber. checkmarx.com

Gambar 4. Tampilan Mitmproxy setelah percobaan pertama



Sumber. checkmarx.com

Gambar 5. Step kedua proses *account takeover*

Setelah melakukan pencarian di awal, maka muncul (data 2) sebuah *username* dari sistem, ini memperlihatkan salah satu teman dari pengguna pertama (friend_of_ceo) yang kita cari. Meskipun daftar teman tidak ditampilkan dalam UI aplikasi, namun bisa dilihat melalui *tools* lainnya.

Sumber. checkmarx.com

Gambar 6. Tampilan Mitmproxy setelah aktivitas permintaan pertemanan terkirim

Setelah proses permintaan pertemanan sudah terkirim, maka adanya penambahan data baru dalam *tools* yang digunakan. Dapat diperoleh nomor telepon dari pengguna yang kita kirimkan *friend request,* data ini diperoleh ketika sudah menekan tombol "Add as Friend", namun jika tidak– seperti langkah pertama– maka data yang diperoleh hanya daftar temannya saja.

Bisa dilihat jika undangan pertemanan ini akan memicu permintaan ke sistem untuk memberikan informasi spesifik mengenai pengguna– data 3,4,6 dan target– data 4,7,8. Nomor telepon pengguna dan target akan terpampang jelas walaupun permintaan pertemanan belum diterima maupun sudah ditolak.

E. Indulging The Perks of Third-Party Data Sharing

Sebenarnya preferensi terhadap transparansi data memiliki banyak sudut pandang yang bisa dilihat, salah satunya pendekatan *win-win* yang diambil antara perusahaan dengan pihak ketiga– perangkat lunak– untuk penukaran informasi pengguna. Data yang dibagikan melalui pihak ketiga rupanya berpotensi meningkatkan kemampuan perusahaan untuk menggunakan data kembali yang mungkin sebelumnya sulit untuk diakses (OECD,2019; melalui Patiroi, 2022). Pembagian informasi dapat dimanfaatkan untuk meningkatkan efisiensi aplikasi karena memungkinkan terciptanya pengalaman yang nantinya berpengaruh pada pemrosesan *big data* dengan tujuan mendapatkan loyalitas pengguna.

Berbagi data sebenarnya merupakan hal yang lumrah, namun penting untuk dipertimbangkan potensi risiko mengingat ini menyangkut data pribadi yang seharusnya dilindungi. Dari sinilah perusahaan terlebih lagi wajib memastikan bahwa data pribadi seseorang yang dibagikan dengan pihak ketiga dilakukan dengan *terms and condition* dan tanggung jawab, serta sesuai dengan undang undang yang berlaku di Indonesia serta memperoleh persetujuan dari individu pemilik data.

Berbicara mengenai undang-undang, terdapat Pasal 26 ayat (1) UU ITE yang mengatur perlindungan data pribadi, "Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan, setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan." Tingginya risiko keamanan data pengguna Zenly diambil alih, menimbulkan dugaan bahwa Zenly sudah melanggar UU ITE pasal 26. Kemudian untuk aplikasi Zenly sendiri meskipun sudah memiliki kebijakan keamanan sendiri, harus tetap bertumpu pada hukum negara aplikasi berada dimana tidak boleh melakukan pelanggaran terhadap undang-undang

yang berlaku. Namun kenyataannya, akses terhadap data pribadi pengguna yang mudah dan tanpa sepengetahuan pemilik data pribadi diambil, hal ini tentu melanggar ketentuan sebagaimana UU ITE diatur.

Dengan terbuktinya bahwa *account takeover* pada Zenly berpeluang besar untuk terjadi, maka perlu adanya perhatian khusus dari perusahaan dan pemerintah akan hal ini. Bagi pengguna Zenly, turut menjaga kebocoran data sudah diluar kendalinya sendiri karena mereka tidak menyadari apa yang sudah dilakukan ternyata masuk kedalam transaksi data elektronik. Maka dari itu perlunya keketatan khusus dari perusahaan maupun dengan pihak ketiga yang ikut berkontribusi dalam pengambilan data seperti dalam kasus ambil alih akun.

Sayangnya, pernyataan dari Zenly pada awal bab terkait yang menyatakan bahwa data pribadi, seperti nomor telepon tidak akan bisa diakses dan hanya bisa jika sudah melakukan pertemanan. Namun setelah tes dilakukan, terbukti adanya ketidaksesuaian antara pernyataan Zenly dengan isu ambil alih akun yang terjadi. Data pengguna yang terpampang dapat digunakan oleh oknum tak bertanggung jawab untuk melakukan penyerangan, teror atau *doxing*.

4. KESIMPULAN

Dapat disimpulkan dari hasil analisis bahwa aplikasi Zenly berpotensi adanya pelanggaran keamanan data pribadi yaitu ambil alih akun dengan akibat kurang ketat dalam menyimpan data privat para penggunanya. Pemerintah juga turut berkontribusi dengan dikeluarkannya pasal 26 UU ITE yang mengatur perlindungan data pribadi. Bahwasanya, penggunaan data yang diambil melalui media elektronik dan menyangkut data pribadi wajib hukumnya untuk meminta persetujuan.

Namun bila sudah terjadi kebocoran data atau penggunaan data pribadi yang salah, maka pengguna Zenly bisa membatasi dan membentuk data secara efektif dan saat pencarian nama dilakukan, alih-alih mengembalikan daftar lengkap yang berisi nama *mutual friends* dari pengguna.

5. DAFTAR REFERENSI

Burney, A., Asif, M., Abbas, Z., & Burney, S. (2018). Google Maps security concerns. Journal of Computer and Communications, 6(1), 275–283. https://doi.org/10.4236/jcc.2018.61027

Choo, D. (2019, April 18). App popular among school children raises parents' concern over location-tracking function. TODAY. https://www.todayonline.com/singapore/more-students-using-zenly-app-parents-concerned-about-location-tracking-function

Deck, A. (2022, September 20). The Zenly implosion: Inside 6 months of tension, culture clash, and conflict. Rest of World. https://restofworld.org/2022/fearing-competition-snap-decided-to-shut-down-zenly-rather-than-sell-it/

London School of Economic. (2018). Children's data and privacy online growing up in digital age. LSE Media and Communication.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. In Pew Research Center. https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/

Mink, J., Yuile, A. R., Pal, U., Aviv, A. J., & Bates, A. (2022). Users can deduce sensitive locations protected by privacy zones on fitness tracking apps. In CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3491102.3502136

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and integrity of social life. Stanford University Press.

Rahmatullah, T. (n.d.). Kajian mengenai privasi dalam informasi digital dihubungkan dengan Directive 95/46/EC dan Directive 2002/58/EC of The European Parliament and of The Council. Jurnal Hukum Media Justitia Nusantara, 7(1), 58–72. https://doi.org/10.13140/RG.2.2.30544.97284

Revilia, D., & Irwansyah, N. (2020). Social media literacy: Millenial's perspective of security and privacy awareness. Jurnal Penelitian Komunikasi Dan Opini Publik, 24(1). https://doi.org/10.33299/jpkop.24.1.2375

TechCrunch is part of the Yahoo family of brands. (2022, April 22). https://techcrunch.com/2022/04/22/how-zenly-made-social-maps-cool-again-and-whats-next/

Undang Undang Republik Indonesia Tentang Informasi dan Elektronik. (2008). Retrieved from https://www.dpr.go.id/doksetjen/dokumen/-Regulasi-UU.-No.-11-Tahun-2008-Tentang-Informasi-dan-Transaksi-Elektronik-1552380483.pdf

Yalon, E. (2022). Zenly fixes user data exposure and account takeover risks. Checkmarx.com. https://checkmarx.com/blog/zenly-fixes-user-data-exposure-and-account-takeover-risks/

Yunita, & Enny. (2023, May 17). The PAPA & digital maturity. Jatinangor.

Zenly. (2023). Retrieved from https://community.zen.ly/hc/en-us/sections/360000114067-Privacy-Security