Doxing Patterns Using Social Engineering in Cyberspace [Pola Pola Doxing Menggunakan Social Engineering di Dunia Maya]

Artanti Tertia Mukti[1)], Mochammad Tanzil Multazam[*,2)]

[1)]Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia
[2)] Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia
*Email Penulis Korespondensi: tanzilmultazam@umsida.ac.id

Abstract. *Social media has become an important part of human life because it has developed rapidly and has had a major influence on aspects of life. However, on the other hand, social media is often misused to commit cyber crimes, one of which is doxing. In short, doxing is a crime committed on the internet by collecting the victim's personal data and then once collected, the data is disseminated on the internet and on social media with the aim of intimidating and threatening the victim. The purpose of the results of this study is to identify what are the patterns of doxing using social engineering that are happening today in cyberspace and what forms of doxing are allowed or not allowed. The method used in this study is normative juridical using a statutory approach (Statue Approach). The types of legal sources used are primary legal sources of Law Number 27 of 2022 concerning Protection of Personal Data.*

Keywords – *Doxing ; Personal Data ; Cybercrime*

Abstrak. *Media sosial telah menjadi bagian penting dalam kehidupan manusia karena telah berkembang pesat dan memberikan pengaruh besar dalam aspek kehidupan. Namun, disisi lain media sosial seringkali disalahgunakan untuk melakukan kejahatan siber, salah satunya adalah Doxing. Secara singkat doxing adalah kejahatan yang dilakukan di internet dengan cara mengumpulkan data pribadi korban kemudian setelah terkumpul, data tersebut disebarluaskan di internet maupun di sosial media dengan tujuan untuk mengintimidasi dan mengancam korban. Tujuan dari hasil penelitian ini adalah untuk mengidentifikasi apa saja pola pola doxing dengan menggunakan rekayasa sosial yang terjadi pada masa kini di dunia maya dan bagaimana bentuk bentuk perbuatan doxing yang diperbolehkan maupun tidak diperbolehkan. Metode yang digunakan pada penelitian ini adalah yuridis normatif dengan menggunakan pendekatan perundang-undangan (Statue Approach). Jenis sumber hukum yang digunakan sumber bahan hukum primer Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

Keywords – *Doxing ; Data Pribadi ; kejahatan siber*

I. PENDAHULUAN

Perkembangan teknologi memberikan dampak yang besar kepada masyarakat dalam kebebasan berpendapat di internet. sebelum teknologi berkembang seperti sekarang pun masyarakat telah bebas untuk memberikan pendapat di muka umum namun setelah muncul internet masyarakat semakin bebas untuk berpendapat di sosial media pada era digital. Perkembangan teknologi informasi dan komunikasi telah banyak membantu masyarakat, segala informasi yang bernilai positif dan negatif dapat dengan mudah diakses di internet sehingga memberikan perubahan yang besar pada perilaku masyarakat.[1]

Kemajuan teknologi informasi bidang jejaring sosial telah terbukti memberikan dampak positif untuk menciptakan kemajuan dalam kehidupan manusia. Salah satunya adalah dengan adanya media sosial, yaitu sebuah wadah untuk bersosialisasi satu dengan yang lain melalui jaringan internet yang membuat manusia dapat berinteraksi dengan mudah dan menjadikan wadah untuk berpartisipasi, berkomunikasi, saling berbagi dan membuat berbagai konten tanpa dibatasi ruang dan waktu. Pada dasarnya, media sosial diciptakan untuk memberikan kemudahan seseorang dalam melakukan kegiatan saling sosialisasi dan komunikasi dengan orang lain.[2] Namun tidak hanya dampak positif, kemajuan teknologi juga dapat berdampak negatif yaitu menjadi sarana efektif perbuatan melawan hukum termasuk kejahatan dunia maya atau yang biasa dikenal dengan kata *cybercrime*.[3] Beberapa kasus cybercrime yang muncul di Indonesia yaitu seperti hacking, penipuan, penyadapan data orang lain, spamming email, dan manipulasi data dengan program komputer untuk mengakses data milik orang lain. Kemajuan teknologi informasi dan teknologi

membuat batas privasi semakin tipis karena berbagai data-data pribadi semakin mudah di tersebar[4]. Data pribadi adalah sesuatu yang melekat pada setiap orang, yang tentunya merupakan sesuatu yang bersifat sensitif. Data pribadi harus dilindungi karena sejatinya merupakan hak privasi setiap orang.

Pemanfaatan teknologi yang bersifat negatif membentuk kejahatan yang disebut cybercrime. kejahatan cyber memiliki banyak jenis, salah satunya yaitu doxing. Doxing, atau doxxing (berasal dari kata "dox", singkatan dari dokumen) dan *dropping* (melempar). secara singkat doxing adalah kejahatan yang dilakukan di internet dengan cara mengumpulkan data pribadi korban kemudian setelah terkumpul, data tersebut disebarluaskan di internet maupun di sosial media dengan tujuan untuk mengintimidasi dan mengancam korban. Awal mula dilakukannya perbuatan doxing dikarenakan pelaku tidak menyukai korban, baik karena korban telah melakukan kesalahan maupun korban memberikan pendapatnya di sosial media yang membuat pelaku tidak menyukai korban. Doxing biasanya dilakukan secara individu maupun kelompok.

Perbuatan doxing sendiri diatur didalam Undang Undang Informasi dan Transaksi Elektronik dan Undang Undang Perlindungan Data Pribadi. Perbuatan doxing terdapat pada Undang Undang Informasi dan Transaksi Elektronik pasal 27 ayat 3 pada UU No.11 Tahun 2008, karena menimbulkan arti yang ambigu pada frasa yang berisi muatan kekerasan atau ancaman kemudian direvisi dan lebih diperjelas maksud dari pasal tersebut yaitu terdapat pada Undang undang Nomor 19 tahun 2016 bahwa yang dimaksud muatan ancaman yaitu menyebarkan data pribadi seseorang, jika disertai dengan muatan ancaman kekerasan secara fisik maka dapat dikenakan pemberat pidana yaitu pada pasal 368 KUHP. Perbuatan Doxing pada Undang Undang Perlindungan Data Pribadi (UU PDP) terdapat pada pasal 67 ayat 1 dan 2, disebutkan bahwa doxing kegiatannya yaitu mengumpulkan data pribadi seseorang kemudian mengungkapkan data tersebut. dalam hal ini dapat diancam pidana penjara dan sanksi.

Perbuatan doxing terkadang dapat dilakukan oleh siapa saja, tidak hanya dari kalangan peretas profesional. perbuatan ini hanya dengan melakukan stalking atau menguntit sosial media target maka data pribadi akan dapat ditemukan dengan mudah, semua ini karena didukung oleh internet yang bersifat terbuka untuk siapa saja (open for everyone). Namun pada kalangan orang yang memiliki pengaruh (public figure) terkadang mereka tidak sadar bahwa terdapat data pribadi yang tersebar, dalam hal ini tentu saja bukan mereka yang menyebarkan data pribadi tersebut, namun melalui berita berita dengan bentuk ataupun video maka akan mudah ditemukan. Dengan internet semua menjadi mudah, mencari data pribadi seseorang hanya dengan cara mengetikkan nama target pada google, kemudian akan muncul nama nama terkait target yang biasanya berupa foto maupun video yang bersifat pribadi.

Perbuatan doxing memiliki banyak jenis. *Doxing Deanonymizing* yaitu jenis doxing dengan cara mengungkapkan identitas target yang menganonimkan diri atau tidak menggunakan nama asli. *Doxing targeting* ini dilakukan dengan cara mengungkapkan suatu informasi yang spesifik tentang seseorang yang memungkinkan mereka untuk dihubungi atau ditemukan dalam hal ini keamanan online korban telah dilanggar, contohnya adalah nomor telepon dan alamat rumah. *Doxing Delegitimizing* dilakukan dengan cara melakukan pengungkapan suatu informasi yang termasuk bersifat sensitif atau intim tentang seseorang, contohnya yaitu catatan medis, keuangan pribadi, catatan hukum. tujuan disebarkannya data tersebut dapat berpotensi merusak reputasi atau kredibilitas nya karena bersifat sangat pribadi sehingga tidak banyak diketahui orang lain.[5]

Maka dari itu penting bagi kita untuk menjaga data pribadi dengan cara yang paling utama dengan tidak terlalu banyak mengunggah sesuatu ke media sosial supaya dapat mencegah terjadinya Doxing atau kejahatan siber lainnya. Karena Doxing dapat berpotensi terjadinya kejahatan yang lebih serius seperti *cyberstalking, harassment, identity theft* dan lain sebagainya.[6] Pada saat ini media sosial telah menjadi bagian penting dari kita, namun tetap diingat bahwa semua informasi yang kita bagikan pada platform tersebut sangat mudah untuk diakses oleh siapa saja dan tidak menutup kemungkinan akan disalahgunakan oleh seseorang yang mempunyai niat jahat. Maka dari itu penting untuk meningkatkan kesadaran tentang bahaya doxing dan mendorong penggunaan internet yang bertanggung jawab dan etis. Sangat penting bagi semua orang untuk lebih menjaga privasi dan keamanan pribadi di dunia maya dan mempertimbangkan resiko yang timbul saat memutuskan untuk membagi informasi secara publik.

Sesuai penjabaran diatas diperlukan penelitian terdahulu yang digunakan sebagai acuan pada penyusunan artikel ilmiah oleh penulis dan juga sebagai pembeda antara penelitian yang sebelumnya dengan penelitian yang saat ini sedang dilakukan. Penelitian pertama oleh Teguh Cahya Yudiana, Sinta Dewi Rosadi, Enni Soerjati Priowirjanto dengan judul "The Urgency Of Doxing On Social Media Regulation and The Implementation Of Right To Be Forgotten On Related Content For The Optimization Of Data Privacy Protection In Indonesia " tujuan dari penelitian ini adalah sebagai perwujudan hak untuk dilupakan di Indonesia pada era transformasi digital, khususnya dalam kasus doxing. Metode yang digunakan adalah penelitian deskriptif untuk menjawab beberapa pertanyaan. hasil dari penelitian ini adalah memberikan usulan kepada pemerintah Indonesia untuk menetapkan regulasi mengenai doxing

di media sosial untuk mengisi kekosongan hukum dengan harapan dapat melindungi privasi data seluruh warga negara. Selain itu, penerapan hak untuk dilupakan menjadi urgensi dalam kasus doxing [7]**.** Penelitian kedua oleh Muhammad Arvy Chico Armando dan Hari Soeskandi dengan judul "Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut UU ITE dan UU PDP" tujuan dari penelitian ini adalah untuk mengetahui apakah pelaku doxing dapat dikenakan pidana menurut UU ITE dan bagaimana ketentuan pidana doxing dalam UU PDP. Metode yang digunakan adalah menggunakan penelitian hukum normatif dengan pendekatan perundang-undangan yaitu dengan meneliti berbagai peraturan yang berkaitan dengan doxing yang menjadi fokus penelitian. Kemudian menggunakan pendekatan konseptual yaitu dengan merujuk analisis pandangan para ahli hukum, doktrin-doktrin, konsep konsep dan asas asas hukum dalam ilmu hukum. Hasil dari penelitian adalah sebuah analisis pengaturan hukum terhadap kejahatan cyber dalam bentuk Doxing, memperjelas makna yang ambigu pada pasal 27 ayat 3 UU ITE setelah di revisi dan disahkan nya Undang Undang Perlindungan Data Pribadi yang akan memberikan jawaban bagi praktisi hukum dalam memidanakan pelaku doxing serta jaminan keamanan data pribadi masyarakat [8]. Penelitian ketiga oleh Bagiartha W, I. P. P. dengan judul "Perilaku Doxing Dan Pengaturannya Dalam Positivisme Hukum Indonesia" tujuan dari penelitian ini adalah mengetahui kategori perbuatan doxing dan pengaturannya dalam perundang undangan Indonesia Metode yang digunakan adalah penelitian normatif dengan menggunakan metode pendekatan perundang- undangan dan pendekatan konseptual. Sumber dan jenis bahan hukum yang digunakan yaitu bahan hukum primer yang berupa pengkajian terhadap perundang undangan. kemudian Bahan hukum sekunder yang berupa kajian literasi dan doktrin-doktrin. Kemudian Bahan hukum tersier yang berupa penerjemahan terminology doxing berdasarkan kamus kebahasaan. Data bahan hukum yang telah terkumpul ini kemudian digunakan dan dokumentasikan melalui studi kepustakaan kemudian di analisa secara deduktif kualitatif. Hasil dari penelitian ini adalah Perbuatan doxing dan peraturannya dalam undang-undang Indonesia adalah bahwa doxing adalah perbuatan illegal yang dengan cara mengungkapkan suatu data ataupun dokumen pribadi Seseorang maupun kelompok yang memiliki ciri serupa dengan cyber crime (kejahatan cyber).[9]

Berdasarkan penjelasan tabel diatas, dapat dilihat penelitian ini dengan penelitian sebelumnya. Penelitian ini mengambil objek penelitian dan topik yang berbeda dengan ketiga penelitian terdahulu. Ketiga peneliti terdahulu lebih banyak membahas terkait doxing secara umum dan peraturan sanksi pidana yang didapatkan oleh pelaku kejahatan doxing. Belum ada yang membahas terkait doxing secara spesifik. Sehingga peneliti hendak mengetahui apasaja pola pola doxing dengan menggunakan social engineering di dunia maya pada masa kini dan bagaimana bentuk bentuk perbuatan doxing yang diperbolehkan maupun tidak diperbolehkan yang ada di masa sekarang.

Berdasarkan pada uraian yang telah dijabarkan diatas, dikarenakan hal tersebut penulis melakukan penelitian yaitu Bagaimana pola pola doxing menggunakan social engineering yang terjadi pada masa sekarang di dunia maya dan Apakah semua perbuatan doxing merupakan tindak pidana.

II. METODE

Penelitian ini merupakan penelitian yuridis normatif dengan menggunakan pendekatan perundang-undangan (Statue Approach). Terdapat dua jenis sumber hukum yang digunakan dalam penelitian ini, yaitu sumber bahan hukum primer dan bahan hukum sekunder. Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Sementara itu, bahan hukum sekunder yaitu buku, jurnal hukum, internet dan pendapat ahli dikumpulkan melalui studi kepustakaan. Setelah semua data terkumpul, kemudian dianalisis menggunakan pendekatan atau metode deduktif yang merupakan sesuatu yang menggunakan logika untuk membuat satu ataupun lebih kesimpulan berlandaskan beberapa premis yang diberikan.

III. HASIL DAN PEMBAHASAN

Kemajuan teknologi dan informasi pada era sekarang membawa dampak yang besar terutama di bidang jejaring sosial, dampak positif nya yaitu sebagai Media untuk bersosialisasi satu sama lain yang dilakukan secara online dengan menggunakan jaringan internet yang memungkinkan manusia untuk saling berinteraksi secara online yang dapat menguatkan hubungan antar pengguna sebagai sebuah ikatan sosial. Dalam penggunaanya saat ini, media sosial tidak hanya untuk media berinteraksi tetapi dapat dijadikan sebagai sumber informasi yang dapat diakses dan dibagikan dengan cepat.[10] Namun disisi lain, media sosial seringkali menjadi wadah yang sangat mudah disalahgunakan untuk penyebaran kejahatan siber. Telah banyak terdapat kasus-kasus kejahatan siber pada platform seperti facebook, Instagram maupun twitter[11]. Sebagai pengguna media sosial, sangat perlu untuk berhati-hati dan menjaga etika

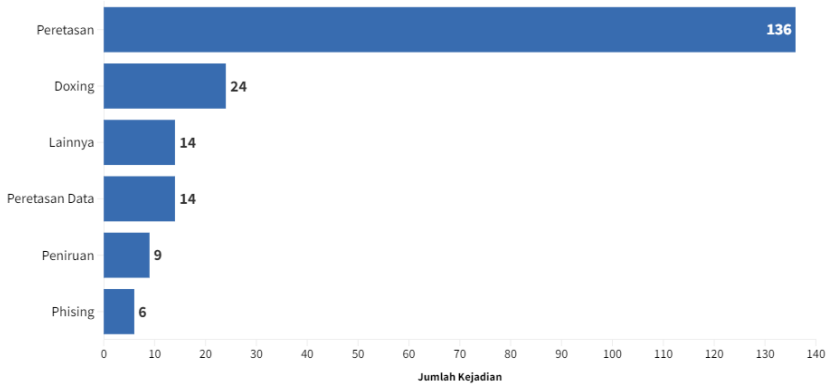
dalam menggunakan sosial media supaya tidak terjadi penyalahgunaan atau pelanggaran hukum *cybercrime* dan menjadi pengguna yang cerdas.

Hal yang paling mudah untuk dilakukan adalah dengan cara tidak *oversharing* di sosial media karena dapat memicu banyak sekali dampak negatif yaitu membuka kesempatan tindak kriminal seperti memicu pencurian data pribadi yang dapat disalahgunakan untuk mengakses akun bank, predator anak, hingga mengakses dokumen dokumen rahasia [12]. Pengguna media sosial seringkali tidak hati-hati dalam mengunggah sesuatu bahkan menggunggah informasi pribadinya sehingga data pribadi dapat dengan mudah didapatkan. Tidak sedikit dari kejahatan dunia maya berawal dari diumbarnya data yang bersifat personal pada akun media sosialnya sehingga data tersebut digunakan oleh orang lain untuk melakukan aksi kejahatan.

Cybercrime atau yang dikenal sebagai kejahatan berbasis komputer merupakan kejahatan yang dilakukan dengan berbasis computer dan jaringan. komputer digunakan sebagai alat untuk melaksanakan kejahatan bahkan sebagai sasarannya. *Cybercrime* dapat mengancam seseorang, keamanan negara atau kesehatan finansial. Beberapa kejahatan yang sering dan banyak terjadi adalah seputar peretasan, pelanggaran hak cipta, melakukan penyadapan yang tidak beralasan dan pornografi. Adapun masalah privasi seseorang yang dilanggar dengan melakukan pengungkapan informasi pribadi[13]. Kejahatan siber memiliki banyak jenis, salah satunya yaitu *Doxing.*

Fenomena Doxing menurut PW Singer dan Allan Friedman (2014), doxing adalah suatu tindakan mengungkapkan dokumen pribadi di depan umum yang merupakan bagian dari aksi protes, lelucon, atau tindakan main hakim sendiri[14]. Secara singkat, Doxing adalah kejahatan yang dilakukan di internet dengan cara mengumpulkan data pribadi korban kemudian setelah terkumpul, data tersebut disebarluaskan di internet maupun di sosial media dengan tujuan untuk mengintimidasi dan mengancam korban. Awal mula dilakukannya perbuatan doxing dikarenakan pelaku tidak menyukai korban, baik karena korban telah melakukan kesalahan maupun korban memberikan pendapatnya di sosial media yang membuat pelaku tidak menyukai korban. Doxing biasanya dilakukan secara individu maupun kelompok.

Kejahatan Doxing dapat menyerang profesi terkenal yang identitasnya seringkali dipublikasikan di internet seperti selebritis ataupun jurnalis, namun dengan berkembangnya internet dan media sosial, data pribadi seseorang akan dengan mudah di akses oleh siapapun. Mulai dari informasi yang dicantumkan pada media sosial bahkan dapat melacak lokasi seseorang dengan menggunakan alamat IP atau *Internet Protocol Address.* Awal mula seseorang memiliki motif dalam melakukan kejahatan doxing adalah seseorang yang memang memiliki niat jahat. Akibat dari kejahatan doxing sering membuat seseorang merasa tidak nyaman untuk mengakses internet karena khawatir dan takut melakukan sesuatu yang akan berakibat terbongkarnya informasi pribadi di media sosial[15]. Dalam hal ini doxing merupakan bentuk pelanggaran privasi seseorang, doxing bisa dikatakan sebagai *cyberbullying.*



Gambar 1. Bentuk serangan digital yang terjadi selama tahun 2021, sumber: SAFEnet

Sebagaimana yang dapat dilihat pada gambar 1. Menurut riset yang dilakukan oleh SAFEnet (Southeast Asia Freedom of Expression Network) pada tahun 2021, Doxing merupakan kejahatan terbanyak nomer 2 setelah peretasan dengan jumlah 24 insiden (12,43%). Telah ditemukan jumlah kejahatan doxing di Indonesia mengalami peningkatan di setiap tahunnya, sejak tahun 2017 hingga 2021. Pada tahun 2017 terdapat 1 insiden, tahun 2018 terdapat 2 insiden, tahun 2019 terdapat 7 insiden, tahun 2020 terdapat 13 insiden dan tahun 2021 terdapat 24 insiden. Korban dari tindak pidana doxing sebanyak 56% berprofesi sebagai jurnalis, sebanyak 22% aktivis dan sebanyak 22% sisanya merupakan

warga sipil.[16] SAFEnet adalah organisasi yang berfokus pada upaya memperjuangkan hak hak digital di Asia Tenggara.

Perbuatan Doxing memiliki macam yang berbeda dalam praktiknya antara lain Doxing Deanonymizing yaitu dengan cara mengungkapkan identitas seseorang yang anonym atau tidak menggunakan nama asli, contohnya adalah seseorang yang menggunakan nama samaran. Doxing Targeting yaitu dengan cara mengungkapkan informasi yang spesifik tentang seseorang yang memungkinkan mereka untuk dihubungi atau ditemukan, atau keamanan online mereka dilanggar, contohnya nomor telepon, alamat rumah, atau nama pengguna dan kata sandi akun. Doxing Delegitimizing yaitu dengan cara melakukan pengungkapan suatu informasi yang termasuk bersifat sensitif atau intim tentang seseorang, contohnya yaitu catatan medis, keuangan pribadi, catatan hukum. tujuan disebarkannya data tersebut dapat berpotensi merusak reputasi atau kredibilitas nya karena bersifat sangat pribadi sehingga tidak banyak diketahui orang lain.[17]

Dampak yang akan dirasakan oleh korban doxing adalah rasa malu karena mendapatkan penghinaan atau bullying di depan umum, mendapatkan diskriminasi, mengalami cyberstalking dan physical stalking, dapat mengalami pencurian identitas dan penipuan dalam hal finansial, dapat mengalami kerusakan reputasi personal dan juga professional yang dikemudian hari akan menyebabkan kerugian secara sosial maupun finansial, menghadapi online trolling yaitu sikap mengganggu, merusak, menipu dalam ruang lingkup media sosial dapat berupa *hate* atau *sarkas*, mengalami trauma psikis disebabkan karena mendapat ancaman langsung via *dm mention*, pesan hingga telepon dari nomor yang tidak dikenal. Semua hal tersebut tentunya dapat menyebabkan kecemasan, serta menurunnya kepercayaan dan harga diri.

Data pribadi adalah sesuatu yang melekat pada setiap orang, yang tentunya merupakan sesuatu yang bersifat sensitif. Data pribadi harus dilindungi karena sejatinya merupakan hak privasi setiap orang.
Menurut Undang Undang Nomor 27 Tahun 2022 Tentang perlindungan Data Pribadi, Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

Undang Undang yang mengatur tentang Perlindungan Data Pribadi

Jenis Data Pribadi menurut Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terdapat pada Pasal 4 ayat 2 dan 3.

a. Data Pribadi yang bersifat spesifik terdapat pada pasal 4 ayat 2 yakni :
    1. Data dan informasi kesehatan,
    2. Data biometrik
    3. Data genetika
    4. Catatan kejahatan
    5. Data anak
    6. Data keuangan pribadi dan/atau
    7. Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
b. Data pribadi yang bersifat umum terdapat Pada pasal 4 ayat 3 yakni :
    1. Nama lengkap
    2. Jenis kelamin
    3. Kewarganegaraan
    4. Agama
    5. Status perkawinan
    6. Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Setiap masing masing orang diwajibkan untuk melindungi kedua data pribadi diatas meskipun telah dijamin keamanannya oleh negara. Namun tidak menutup kemungkinan untuk terjadinya cybercrime.

Larangan perbuatan doxing pada Undang Undang Perlindungan Data Pribadi (UU PDP) terdapat pada pasal 65 ayat 1 dan 2, Unsur yang ada didalam nya adalah :

1. Larangan memperoleh atau mengumpukan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
2. Larang mengungkapkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.

Pada Undang Undang Perlindungan Data Pribadi pasal 67 ayat 1 dan 2 terdapat ketentuan pidana bagi yang melakukan doxing. Dalam pasal tersebut pelaku disebutkan sebagai orang yang mengumpulkan data pribadi seseorang dan mengungkapkan data pribadi yang bukan miliknya. Kalimat tersebut termasuk dari definisi doxing.
Maka pelaku doxing yang mengumpulkan data pribadi seseorang menurut UU PDP diancam dengan pidana penjara paling lama 5 tahun atau denda paling banyak 5 Miliar Kemudian bagi pelaku yang mengungkapkan data pribadi dengan cara mengumpulkan data pribadi tersebut diancam dengan pidana penjara paling lama 4 tahun dan denda paling banyak 4 Miliar

Inti dari isi undang undang perlindungan data pribadi yang berkaitan dengan doxing adalah

1. Jenis data pribadi
2. Hak pemilik data pribadi
3. Ketentuan pidana

Platform sosial media telah memiliki aturan mengenai doxing dalam kebijakan media dan informasi pribadi. Salah satunya ada pada platform Twitter yang tertulis " membagikan informasi pribadi seseorang secara online tanpa izin yang bersangkutan, terkadang disebut " doxing", merupakan pelanggaran terhadap hak privasinya dan peraturan twitter. Membagikan informasi pribadi dapat menimbulkan resiko keamanan dan keselamatan serius bagi yang terkena dampaknya, hal ini juga dapat mengakibatkan gangguan fisik, mental, dan keuangan.

Berdasarkan kebijakan, jenis informasi yang dilarang dibagikan tanpa seizin pemiliknya yaitu informasi alamat rumah atau lokasi fisik termasuk alamat jalan dan koordinat GPS, informasi aktual termasuk informasi yang dibagikan ke twitter secara langsung maupun melalui URL, dokumen identitas seperti kartu tanda pengenal dan jaminan sosial, informasi kontak seperti alamat, nomor telepon dan email yang tentunya tidak tersedia untuk publik, informasi keuangan seperti detail rekening bank dan kartu kredit, informasi pribadi lainnya seperti data biometric atau rekam medis, media individu pribadi tanpa izin dari orang yang muncul di media tersebut. Perbuatan yang juga dilarang yaitu mengancam atau mengungkapkan informasi pribadi orang ke publik, membagikan informasi yang memungkinkan individu untuk diretas atau mendapatkan akses ke informasi pribadi seseorang tanpa persetujuan pemiliknya, contohnya membagikan kredensial masuk untuk layanan perbankan online.[18]

A. Pola Pola Doxing yang terjadi pada masa kini menggunakan social engineering

Social Engeneering atau yang bisa disebut dengan rekayasa sosial melibatkan manipulasi sosial dan psikologis untuk mempengaruhi orang lain untuk mengungkapkan informasi sensitif atau melakukan tindakan tertentu yang mungkin tidak mereka lakukan dalam keadaan normal.[19] Teknik tenik rekayasa sosial dapat berupa rekayasa sosial online, phising atau penipuan telepon, yang dapat digunakan untuk memancing informasi pribadi korban. Pelaku dapat menyerang berbagai platform seperti email, media sosial dan lain-lain. Dalam Doxing, rekayasa sosial digunakan sebagai alat untuk mendapatkan informasi pribadi korban. Pelaku doxing dapat memanfaatkan teknik rekayasa sosial untuk memperoleh kepercayaan korban dengan cara memancing informasi pribadi melalui komunikasi online atau bahkan mencari informasi publik. Dalam proses doxing terdapat proses sosial engineering dengan melalui tren di media sosial, dengan cara memanfaatkan tren populer atau topik yang sedang viral di media sosial untuk memancing informasi pribadi dari orang lain dan kemudian mengungkapkannya secara online.

Pelaku Rekayasa Sosial dapat memanipulasi emosi pengguna media sosial untuk mengunggah data pribadi mereka secara sukarela, dengan cara memanfaatkan tren tren yang ada di media sosial. Pelaku akan menggunakan tren atau isu yang sedang popular sebagai cara untuk menarik perhatian dan kemudian mempengaruhi orang orang untuk mengikuti tren tersebut. Pelaku akan mengarahkan pengguna media sosial untuk melakukan tindakan yang akan merugikannya seperti pengguna medsos akan dipaksa untuk mengikuti tren dengan cara mengungkapkan informasi pribadi. Pelaku dapat berperan sebagai peserta tren dan meminta pengikut tren untuk mengungkapkan detail pribadi seperti nama lengkap, alamat pribadi, nomor telepon hingga tanggal lahir. Sehingga pengguna media sosial yang terpengaruh oleh trend dan ingin berpartisipasi mungkin tidak menyadari bahwa mereka telah memberikan informasi pribadi.

Pada era sekarang yang telah memiliki teknologi dan informasi yang maju dan didukung oleh internet, Pada tahun 2023 hampir 60,4% orang aktif menggunakan atau mempunyai media sosial[20]. Di media sosial kita bisa melihat sesuatu yang viral mulai dari konteks yang positif maupun negatif. Konten konten pada media sosial dapat cepat tersebar atau banyak diduplikasi oleh pengguna media sosial dengan cara saling membagikan ulang konten tersebut kepada pengguna lain ke media sosial mereka yang kemudian juga dapat menjadikan fenomena baru atau *Trend*. Berikut adalah tren di media sosial yang dapat mengakibatkan terjadinya doxing :

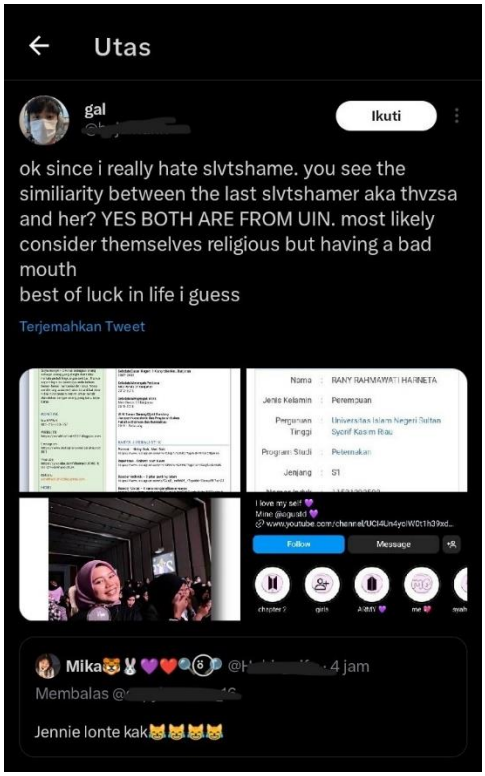
1. Trend Spill The Tea

Trend “Spill the tea” adalah sebuah istilah yang tidak asing terutama bagi pengguna twitter. Spill the Tea dilakukan seseorang yang membuat unggahan dengan maksud menceritakan sebuah permasalah yang terjadi seseorang[21] atau bahkan digunakan untuk mengungkapkan sebuah kasus dengan permintaan warganet untuk membuka siapa pelakunya dengan mengatakan “*spill the tea,* Nder!” lalu dilanjutkan dengan mengungkapkan akun media sosial seseorang yang dimaksud kemudian berlanjut mengungkapkan data pribadi lain seperti tempat kerja, alamat rumah, bahkan informasi keluarga nya. Jika menyangkut ke permasalahan yang mengandung unsur negatif, doxing disini dianggap sebagai sesuatu yang normal karena dianggap sebagai bagian dari sanksi sosial. Trend “ *spill the tea”* memang terbukti sering membuat kasus yang buntu menjadi viral. Kemudian setelah mendapatkan perhatian dari banyaknya warganet selanjutnya penegak hukum akan menindaklanjuti kasus tersebut. Trend ini seringkali di salah gunakan untuk melakukan doxing, melalui trend ini pengguna sosial media dengan mudah dapat mengungkapkan informasi pribadi orang lain secara terbuka. Fenomena “ Spill The Tea” ini terkadang sengaja untuk membuat seseorang yang telah melakukan sesuatu yang negatif agar terkena *cancel culture. Cancel Culture* merupakan suatu budaya yang dilakukan oleh publik pada platform media sosial dengan cara pemboikotan kepada individu tertentu yang memiliki tingkat popularitas karena hal tertentu yang di nilai negatif oleh masyarakat seperti rasisme dan etnis, pelecehan seksual dan ujaran kebencian terhadap wanita, identitas gender, transphobia dan lain sebagainya.

Berikut merupakan contoh dari Doxing yang illegal :

Gambar 2. Screenshot Doxing pada platform Twitter

Sebagaimana yang dapat dilihat pada gambar 2, Artis bernama Jefri Nichol telah melakukan doxing salahsatu warganet pada platform twitter. Jefri Nichol mengira bahwa warganet tersebut adalah *haters* nya sehingga ia melakukan doxing kemudian di ekspos profil beserta foto tanpa sensor dan alamat rumah warganet di sosial medianya dengan jumlah 1,2 juta followers. Dalam hal ini korban merasa dirugikan oleh tindakan yang dilakukan jefri nichol yang telah menyebarkan data pribadinya tanpa izin. Meski jefri nichol telah meminta maaf kepada korban, namun perbuatan yang ia lakukan tetap tidak etis.



Gambar 3. Screenshot Doxing pada platform Twitter

Sebagaimana yang dapat dilihat pada gambar 3. Salah satu Akun Twitter melakukan doxing dengan cara menyebarkan akun Instagram dan PPDIKTI korban. Awal mula ia melakukan doxing karena ingin membuat korban merasa jera karena akun korban diduga memberikan komentar kotor di twitter terhadap K-Pop idol yaitu jennie blackpink. Namun ia melakukan doxing ke orang yang salah.

Gambar 4. Screenshot Doxing pada platform Instagram

Sebagaimana yang dapat dilihat pada gambar 4. Rachel Vennya seorang seleb Instagram melakukan doxing terhadap salah satu pengikutnya, ia mengunggah foto pengikutnya yang telah membuat komentar hinaan. Rachel Vennya melakukan sayembara terbuka untuk menemukan biodata lengkap pengikut tersebut pada akun media sosialnya yaitu Instagram dengan imbalan Rp15 juta. Hal ini membuat banyak orang berlomba-lomba mencari biodata pengikut tersebut hingga banyak email yang masuk. Kegiatan ini pun ramai diperbincangkan di media sosial karena banyak mengatakan hal ini termasuk kedalam kegiatan doxing yang sebenarnya tidak boleh dilakukan. Dalam hal ini

perbuatan yang dilakukan Rachel Vennya tidak diperbolehkan, karena bertujuan untuk mengancam serta mengajak orang lain yakni pengikutnya untuk turut melakukan doxing.

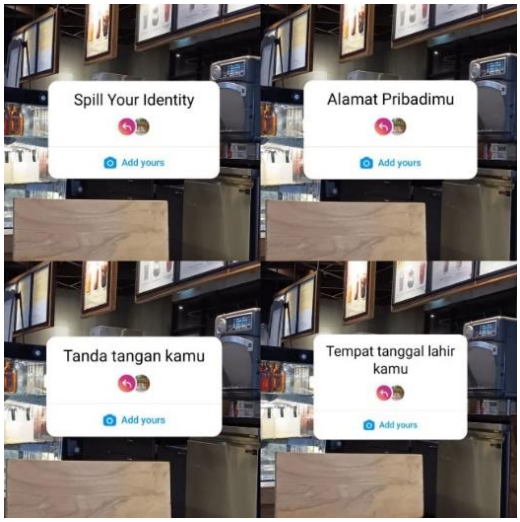
Berikut merupakan contoh dari Doxing yang legal :

Gambar 5. Screenshot Doxing pada platform Twitter

Sebagaimana yang dapat dilihat pada gambar 5. Viral di sosial media video prajurit TNI yang diduga menendang sepeda motor seorang ibu yang sedang membonceng anaknya. kemudian Akun twitter dengan nama dhemit_is_back melakukan doxing terhadap plat nomer TNI tersebut, didalam gambar screenshot yang disebarkan terdapat nama pemilik kendaraan dan alamat rumah. Dalam hal ini doxing diperbolehkan, karena data yang didapatkan dicari pada informasi terbuka yang dapat diakses dengan bebas.

2. Trend *add yours*

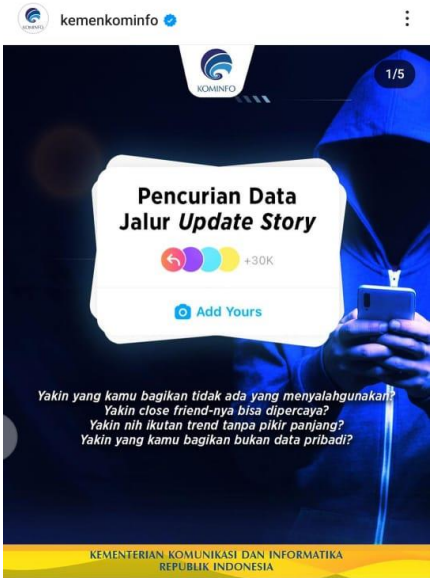
Trend “add yours” pada instagram yaitu sebuah fitur yang dapat diikuti atau bahkan memulai challenge yang dapat bebas diakses dan dilanjutkan oleh pengguna lain atau bisa disebut saling sharing. Dalam fitur ini pengguna dapat menjawab beberapa pertanyaan dapat berupa tulisan dan foto dengan *caption*. Sempat ramai hingga memancing keributan karena pengguna platform Instagram dengan mudahnya membagikan informasi berharga contohnya seperti nama orang tua, tanggal lahir hingga nomor identitas kependudukan. Tanpa disadari, keikutsertaan kita pada tren tren yang sedang ramai memancing kejahatan karena dari informasi yang dibagikan bisa saja disimpan lalu digunakan oleh orang orang yang tidak bertanggung jawab.[22]



Gambar 6. Fitur Add Yours di Instagram

Sebagaimana yang dapat dilihat pada gambar 6. Fitur *Add Yours* di Instagram yang sempat ramai menjadi bahan perbincangan karena terdapat data pribadi yang kemungkinan dapat disalahgunakan oleh orang yang tidak bertanggung jawab. Seperti, Nama (Nama lengkap, Nama panggilan semasa kecil, Nama ibu dan lain lain), Spill nomer identitas (KTP), Tanggal Lahir, Alamat Pribadi dan lain sebagainya.

Ramai nya fitur *add yours* ini, Safenet mengungkapkan kekhawatirannya pada laman Instagram @safenetvoice, tren seperti ini disebut sebagai bahan dari bentuk rekayasa sosial dengan cara menjebak seseorang melakukan hal tertentu secara sukarela. Karena seringakali hal yang diminta adalah hal yang tidak seharusnya disebarluaskan , seperti data pribadi. Data yang dikumpulkan nantinya akan dipergunakan oleh seseorang yang tidak bertanggung jawab kemudian akan dilakukan profiling untuk dijadikan bahan untuk melakukan kejahatan. Profiling adalah mengumpulkan informasi untuk mengidentifikasi seseorang. Data datanya dapat berasal dari informasi yang diungkap sendiri maupun menelusuri orang orang sekitarnya.



Gambar 7. Himbauan pengamanan data pribadi oleh kemenkominfo sumber:instragram

Sebagaimana yang dapat dilihat pada gambar 7. Kementrian Komunikasi dan Informatika telah memberikan himbauan melalui media sosial untuk para pengguna berhati-hati dalam beberapa *challenges* yang ada pada di fitur tersebut. Kemenkominfo pun menyebutkan contoh contoh data pribadi yang dapat disalahgunakan yaitu Nama (Nama lengkap, Nama semasa kecil, Nama ibu), Nomor Identitas, Alamat Pribadi, Data biometrikmu (Sidik jari, scan retina, dan lain lain), Informasi atas properti pribadi (SIM, Nomor Paspor, Plat Nomor Kendaraan dan lain lain), Informasi Aset Teknologi (Alamat Internet Protocol). Himbauan ini terkait aktivitas *cybercrime* dan kesalahan yang dilakukan oleh pengguna data pribadi yang sebetulnya seringkali sudah dilakukan himbauan. Mengingat kasus penipuan di

media sosial termasuk dalam kasus yang cukup tinggi, karena tidak menutup kemungkinan dapat berakibat pada terjadinya kejahatan cyber lainnya.[23]

Berbagai fitur yang membuat seseorang untuk membagi foto terkini atau bahkan informasi informasi yang bersifat pribadi berpotensi untuk disalahgunakan oleh orang yang tidak bertanggung jawab. Mengikuti tren yang sedang ramai boleh saja, tetapi tetap menjadi pengguna yang cerdas dengan tidak menampilkan data pribadi ke media sosial, karena trend tersebut cenderung membuat pengguna menjadi *oversharing* dapat membahayakan pengguna. Sebagai pengguna sosial media harus tetap selektif dan bijak dalam mengunggah sesuatu pada sosial media

Memilih suatu tren tentunya harus bijak dan di pikirkan baik baik, harus pintar dalam memilih dan memilah tren mana yang cocok di ikuti, jika termasuk dalam hal yang privasi sebaiknya tetap disimpan untuk pribadi bukan untuk dipublikasi. Tidak menyebarkan data pribadi di media sosial manapun, karena media sosial rentan terjadi kejahatan siber. Sekecil apapun data pribadi seperti tempat tinggal dan tanggal lahir yang di unggah dapat menjadi bahan untuk terjadinya kejahatan siber. [24]

B. Klasifikasi Doxing illegal dan legal

Tabel 1. Klasifikasi Doxing Ilegal

No	Doxing Ilegal	Deskripsi
1	Publikasi Ilegal	Melakukan Doxing dengan cara mengungkapkan informasi pribadi seseorang tanpa izin yang tentunya melanggar privasi korban. Seperti mengungkapkan informasi medis rahasia tanpa izin.
2	Pelecahan Online	Melakukan Doxing dengan cara mengungkapkan informasi pribadi seseorang dengan tujuan melecehkan, mengintimidasi, atau mengancam individu secara online. Seperti mengungkapkan alamat rumah dan nomor telepon pribadi.
3	Penganiayaan Online	Melakukan Doxing dengan cara mengungkapkan informasi yang merugikan seseorang secara online, seperti mengungkapkan informasi dengan tujuan untuk melakukan pelecehan dan pemerasan.
4	Penyebaran Konten Sensitif	Melakukan Doxing dengan cara mengungkapkan dan menyebarkan konten bersifat sensitif yang tentunya melanggar privasi seseorang. Seperti mempermalukan seseorang dengan menyebarkan foto atau video intim tanpa izin yang bersangkutan perbuatan ini dapat merugikan individu secara emosional.

Tabel 2. Klasifikasi Doxing Legal

No	Doxing Legal	Deskripsi
1	Jurnalistik	Melakukan Doxing dengan cara mengungkapkan informasi publik yang sah yang bertujuan untuk penyelidikan atau pelaporan berita yang bertanggung jawab.
2	Penegakan Hukum	Melakukan Doxing dengan cara mengungkapkan informasi pribadi dalam konteks investigasi dan penegakan hukum yang sah.

4	Keamanan Cyber	Melakukan Doxing dengan cara mengungkapkan informasi yang diperoleh secara legal untuk melindungi keamanan sistem atau jaringan dari serangan dan mencegah kebocoran data. Seperti dalam rangkan penanggulangan ancaman keamanan cyber.

Sebagaimana yang dapat dilihat pada tabel 1 dan tabel 2 tentang klasifikasi doxing illegal dan legal. Dapat disimpulkan bahwa terdapat perbedaan yang dominan antara doxing yang dianggap illegal dan legal yaitu pada tujuannya. Doxing yang illegal atau dilarang untuk dilakukan adalah yang melibatkan kegiatan melanggar privasi seseorang, mencuri identitas atau merugikan individu secara online. Dalam hal ini doxing dilakukan untuk hal yang merugikan orang lain seperti pencurian identitas, penipuan keuangan, penganiayaan dan pelanggaran privasi. Disisi lain, Doxing yang illegal dilakukan untuk pengungkapan informasi yang sah untuk kepentingan umum, seperti untuk keperluan jurnalistik, keamanan cyber dan penegakan hukum. Dalam hal ini doxing dilakukan untuk tujuan yang baik yaitu untuk melindungi keamanan, mencegah kejahatan dan memberikan informasi penting kepada masyarakat.

Pengaturan terkait pemrosesan data pribadi untuk kepentingan penegakan hukum yang lebih spesifik dan jelas terdapat pada Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi pasal 16 ayat 2, dapat disimpulkan mengenai pemrosesan data oleh otoritas resmi dalam penegakan hukum yaitu :

1. Pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum dan transparan
2. Melakukan proses data pribadi sesuai dengan tujuannya
3. Melakukan proses data pribadi dengan menjamin hak subjek data pribadi
4. Melakukan proses data pribadi secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan
5. Melakukan proses data pribadi dengan melindungi keamanan data pribadi dari pengakses yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan penghilangan data pribadi
6. Melakukan proses data pribadi dengan memberitahukan tujuan dan aktivitas proses, serta kegagalan perlindungan data pribadi
7. Data pribadi dimusnahkan atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan subjek pribadi , kecuali ditentukan lain oleh peraturan perundang undangan
8. Melakukan proses data pribadi secara bertanggungjawab dan dapat dibuktikan dengan jelas,

IV. SIMPULAN

Media sosial merupakan bagian yang tidak dapat dipisahkan dari kehidupan manusia modern dan telah memberikan kemudahan dalam berinteraksi, berbagi informasi dan terhubung dengan orang di seluruh dunia. Namun terdapat resiko besar terkait kejahatan cyber yang terjadi di platform sosial media dan masih banyak orang yang menyalahgunakan media sosial. Salah satunya adalah Doxing. Doxing merupakan tindak kejahatan yang dilakukan di internet dengan cara mengumpulkan data pribadi korban kemudian setelah terkumpul, data tersebut disebarluaskan di internet maupun di sosial media dengan tujuan untuk mengintimidasi dan mengancam korban. Tindak kejahatan doxing seringkali dilakukan di media sosial yang tentunya dapat merugikan korban karena terdapat data pribadinya yang disebarkan. Didalam Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terdapat data pribadi spesifik dan umum.

Perbuatan Doxing pada Undang Undang Perlindungan Data Pribadi (UU PDP) di dalam pasal 65 ayat 1 dan 2, menyebutkan bahwa kegiatan doxing adalah mengumpulkan data pribadi seseorang kemudian mengungkapkan data tersebut. perbuatan ini diancam pidana penjara dan sanksi. Pelaku disebutkan sebagai seseorang yang mengumpulkan data pribadi seseorang dan mengungkapkan data pribadi yang bukan miliknya. Maka pelaku doxing yang mengumpulkan data pribadi seseorang menurut undang undang pasal 67 ayat 1 dan 2 perlindungan data pribadi diancam pidana penjara paling lama 5 tahun atau denda paling banyak 5 Miliar untuk pelaku yang mengungkapkan data pribadi hasil dari data pribadi mengumpulkan data pribadi tersebut diancam dengan pidana penjara paling lama 4 tahun dan denda paling banyak 4 Miliar.

Pola Pola doxing pada masa kini yaitu melalui social engineering atau rekayasa sosial. Pelaku Rekayasa Sosial dapat memanipulasi emosi pengguna media sosial untuk mengunggah data pribadi mereka secara sukarela, dengan cara memanfaatkan tren tren yang ada di media sosial. Pelaku akan mengarahkan pengguna media sosial untuk melakukan tindakan yang akan merugikannya seperti pengguna medsos akan dipaksa untuk mengikuti tren dengan cara mengungkapkan informasi pribadi. Pelaku dapat berperan sebagai peserta tren dan meminta pengikut tren untuk mengungkapkan detail pribadi seperti nama lengkap, alamat pribadi, nomor telepon hingga tanggal lahir. Sehingga

pengguna media sosial yang terpengaruh oleh tren dan ingin berpartisipasi mungkin tidak menyadari bahwa mereka telah memberikan informasi pribadi. Tren tersebut adalah tren *spill the tea* dan tren *add yours.*

Doxing secara umum memang tidak diperbolehkan karena dapat merugikan privasi seseorang, namun dalam beberapa kasus, terdapat doxing yang diperbolehkan seperti ketika informasi yang diungkapkan adalah informasi publik atau dibagikan dan dapat diakses secara terbuka, namun tetap saja hal tersebut harus dilakukan dengan hati-hati dan sesuai dengan hukum yang berlaku. Salah satu contoh bahwa pengungkapan informasi pribadi seseorang dapat diperbolehkan seperti dalam kasus investigasi kriminal atau keamanan nasional yang dilakukan oleh lembaga yang berwenang. Namun meski terdapat kegiatan doxing yang diperbolehkan, pada dasarnya doxing selalu melanggar hak privasi seseorang karena akan menimbulkan berbagai konsekuensi negatif, kecuali dalam keadaan tertentu seperti yang dilakukan oleh pihak berwenang untuk menangani kejahatan atau pelanggaran hukum tertentu dilakukan dengan cara yang proporsional dan sesuai dengan hukum yang berlaku.

UCAPAN TERIMA KASIH

Terima kasih kepada kedua orangtua saya Bapak Mukti Prijono dan Ibu Rijastuti, kedua kakak saya Tyagita Winaya Mukti dan Cahyarani Dewi Mukti yang tak henti hentinya mendoakan serta memberikan dukungan moril dan materil agar penelitian ini berjalan dengan lancar. Serta, tak lupa juga terimakasih kepada teman teman kelas hukum 8 A1 yang telah memberikan semangat pada saat penelitian ini berlangsung.

REFERENSI

[1] A. S. Cahyono, "Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat Di Indonesia," *Publiciana*, vol. 9, no. 1, Art. no. 1, 2016, doi: 10.36563/publiciana.v9i1.79.

[2] D. D. N. Dzikra, "Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial," *J. Rechten Ris. Huk. Dan Hak Asasi Mns.*, vol. 2, no. 1, pp. 1–7, Jun. 2022, doi: 10.52005/rechten.v2i1.50.

[3] A. A. Agus and R. Riskawati, "Penaganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," *SUPREMASI J. Pemikir. Penelit. Ilmu-Ilmu Sos. Huk. Dan Pengajarannya*, vol. 11, no. 1, Art. no. 1, Aug. 2019, doi: 10.26858/supremasi.v11i1.3023.

[4] R. Aswandi, P. R. N. Muchin, and M. Sultan, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)," Jun. 2020. Accessed: Apr. 21, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Perlindungan-Data-Dan-Informasi-Pribadi-Melalui-Aswandi-Muchin/3b6c30cc8dc160381876098e31d4db4a13788d24

[5] M. Yoedtadi, "Doxing Teror di Ranah Maya Book Chapter Komunikasi dalam Gagasan dan Implementasinya," 2022, pp. 80–91.

[6] P. Khanna, P. Zavarsky, and D. Lindskog, "Experimental Analysis of Tools Used for Doxing and Proposed New Transforms to Help Organizations Protect against Doxing Attacks," *Procedia Comput. Sci.*, vol. 94, pp. 459–464, 2016, doi: https://doi.org/10.1016/j.procs.2016.08.071.

[7] T. C. Yudiana, S. D. Rosadi, and E. S. Priowirjanto, "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia," *Fac. Law Univ. Padjadjaran*, vol. Vol 9, No 1 (2022): Padjadjaran Jurnal Ilmu Hukum (Journal Of Law), 2022, [Online]. Available: http:

[8] M. A. C. Armando and H. Soeskandi, "Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut UU ITE Dan UU PDP," *Bur. J. Indones. J. Law Soc.-Polit. Gov.*, vol. 3, no. 1, pp. 559–568, Dec. 2022, doi: 10.53363/bureau.v3i1.201.

[9] I Putu Pasek Bagiartha W, "Perilaku Doxing Dan Pengaturannya Dalam Positivisme Hukum Indonesia," *J. Huk. Agama Hindu Widya Kerta*, vol. 4, no. 2, Nov. 2021, doi: 10.53977/wk.v4i2.386.

[10] A. N. Anisa, “Peranan Jejaring Sosial Tiktok Dalam Memperoleh Informasi,” other, Universitas Komputer Indonesia, 2021. doi: 10/13.%20Unikom_41816133_Aulia%20Nur%20Anisa_BAB%20IV.pdf.
[11] Y. Fitriani and R. Pakpahan, “Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace,” *J. Hum. Bina Sarana Inform.*, Apr. 2020, Accessed: Apr. 28, 2023. [Online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala/article/view/6446
[12] H. Akhtar, “Perilaku Oversharing di Media Sosial: Ancaman atau Peluang?,” *Psikologika J. Pemikir. Dan Penelit. Psikol.*, vol. 25, no. 2, Art. no. 2, Jul. 2020, doi: 10.20885/psikologika.vol25.iss2.art7.
[13] A. Gani, “Cybercrime (Kejahatan Berbasis Komputer),” *JSI J. Sist. Inf. Univ. Suryadarma*, vol. 5, no. 1, Art. no. 1, Feb. 2020, doi: 10.35968/jsi.v5i1.18.
[14] S. Winarno, “Waspada Doxing,” *Arsip Publ. Ilm. Biro Adm. Akad.*, no. 0, Art. no. 0, Feb. 2020, Accessed: May 01, 2023. [Online]. Available: http://research-report.umm.ac.id/index.php/API-BAA/article/view/3572
[15] C. N. Putri, “Kajian Kriminologi Kejahatan Penyebaran Data Pribadi (Doxing) Melalui Media Sosial,” Feb. 07, 2023. http://digilib.unila.ac.id/69177/ (accessed May 02, 2023).
[16] S. Voice, “Represi Digital di Indonesia Masih Terus Berlanjut - SAFEnet,” Mar. 05, 2022. https://safenet.or.id/id/2022/03/represi-digital-di-indonesia-masih-terus-berlanjut-sepanjang-2021/ (accessed May 01, 2023).
[17] J. I. Grant, “Doxing,” *eSafety Commissioner*, May 23, 2020. https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing (accessed May 02, 2023).
[18] X Corp, “Kebijakan informasi pribadi dan doxxing di Twitter | Bantuan Twitter,” Desember 2022. https://help.twitter.com/id/rules-and-policies/personal-information (accessed May 10, 2023).
[19] M. Muhammad, “Peningkatan Korban Kejahatan Siber Selama Pandemi COVID19,” *Nusant. J. Ilmu Pengetah. Sos.*, vol. 9, no. 6, Art. no. 6, Jul. 2022, doi: 10.31604/jips.v9i6.2022.2043-2054.
[20] S. Widi, “Pengguna Media Sosial di Indonesia Sebanyak 167 Juta pada 2023,” *Dataindonesia.id*. https://dataindonesia.id/digital/detail/pengguna-media-sosial-di-indonesia-sebanyak-167-juta-pada-2023 (accessed May 04, 2023).
[21] T. Rahayu, “Fenomena Spill The Tea Kekerasan Seksual Di Media Sosial Pada Generasi Z Kota Bandung,” other, Universitas Pendidikan Indonesia, 2022. Accessed: May 03, 2023. [Online]. Available: http://repository.upi.edu
[22] Universitas Pasundan, “Fitur ‘Add Yours’ Instagram dan Ancaman Penyalahgunaan Data, Sandhika Galih: Pahami Literasi Digital,” *Universitas Pasundan*, Dec. 01, 2021. https://www.unpas.ac.id/fitur-add-yours-instagram-dan-ancaman-penyalahgunaan-data-sandhika-galih-pahami-literasi-digital/ (accessed May 10, 2023).
[23] N. S. Novitasari and T. Tantimin, “Kajian Hukum Terhadap Bahaya Pengumpulan Informasi Rekayasa Sosial Melalui Fitur Add Yours Instagram,” *AL-MANHAJ J. Huk. Dan Pranata Sos. Islam*, vol. 5, no. 1, Art. no. 1, Apr. 2023, doi: 10.37680/almanhaj.v5i1.2420.
[24] Zalfa, “Hindari Profilling : Modus Kejahatan dari Fitur Add Yours Instagram – LPM Dimensi,” Desember 2021. https://www.lpmdimensi.com/2021/12/hindari-profilling-modus-kejahatan-dari-fitur-add-yours-instagram/ (accessed May 10, 2023).

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.