DEVIANCE: JURNAL KRIMINOLOGI
Volume 3 Nomor 2 Desember 2019
Hal: 157-169

Pencegahan Viktimisasi Pencurian Data Pribadi

Claudia Clarentia Ciptohartono, Mohammad Kemal Dermawan
Universitas Indonesia
claudia.clarentia@gmail.com

Abstrak: Penelitian ini membahas strategi pencegahan viktimisasi pencurian data pribadi di Indonesia. Dengan keberadaan internet, kehidupan manusia tidak lagi berlangsung hanya di dunia fisik saja tetapi sudah merambah ke dunia maya, begitu pula dengan kejahatan. Transisi kejahatan didukung oleh keberadaan internet yang mendukung akses ke dunia maya lewat *smartphone*. Penelitian ini bertujuan untuk meningkatkan kesadaran keamanan masyarakat dan mencegah masyarakat menjadi korban kejahatan pencurian data pribadi. Penelitian dilakukan dengan *mixed-method* kuantitatif dan kualitatif menggunakan kuesioner terstandar dan survei viktim serta *self-report* mengenai pengetahuan, persepsi, dan perilaku masyarakat. Terdapat 179 responden dengan batasan: berusia dewasa, berdomisili di Jabodetabek, dan menggunakan *smartphone* pribadi. Hasil penelitian menunjukkan bahwa nilai kesadaran keamanan responden terhadap alat (*smartphone)*, sistem, dan ruang (internet) cukup baik yaitu 67,03% pada tingkat kesadaran tinggi. Namun jika dinilai secara terpisah, penilaian terhadap kesadaran menjadi semakin menurun dan berada di tingkat rendah-menengah dengan nilai paling rendah pada kesadaran terhadap ruang. Kemudian penilaian kesadaran terhadap data pribadi, yaitu 56,98% pada tingkat kesadaran menengah dan jika dinilai secara terpisah antara pengetahuan, sikap, dan persepsi dengan perilaku hasilnya semakin menurun. 44,69% responden memiliki kesadaran dengan nilai nol pada perilaku terhadap data pribadi umum. Tidak mengherankan jika hasil survei menunjukkan 94,97% responden pernah menjadi korban pencurian data pribadi, terutama pada kejahatan pencurian data dengan tingkat rendah. Untuk itu, strategi pencegahan viktimisasi yang terbaik adalah dengan memperbaiki aspek penentu kesadaran keamanan terutama dalam berperilaku dalam kepemilikan data pribadi dan *smartphone*, juga dalam menggunakan sistem, aplikasi, dan internet.
Kata kunci: viktimisasi, pencurian data pribadi, strategi pencegahan kejahatan

Abstract: *This research discusses strategies to prevent the victimization of personal data theft in Indonesia. With the existence of the internet, human life no longer takes place only in the physical world but has penetrated into cyberspace, as well as crime. The crime transition is supported by the existence of the internet that supports access to cyberspace via smartphones. This research aims to increase public safety awareness and prevent people from becoming victims of personal data theft crimes. The study was conducted with mixed quantitative and qualitative methods using standardized questionnaires and public survey surveys and self-reports on knowledge, perceptions, and behavior. There are 179 respondents with restrictions: adults, domiciled in Greater Jakarta, and using a personal smartphone. The results showed that the value of respondents' security awareness of tools (smartphones), systems, and spaces (internet) was quite good at 67.03% at a high level of awareness. However, if assessed separately, the assessment of consciousness becomes increasingly decreased and is at the low-middle level with the lowest value on awareness of space. Then the assessment of awareness of personal data, which is 56.98% at an intermediate level of awareness and if assessed separately between knowledge, attitudes, and perceptions with behavior the results decrease. 44.69% of respondents have zero value awareness of the behavior of public personal data. It is not surprising if the survey results showed that 94.97% of respondents had been victims of personal data theft, especially on*

low-level data theft crimes. For this reason, the best prevention strategy for victimization is to improve the determinants of security awareness, especially in behaving in the possession of personal data and smartphones, as well as in using systems, applications and the internet.
Key Words: *victimization, personal data theft, crime prevention strategies*

Pendahuluan

Dengan keberadaan internet, kehidupan manusia tidak lagi berlangsung hanya di dunia fisik saja tetapi sudah merambah ke dunia maya. Begitu pula dengan kejahatan. Sudah terjadi transisi ruang kehidupan yang begitu luas (Jaishankar, 2008) yang dilakukan lewat *smartphone* dan dihubungkan lewat sistem ke internet. Menurut survei APJII 2018, jumlah pengguna internet di Indonesia sudah menembus angka 171,17 juta jiwa dengan tingkat penetrasi mencapai 64,8%. Jumlah ini terus meningkat menilik survei APJII 2017 yang mencatat pengguna internet di Indonesia sejumlah 143,26 juta jiwa dengan tingkat penetrasi 54,68%. (APJII, 2019) Hampir seluruh pengguna internet di Indonesia mengakses dunia maya lewat *smartphone*, sedangkan pengguna *mobilephone* atau telepon seluler sudah mencapai 59,59%. (BPS, 2017) Ini berarti lebih dari setengah penduduk Indonesia rentan akan kejahatan di dunia maya.

Nama lengkap, nomor dan data atau informasi formal penting terkait kenegaraan maupun perusahaan, gambar dan video pribadi, percakapan pribadi, dan berbagai kebutuhan pribadi. Jika dilihat lebih lanjut, keberadaan *smartphone* dan internet ini membuat kita semua secara tak sadar memiliki identitas digital yang dapat diakses oleh orang-orang yang tak bertanggung jawab sehingga dapat menjadikan kita korban tanpa kita sadari.

Pada tahun 2016 sempat sangat gempar dikarenakan terkuaknya proyek besar yang dikerjakan Cambridge Analytica untuk Kampanye Donald Trump di Amerika Serikat dan Kampanye Brexit di Inggris. Cambridge Analytica "mencuri" data sekitar 50 juta akun Facebook pada tahun 2014 yang digunakan sebagai tambang persona untuk kemudian dianalisis untuk keperluan proyek kampanye politik. (Tirto, 2019) Ini merupakan kasus eksploitasi data pribadi terbesar yang pernah terjadi selama ini dan meningkatkan kesadaran masyarakat akan pentingnya hak atas data pribadi.

Karena kasus itulah, rasa aman pengguna Facebook yang tersebar di seluruh dunia berada dalam situasi yang kritis. Dalam teori hierarki kebutuhan manusia, rasa aman berada pada tingkat kedua di atas kebutuhan dasar fisiologis manusia seperti sandang, pangan, dan papan. (Maslow, 1943) Hal ini menunjukkan bahwa rasa aman merupakan kebutuhan manusia yang penting.

Di Indonesia sendiri juga mengalami kasus peretasan yang dilakukan seorang *hacker* dari Pakistan yang mencuri 13 juta data akun dari situs perbelanjaan Bukalapak. (Kompas, 2019) Sekalipun dibantah oleh Bukalapak, data ini akan

dijual di pasar gelap yang ada di internet, atau lebih dikenal dengan *Dark Web* (Situs Gelap). Sistem yang kuat seharusnya menjadi kewajiban dari seluruh pemain besar di dunia internet. (Detik, 2019) Dan bahkan dari lapas, kejahatan lewat internet dan telepon seluler tetap dapat dilakukan, seperti pada kasus pengungkapan sindikat penipuan online dari Tapanuli Utara sebesar Rp 1,17 miliar. (Kompas, 2019)

Data pribadi yang tidak memiliki wujud fisik sering diabaikan keberhargaannya terutama jika dihubungkan dengan kehidupan sosial. Masyarakat menjadi rentan karena seharusnya dan sebaiknya kita sendiri menjaga data pribadi yang kita miliki dan taruh di internet sebagai usaha untuk mecegah viktimisasi atas data pribadi masing-masing. Keramahan dan ketidaktahuan yang membudaya juga memberi banyak celah dalam melakukan kejahatan terkait kepemilikan data pribadi. Seperti yang diungkapkan oleh Kepala Sub Direktorat Penyidikan Kementerian Kominfo, kebiasaan orang Indonesia yang gampang memaafkan juga menjadi penyebab fraud (kecurangan) jarang dilaporkan. Sifat pemaaf ini berdampak pada banyaknya kasus penipuan yang terjadi di mana-mana, terutama di dunia maya. Namun kebanyakan korban penipuan online justru memilih bungkam ketimbang melaporkannya ke pihak berwajib, jika kerugiannya di atas Rp 500.000 baru masyarakat akan melapor. (Msn, 2019)

Menjadi korban dari pencurian data digital ini seringkali tidak diberitakan jika hanya dialami oleh satu atau dua individu secara terpisah. Kecuali jika ini melibatkan pihak terkenal atau figur publik dan pemberitaan inilah yang paling banyak muncul di media. Pencurian atau penyebaran data berupa video porno, foto "syur", dan berbagai data intim pribadi yang telah dialami oleh beberapa artis dan pejabat sudah tidak asing lagi bagi kita. Seperti kasus yang menimpa artis VA dan merebak ke seluruh jaringan prostitusi onlinenya , penyebaran video 'Vina Garut' , dan yang paling heboh pada kasus sensasionl yang terjadi pada 2010 yang menimpa 2 artis dan seorang penyanyi pria. Merebaknya kasus Ransomware WannaCry, Muslim Cyber Army, dan serangan pada beberapa perusahaan dalam negeri dalam 2 tahun terakhir ini adalah salah satu contoh kecerobohan yang terjadi lewat sistem sehingga kita dapat menjadi korban.

Kecerobohan dari manusia sendiri merupakan celah terbesar, contohnya dengan membuat kata sandi yang mudah ditebak atau tidak pernah mengganti kata sandi secara reguler. Atau membiarkan orang lain mengakses *smartphone* kita dan memberikan nomor telepon kita kepada orang asing. Kekhawatiran terbesar dalam masalah keamanan informasi pada era saat ini adalah serangan yang lebih terkenal dengan *social engineering attack*. (Kearney, 2010) Sebuah serangan yang memanfaatkan kelemahan manusia. Karena pekerja di sektor IT yang paling membutuhkan keamanan sekalipun masih sering terjadi kelalaian dan mengalami serangan dalam berbagai bentuk. Apalagi masyarakat umum yang awam dan terutama kurang akan pengetahuan ini. Karena selama masih ada partisipasi manusia, di situlah kejahatan bekerja dengan memanfaatkan kelemahan dari kelalaian, rasa aman, dan kepercayaan.

Untuk itulah dibutuhkan strategei pencegahan kejahatan yang tepat agar seluruh lapisan masyarakat yang merupakan sasaran dari kerentanan kejahatan pencurian data ini terhindar dari viktimisasi. Hal ini akan sangat membantu dalam meningkatkan kesadaran akan pentingnya menjaga kemanan data pribadi agar tidak dicuri oleh pihak lain yang tidak diinginkan dan merugikan di kemudian hari.

Metode Penelitian

Populasi dalam penelitian ini adalah seluruh kontak pada *smartphone* peneliti yang terbagi dari aplikasi *WhatsApp* dan *Telegram* dengan sistem *broadcast* sejumlah 400 dalam waktu 24 jam. Sampel yang diambil adalah yang dianggap mampu mewakili karakteristik populasi, yaitu yang berdomisili di Jabodetabek, karena sampel ini merunut dari kota dengan target kejahatan tertinggi, penggunaan smartphone terbanyak, dan penetrasi internet tertinggi di Indonesia (menurut survei susenas 2018), yaitu Jakarta.

Objek atau target data pada penelitian kuantitatif deskriptif ini terbagi menjadi 3 kategori besar, yaitu: Kesadaran keamanan yang mencakup: pengetahuan, persepsi, sikap, dan perilaku dalam menggunakan dan mengelola Alat, Sistem, dan Ruang (Penyelenggara Sistem Elektronik). Alat, sistem, dan ruang ini masing-masing diwujudkan dalam *smartphone*, sistem operasi dan aplikasi, dan internet yang digunakan sebagai media penyimpanan, penyalur, dan penjaga dari data pribadi. Berikut adalah modul yang digunakan dalam melakukan penelitian ini:

Tabel 1. Modul Penelitian Pencegahan Viktimisasi Pencurian Data Pribadi

Modul	Tujuan
1. Karakteristik Responden	Untuk memperoleh data Responden, yaitu: usia, jenis kelamin, dan domisili sebagai data demografi. Kemudian pendidikan, wawasan, kegiatan utama, pendapatan, pelatihan terkait *IT* dan data pribadi.
2. Kesadaran Keamanan terhadap Penyelenggara Sistem Elektronik dan Data Pribadi	Untuk memperoleh kesadaran keamanan terkait *smartphone* sebagai alat, penyedia sistem operasi dan aplikasi sebagai sistem, dan penyedia jasa internet sebagai ruang terjadinya pencurian data pribadi.
3. Kerentanan korban pemilik data pribadi	Untuk memperoleh kerentanan korban dan mendapatkan data terkait kebaruan, frekuensi, kelemahan dan viktimisasi dari sisi korban.
4. Pelaku pencurian data pribadi	Untuk memperoleh kerentanan korban dan mendapatkan data dari pelaku terkait jenis pencurian data pribadi, kebaruan, frekuensi, target, dan penetapan viktim dari sisi pelaku.

Untuk analisis data dilakukan dengan beberapa tahap, yaitu:

1. Menemukan tingkat kesadaran, sikap, dan perilaku masyarakat akan keamanan data pribadi.
2. Menemukan tingkat kesadaran, sikap, dan perilaku masyarakat akan keamanan alat, sistem, dan ruang. (*smartphone*, sistem operasi dan aplikasi, dan internet)
3. Menemukan korban pencurian data pribadi: Merumuskan karakteristik kerentanan
4. Menemukan pelaku pencurian data pribadi: Merumuskan karakteristik tendensi
5. Merumuskan strategi pencegahan viktimisasi pencurian data pribadi.: Metode untuk mempersulit pencurian data pribadi

Hasil dan Pembahasan

Pada tabel berikut ini akan ditampilkan data dari masing-masing kesadaran terhadap alat, sistem dan ruang yang dibagi menjadi tiga kategori penilaian untuk tingkat kesadaran keamanan responden.

Tabel 2. Kesadaran terhadap alat, sistem, dan ruang

Tingkat kesadaran keamanan	Rendah	Menengah	Tinggi
TOTAL	2 (0,11%)	57 (31,84%)	120 (67,03%)
Alat (*smartphone*)	33 (18,43%)	128 (71,5%)	18 (10,05%)
Sistem (sistem operasi dan aplikasi)	52 (29,05%)	122 (68,15%)	5 (2,79%)
Ruang (internet)	79 (44,13%)	99 (55,3%)	1 (0,55%)

Semakin terjadi perpindahan ruang dari fisik ke ruang maya, maka kesadaran responden semakin berkurang. Rata-rata responden memang cukup baik dengan mendapatkan nilai menengah dari hasil penilaian dengan batas terendah pada penilaian kesadaran ini. Namun hal ini membuktikan bahwa ada kemungkinan responden menjadi korban dari pelanggaran-pelanggaran kecil dari kejahatan pencurian data pribadi

Tabel 3. Kesadaran terhadap data pribadi

Tingkat kesadaran keamanan terhadap data pribadi	Tidak ada	Rendah	Menengah	Tinggi
TOTAL	-	61 (34,07%)	102 (56,98%)	16 (8,93%)
Pengetahuan	-	30 (16,75%)	93 (51,95%)	56 (31,28%)
Sikap	-	2 (1,11%)	73 (40,78%)	104 (58,1%)
Persepsi	-	37 (20,67%)	104 (58,1%)	38 (21,22%)
Perilaku (Data Umum)	80 (44,69%)	68 (37,98%)	27 (15,08%)	4 (2,23%)
Perilaku (Data Sensitif)	63 (35,19%)	74 (41,34%)	29 (16,2)	13 (7,26%)
Total	39,94%	39,66%	15,64%	4,74%

Jika dilihat secara total, kesadaran terhadap keamanan data pribadi terlihat pada tingkat rendah-menengah. Namun jika dilihat perbagian dari variabel penenti nilai akan terlihat penyimpangan pada data sebagai berikut:

- Pengetahuan dan Sikap responden terhadap keamanan data pribadi tergolong menengah-tinggi dan sangat jatuh pada perilaku.
- Pada praktiknya atau lebih tepat disebut perilaku, 39,94% responden tidak memiliki perilaku yang menjunjung keamanan data pribadi sama sekali atau sama dengan 0 (nol). Nilai yang tidak ada pada variabel lain seperti pengetahuan, sikap, dan persepsi karena pada dasarnya manusia selalu berusaha memikirkan yang terbaik. Tetapi faktanya berperilaku yang tepat tidak semudah itu bagi sebagian responden. Dan tidak jauh berbeda, 39,66% memilliki kesadaran keamanan data pribadi yang rendah.

Tabel 4. Hubungan jenis kelamin dengan tingkat jumlah korban

	Laki-laki	Perempuan	Total
Jumlah korban kejahatan pencurian data (survei)	78 (96,26%)	92 (93,87%)	170 (94,97%)

Jumlah korban kejahatan umum (BPS)	63,25%	36,75%	1,08%

Dari total 179 responden, 170 responden atau 94,97% pernah mengalami viktimisasi pencurian data pribadi. Dan jika dilihat menurut jenis kelamin ternyata memberikan hasil yang berbeda dengan kejahatan konvensional pada umumnya. Karena antara laki-laki dan perempuan memiliki persentase yang tidak berbeda jauh, sekalipun jumlah korban laki-laki sedikit lebih banyak.

Tabel 5. Hubungan jenis kelamin dengan tingkat kerentanan sebagai korban

Tingkat korban kejahatan pencurian data	Tidak pernah	Rendah	Menengah	Tinggi
Laki-laki	3	50	25	3
Perempuan	6	72	19	1
Total	9	122	44	4

Dari 179 responden viktimisasi pencurian data pribadi hanya total 4 orang (5,7%) yang seringkali mengalaminya atau termasuk pada tingkat viktimisasi tinggi dan 75% berdomisili di Jakarta. Dan responden yang mengkau tidak pernah mengalami menjadi korban ada 9 orang atau 5%. Dengan angka paling tinggi pada tingkat korban kejahatan pencurian data rendah, laki-laki memiliki kecenderungan menjadi korban pada tingkat yang menengah dan tinggi, sedangkan perempuan cenderung mengalami viktimisasi pada tingkat yang rendah. Dan dari data di atas dapat disimpulkan bahwa pengaruh jenis kelamin secara umum tidak perlu diperhitungkan.

Untuk hubungan data dari usia, pada lansia kerentanan sedikit berkurang dan yang merupakan korban tingkat tinggi tidak ada. Sehingga dapat disimpulkan bahwa pengaruh usia secara umum tidak perlu diperhitungkan. Dari data lain juga dapat disimpulkan bahwa pengaruh lokasi secara umum tidak perlu diperhitungkan karena jumlah viktim yang banyak dari Jakarta dikarenakan jumlah responden terbanyak juga dari Jakarta.

Untuk hubungan dari keberadaan latar belakang pendidikan IT mampu memberikan dampak yang cukup lebih baik. Namun pendidikian IT maupun tambahan wawasan data pribadi dari kehidupan sehari-hari kembali lagi tidak mampu memberikan pengaruh yang signifikan. Hal ini dikarenakan ada banyak sekali faktor dari luar yang menyebabkan seseorang menjadi korban, terutama yang berkaitan dengan sisi manusia. Bertambah tinggi paparan seseorang terhadap kejahatan, semakin banyak juga kerentanannya. Untuk itulah penelitian ini juga dibuat dengan menilai seseorang dari pengalamannya yang memberikan perilaku sebagai faktor kunci penentu.

Untuk ringkasan hubungan tingkat kesadaran responden terhadap keamanan alat, ruang dan sistem dan pengaruhnya dengan tingkat pengalaman menjadi korban:

- Semakin kesadaran berpindah ke arah ruang maya, maka kemungkinan seseorang menjadi korban berkurang. Akan tetapi kemungkinan untuk menjadi korban dari tingkat menengah menjadi lebih besar
- Dengan tingkat kesadaran menengah semakin banyak tendensi menjadi korban di tingkat rendah.
- Dari data kesadaran gabungan kembali lagi didapatkan data yang kurang baik karena, semakin tingginya kesadaran maka kembali lagi kerentanan korban di tingkat rendah menjadi banyak.

Untuk ringkasan hubungan tingkat kesadaran responden terhadap keamanan alat, ruang dan sistem dan pengaruhnya dengan tingkat pengalaman menjadi pelaku:

- Semakin kesadaran berpindah ke arah ruang maya, maka kemungkinan seseorang melakukan pelanggaran semakin berkurang
- Dengan tingkat kesadaran menengah semakin banyak tendensi menjadi pelaku di tingkat rendah.
- Semakin tinggi kesadaran seseorang, maka tendensi menjadi pelaku semakin berkurang.
- Dari data kesadaran gabungan kembali lagi didapatkan data yang kurang baik karena, semakin tingginya kesadaran maka semakin banyak dilakukannya pelanggaran di tingkat rendah.

Tabel 6 Pengalaman korban pencurian data pribadi umum

Korban pencurian data pribadi umum	Nama lengkap atau tanggal lahir	Foto atau video	Alamat surel (e-mail) atau telepon	Total pencurian data pribadi umum
Tidak pernah	(46,1%) 83	(68,3%) 123	(12,8%) 23	42,4%
Pernah, sekali	(20,6%) 37	(17,2%) 31	(6,1%) 11	14,6%
Lebih dari dua kali	(6,1%) 11	(5%) 9	(10%) 18	7%
Beberapa kali	(22,8%) 41	(7,8%) 14	(41,7%) 75	24,1%

Seringkali	(4,4%) 8	(1,7%) 3	(29,4%) 53	11,8%

Dari tabel di atas terlihat bahwa jumlah paling banyak terdapat dalam menargetkan pencurian alamat surel (e-mail) atau nomor telepon, kemudian diikuti pencurian foto atau video, dan nama dan tanggal lahir. Sehingga perlu ada perhatian khusus dalam alamat surel (e-mail) atau nomer telepon.

Pada perolehan data yang didapatkan lewat survei, total dari responden yang pernah melakukan pencurian data ada 144 responden, yakni sebesar 80,44% yaitu dengan rincian sebagai berikut:

Tabel 7 Pengalaman pelaku pencurian data pribadi umum

Tingkat pelaku kejahatan pencurian data	Tidak pernah (0)	Rendah	Menengah	Tinggi	Total
Laki-laki	14 (17,28%)	59 (72,83%)	8 (9,87%)	0	67 (82,71%)
Perempuan	21 (21,42%)	75 (76,53%)	2 (2,04%)	0	77 (78,57%)
Total	35 (19,55%)	134 (74,86%)	10 (5,58%)	0	144 (80,44%)

Dalam menentukan pelaku juga tidak terdapat perbedaan signifikan antar jenis kelamin, namun untuk tingkat kejahatan yang dilakukan sama seperti dalam menentukan korban. Paling banyak dilakukan pada tingkat yang rendah dan dengan persentase yang serupa.

Bagian ke 19 dari kuesioner merupakan sebuah *self-repot* kondisional yang dibuat dengan 3 tahapan.

I. Mengambil data pihak lain tanpa seizin pemiliknya.

   Dari 179 responden, 88,8% yaitu 159 orang menyatakan tidak pernah dan 11,2% sejumlah 20 menyatakan pernah. Berbeda dengan model survei pelaku, yang mendapatkan rata-rata jumlah pelaku dari responden sebesar 80,44%). Dari sini terlihat penyimpangan karena kurangnya kesadaran akan data pribadi, baik sehingga menjadi korban maupun menjadi pelaku. Hanya 11,2% responden yang sadar akan apa itu data pribadi.

II. Mengambil data pihak lain tanpa seizin pemiliknya dan dengan tujuan memperoleh informasi rahasia.

Dari 20 responden, 60% yaitu 12 orang menyatakan tidak pernah mengambilnya dengan tujuan memperoleh informasi rahasia dan 40% yaitu sejumlah 8 menyatakan pernah. Dari sini terlihat pelaku yang tidak hanya melakukan pelanggaran, namun kejahatan dari pencurian data.

III. Mengambil data pihak lain tanpa seizin pemiliknya dan dengan tujuan memperoleh informasi rahasia dan kemudian diberikan untuk mendapatkan imbalam (dalam bentuk apapun).

Dari 8 responden, yaitu 87,5% yaitu 7 orang menyatakan tidak pernah membagikannya dengan tujuan imbalan. Hanya satu responden yang melakukannya dan memiliki latar belakang pendidikan IT, wawasan DP, dan pernah mengikuti paparan DP namun tidak bekerja di sektor IT. Target yang menjadi sasaran pelaku adalah keluarga, pasangan, teman dekat, dan rekan kerja.

Pelaku mengungkapkan bahwa tidak selalu membutuhkan alat dan sekalinya menggunakan alat, alat tersebut sesungguhnya juga bukan *software* yang digunakan untuk mengambil data pribadi sama sekali. Di kalangan IT yang tidak paham faktor sosial tidak akan berpikiran untuk menggunakan *netcut,* karena untuk menggunakan program ini dalam kejahatan dibutuhkan kemampuan dari *social engineering*, tidak hanya teknis.

Dari data di atas, hanya ada satu responden yang melakukan kejahatan pencurian data serius secara sadar. Karena selain mengambilnya tanpa izin, juga untuk mendapatkan informasi rahasia, dan ketika meminta bantuan pihak lain responden ini memberikan imbalan. Dari data di atas juga didapatkan infromasi:

- 100% pelaku melakukannya lebih dari sekali.
- 90% pelaku melakukannya terhadap orang yang dikenal.
- 5 responden, 25% pernah melakukannya dengan menyiapkan rencana. Menandakan kesiapan dan kesadaran pelaku dalam berbagai aspek pencurian data pribadi.
- 11 responden, 55% melakukannya tidak sengaja karena target tidak mempermasalahkannya. Menandakan bahwa pelaku sadar akan data pribadi dan korban mempercayai pelaku dan kemungkinan tidak menyadari pentingnya data pribadi.
- 11 responden, 55% melakukannya tidak sengaja karena target tidak menyadarinya. Menandakan rendahnya kesadaran korban karena tidak menjaga data pribadinya dari akses pelaku.
- 10 responden, 50% melakukannya secara sengaja karena target sedang lalai. Menandakan pelaku yang sadar dan korban yang tidak sadar dalam menjaga keamanan data pribadinya.
- 1 responden, 5% melakukannya tanpa latar belakang IT maupun Data Pribadi sama sekali. Yang berarti bertambahnya latar belakang sangat membuka peluang seseorang dalam melakukan tindak pencurian data pribadi.
- 0 responden, 0% adalah lansia.

Dalam membangun strategi pencegahan viktimisasi pencurian data pribadi ini digunakan teori dari pencegahan kejahatan sesuai yang sudah dijabarkan di atas, yaitu pencegahan kejahatan khususnya melalui pendekatan situsional *(Situational Crime Prevention*). Sebagai pencegahan yang paling mendasar, strateginya adalah dengan mengurangi peluang dan mengubah lingkungan fisik dalam beberapa cara yang membuat kejahatan menjadi kurang enak dilakukan bagi pelaku potensial. Dan karena kasus ini tidak hanya melibatkan lingkungan fisik, maka lingkungan maya juga dimasukkan dalam ranah strategi pencegahan ini.

Kesadaran Keamanan terhadap Alat, Sistem, dan Ruang

Seluruh pihak sangat mempengaruhi keamanan dan kesadaran yang dirasakan masyarakat. Dari alat yang dilihat, penetrasi teknologi, dan internet berlangsung terlalu cepat sehingga banyak orang yang belum mampu memahami teknologinya. Masyarakat sering menggunakan istilah *gaptek* pada pihak yang tidak cakap dalam menghadapi penetrasi teknologi ini sebagai ejekan atau candaan. Padahal seharusnya hal ini dipandang dengan serius, tetapi tidak ada pihak yang berusaha memberikan sosialisasi mendasar bahwa edukasi harus diberikan secara menyeluruh dan mendasar.

Kesadaran keamanan ini harus diberikan sejak dari penggunaan alat yaitu *smartphone*, untungnya kebiasaan penggunaan *smartphone* ini sudah cukup baik nilainya. Namun sesuai hasil dari data sebelumnya, semakin menuju ke arah ruang maya maka kesadaran berkurang dan kerentanan bertambah.

Keamanan terhadap Data Pribadi

Dari ketiga faktor sebelumnya, yang paling harus dijaga dan memiliki kesadaran yang rendah adalah kesadaran terhadap data pribadi. Karena semakin spesifik dan abstrak faktor yang harus dijaga, semakin jarang dan sulit masyarakat menguasainya. Dari data yang didapatkan, masyarakat cukup tahu dan cukup sering mendapatkan wawasan ini.

Teknologi juga membantu memudahkan menyebarkan banyak hal baik, terutama untuk negeri berkembang dengan efek domino yang besar. Penggunaan media sosial dan media berita digital dapat menjadi alat yang terbaik untuk meningkatkan kebutuhan masyarakat. Sekalipun lewat film dan buku, yang malahan mungin akan memberikan efek yang lebih baik terhdap sosialisasi kesadaran keamanan data pribadi ini. Karena lewat cerita akan lebih memberikan kesan pada masyarakat untuk berperilaku dan bertindak di kehidupan.

Berikut beberapa rangkuman tambahan strategi pencegahan viktimisasi pencurian data pribadi:

1. Mewujudkan pengetahuan, sikap, dan persepsi yang didapatkan dalam berperilaku, karena buat apa tahu jika tidak diaplikasikan.

2. Memberikan sosialisasi dan paparan yang lebih mengarahkan pada perilaku nyata.
3. Menjelaskan dengan detail perbedaan antara data pribadi dan data umum.

Penutup

Data pribadi sesungguhnya dapat digunakan untuk hal baik, sayang sekali akibat dari kemudahan penyimpanan dan transaksi data malahan menyebabkan hal sebaliknya. Dan hal ini tidak hanya berlaku bagi perusahaan maupun Lembaga, tetapi pihak perorangan juga harus mampu ikut menjaganya.

Seperti yang sudah disimpulkan sebelumnya, semakin spesifik dan abstrak faktor yang harus dijaga, semakin jarang dan sulit masyarakat menguasainya. Widiyanti Ninik dan Yulius Waskita (1987), menyampaikan bahwa usaha pencegahan dapat pula mempererat kerukunan, meningkatkan rasa tanggung jawab tehadap sesama anggota masyarakat. Budaya komunal ini harus dimanfaatkan bukan untuk memiliki bersama ranah pribadi, namun untuk menjaga bersama kepemilikan ranah pribadi dan menghormati keberbedaannya.

Berikut beberapa saran dari peneliti setelah melihat beberapa kekurangan untuk penelitian berikutnya:

1. Agar dilaukan pengujian terhadap penambahan wawasan dan atau penelitian longitudinal agar startegi pencegahan yang disarankan dapat lebih dimaksimalkan dan mendapatkan bukti empirisnya.
2. Demografi yang didapatkan sudah lebih bagus tetapi akan lebih baik jika diimplementasikan dalam skala besar yang lebih luas.
3. Dapat dibuat penelitian yang lebih spesifik dari berbagai ranah yang sudah diuji dalam penelitian ini, khususnya bagian kesadaran keamanan akan internet dan data pribadi. Terutama isu terkait data pribadi ini akan terus berkembang, khususnya di Indonesia.
4. Dapat membantu memberikan sudut pandang tambahan pada berbagai usaha pihak swasta maupun pemerintah dalam membangun regulasi.

Daftar Pustaka

Bukalapak Bantah Jutaan Akun Penggunanya Dicuri Hacker. (2019) Diakses dari https://tekno.kompas.com/

Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Kearney, P. (2010). Security: The Human Factor. Cambridgeshire: IT Governance Publishing.

Kominfo: Soal jarangnya laporan penipuan online, orang Indonesia pemaaf. (2019) DIakses dari https://www.msn.com/

Laporan Survei: Penetrasi & Profil Perilaku Pengguna Internet Indoensia (2019) dalam Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dan Polling Indonesia. Diakses dari https://apjii.or.id/

Pengakuan Hacker yang Klaim Angkut Jutaan Akun Bukalapak. (2019) Diakses dari https://inet.detik.com/security/

Polri Ungkap Sindikat Penipuan "Online" yang Dikendalikan dari Lapas, (2019) Diakses dari https://nasional.kompas.com/

Statistik Telekomunikasi Indonesia (2017) dalam Badan Pusat Statistik (BPS). Diakses dari https://www.bps.go.id/publication/

The Great Hack, Dokumenter Soal Cambridge Analytica Rilis Hari Ini. (2019) Diakses dari https://tirto.id/eeVX

Widiyanti, Ninik dan Waskita, Yulius. (1987). Kejahatan dalam masyarakat dan pencegahannya. Jakarta: Bima Aksara