JOURNAL JUSTICIABELLEN (JJ)
Vol. 02, No. 02, Juli 2021, h. 104-119
Available Online at https://jurnal.unsur.ac.id/index.php/JJ
P-ISSN: 2774-3764 E-ISSN:2774-8375

CYBERCRIME DI ERA INDUSTRI 4.0 DAN MASYARAKAT 5.0 DALAM PERSPEKTIF VIKTIMOLOGI

Angkasa[1], Rili Windiasih[2]
[12]Universitas Jenderal Soedirman
[1]*E-Mail* : *drangkasa_64@yahoo.com*
[2]*E-Mail : rili.1997unsoed@gmail.com*

Masuk : 25 Maret 2022	Penerimaan : 16 Juli 2022	Publikasi :20 Juli 2022

ABSTRAK

Era Industri 4.0 dan Masyarakat 5.0 mempunyai karakteristik yang berbeda dan berdampak pula bagi jenis viktimisiasi khususnya akibat *cybercrime*. Hal ini berkorelasi dengan karakter pada era tersebut antara lain digitalisasi, rekayasa intelegensia dan *internet of thing,* Melalui penelitian kepustakaan dapat dijelasakan bahwa dalam perspektif viktimologi korban atas *cybercrime*. Korban *cybercrime* mengalami berupa kerugian materi, akibat psikologis akibat fisik dan akibat sosial. Viktimisasi cybercrime dapat dijelaskan dengan *The Lifestyle-Routine Activities Theory* (L-RAT). Perlindungan hukum korban *cybercrime* mendasarkan Undang-Undang Nomor 19 Tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dapat dikatakan tidak terdapat perlindungan hukum secara signifikan dapat dirasakan oleh para korbannya Seharusnya terdapat sanksi berupa restitusi dan/atau pemberian kompensasi. Hal ini selaras dengan karakter masyarakat 5.0 yang lebih menghormati keberadaan manusia.

Kata Kunci: Hukum; Kompensasi; Perlindungan; Siber; Teknologi.

ABSTRACT

The Industrial Era 4.0 and Society 5.0 have different characteristics and this has an impact on the types of victimization, especially those caused by cybercrime. This correlates with the characteristics of that era, including digitalization, intelligent engineering and the internet of things. Through library research, it can be explained from a victimological perspective that victims of cybercrime suffer losses in the form of material losses, psychological suffering, physical suffering and social suffering. Cybercrime victimization can be explained by the lifestyle-routine activities theory (L-RAT). The legal protection of cybercrime victims is based on Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions and it can be said that there is no significant legal protection that can be felt by the victims. There should be sanctions in the form of restitution and/or compensation. This corresponds to the nature of society 5.0 which is more respectful of human existence.

Keywords: *Compensation; Cyber; Law; Protection; Technology.*

A. PENDAHULUAN

Tulisan ini bertujuan mengemukakan suatu pemikiran tentang kondisi yang terjadi pada Era Revolusi Industri 4.0 dan Sosial 5.0 dalam perspektif Viktimologi. Pada era tersebut yang mempuyai karakteristik yang spesifik berupa meningkatnya digitailsasi rekayasa intelegensia dan *internet of thing*. Dampak terhadap kehidupan sosial adalah kondusif terjadinya *cybercrime* khususnya internet dipakai sebagai sarana untuk melakukan kejahatan, walaupun tidak tertutup kemungkinan yang menjadi sasaran adalah komputernya berupa data maupun sistem yang ada di dalam komputer tersebut. *Cybercrime* yang terjadi dalam tulisan ini dilihat dari perspektif viktimologi dimaksudkan sebagai cara pandang yang mendasarkan atas 3 aspek selaras dengan tujuan viktimologi sebagaimana yang dikemukakan oleh Zvonimir-Paul Separovic meliputi ananilis berbagai aspek masalah korban, menjelasakan sebab-sebab terjadinya viktimisasi dan menciptakan suatu sistem guna mengurangi penderitaan korban (Separovic, 1985).

Pertama terkait dengan berbagai aspek masalah korban atas viktimisasi yang terkait dengan Era Revolusi Industri 4.0 dan Sosial 5.0. Untuk membahas ini maka akan dibahas tentang bentuk-bentuk kejahatan yang sangat dekat dengan karakter yang dimiliki dapa era ini, karena untuk dapat melihat aspek korban harus pula melihat aspek kejahatannya sebagai perilaku yang menciptakan korban. Untuk adanya korban harus berlangsung adanya kejahatan atau viktimisasi. Hal ini mendasarkan pula atas pendapat Stanciu memberikan batasan tentang korban harus terdapat unsur penderitaan dan ketidakadilan (Stanciu, 1976).

Berbagai aspek masalah korban yang dikaji diantaranya tentang kerugian dan/atau penderitaan korban akibat atau efek atas viktimisasi yang terjadi. Hasil analisis ini dapat dipakai sebagai landasan dalam menciptakan suatu sistem guna mengurangi penderitaan korban. Hal tersebut antara lain didasarkan atas pendapat yang dikemukakan Shapland sebagai bahwa untuk dapat membantu para korban dengan baik maka harus diketahu dengan baik tentang efek viktimisasi yang dirasakan oleh korban (Shapland, 1986).

Aspek yang kedua terkait dengan penyebab terjadinya viktimisasi berdasarkan teori viktimologi dan aspek yang ke tiga membuat suatu formulasi

policy dalam upaya mengurangi penderitaan korban. Untuk dapat memberikan gambaran yang lebih utuh maka dalam tulisan ini juga dideskripsikan tentang berbagai aspek tentang Era Revolusi Industri 4.0 dan Sosial 5.0, yang dilanjutkan dengan kejahatan yang potensial dengan karakter yang dimiliki pada era tersebut. Berdasarkan latar belakang tersbut maka dapat diajukan tiga permasalahan sesuai dengan pendekatan yang dipakai yakni pendekatan viktimologi sebagai berikut. *Pertama,* bagaimanakah kerugian dan/atau penderitaan korban *cybercrime* yang terjadi di era Industri 4.0. *Kedua*, apakah yang menjadi penyebab terjadinya *cybercrime*, dan yang *ketiga* adalah bagaimanakah perlindungan hukum bagi korban yang mampu memberikan manfaat secara signifikan kepada para korbannya.

B. METODE

Penelitian ini menggunakan pendekatan metode deskriptif dan jenis penelitian yang digunakan adalah penelitian kepustakaan. Deskriptif di sini dimaksudkan melakukan penelitian bertujuan untuk menjelaskan dan menjawab secara lebih rinci permasalahan yang akan diteliti dan dijelasakan dengan penjelasan secara kualitatif. Data utama sesuai dengan pengunaan penelitian berupa kepustakaan maka dalam penelitian ini adalah data sekunder artinya data yang sudah tersaji yang terhimpun dalam suatu dokumen atau naskah. Data yang dimaksud terutama jurnal-jurnal terakreditasi dan bereputasi baik nasional maupun internasional. Selain itu data diambil dari bahan hukum primer sebagai sautu bahan hukum yang mempunyai otoritas atau dikenal pula bersifat autoritatif. Dalam hal ini terutama hukum positif berupa norma hukum Undang-Undang Nomor 19 Tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

C. HASIL ATAU PEMBAHASAN

1. Berbagai Aspek Tentang Era Revolusi Industri 4.0 dan Sosial 5.0

Industri.4.0 merupakan inisiatif dari Jerman dan kemudian diadopsi secara global dalam satu decade terakhir (Xu et al., 2021). Istilah Industri 4.0 diperkenalkan secara publik pada tahun 2011 di Hannover Fair yang berawal dari

sebuah proyek dalam strategi teknologi tinggi pemerintah Jerman. Ini memajukan konsep *Cyber Physical Systems* (CPS) menjadi *Cyber Physical Production Systems* (CPPS). Industri 4.0 dianggap sebagai revolusi berbasis teknologi untuk mencapai efisiensi dan produktivitas yang lebih tinggi dan, sebagai strategi teknologi tinggi pemerintah, untuk meningkatkan daya saing Jerman di pasar global. Indusri 4.0 berfokus pada teknologi, fleksibilitas, dan produktivitas. Industri 4.0 bermaksud untuk mengatasi tantangan seperti efisiensi sumber daya dan energi, produksi perkotaan, kebutuhan masyarakat, dan perubahan demografis.

Di belakang industri 4.0 terdapat beberapa revolusi industri dengan karakteristiknya masing-masing meliputi revolusi industri pertama, kedua dan ketiga. Revolusi Industri pertama ditandai adanya transisi dari metode produksi manual ke metode produksi dengan menggunakan mesin bertenaga uap atau air. Dilanjutkan revolusi industri kedua terdapat perubahan dimana pabrik yang ada diubah menjadi jalur produksi modern yang berimplikasi pada terjadinya nilai produktivitas yang tinggi dan berdampak lanjut pada pertumbuhan ekonomi yang sangat signifikan. Pada revolusi industri ke tiga terdapat penggunaan komputer dan dibarengi dengan teknologi komunikasi seperti yang dikenal dengan *Programmable Logic Controller* (PLC) dalam upaya untuk mendukung proses produksi yang cenderung mengarah ke otomatisasi produksi. Revolusi industri 4.0 Tahun 2010 terjadi rekayasa intelegensia atau *Articifial Intellegence* (AI) selain *Internet of Thing (IoT),* muncul *big data*, percetakan *3D.* Industri 4.0 lebih pada digitalisasi dan teknologi berbasis AI untuk meningkatkan efisiensi dan fleksibilitas produksi (Breque et al., 2021). Oleh karenanya maka revolusi industry 4 ini tidak hanya dikatakan sebagai perkembangan belaka dari revolusi industri 3, namun juga dimaknai sebagai iniovasi baru, karena terdapat perkembangan yang sangat signifikan. Pada tahap ini lebih didorong dengan berlangsungnya globalisasi yang menjadikan masyarakat semakin mudah dalam beraktivitas dengan waktu yang lebih efektif dan efisien. Di era revolusi industri 4.0 ini juga terjadi digitalisasi dan penghijauan ekonomi dianggap sebagai konsep kembar yang mendorong pembangunan berkelanjutan. Mereka menjalankan program tersebut secara beriringan, diantaranya teknologi digital baru termasuk

kecerdasan buatan (AI) digunakan untuk mengumpulkan, menilai, menganalisis data, dan mengomunikasikan hasil tersebut ke publik yang lebih luas. Pada revolusi industry 4.0 dapat dikatakan bahwa dunia telah mengalami transformasi substansial dengan inovasi sebagai kekuatan pendorong. Indistri 4.0 memungkinkan produksi menjadi fleksibel dan produk-produknya berkualitas tinggi namun secara keseluruhan lebih efisien (Wang et al., 2016).

Selain istilah industri 4.0. dikenal juga istilah *society* 4.0 yang di belakangnya terdapat pula *society* 1.0, *society* 2.0 dan *society* 3.0 dan kini sampai pada tahap *society* 5.0 sebagai peradaban manusia yang masing-masing juga memiliki karakteristik tersendiri. Pada *society* 1.0 manusia masih berada di era berburu dan mengenal tulisan. Pada *society* 2.0 adalah pertanian di mana manusia sudah mulai mengenal bercocok tanam. Kemudian pada *society* 3.0 sudah memasuki era industri yaitu ketika manusia sudah mulai menggunakan mesin untuk menunjang aktivitas sehari-hari, setelah itu muncullah *society* 4.0 yang dialami saat ini, yaitu manusia yang sudah mengenal komputer hingga internet juga penerapannya di kehidupan (Puspita et al., 2020).

Selanjutnya muncul konsep *Society 5.0* dan *Industry 5.0* tapi kemunculan ini bukanlah kelanjutan kronologis sederhana atau alternatif paradigma Industri 4.0. *Society* 5.0 bertujuan untuk menempatkan manusia pada titik tengah inovasi, memanfaatkan dampak teknologi dan hasil Industri 4.0 dengan integrasi teknologi untuk meningkatkan kualitas hidup, tanggung jawab sosial, dan keberlanjutan. Perspektif terobosan ini memiliki poin yang sama dengan tujuan Tujuan Pembangunan Berkelanjutan Perserikatan Bangsa-Bangsa (Carayannis & Morawska-Jancelewicz, 2022).

Berdasar pada konsep Mazzucato industri 5.0. dan masyarakat 5.0 menyerukan bahwa inovasi berorientasi misi, inovasi sosial yang bersifat lintas disiplin, lintas sektor dan lintas aktor dengan peran penting warga sebagai peserta aktif proses inovasi. Misi penelitian dan inovasi dengan demikian harus bertujuan untuk meningkatkan kesejahteraan masyarakat (Mazzucato, 2018). Industri 5.0 dipahami sebagai kekuatan industri untuk mencapai tujuan sosial di selain tujuan pekerjaan dan pertumbuhan ekonomi, serta untuk menjadi penyedia kemakmuran yang tangguh, dengan membuat produksi menghormati batas-batas yang telah ada

pada diri masyarakat dan juga lebih bertujuanan menempatkan kesejahteraan pekerja industri di pusat proses produksi (Breque et al., 2021).

Society 5.0 dan *Industry 5.0* merefleksikan pergeseran mendasar masyarakat dan ekonomi menuju paradigma baru untuk menyeimbangkan pembangunan ekonomi dengan penyelesaian masalah sosial dan lingkungan dan untuk mengatasi tantangan yang terkait dengan interaksi manusia-mesin dan pencocokan keterampilan (Breque et al., 2021). Komisi Eropa mengumumkan Industri 5.0. yang memiliki perbedaan dengan Industri 4.0 dianggap didorong oleh teknologi, sedangkan Industri 5.0 didorong oleh nilai khususnya nilai kesejahteraan hidup bagi masyarakat. Dalam paradigma baru ini, pentingnya pengetahuan tidak ditentukan secara eksklusif oleh daya saing dan produktivitas, tetapi dengan mempertimbangkan penciptaan kesejahteraan sosial, dampaknya terhadap kualitas hidup dan penciptaan bersama pengetahuan sebagai bagian dari masyarakat serta kemitraan swasta (Morawska-Jancelewicz, 2021).

2. Era Industri 4.0, Sosial 5.0, dan Viktimisasi

Era Industri 4.0, Sosial 5.0, dengan karakteristik yang dimililik terutama adanya digitalisasi pada industri 4.0 yang dikaitkan dengan komunikasi digital berpotensi terjadinya *cybercrime*. Mendasarkan referensi yang ada meliputi pendapat para para pakar maupun batasan yang diberikan oleh suatu lembaga maka *cybercrime* dapat dikatagorikan menjadi dua pandangan dan dapat pula dikatakan mengalami suatu perkembangan. Pengertian *cybercrime* pada awalnya merujuk pada penggunaan computer yang dimiliki pihak tertentu secara tidak saah atau *illegal* dan juga termasuk di dalamnya melakukan perusakan dan/atau pengambilan data yang ada di dalamnya. Hal ini dapat dicermati antara lain pendapat dari Andi Hamzah, yang berpendapat bahwa *cybercrime* merupakan kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal (Hamzah, 1996). Pengertian ini identik dengan pengertian *cybercrime* dalam arti sempit yang dirumuskan dalam dokumen kongres PBB tentang *The Prevention of Crime and The Treatment of Offlenderes* di Havana, Cuba pada tahun 1999 dan di Wina yang menyatakan *cybercrime* :*any illegal behaviour directed by means of electronic operations that targets the security of*

computer systems and the data processed by them (Kurnia Putra, 2014). Batasan ini dapat diartikan *cybercrime* merupakan perbuatan bertentangan dengan hukum yang langsung berkaitan dengan sarana elektronik dengan sasaran pada proses data dan sistem keamanan komputer (Saragih & Azis, 2020).

Dalam perkembangan selanjutnya *cybercrime* mempunyai makna yang lebih luas yakni termasuk di dalamnya setiap kejahatan yang menggunakan computer sebagai sarananya. Batasan ini oleh PBB dikatagorikan sebagai *cybercrime* dalam arti luas yang batasannya adalah: *any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network* (Riadi et al., 2017). Batasan ini dapat diartikan sebagai perbuatan yang melawan hukum dengan menggunakan sarana atau berkaitan dengan sistem atau jaringan komputer termasuk kejahatan memiliki secara *illegal*, menawarkan atau mendistribusikan informasi melalui sarana sistem atau jaringan komputer. Pengertian ini senada dengan yang dibuat oleh *Organization of European Community Deveplopment*, bahwa *cybercrime* adalah *"any illegal, unethical or unauthorized behaviour relating to the automatic processing and/or the transmission of data*". Peter Stephenson memberikan pernyataannya tentang *cybercrime*:

> *"The easy of cybercrime is crimes directed at computer or a computer system. The nature of cybercrime, however, is more complex. As we will see later, cyber rime can take the form of simple snooping into a computer system for which we have no authorization it can be the feeing of computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system"* (Stephenson, 2000).

Di dalam batasan ini perluasan kejahatan terhadap computer sedikit diperluas dengan pencurian uang menggunakan *system computer.* Dalam perkembanganya *cybercrime* sangat diperluas batasannya, tidak hanya kejahatan terhadap computer misalnya penggunanan secara *illegal*, pencurian data maupun perusakan terhadap data maupun systemnya namun termasuk semua aktivitas kejahatan yang menggunakan computer sebagai salah satu/atau keseluruan dari kejahatan yang dilakukan (Brenner, 2012).

Secara umum berdasar pendapat (Antonescu & Birău, 2015) *cybercrime* adalah:

> *"Generally, cybercrime includes a wide range of illegal activities such as : cyber bullying, cyber terrorism, identity theft, cyber stalking, virtual pornography (via the Internet), cyber espionage (illegally obtaining confidential data), computer hacking, computer fraud, online harassment, phishing, online piracy, blackmailing proceeding, cyber extortion, spam attacks, copyright infringement, computer virus programs (installing malicious software programs such as Trojan horse viruses).*

Terdapat batasan sederhana namun dapat mencakup beberapa deskripsi ttg cybercrime di atas dikemukakan oleh Raj Sinha dan Niraj Kumar Vedpuria yang menyatakan sebagai berikut: *Cybercrimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both* (Sinha & Vedpuria, 2018).

3. *Cybercrime* dan Korban *Cybercrime*

Cybercrime dapat berbentuk berbagai macam aktivitas yang *illegal*, oleh karenanya korban yang ditimbulkan juga bervariasi sesuai dengan bentuk *cybercrime* nya (Correia, 2019). Furnell membagi bentuk *cybercrime* menjadi 3 meliputi perangkatnya *(device),* kemudian uang *(money)* seperti pemalsuan pembayaran, penipuan terhadap konsumen dan yang ketiga adalah seseorang menjadi korban *(the person of the victim)* antara lain dalam bentuk mengirimkan ancaman serta melakukan penguntitan secara online (Furnell, 2001).

Dalam perspektif viktimologi terjadinya viktimisasi dapat memunculkan empat dampak. Shapland telah membahas dalam tulisannya yang berjudul *The effects of the offence* (Shapland et al., 1985). Efek yang dapat ditimbulkan oleh suatu tindak pidana bagi korban dapat berupa kerugian materi *(financial loos),* akibat psikologis *(psychological effect)* akibat fisik *(physical effects),* akibat sosial *(social effects)* (Lamet & Wittebrood, 2009; Shapland et al., 1985). Beberapa studi yang ada tentang dampak viktimisasi dunia maya menunjukkan bahwa dampak ini dapat parah dan dapat menyerupai kejahatan tradisional (Holt & Bossler, 2008). Namun demikian karena *cybercrime* mempunyai karakteristik sendindiri maka bentuk dampaknya pun dapat berbeda.

Efek yang dapat ditimbulkan oleh *cybercrime* menurut (Dignan, 2004) lebih didominasi oleh kerugian materi menyangkut keuangan *(financial loos)* berupa hilangnya uang serta penderitaan psikologis *(psychological effect)* (Leukfeldt et al., 2019). Efek psikologis yang dapat ditimbulkan terhadap korban adalah mengalami stress dari tingkat ringan hingga berat, bahkan dalam beberapa kasus menimbulkan bunuh diri (Borwell et al., 2021). Hal ini sebagaimana tampak dalam riset yang dilakukan oleh Chang terhadap kasus peretasan Ashley Madison (Chang et al., 2016). suatu situs layanan kencan *online* untuk orang yang sudah menikah dengan kata lain situs yang menyediakan prasarana untuk melakukan perselingkungan. Situs tersebut servernya di sebuah perusahaan Kanada bernama Avid Life Media (ALM). Ashley Madison mempunyai slogan *"Life is short. Have an affair"*. Ashley Madison mengklaim memiliki keanggotaan internasional 37,6 juta yang berdomisili tidak kurang dari 40 negara, semuanya meyakinkan bahwa penggunaan layanan ini akan "anonim", "100% rahasia". Saat situs tersebut diretas dan dipublikasikan dalam suatu media terlihatlah keanggotannya antara lain terdiri dari politisi, pendeta, anggota militer, pegawai negeri sipil, selebriti serta ratusan tokoh masyarakat lainnya. Hal ini dibuktikan dengan adanya bukti pembayaran melalui *credit card* yang memang merupakan persyaratan mutlak untuk menjadi member Ashley Madison. Hal ini tentu saja terjadi semacam bencana besar dan sangat mempengaruhi kedudupan masyarakat. Mereka para member menjadi korban dan merasakan dampak psikologis yang luar biasa karena identitas mereka dibuka secara publik. Atas tragedi ini maka banyak pasangan suami isteri kemudian bercerai, para pejabat mengundurkan diri dan terdapat pula yang melakukan bunuh diri karena merasakan begitu beratnya dampak psikologis yang dialaminya. Bunuh diri antara lain dilakukan oleh seorang pendeta di Louisiana karena merasa tidak kuat menahan rasa malu dihadapan para jamaahnya. Efek psikologis bagi korban juga dapat berlangsung dengan durasi yang lama sejalan dengan konten yang masih tetap berada dalam dunia maya. Ini juga dapat dimanfaatkan semacam senjata oleh para penjahatnya untuk memeras korban (Jahankhani et al., 2014). Dampak psikologis lainnya sebagai korban *cybercrime* dapat terdiri dari: stres, kecemasan, kemarahan, dan ketakutan akan viktimisasi berulang (Brands & van Wilsem, 2021). Demikian pula yang

dinyatakan oleh Janoff-Bulman & Frieze bahwa efek psikologis yang diderita korban dapat bervariasi dari syok, ketidak berdayaan, kecemasan dan depresi hingga PTSD, perasaan dalam kesendirian, dan fobia (Janoff-Bulman & Frieze, 1983). Korban mengalami trauma emosional, mereka juga mengalami lebih banyak kepanikan dan depresi. Di kemudian hari para korban semakin sulit untuk mempercayai lagi orang lain secara *online*.

Dampak materi atau keuangan *(financial loos)* berdasarkan Center for Strategic and International Studies (CSIS), bekerja sama dengan McAfee, mempresentasikan *Economic Impact of Cybercrime* laporan global yang berfokus pada dampak signifikan kejahatan dunia maya terhadap ekonomi di seluruh dunia, menyimpulkan bahwa hampir $600 miliar, hampir satu persen dari PDB global, hilang akibat kejahatan dunia maya setiap tahun, naik dari studi tahun 2014 yang menempatkan kerugian global sekitar $445 miliar (Dinisman & Moroz, 2017). Beberapa bentuk pengeluaran sebagai korban *cybercrime* terkait dengan pembayaran untuk menebus data terenkripsi, serta biaya mengamankan jaringan, membeli asuransi siber, dan membayar pemulihan dari serangan siber. Kerugian finansial dapat pula diperhitungkan dari waktu dan sumber daya yang digunakan untuk menyelesaikan masalah, atau hilangnya pendapatan karena ketidak mampuan untuk bekerja, juga dianggap sebagai dampak finansial (Shapland & Hall, 2007). Dampak fisik tidak langsung seperti masalah kulit, kurang tidur, sakit kepala, dan penurunan berat badan lebih sering terjadi pada kejahatan dunia maya pembohongan. Hal ini, sering diakibatkan oleh gangguan psikologis dampak viktimisasi. Dampak sosial antara lain munculnya pandangan negatif dari masyarakat terhadap korban sebagaimana yang terjadi pada para korban yang terbagung dalam Ashley Madison.

4. Teori Viktimisasi *Cybercrime*

Viktimisasi atas *cybercrime* dapat dijelaskan dengan *Lifestyle theory* dan *Routine activity theory*. *Lifestyle theory* ini pertama kali dikemukakan secara rinci oleh (Hindelang et al., 1978). *Lifestyle* dimaksudkan sebagai kegiatan rutin dalam kesehariannya. *Lifestyle theory* adalah model teori dalam perspektif viktimologi yang berpendapat bahwa kemungkinan individu akan mengalami viktimisasi

pribadi sangat bergantung pada konsep gaya hidupnya (Stevens, 2003). Probabilitas viktimisasi meningkat sebagai fungsi dari gaya hidup yang berkorelsi dengan meningkatkan jumlah waktu yang dihabiskan di tertentu di antara orang asing. Apa yang dilakukan orang, bagaimana mereka berperilaku, menempatkan mereka pada risiko yang lebih atau kurang untuk terjadinya viktimisasi.

Routine Activity Theory merupakan salah satu teori pertama kali dikembangkan oleh Lawrence Cohen dan Marcus Felson yang menyatakan bahwa terdapat 3 syarat untuk dapat terjadinya viktimisasi meliputi: Pelaku yang potensial *(potential offender);* target yang sesuai dengan kehendak pelaku *(a suitable target)* dan, tidak adanya penjaga yang memadai dan mampu melindungi seseorang ataupun propertinya *(the absence of a capable guardian)* (Kitteringham & Fennelly, 2020). Ketiga syarat harus bersatu padu agar viktimisasi dapat terwujud dan kemudian menimbulkan korban.

Kedua teori tersebut merupakan terori yang sudah mapan dalam kriminologi dan juga viktimologi dalam empat dekade terakhir. Dalam perkembangannya kedua teori tersebut dintegrasikan yang kemudian dikenal dengan *Lifestyle-routine activity theory (L-RAT)* (Garofalo, 1987). *Lifestyle- routine activity theory* merupakan teori yang memandang lensa konvergensi pelaku yang termotivasi oleh adanya target/korban yang menarik dan di sisi lain pada pihak korban tidak terdapat aspek yang melindunginya secata memadai. Namun demikian terdapat sisi perbedaan pada kedua teori tersebut, dimana teori *lifestyle* lebih menitik beratkan bahwa seseorang dengan gaya hidup tertentu cenderung mempunyai risiko menjadi korban yang relevan dengan gaya hidupnya (Pratt & Turanovic, 2015). Namun untuk *routine activity theory* dipersaratkan adanya 3 aspek yang kesemuanya harus ada untuk terjadinya viktimiasi meliputi *potential offender, a suitable target* serta *the absence of a capable guardian* (Maxfield, 1987).

Dalam pandangan Yar, *the lifestyle-routine activities theory* dapat juga dipakai untuk menjelaskan viktimisasi akibat *cybercrime* (Holt & Bossler, 2008). *L-RAT* menunjukkan bahwa viktimisasi kemungkinan besar terjadi ketika individu ditempatkan dalam situasi berisiko tinggi, berada di dekat pelaku yang termotivasi, tampaknya korban menjadi target yang menarik bagi penjahat, dan di sisi lain korban juga tidak memiliki pelindung atau pengaman saat mengunakan

komputer (Miethe & Meier, 1994). Studi awal *L-RAT* menunjukkan bahwa gaya hidup dan kegiatan rutin mempengaruhi risiko menghadapi peluang untuk menjadi korban viktimisasi (Cohen et al., 1981). Salah satu bentuk viktimisasi *cybercrime* mendasarkan atas *L-RAT* adalah pelecehan *online* serta *cyberstalking.* Karakteristik ini mungkin berlaku untuk pelecehan *online* mengingat mereka yang menghabiskan banyak waktu mengobrol dengan orang lain secara *online* juga dapat mengembangkan hubungan emosional yang intens dengan orang lain, meskipun jarak fisik memisahkan (Bocij, 2004). Individu, terutama wanita, dapat meningkatkan peluang mereka untuk berhubungan dengan calon pelaku pelecehan secara *online* dengan tertarik pada komputer dan secara teratur menggunakan komunikasi yang dimediasi komputer seperti ruang obrolan atau situs jejaring sosial untuk terhubung dengan orang lain (Finn, 2004). Berdasarkan *L-RAT* dapat pula menjelaskan potesi seseorang menjadi korban *cybercrime* untuk viktimisasi tertentu, seperti pencurian kartu kredit maupun serangan virus.

5. Kebijakan Untuk Mengurangi Penderitaan Korban *Cybercrime*

Kebijakan yang dapat dipakai dalam upaya mengurangi penderitaan terhadap korban atas *cybercrime* adalah dengan memberikan perlindungan hukum terhadapnya. Perlindungan hukum dimaksudkan adalah pemberian hak kepada setiap subjek hukum yang didasarkan atas peraturan perundang-undangan yang berlaku. Dengan demikian perlindungan hukum terhadap korban artinya memberikan hak terhadap korban atas terjadinya viktimisaisi *cybercrime* yang menimpanya.

Dalam hukum positif Indonesia, hak yang relevan dengan dengan perlindungan hukum terhadap korban *cybercrime* adalah Undang-Undang Nomor 19 Tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Namun demikian apabila dicermati dalam peraturan perundang tersebut di atas dapat dikatan tidak terdapat perlindungan hukum secara signifikan dapat dirasakan oleh para korbannya.

Sesungguhnya perlindungan hukum dapat diberikan kepada korban melalui satu rangkaian dengan penjatuhan sanksi terhadap pelaku. Sayangnya sanki terhadap pelaku sebagaimana diatur dalam ketentuan Pasal 45, 45A dan 45B,

lebih ke arah penjatuhan pidana penjara dan sanksi berupa denda misalnya yang terdapat dalam Pasal 45 ayat (1).

> Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

Model sanksi seperti ini tentunya tidak memberikan manfaat secara langsung dan dignifikan terhadap korban. Padahal di sisi lain korban cenderung mengalami kerugian dan/atau penderitaaan. Sehingga lebih tepat apabila terdapat sanksi pidana restitusi maupun pemberian kompensasi. Restitusi yang diberikan kepada korban disesuaikan dengan besaran kerugian dan/atau penderitaan kepada korban. Demikian pula dengan kompensasi yang diberikan oleh pemerintah adalah dengan landasan filosofis negara telah gagal dalam melindungi warga negaranya. Kompensasi utamanya adalah untuk perbaikan atas penderitaan psikologis, negara dapat memberikan semacam rehabilitasi psikis secara Cuma-Cuma atau gratis melalui klinik-klinik yang dimiliki oleh pemerintah.

Solusi berupa penjatuhan restitusi dan kompensasi adalah juga selaras dengan karakteristik *society* 5.0 yang mengedepankan adanya kesejahtreraan masyarakat. Korban tentunya akan dapat merasakan manfaatnya langsung atas pemberian restitusi atau kompensasi yang dapat membantu pemulihan kerugian dan/atau penderitaan yang dirasakan oleh korban.

D. PENUTUP

Berdasar atas pembahasan tersebut di atas dapat disimpulkan beberapa hal sebagai berikut: Korban *cybercrime* mengalami berupa kerugian materi *(financial loos),* akibat psikologis *(psychological effect)* akibat fisik *(physical effects),* akibat sosial *(social effects)*. Viktimisasi *cybercrime* dapat dijelaskan dengan *the lifestyle-routine activities theory (L-RAT).* Perlindungan hukum korban *cybercrime* mendasarkan Undang-Undang Nomor 19 Tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dapat dikatakan tidak terdapat perlindungan hukum secara signifikan

dapat dirasakan oleh para korbannya Seharusnya terdapat sanksi berupa restitusi dan/atau pemberian kompensasi.

E. DAFTAR PUSTAKA

Antonescu, M., & Birău, R. (2015). Financial and Non-financial Implications of Cybercrimes in Emerging Countries. *Procedia Economics and Finance*, *32*(15), 618–621. https://doi.org/10.1016/s2212-5671(15)01440-9

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family*. Greenwood Publishing Group.

Borwell, J., Jansen, J., & Stol, W. (2021). The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory. *Social Science Computer Review*, 1–22. https://doi.org/10.1177/0894439320983828

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, *18*(2), 213–234. https://doi.org/10.1177/1477370819839619

Brenner, S. W. (2012). *Cybercrime and The Law: Challenges, Issues, and Outcomes*. Northeastern University Press.

Breque, M., De Nul, L., & Petridis, A. (2021). *Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry*. Directorate-General for Research and Innovation.

Carayannis, E. G., & Morawska-Jancelewicz, J. (2022). The Futures of Europe: Society 5.0 and Industry 5.0 as Driving Forces of Future Universities. *Journal of the Knowledge Economy*, 1–27. https://doi.org/10.1007/s13132-021-00854-2

Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2016). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation and Governance*, *12*(1), 101–114. https://doi.org/10.1111/rego.12125

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review*, *46*(5), 505. https://doi.org/10.2307/2094935

Correia, S. G. (2019). Responding to Victimisation in a Digital Word: a Case Study of Fraud and Computer Misuse Reported in Wales. *Crime Science*, *8*(4), 1–12. https://doi.org/10.1186/s40163-019-0099-7

Dignan, J. (2004). *Understanding Victims and Restorative Justice*. McGraw-Hill Education (UK).

Dinisman, T., & Moroz, A. (2017). *Understanding victims of crime*. Victim Support. https://doi.org/10.13140/RG.2.2.17335.73124

Finn, J. (2004). A Survey of Online Harassment at a University Campus. *Journal of Interpersonal Violence*, *19*(4), 468–483. https://doi.org/10.1177/0886260503262083

Furnell, S. M. (2001). Categorising Cybercrime and Cybercriminals. *Journal of Information Warfare*, *1*(2), 35–44.

Garofalo, J. (1987). Reassessing the Lifestyle Model of Criminal Victimization.

Positive Criminology, 23–42.

Hamzah, A. (1996). *Hukum Pidana Yang Berkaitan Dengan Komputer*. Sinar Grafika.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Janoff-Bulman, R., & Frieze, I. H. (1983). A Theoretical Perspective for Understanding Reactions to Victimization. *Journal of Social Issues*, *39*(2), 1–17. https://doi.org/10.1111/j.1540-4560.1983.tb00138.x

Kitteringham, G., & Fennelly, L. J. (2020). Environmental crime control. In *Handbook of Loss Prevention and Crime Prevention*. INC. https://doi.org/10.1016/b978-0-12-817273-5.00019-3

Kurnia Putra, A. (2014). Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional. *Jurnal Ilmu Hukum Jambi*, *5*(2), 95–109.

Lamet, W., & Wittebrood, K. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers [Never the same again: The consequences of crime for victims]*. The Hague: The Netherlands Institute for Social Research (SCP).

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2019). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims and Offenders: An International Journal of Evidence-Based Research, Policy, and Practice*, *15*(1), 60–77. https://doi.org/10.1080/15564886.2019.1672229

Maxfield, M. G. (1987). Lifestyle and Routine Activity Theories of Crime: Empirical Studies of Victimization, Delinquency, and Offender Decision-Making. *Journal of Quantitative Criminology*, *3*(4), 275–282. http://www.jstor.org/stable/23365565

Mazzucato, M. (2018). *Mission-Oriented in the European Union A problem-solving approach to fuel innovation-led growth*. Publications Office of the European Union. https://doi.org/10.2777/36546

Miethe, T. D., & Meier, R. F. (1994). *Crime and Its Social Context: Toward an Integrated Theory of Offenders, Victims, and Situations*. Suny Press.

Morawska-Jancelewicz, J. (2021). The Role of Universities in Social Innovation Within Quadruple/Quintuple Helix Model: Practical Implications from Polish Experience. In *Journal of the Knowledge Economy*. Springer US. https://doi.org/10.1007/s13132-021-00804-y

Pratt, T. C., & Turanovic, J. J. (2015). Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization. *Victims and Offenders: An International Journal of Evidence-Based Research, Policy, and Practice*, *11*(3), 1–20. https://doi.org/10.1080/15564886.2015.1057351

Puspita, Y., Fitriani, Y., Astuti, S., & Novianti, S. (2020). Selamat Tinggal

Revolusi Industri 4.0, Selamat Datang Revolusi Industri 5.0. *Prosiding Seminar Nasional Pendidikan*, 122–130. https://jurnal.univpgri-palembang.ac.id/index.php/Prosidingpps/article/view/3794/3565

Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security*, *15*(5), 155–160. https://www.researchgate.net/publication/317620078

Saragih, Y. M., & Azis, D. A. (2020). Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi. *Soumatera Law Review*, *3*(2), 265–279. https://pesquisa.bvsalud.org/portal/resource/en/mdl-20203177951%0Ahttp://dx.doi.org/10.1038/s41562-020-0887-9%0Ahttp://dx.doi.org/10.1038/s41562-020-0884-z%0Ahttps://doi.org/10.1080/13669877.2020.1758193%0Ahttp://sersc.org/journals/index.php/IJAST/article

Separovic, Z. P. (1985). *Victimology: Studies of Victims*. Pravni fakultet.

Shapland, J. (1986). Victim assistance and the criminal justice system: The victim's perspective. In E. A. Fattah (Ed.), *From Crime Policy to Victim Policy: Reorienting the Justice System*. Palgrave Macmillan, a division of Macmillan Publishers. https://doi.org/10.1007/978-1-349-08305-3

Shapland, J., & Hall, M. (2007). What Do We Know About The Effects Of Crime On Victims? *International Review OfVictimology*, *14*, 175–217. https://doi.org/10.1111/ecca.12229

Shapland, J., Willmore, J., & Duff, P. (1985). *Victim in The Criminal Justice System* (A. E. Bottonms (ed.)). Gower Publishing Company Limited.

Sinha, R., & Vedpuria, N. K. (2018). Social Impact of Cyber Crime : A Sociological Analysis. *International Journal of Management, IT & Engineering*, *8*(10 (1)), 254–259. https://doi.org/10.13140/RG.2.2.20922.93126

Stanciu, V. V. (1976). Victim Producing Civilizations and Situations. In *Victim and Society, Visage Press, Inc, Washington Dc*. Victim and Society, Visage Press, Inc.

Stephenson, P. (2000). *Computer-Related Crime A handbook for corporate*. By CRC Prss LLC.

Stevens, M. (2003). *Victimology Theory*. Internet Archive Wayback Machine. https://web.archive.org/web/20100628233200/http://faculty.ncwc.edu:80/mstevens/300/300lecturenote01.htm

Wang, S., Wan, J., Zhang, D., Li, D., & Zhang, C. (2016). Towards Smart Factory for Industry 4.0: A Self-Organized Multi-Agent System with Big Data Based Feedback and Coordination. *Computer Networks*, *101*, 158–168. https://doi.org/10.1016/j.comnet.2015.12.017

Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0—Inception, Conception and Perception. *Journal of Manufacturing Systems*, *61*(October), 530–535. https://doi.org/10.1016/j.jmsy.2021.10.006