P-ISSN: 2088-9372 E-ISSN: 2527-8991

Jurnal Manajemen dan Organisasi (JMO),
Vol. 12 No. 3, Desember 2021, Hal. 239-251

Cybercrime dan *Cybersecurity* pada *Fintech*: Sebuah Tinjauan Pustaka Sistematis

Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review

Alexander Anggono
Program Studi Magister Akuntansi, Universitas Trunojoyo Madura
email: alexander.anggono@trunojoyo.ac.id
Tarjo
Program Studi Magister Akuntansi, Universitas Trunojoyo Madura
email: tarjo@trunojoyo.ac.id
Moh. Riskiyadi*
Program Studi Magister Akuntansi, Universitas Trunojoyo Madura
email: mohriskiyadi@gmail.com

ABSTRACT

This study is intended to determine the cybercrime challenges faced by the fintech industry as well as anticipatory actions in the form of cybersecurity to overcome these challenges. This study employs a systematic literature review method from various articles discussing cybercrime and cybersecurity in fintech that were published in reputable online databases. The findings indicate that cybercrime problems in fintech consist of cybercrime regulations that are not strict, data and information theft, and intellectual property theft in which impacting on the reputation of fintech. Cybersecurity as an attempt to tackle cybercrime in fintech can be performed through proactive action, strengthening regulations, and establishing a reliable cybersecurity framework or procedure. The implications of this research are as an additional reference for academics, practitioners, regulators, and fintech actors related to the fast pace development of cybercrime and cybersecurity in fintech. The limitation of this study is that it only provides an overview and elaborate the results of prior studies instead of provide a further analysis of the relationship between the articles discussed. Recommendations for further research are to increase the scope of the articles studied or apply other literature review methods or conduct empirical research to confirm the results of this study.

Keywords*: Cybercrime, cybersecurity, financial technology, fintech regulation, intellectual property theft*.

ABSTRAK

Penelitian ini bertujuan untuk mengetahui tantangan *cybercrime* yang dihadapi industri *fintech* serta tindakan antisipasi berupa *cybersecurity* untuk menanggulangi tantangan tersebut. Penelitian ini menggunakan metode tinjauan pustaka sistematis dari berbagai artikel yang membahas *cybercrime* dan *cybersecurity* pada *fintech* yang dipublikasikan pada database online bereputasi. Hasil penelitian menunjukkan bahwa masalah *cybercrime* pada *fintech* meliputi regulasi *cybercrime* yang belum kuat, pencurian data dan informasi serta pencurian kekayaan intelektual sehingga memberikan dampak pada reputasi *fintech*. *Cybersecurity* untuk menanggulangi *cybercrime* pada *fintech* dapat melalui tindakan proaktif, penguatan regulasi dan pembentukan kerangka kerja atau prosedur *cybersecuriy* yang handal. Implikasi penelitian ini sebagai tambahan referensi bagi akademisi, praktisi, regulator dan pelaku *fintech* terkait perkembangan *cybercrime* dan *cybersecurity* pada *fintech*. Keterbatasan penelitian ini sebatas memberikan gambaran dan elaborasi dari hasil penelitian dari masing-masing artikel yang dipilih, namun tidak memberikan analisis lanjutan mengenai keterkaitan antar artikel yang dibahas. Rekomendasi penelitian selanjutnya dapat menambah ruang lingkup artikel yang diteliti atau menerapkan metode tinjauan pustaka lain atau melakukan penelitian empiris untuk mengkonfirmasi hasil penelitian ini.

Kata kunci: *Cybercrime, cybersecurity, financial technology,* regulasi *fintech*, pencurian kekayaan intelektual.

Corresponding author

PENDAHULUAN

Teknologi informasi yang meningkat pesat menyebabkan perubahan sosial, ekonomi dan budaya yang sangat signifikan (Fahlevi *et al.*, 2019) serta memberikan manfaat dan dampak yang sama besar bergantung dari pengguna dari teknologi informasi tersebut (Deb, 2014; Riskiyadi, 2020). Manfaat positif yang dapat diperoleh dari teknologi informasi adalah memudahkan individu atau kelompok dalam melakukan aktifitasnya, sedangkan dampak negatif timbul karena penyalahgunaan teknologi oleh individu atau kelompok untuk tindakan kejahatan dunia maya (*cybercrime*) yang dapat merugikan orang lain (Gani, 2018).

Kemajuan teknologi yang semakin pesat juga diiringi dengan sistem keamanan yang semakin meningkat sebagai respon dari tindakan *cybercrime* yang semakin meningkat drastis (Peters *et al*., 2018). Akibatnya pelaku *cybercrime* selalu lebih aktif dan cepat membuat terobosan baru terhadap sistem keamanan yang dibentuk oleh anti *cybercrime* atau lebih dikenal dengan keamanan siber (*cybersecurity*). Kondisi yang sangat menghawatirkan terjadi apabila pelaku *cybercrime* adalah ahli juga dalam tindakan anti *cybercrime*, sehingga modus baru *cybercrime* sulit untuk dideteksi dan dipecahkan dengan *cybersecurity*. Serangan *cybercrime* yang terus berkembang pesat tetapi *cybersecurity* yang stagnan merupakan masalah yang harus segera dipecahkan (Corbet & Gurdgiev, 2017).

Kerugian dari *cybercrime* sulit untuk diperkirakan dan diverifikasi sebab disamping kerugian finansial, kerugian lain akibat rusak, hilang atau bocornya data privat menyebabkan turunnya reputasi suatu perusahaan (B. Shekar & Prabha, 2020). Akibat serangan *cybercrime* seluruh negara di dunia terdampak, khususnya bagi negara yang masih tahap berkembang dalam bidang teknologi informasi dan komunikasi yang ditandai dengan tingkat *cybercrime* yang meningkat drastis (Kshetri, 2019). Langkah antisipasi harus ditetapkan oleh pemerintah untuk menangkal *cybercrime* diaksud dengan menetapkan dan menerapkan regulasi tentang kejahatan *cybercrime* dan mendorong pihak swasta untuk ikut berkontribusi dalam memerangi *cybercrime* dengan memperkuat *cybersecurity* (Falco, 2019; Kshetri, 2019; Sunkpho *et al*., 2018). Terobosan lain yang dapat ditempuh untuk menekan *cybercrime,* dengan memberikan pendidikan etika dalam memanfaatkan teknologi informasi bagi para generasi muda (Danuri & Suharnawi, 2017) atau dengan merancang *cybersecurity* yang handal (Chang, 2017; Joveda *et al*., 2019).

Perkembangan teknologi informasi dan komunikasi melahirkan banyak terobosan, salah satunya teknologi keuangan (*fintech*) (Lee & Jae, 2018; Sangwan *et al*., 2019) yang berkembang untuk teknologi pembayaran, transfer dana, remitansi atau transfer dana dari luar negeri, *lending* atau pinjaman, *crowdfunding* atau urun dana, intermediasi atau perantara keuangan, investasi ritel, perencanaan keuangan, riset keuangan dan jasa keuangan lainnya *(Das, 2019; Suryono et al.,* 2020). Hadirnya *fintech* dapat diterima dengan baik oleh masyarakat, sebab *fintech* mampu berevolusi menjadi sarana yang ampuh dalam memberikan efektifitas dan efisiensi (Kou, 2019) sesuai dengan kebiasaan dan gaya hidup masyarakat (M. C. Shekar & Kumaran, 2019; Wang, 2021). Meskipun di sisi lain, keberadan *fintech* juga memberikan ancaman serius terhadap keberlangsungan lembaga keuangan, perbankan dan asuransi yang masih berkembang secara konvesional (Broby, 2021; Şcheau, 2017). Perkembangan *fintech* juga terus menjadi topik yang populer diberitakan media (Zavolokina *et al*., 2016) serta peningkatan yang drastis setiap tahunnya di sisi penelitian sejak awal kemunculannya (Kou, 2019).

Fintech yang berkembang pesat bukan tidak memiliki risiko dalam penerapannya. Risiko yang dihadapi *fintech* berupa risiko teknologi dan risiko bisnis yang berbeda-beda tergantung dari karateristik masing-masing *fintech* (Namchoochai *et al*., 2020; Suryono *et al*., 2020). Risiko finansial dan risiko teknologi dari *fintech* meliputi risiko diversifikasi, risiko ditransfer, risiko dikendalikan dan risiko didanai (Rahmanto & Nasrulloh, 2019) dengan risiko teknologi merupakan tantangan terbesar dari *fintech*. Risiko teknologi berkenaan dengan risiko keamanan data akibat tindakan *cybercrime* (Singh & Rajput, 2019). Para pelaku *cybercrime* dapat memanfaatkan celah *fintech* untuk melakukan penipuan, pemerasan, pencucian uang dan aktivitas kejahatan lainnya yang melanggar ketentuan peraturan (Nikkel, 2020), sehingga diperlukan kesadaran para pelaku *fintech* untuk meningkatkan *cybersecurity* guna melindungi data yang

Jurnal Manajemen dan Organisasi (JMO),
Vol. 12 No. 3,
Desember 2021,
Hal. 239-251

dimilikinya dari segala bentuk *cybercrime* serta terus berinovasi dan mengembangkan teknologi terkini (S. J. (H R. C. Kaur, 2020).

Guna meningkatkan pemahaman akademisi, praktisi, regulator dan pelaku *fintech* perlu dilakukan kajian literatur tentang tantangan teknologi dan antisipasi yang telah dilakukan oleh *fintech* selama ini. Kajian literatur yang mengulas *cybercrime* dan *cybersecurity* pada *fintech* diharapkan dapat memberikan gambaran tentang dinamika perkembangan *cybercrime* dan *cybersecurity* pada *fintech*. Penelitian ini dikembangkan dari penelitian sebelumnya yang mengulas tentang *fintech* (Li & Xu, 2021; Milian *et al*., 2019) dan tantangan secara umum yang dihadapi *fintech* (Adeyoju, 2019; Suryono *et al*., 2020). Penelitian ini bertujuan untuk mengidentifikasi penelitian-penelitian yang telah dilakukan selama ini dan memberikan gambaran perkembangan *cybercrime* dan *cybersecurity* pada *fintech*, dengan harapan sebagai penambah wawasan dan pengetahuan bagi para pihak yang berkepentingan terhadap *fintech* dan peluang untuk penelitan di masa depan (Kitchenham & Brereton, 2013; Xiao & Watson, 2019).

Penelitian ini dilakukan dengan memilih, mengumpulkan, ekstraksi dan analisis artikel yang sesuai dengan pertanyan penelitian sehingga diperoleh hasil yang mencakup keseluruhan artikel yang dipilih. Hasil penelitian ini memberikan gambaran *cybercrime* dan *cybersecurity* pada *fintech* yang dapat menjadi acuan teori, kerangka dan model penelitian sehingga dapat bermanfaat untuk meningkatkan wawasan dan pengetahuan tentang tantangan *cybercrime* dan antisipasi *cybersecurity* pada *fintech* serta memberikan peluang untuk penelitian di masa depan.

Tinjauan Pustaka

Cybercrime dan *Cybersecurity*

Cybercrime merupakan istilah umum untuk kejahatan yang menyerang sistem komputer atau jaringan internet, dengan tujuan pencurian data, keuangan dan penyebaran kode perangkat lunak berbahaya (B. Shekar & Prabha, 2020) yang merupakan tindakan ilegal di bidang teknologi informasi dan komunikasi sebagai bentuk modifikasi dari kejahatan konvensional (Aravazhi, 2020). *Cybercrime* merupakan tindakan yang dilakukan oleh pelaku untuk menghancurkan jaringan organisasi dengan mencuri data berharga, dokumen, meretas rekening bank dan mentransferkan ke rekening mereka (Irfan *et al*., 2018). Untuk mempelajari tindakan kejahatan tersebut diperlukan *cybercriminology* yang merupakan penggabungan pengetahuan dari kriminologi, psikologi, sosiologi, ilmu komputer, dan *cybersecurity* untuk memberikan pemahaman mendalam tentang *cybercrime* (Choi & Lee, 2018). Beberapa faktor utama yang menyebabkan *cybercrime* berkembang dengan pesat yaitu alat, cara dan media *cybercrime* dengan sangat mudah diakses dan dipelajari di internet, peningkatan teknologi yang meningkat pesat terkait dengan kecepatan proses, pengolahan dan analisis data, *bandwidth* internet dan aktifitas jaringan internet lainnya serta terjangkaunya akses manual ke sumber informasi atau server (Singh & Rajput, 2019).

Berbagai bentuk *cybercrime* yang sering digunakan oleh pelaku (Cascavilla *et al*., 2021; Maigida *et al*., 2019), diantaranya berupa *spoofing* email merupakan pemalsuan *header email*. Pesan email yang diterima tampaknya telah dikirim oleh sumber asli, aktual dan terpercaya. Modus tersebut biasanya digunakan dalam kampanye *spam* atau *phising*. Target mungkin membuka email karena berpikir bahwa email tersebut telah dikirim oleh sumber yang sah. Peretasan (*hacking*) merupakan pembobolan sistem komputer secara rahasia dan mencuri data berharga dari sistem tanpa izin. Penyebaran virus atau *malware* merupakan sekumpulan instruksi *cyber* yang mampu melakukan beberapa operasi jahat. Virus dan *malware* menghentikan fungsi normal dari program sistem dan menyisipkan beberapa kelainan dari kinerja sistem yang terserang. Virus dan *malware* dapat menyebar melalui email, pesan *chating*, penyimpanan data, multimedia, internet dan media eloktonik lainnya. *Phishing* merupakan tindakan mencuri informasi pribadi seperti kata sandi, detail kartu kredit, data pengguna korban yang ditarget melalui internet. Bentuk *cybercrime* ini dilakukan dengan *spoofing* email dan pesan instan kepada para korban. Peretas membuat tautan langsung yang mengarahkan korban yang ditargetkan ke halaman *website* palsu yang terlihat identik dengan yang *website* yang sebenarnya. *Stalking* adalah penggunaan internet untuk sarana elektronik lainnya untuk membuntuti atau memata-

matai seseorang yang dijadikan korban. *Stalking* dapat berupa pelecehan, *hatespeech*, *cyberdefamation* dalam ruang lingkup *cyber*. *Stalking* umumnya melibatkan perilaku melecehkan, mengancam atau meneror yang dilakukan seseorang berulang kali, seperti membuat panggilan telepon, pengiriman pesan dan jenis intimidasi atau terror lainnya. *Defamation* merupakan pencemaran martabat korban di dunia maya yang merugikan reputasi seseorang atau organisasi di mata publik melalui ruang *cyber*. Pencemaran martabat dilakukan dengan membuat pernyataan fitnah untuk menjatuhkan reputasi individu atau perusahaan sebagai korban. *Scripting website* merupakan jenis kerentanan keamanan komputer atau sistem yang biasanya ditemukan dalam situs website yang memungkinkan dilakukan injeksi kode atau *script* oleh para pelaku *cybercrime*. Kerentanan *script website* tersebut dieksploitasi oleh pelaku untuk meminta kontrol akses ke server *website* (Aravazhi, 2020).

Guna melakukan tindakan antisipatif untuk menanggulangi *cybercrime* tersebut, diperlukan *cybersecurity*, yaitu tindakan pelindungan atas segala macam bentuk serangan *cybercrime* dan tindakan pemulihan akibat *cybercrime*. Beberapa hal yang harus dipenuhi dalam *cybersecurity* (Humayun *et al*., 2020; Rabii *et al.*, 2020) adalah ketersediaan (*availability*), kerahasiaan (*confidentiality*), integritas (*integrity*), otentikasi (*authentication*) dan akuntabilitas (*accountability*). Ketersediaan (*availability*) merupakan kemampuan dan ketersediaan informasi atau data yang diperlukan untuk diakses kapanpun hanya oleh pihak yang berwenang. Kerahasiaan (*confidentiality*) merupakan tindakan melindungi informasi atau data dari para pihak yang tidak memiliki akses. Integritas (*integrity*) merupakan integritas atau keutuhan data dalam sistem untuk mencegah perubahan yang tidak sah terjadi. Otentikasi (*authentication*) merupakan tindakan analisis yang mengacu pada pengukuran identitas pengguna yang sebenarnya. Akuntabilitas (*accountability*) merupakan tanggung jawab yang tidak boleh diabaikan oleh pengguna dalam partisipasinya menggunakan sistem, yang meliputi tanggung jawab, kemauan, transparansi dan daya tanggap oleh para pengguna sistem yang digunakan (Singh & Rajput, 2019).

Cybercrime pada *Fintech*

Cybercrime yang umum terjadi dalam teknologi informasi dan komunikasi juga dapat terjadi dan menyerang *fintech. Cybercrime* berupa *cyberlaundering* merupakan kejahatan yang marak terjadi saat ini, yang meliputi berbagai tahap konversi (*placement*), pelapisan (*layering*) dan pengintegrasian (*integration*) (Wibawa, 2017), atau hasil dari tindakan *cybercrime* disembunyikan dalam bentuk *cyberlaundering*. Salah satu bentuk *cyberlaundering* yang marak digunakan oleh para pelaku adalah *cryptocurrency* (Mabunda, 2018). *Cyberlaundering* secara efektif dapat ditangkal dengan legalisasi pendapatan ilegal (Karlov, 2018).

Berbagai macam serangan *cybercrime* yang marak dilakukan oleh pelaku adalah *fintech attack*. Serangan yang sering terjadi adalah memanfaatkan celah *cybersecurity* otentikasi multi-faktor atau perlindungan koneksi aplikasi oleh para pelaku. *Trojan mobile banking* yang menyerang kode keamanan *mobile banking* hingga dapat menyebar ke domain publik. *Ransomware*, menyusupkan aplikasi jahat dan mengunci data pengguna dengan tujuan meminta uang tebusan. *Magecarting* merupakan serangan *cybercrime* yang menargetkan sistem transaksi pembayaran online (Nikkel, 2020). Risiko lainnya terkait dengan *cybercrime* semakin besar dengan semakin berkembangnya teknologi dan kecepatan jaringan yang semakin meningkat dari masa ke masa. Pengembangan *fintech* merupakan evolusi profesi dengan kompetensi teknis dan etika untuk mengurangi risiko yang muncul (Ng & Kwok, 2017), umumnya risiko terkait dengan tindakan *cybercrime*.

Berbagai penelitian menyebutkan *hacking, phising* dan *malware* berpengaruh terhadap *cybersecurity compliance* di sektor keuangan (Kwarto & Angsito, 2018). Pelaku *cybercrime* lebih menyukai melakukan tindakan kejahatan pada *e-commerce* dan sistem pembayaran online karena sebagian besar informasi pribadi dan data kartu kredit disimpan dan diproses dalam aplikasi tersebut (Aravazhi, 2020). *Cybercrime* masih sangat sulit di antisipasi oleh pengguna *e-commerce* sehingga memberikan dampak turunnya kepercayaan pengguna pada *e-commerce* (Batmetan *et al*., 2018). Penelitian lain menyebutkan perkembangan *e-commerce* menjadi terhambat karena

kurang selarasnya regulasi, lemahnya perlindungan konsumen atas *cybercrime* (Pratamasari, 2020). Untuk itu, baik regulator maupun pelaku bisnis memandang bahwa tindakan pencegahan kritis harus dilakukan dan penerapan hukum harus terus mengikuti perkembangan kejahatan *cybercrime* (Fahlevi *et al*., 2019). Berbagai metode *cybersecurity* yang dapat diterapkan untuk menangkal serangan *cybercrime* pada *fintech*, diantaranya dengan metode *Model to Encounter Cyber Attacks* atau MECA (Cyriac & Sadath, 2019).

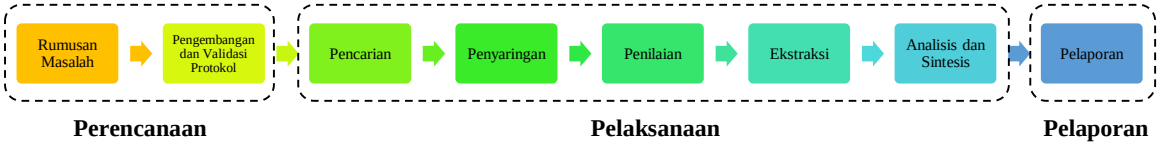
Mendeteksi dan menginvestigasi tindakan *cybercrime* pada perusahaan *fintech* tidak dapat dilakukan dengan proses forensik digital tradisional. *Cybercrime* yang melibatkan server publik berupa *cloud* publik yang umum digunakan oleh perusahaan *fintech* diperlukan investigasi digital forensik dengan model tingkat tinggi (Baror & Venter, 2019), berkenaan dengan pertukaran data yang selalu dinamis dalam ruang penyimpanan server publik. Tidak dimungkinkan melakukan pembekuan server publik seperti layaknya forensik digital tradisional. Penerapan *cybersecurity* yang handal harus dirancang dengan matang diawal perusahan *fintech* digagas. Selanjutnya *cybersecurity* yang telah terpasang wajib disandingkan dengan teknik deteksi dan investigasi yang handal pula untuk melakukan pemulihan data seandainya terjadi serangan *cybercrime.*

METODE PENELITIAN

Penelitian ini menggunakan metode tinjauan pustaka sistematis (*systematic literatur review*) dengan pertanyaan penelitian Bagaimana tantangan *cybercrime* yang dihadapi *fintech?* dan Bagaimana *cybersecurity* pada *fintech* dalam mengantisipasi ancaman *cybercrime*? untuk memberikan gambaran perkembangan tantangan utama yang dihadapi *fintech* berupa tindakan kejahatan *cybercrime* dan langkah antisipasi yang telah dilakukan *fintech* untuk menghadapi kejahatan tersebut. Sehubungan *fintech* merupakan inovasi baru di bidang keuangan yang banyak dibahas sejak 5 tahun terakhir, sehingga pencarian publikasi artikel pada penelitian ini kami batasi dari tahun 2016 sampai dengan 2021. Penelitian ini melakukan identifikasi, penilaian dan menginterpretasikan temuan pada suatu topik penelitian untuk menjawab pertanyaan penelitian (Jesson *et al*., 2011).

Proses pencarian artikel awal dilakukan dilakukan pada portal Gooogle Scholar yang selanjutnya dilakukan penelusuran pada database online bereputasi seperti ScienceDirect, Elsevier, ACM Digital Library, ABI/Inform Complete, Academic Search Complete, IEEE Xplore, SSRN, Springer, Emerald, Taylor & Francis, World Scientific dan IGI Global dengan kata kunci "*cybercrime cybersecurity fintech*" namun belum ditemukan artikel yang memadai, sehingga dilakukan pengembangan pencarian pada. Selanjutnya tinjauan protokol dilakukan dengan merumuskan pertanyaan penelitian dengan mengklasifikasikan kata kunci sesuai dengan strategi populasi, intervensi, perbandingan, hasil, dan konteks dari artikel-artikel yang diperoleh. Kriteria inklusi dan eksklusi ditentukan dengan memilih artikel yang sesuai dengan pertanyaan penelitian, dengan mengesampingkan subjektifitas peneliti dalam pemilihan artikel. Selanjutnya untuk kepentingan mengorganisir artikel yang telah dipilih digunakan software Mandeley. Proses ekstraksi dan sintesis data menggunakan analisis tematik dan meta analisis (Bown & Sutton, 2010).

Tahapan penelitian ini meliputi: perencanaan, pelaksanaan dan pelaporan, yang terbagi dalam 8 langkah yaitu merumuskan masalah, mengembangkan dan memvalidasi protokol tinjauan, mencari literatur, melakukan penyaringan literatur yang sesuai, menilai kualitas literatur, ektraksi data, analisis dan sintesis data, dan melaporkan hasil (Uman, 2011; Xiao & Watson, 2019), sebagaimana gambar 1 berikut:



Gambar 1. Metode Tinjauan Pustaka Sistematis

Proses pencarian, penyaringan dan penilaian artikel untuk mentukan artikel-artikel yang sesuai dengan tujuan penelitian dilakukan dengan melihat topik yang dibahas pada masing-masing artikel. Berdasarkan artikel-artikel yang telah dipilih tersebut dilakukan ekstraksi dan analisis berdasarkan pertanyaan penelitian sehingga diperoleh gambaran yang komprehensif dari *cybercrime* pada *fintech* dan antisipasi *cybersecurity* untuk menanggulangi ancaman tersebut.

HASIL DAN PEMBAHASAN

Pemilihan Artikel

Hasil pencarian artikel dengan kata kunci "*cybercrime cybersecurity fintech*" pada google scholar diperoleh hasil sebanyak 1.320, selanjutnya dari hasil tersebut dilakukan pemilihan artikel yang sesuai dengan database online bereputasi yaitu ScienceDirect, Elsevier, ACM Digital Library, ABI/Inform Complete, Academic Search Complete, IEEE Xplore, SSRN, Springer, Emerald, Taylor & Francis, World Scientific dan IGI Global. Berdasarkan hasil pemilihan artikel tersebut diperoleh hasil yang sesuai dengan topik sejumlah 35 artikel dari berbagai sumber database online, tahun terbit, metode penelitian yang digunakan serta sub topik yang membahas *cybercrime* dan *cybersecurity* pada *fintech.*

Klasifikasi Artikel

Terjadi peningkatan publikasi artikel setiap tahunnya yang dapat diamati dari meningkatnya jumlah publikasi artikel tentang *cybercrime* dan *cybersecurity* pada *fintech* sejak tahun 2017 sampai dengan 2021 sebagaimana Tabel 1. Sebaran publikasi artikel pada sumber database online bereputasi dengan topik serupa tersebar beragam dengan mayoritas artikel dipublikasikan pada SSRN sebagaimana Tabel 2.

Tabel 1. Klasifikasi Artikel Berdasarkan Tahun Terbit

Tahun	Jumlah
2017	2
2018	3
2019	9
2020	9
2021	12
Jumlah	35

Tabel 2. Klasifikasi Artikel Berdasarkan Sumber Online

Sumber Online	Jumlah
Elsevier	5
Emerald	3
IEEE Xplore	3
IGI Global	2
Springer	5
SSRN	14
Taylor & Francis	2
World Scientific	1
Jumlah	35

Klasifikasi artikel berdasarkan metode penelitian dari artikel-artikel yang telah ditentukan didominasi oleh artikel dengan metode penelitian tinjauan pustaka yang diperoleh dari data sekunder berupa literatur, hasil penelitian dan laporan. Klasifikasi artikel berdasarkan metode penelitian yang digunakan sebagaimana Tabel 3 berikut:

Tabel 3. Klasifikasi Artikel Berdasarkan Jenis Penelitian

Jenis Penelitian	Jumlah
Empiris - Data Primer	7
Empiris - Data Sekunder	3
Empiris - Eksperimen	2
Tinjauan Pustaka - Data Sekunder	23
Jumlah	35

Klasifikasi artikel berdasarkan topik yang membahas ancaman *cybercrime* pada *fintech* dan antisipasi *cybersecurity* untuk menanggulanginya sebagaimana Tabel 4 berikut:

Tabel 4. Klasifikasi Artikel Berdasarkan Jenis Penelitian

Topik	Jumlah	Penulis
Ancaman *cybercrime* dan antisipasi *cybersecurity* pada *fintech*	14	(Adeyoju, 2019; Boitan & Marchewka-Bartkowiak, 2021; Corbet & Gurdgiev, 2017; Cyriac & Sadath, 2019; Faya & Ogbuefi, 2019; Huang & Madnick, 2020; G. Kaur et al., 2021; Malladi *et al*., 2021; Mehrotra & Menon, 2021; Milian *et al*., 2019; Namchoochai *et al*., 2020; Ng & Kwok, 2017; Palmié *et al*., 2019; Sharma, 2019)
Persepsi atas *cybersecurity fintech* dalam menanggulagi *cybercrime*	2	(Asante-Offei & Yaokumah, 2021; Ogbanufe & Kim, 2018)
Dampak, penyebab, modus dan investigasi forensik *cybercrime* pada *fintech*	3	(Al-Harrasi *et al*., 2021; Nikkel, 2020; Vedral, 2021)
Regulasi pengaturan *fintech* untuk antisipasi *cybercrime* dengan *cybersecurity*	6	(Amstad, 2019; Bagby & Packin, 2020; Bagby & Reitter, 2019; Laidlaw, 2021; Ojo & Nwaokike, 2019; Teigland *et al*., 2018)
Kerangka kerja dan prosedur *cybersecurity* untuk antisipasi risiko *cybercrime*	10	(Bouveret, 2019; Chari, 2020; Creado & Ramteke, 2020; Lubin, 2021; Najaf *et al*., 2021; Noor et al., 2019; Santucci, 2018; Singh & Rajput, 2019; Uddin *et al*., 2020; Yusif & Hafeez-Baig, 2021)

Permasalahan utama yang dirasakan *fintech* adalah berbagai macam bentuk *cybercrime* yang dapat menghambat operasi bisnisnya, sehingga diperlukan perjuangan ekstra dalam menerapkan *cybersecurity* untuk melawan ancaman *cybercrime* tersebut.

Masalah *Cybercrime* pada *Fintech*

Masalah utama yang dihadapi *fintech* adalah *cybercrime* yang selalu muncul modus baru seiring dengan perkembangan teknologi informasi dan komunikasi (Al-Harrasi *et al*., 2021; Vedral, 2021). Masalah *cybercrime* menyebabkan berbagai kendala meliputi regulasi penanggulangan *cybercrime* pada *fintech* masih belum kuat, hilang, berubah atau bocornya data dan informasi, serta pencurian kekayaan intelektual (Faya & Ogbuefi, 2019) yang menyebabkan merosotnya kepercayaan publik (Adeyoju, 2019; Boitan & Marchewka-Bartkowiak, 2021; Corbet & Gurdgiev, 2017; Cyriac & Sadath, 2019; Faya & Ogbuefi, 2019; Huang & Madnick, 2020; G. Kaur *et al*., 2021; Malladi *et al*., 2021; Mehrotra & Menon, 2021; Milian *et al*., 2019; Namchoochai *et al*., 2020; Ng & Kwok, 2017; Palmié *et al*., 2019; Sharma, 2019).

Uraian kendala tersebut sebagai berikut:

1. Regulasi

Fintech mengalami kendala regulasi dan penerapannya, sebab regulasi sering lambat merepon perkembangan teknologi informasi dan komunikasi yang berkembang drastis. Di sisi yang lain regulasi perlindungan data dan informasi *fintech* merupakan tantangan global yang melibatkan negara-negara lain di dunia dan sebagian negara masih belum mendukung *fintech* di negaranya, sebab sebagian negara beranggapan *fintech* berpotensi merusak stabilitas keuangan konvesioal. Dampak global yang ditimbulkan *fintech* membutuhkan regulasi yang berlaku internasional (Laidlaw, 2021) dan hal tersebut membutuhkan proses yang cukup lama. Dalam berbagai kondisi regulasi *cybercrime* pada *fintech* masih menerapkan regulasi *cybercrime* yang bersifat umum yang menyebabkan pelaksanaan regulasi tersebut tidak maksimal diterapkan pada *fintech*. Sifat *fintech* yang dinamis menuntut regulasi yang dinamis pula agar mampu mengatur *fintech* yang berkembang sangat drastis (Bagby & Packin, 2020; Bagby & Reitter, 2019; Faya & Ogbuefi, 2019; Ojo & Nwaokike, 2019; Teigland *et al*., 2018).

2. Data dan Informasi

Potensi serangan *cybercrime* pada *fintech* menyebabkan risiko hilang, berubah atau bocornya suatu data atau informasi yang dimiliki *fintech,* sebab ancaman *cybercrime* selalu lebih

unggul dibandingkan dengan *cybersecurity* yang dimiliki *fintech,* sehingga diperlukan pembaharuan *cybersecurity* untuk menanggulangi segala bentuk ancaman *cybercrime* yang mengalami perkembangan pesat dari waktu ke waktu (Akhta *et al*., 2021).

3. Pencurian Kekayaan Intelektual

Berkembangnya teknologi inovatif maka muncul peningkatan pencurian hak kekayaan intelektual berupa pencurian hak paten, hak cipta dan rahasia dagang yang diawali dengan serangan *cybercrime* pada *fintech* yang menjadi korban (Al-Harrasi *et al*., 2021).

4. Kepercayaan Publik

Dampak dari permasalahan sebagaimana disampaikan di atas menyebabkan tergerusnya kepercayaan publik terhadap *fintech*. Kepercayaan publik sulit dikembalikan apabila pernah terjadi kebocoran data atau informasi akibat serangan *cybercrime* pada *fintech* (Asante-Offei & Yaokumah, 2021; Ogbanufe & Kim, 2018).

Antisipasi *Cybersecurity* pada *Fintech*

Perkembangan *fintech* yang sangat pesat rentan terhadap serangan *cybercrime,* sehingga *fintech* harus merencanakan dan membangun *cybersecurity* yang handal dan efektif untuk melindungi data dan keuangan dari serangan *cybercrime* yang sewaktu-waktu dapat melanda *fintech*. Langkah terbaik untuk melindungi data dan informasi *fintech* dengan menerapkan *cybersecurity* yang handal sejak awal bisnis *fintech* digagas dan *cybersecurity* harus menjadi prioritas utama. Langkah yang dapat ditempuh untuk melindungi *fintech* dari serangan *cybercrime* meliputi:

1. Tindakan Proaktif

Tindakan proaktif *cyersecurity* dalam menanggulangi *cybercrime* yang perlu tempuh oleh *fintech* dan pemerintah sebagai pemangku kebijakan dalam penerapan regulasi (Chang *et al*., 2018; Faya & Ogbuefi, 2019) adalah:

a. Mengembangkan kerangka kerja *cyersecurity* secara komprehensif yang mencakup pencegahan, pendeteksian, pemantauan, pembagian informasi, literasi keuangan dan teknologi serta rencana pemulihan atau *recovery*.
b. Perlindungan arsitektur akses data dan informasi secara komprehensif untuk menanggulangi risiko *cybercrime* dari penggunaan data global.
c. Pengawasan regulasi untuk memastikan *fintech* menerapkan *cybersecurity* yang handal dan tangguh.
d. Peningkatan kesadaran dan pemahaman pentinya *cybersecurity* dengan edukasi dan pelatihan bagi para pengguna layanan *fintech*.

2. Regulasi *Fintech*

Perusahaan *fintech* membutuhkan peraturan perundang-undangan yang dinamis yang dapat mengatasi risiko saat kondisi *fintech* yang berubah dengan cepat. Peraturan perundang-undangan tidak boleh menghambat inovasi dan kreasi dari pengembangan *fintech* secara komprehensif dan sistematis (Fahlevi *et al*., 2019). Regulasi juga memberikan kepastian hukum atas segala tindakan *cybercrime* yang membahayakan *fintech* sehingga para pelaku usaha, pelanggan dan regulator pegawas memiliki sandaran yang jelas tentang bagaimana harus berbuat dan bertindak sesuai dengan peraturan yang berlaku. Regulasi harus mendukung penuh pengembangan *fintech* dengan tetap berpegang teguh pada prinsip-prinsip menjaga harkat dan martabat bangsa (Amstad, 2019; Bagby & Packin, 2020; Bagby & Reitter, 2019; Laidlaw, 2021; Ojo & Nwaokike, 2019; Teigland *et al*., 2018).

3. Langkah Teknis dalam Menerapkan *Cybersecurity* pada *Fintech*

Langkah teknis yang dapat dilakukan untuk menanggulangi *cybercrime* pada *fintech* dengan membuat kerangka kerja dan prosedur *cybersecurity* yang handal (Creado & Ramteke, 2020; Najaf *et al*., 2021; Singh & Rajput, 2019; Uddin *et al*., 2020) dengan memetakan risiko yang rentan *cybercrime* (Bouveret, 2019; Chari, 2020; Lubin, 2021; Santucci, 2018) dan menetapkan sensitifitas yang tinggi untuk mendeteksi *cybercrime* (Noor *et al.*, 2019) serta meningkatkan sumber daya, melakukan pengawasan yang intensif (Yusif & Hafeez-Baig, 2021) dan melakukan investigasi forensik apabila tekah terjadi *cybercrime* (Nikkel, 2020).

Risiko *cybercrime* yang memanfaatkan celah keamanan *cybersecurity* pada *fintech* menjadi pintu masuk terjadinya *cybercrime* sehingga dibutuhkan langkah *cybersecurity* yang tepat (Aravazhi, 2020) dengan berbagai tindakan berikut:

a. Melindungi dan memantau titik akses nirkabel, titik akses jaringan, dan perangkat yang terhubung ke jaringan dengan sistem keamanan berlapis dan mengontrol seluruh akses pengguna ke sumber informasi.
b. Mengontrol dan membatasi hak akses pengguna internal ke file atau data hanya yang berhubungan tugas pekerjaan.
c. Mencegah dan mengamankan semua pengguna dan pengelola sistem yang menjadi target *cybercrime*.
d. Otentifikasi pada program pemindaian virus, *trojan, malware* dan program jahat lainnya.
e. Melakukan pemindaian secara berkala menggunakan program *antispyware* untuk mendeteksi *spyware, adware* dan *bot* (robot perangkat lunak) dan program berbahaya lainnya.
f. Penyediaan edukasi dan pelatihan tentang kesadaran pentingnya keamanan dan kehati-hatian dalam menggunakan layanan internet.

KESIMPULAN

Cybercrime merupakan keniscayaan yang selamanya terus ada seiring dengan perkembangan teknologi informasi dan komunikasi yang berkembang pesat, sehingga diperlukan *cybersecurity* yang handal dan efektif untuk menanggulanginya. Tantangan *cybercrime* pada *fintech* meliputi regulasi *cybercrime* yang belum kuat, pencurian data dan informasi serta pencurian kekayaan intelektual sehingga berdampak pada reputasi *fintech*. Guna melakukan mitigasi terhadap tantangan *cybercrime* tersebut diperlukan *cybersecurity* melalui tindakan proaktif, penguatan regulasi dan pembentukan kerangka kerja atau prosedur *cybersecuriy* yang handal, efektif dan efisien.

Acknowledgement:

We gratefully acknowledge funding provided by the Lembaga Penelitian Pengabdian kepada Masyarakat (LPPM) Universitas Trunojoyo Madura.

DAFTAR PUSTAKA

Adeyoju, A. (2019). Cybercrime and Cybersecurity: FinTech's Greatest Challenges. *SSRN Electronic Journal*, 1–5. https://doi.org/10.2139/ssrn.3486277.

Akhta, S., Sheorey, P. A., Bhattacharya, S., & Ajith, K. V. V. (2021). Cyber Security Solutions for Businesses in Financial Services: Challenges, Opportunities, and the Way Forward. *International Journal of Business Intelligence Research*, *12*(1), 82–97. https://doi.org/10.4018/IJBIR.20210101.oa5.

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2021). Towards Protecting Organisations' Data by Preventing Data Theft by Malicious Insiders. *International Journal of Organizational Analysis*, 20–21. https://doi.org/10.1108/IJOA-01-2021-2598.

Amstad, M. (2019). Regulating Fintech: Objectives, Principles, and Practices. *Asian Development Bank Institute Working Paper Series 1016*, 1–13. https://doi.org/10.2139/ssrn.3541003.

Aravazhi, M. S. (2020). Understanding Cyber Crime and Cyber Laundering: Threat and Solution. *EPRA International Journal of Research and Development (IJRD)*, *5*(1), 34–38. https://doi.org/10.36713/epra2016.

Asante-Offei, K. O., & Yaokumah, W. (2021). Cyber-Identity Theft and Fintech Services: Technology Threat Avoidance Perspective. *Journal of Information Technology Research*, *14*(3), 1–19. https://doi.org/10.4018/jitr.2021070101.

Bagby, J. W., & Packin, N. G. (2020). RegTech and Predictive Lawmaking: Closing the RegLag between Prospective Regulated Activity and Regulation. *Michigan Business & Entrepreneurial Law Review*, *10*(2), 127–177.

https://doi.org/10.36639/mbelr.10.2.regtech.
Bagby, J. W., & Reitter, D. (2019). Anticipatory FinTech Regulation: On Deploying Big Data Analytics to Predict the Direction, Impact and Control of Financial Technology. *SSRN Electronic Journal*, 1–59. https://doi.org/10.2139/ssrn.3456844.
Baror, S. O., & Venter, H. S. (2019). A Taxonomy for Cybercrime Attack in the Public Cloud. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*, 505–515.
Batmetan, J. R., Watung, H., Nayoan, L., & Untu, A. E. (2018). Pengaruh Perilaku Cyber Crime Terhadap Pengguna Aplikasi E-commerce. *OSF Preprints*, 1–5. https://doi.org/10.31219/osf.io/gukcf.
Boitan, I. A., & Marchewka-Bartkowiak, K. (2021). *Fostering Innovation and Competitiveness with Fintech, RegTech, and SupTech*. IGI Global. USA: Hershey PA.
Bouveret, A. (2019). Cyber Risk for the Financial Services Sector. *Journal of Financial Transformation*, *49*, 78–85.
Bown, M. J., & Sutton, A. J. (2010). Quality Control in Systematic Reviews and Meta-analyses. *European Journal of Vascular & Endovascular Surgery*, *40*(5), 669–677. https://doi.org/10.1016/j.ejvs.2010.07.011.
Broby, D. (2021). Financial Technology and the Future of Banking. *Financial Innovation*, *7*(47), 1–19. https://doi.org/10.1186/s40854-021-00264-y.
Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime Threat Intelligence: A Systematic Multi-vocal Literature Review. *Computers and Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258.
Chang, L. Y. C. (2017). Cybercrime and Cyber Security in ASEAN. *Comparative Criminology in Asia*, 135–148. https://doi.org/10.1007/978-3-319-54942-2.
Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). 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.
Chari, K. (2020). Fraud Risk in Digitized Fintech Ecosystem: Troubling Trends, Issues and Approaches to Mitigate Risk. *SSRN Electronic Journal*, 1–8. https://doi.org/10.2139/ssrn.3680456.
Choi, K., & Lee, C. S. (2018). The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity. *International Journal of Cybersecurity Intelligence and Cybercrime*, *1*(1), 1–4. https://doi.org/10.52306/01010218YXGW4012.
Corbet, S., & Gurdgiev, C. (2017). Financial Digital Disruptors and Cyber-Security Risks: Paired and Systemic. *Forthcoming in Journal of Terrorism & Cyber Insurance*, *1*(2), 1–20. https://doi.org/10.2139/ssrn.2892842.
Creado, Y., & Ramteke, V. (2020). Active Cyber Defence Strategies and Techniques for Banks and Financial Institutions. *Journal of Financial Crime*, *27*(3), 771–780. https://doi.org/10.1108/JFC-01-2020-0008.
Cyriac, N. T., & Sadath, L. (2019). Is Cyber Security Enough-A Study on Big Data Security Breaches in Financial Institutions. *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, 380–385. https://doi.org/10.1109/ISCON47742.2019.9036294.
Danuri, M., & Suharnawi. (2017). Trend Cyber Crime dan Teknologi Informasi di Indonesia. *Informasi Komputer Akuntansi Dan Manajemen*, *13*(2), 55–65. https://doi.org/10.53845/infokam.v13i2.133.
Das, S. R. (2019). The Future of Fintech. *Financial Management*, *48*(4), 981–1007. https://doi.org/10.1111/fima.12297.
Deb, S. (2014). Information Technology, Its Impact on Society and Its Future. *Advances in Computing*, *4*(1), 25–29. https://doi.org/10.5923/j.ac.20140401.07.
Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. *E3S Web of Conferences*, *125*(20101), 1–5. https://doi.org/10.1051/e3sconf/201912521001.
Falco, G. (2019). Cybersecurity Principles for Space Systems. *Journal of Aerospace Information*

Systems, *16*(2), 61–70. https://doi.org/10.2514/1.I010693.
Faya, M., & Ogbuefi, N. (2019). Cybersecurity in the Age of FinTech and Digital Business. *Cyber Secure Nigeria 2019 Conference*, 6–10. https://ssrn.com/abstract=3606866.
Gani, A. G. (2018). Cybercrime (Kejahatan Berbasis Komputer). *Jurnal Sistem Informasi*, *5*(1), 16–29. https://doi.org/https://doi.org/10.35968/jsi.v5i1.18.
Huang, K., & Madnick, S. (2020). Cyber Securing Cross-border Financial Services: Calling for a Financial Cybersecurity Action Task Force. *Working Paper CISL# 2020-08*, 1–10. https://doi.org/10.2139/ssrn.3570140.
Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2.
Irfan, M., Ramdhani, M. A., Darmalaksana, W., Wahana, A., & Utomo, R. G. (2018). Analyzes of Cybercrime Expansion in Indonesia and Preventive Actions. *IOP Conference Series: Materials Science and Engineering*, *434*(012257), 1–6. https://doi.org/10.1088/1757-899X/434/1/012257.
Jesson, J. K., Matheson, L., & Lacey, F. M. (2011). *Doing Your Literature Review: Traditional and Systematic Techniques*. SAGE Publications. California: Thousand Oaks.
Joveda, N., Khan, M. T., & Pathak, A. (2019). Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of Financial Information. *International Journal of Economics and Finance*, *11*(10), 54. https://doi.org/10.5539/ijef.v11n10p54.
Karlov, R. G. (2018). The Impact of New Methods of Money Laundering on the Economy of the State. *KnE Social Sciences*, *3*(2), 491. https://doi.org/10.18502/kss.v3i2.1581.
Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends. In *Springer*. Switzerland AG. http://www.springer.com/series/16360.
Kaur, S. J. (H R. C. (2020). Reviewing Existential Threats Involved in Fintech. *UGC Care Journal*, *40*(36), 58–62.
Kitchenham, B., & Brereton, P. (2013). A Systematic Review of Systematic Review Process Research in Software Engineering. *Information and Software Technology*, *55*(12), 2049–2075. https://doi.org/10.1016/j.infsof.2013.07.010.
Kou, G. (2019). Introduction to the special issue on FinTech. *Financial Innovation*, *5*(1), 4–6. https://doi.org/10.1186/s40854-019-0161-1.
Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527.
Kwarto, F., & Angsito, M. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance di Sektor Keuangan. In *Jurnal Akuntansi Bisnis* (Vol. 11, Issue 2, pp. 99–110). https://doi.org/10.30813/jab.v11i2.1382.
Laidlaw, E. (2021). Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows. *SSRN Electronic Journal*, 1–81. https://doi.org/10.2139/ssrn.3790936.
Lee, I., & Jae, Y. (2018). Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges. *Business Horizons*, *61*(1), 35–46. https://doi.org/10.1016/j.bushor.2017.09.003.
Li, B., & Xu, Z. (2021). Insights into Financial Technology (FinTech): A Bibliometric and Visual Study. *Financial Innovation*, *7*(69), 1–28. https://doi.org/10.1186/s40854-021-00285-7.
Lubin, A. (2021). Insuring Evolving Technology. *Connecticut Insurance Law Journal . Indiana Legal Studies Research Paper No. 441*, *28*(1), 1–31.
Mabunda, S. (2018). Cryptocurrency: The New Face of Cyber Money Laundering. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, IcABCD 2018*, 1–6. https://doi.org/10.1109/ICABCD.2018.8465467.
Maigida, A. M., Abdulhamid, S. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic Literature Review and Metadata Analysis of Ransomware Attacks and Detection Mechanisms. *Journal of Reliable Intelligent Environments*, *5*(2), 67–89.

https://doi.org/10.1007/s40860-019-00080-3.
Malladi, C. M., Soni, R. K., & Srinivasan, S. (2021). Digital Financial Inclusion: Next Frontiers—Challenges and Opportunities. *CSI Transactions on ICT*, *9*(2), 127–134. https://doi.org/10.1007/s40012-021-00328-5.
Mehrotra, A., & Menon, S. (2021). Second Round of FinTech - Trends and Challenges. *2nd International Conference on Computation, Automation and Knowledge Management, ICCAKM 2021*, 243–248. https://doi.org/10.1109/ICCAKM50778.2021.9357759.
Milian, E. Z., Spinola, M. de M., & Carvalho, M. M. d. (2019). Fintechs: A Literature Review and Research Agenda. *Electronic Commerce Research and Applications*, *34*(100833), 1–21. https://doi.org/10.1016/j.elerap.2019.100833.
Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech Firms and Banks Sustainability: Why Cybersecurity Risk Matters? *International Journal of Financial Engineering*, *08*(02), 2150019. https://doi.org/10.1142/S2424786321500195.
Namchoochai, R., Kiattisin, S., Darakorn Na Ayuthaya, S., & Arunthari, S. (2020). Elimination of FinTech Risks to Achieve Sustainable Quality Improvement. *Wireless Personal Communications*, *115*, 3199–3214. https://doi.org/10.1007/s11277-020-07201-9.
Ng, A. W., & Kwok, B. K. B. (2017). Emergence of Fintech and Cybersecurity in a Global Financial Centre: Strategic Approach by a Regulator. *Journal of Financial Regulation and Compliance*, *25*(4), 1–14. https://doi.org/10.1108/jfrc.2008.31116baa.001.
Nikkel, B. (2020). Fintech Forensics: Criminal Investigation and Digital Evidence in Financial Technologies. *Forensic Science International: Digital Investigation*, *33*, 200908. https://doi.org/10.1016/j.fsidi.2020.200908.
Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A Machine Learning-based FinTech Cyber Threat Attribution Framework Using High-level Indicators of Compromise. *Future Generation Computer Systems*, *96*, 227–242. https://doi.org/10.1016/j.future.2019.02.013.
Ogbanufe, O., & Kim, D. J. (2018). Comparing Fingerprint-based Biometrics Authentication Versus Traditional Authentication Methods for e-Payment. *Decision Support Systems*, *106*, 1–14. https://doi.org/10.1016/j.dss.2017.11.003.
Ojo, O., & Nwaokike, U. (2019). Disruptive Technology and the Fintech Industry in Nigeria: Imperatives for Legal and Policy Responses. *Gravitas Review of Business and Property Law*, *9*(3), 1–19. https://doi.org/10.2139/ssrn.3306164.
Palmié, M., Wincent, J., Parida, V., & Caglar, U. (2019). The Evolution of the Financial Technology Ecosystem: An Introduction and Agenda for Future Research on Disruptive Innovations in Ecosystems. *Technological Forecasting & Social Change*, *151*, 119779. https://doi.org/10.1016/j.techfore.2019.119779.
Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding Cyber-Risk and Cyber-Insurance. *Macquarie University Faculty of Business & Economics Research Paper*, 1–30. https://doi.org/10.2139/ssrn.3200166.
Pratamasari, A. (2020). Cybersecurity and Custom Regulations as Trade Barriers in ASEAN e-Commerce : Case of Indonesian e-Commerce. *Global Strategis*, *14*(1), 1–16. https://doi.org/10.20473/jgs.14.1.2020.1-16.
Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and Cyber Security Maturity Models: A Systematic Literature Review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039.
Rahmanto, D. N. A., & Nasrulloh. (2019). Risiko dan Peraturan: Fintech untuk Sistem Stabilitas Keuangan. *Inovasi*, *15*(1), 44–52. https://doi.org/10.29264/jinv.v15i1.4339.
Riskiyadi, M. (2020). Investigasi Forensik terhadap Bukti Digital dalam Mengungkap Cybercrime. *CyberSecurity Dan Forensik Digital*, *3*(2), 12–21. https://doi.org/10.14421/csecurity.2020.3.2.2144.
Sangwan, V., Harshita, Prakash, P., & Singh, S. (2019). Financial Technology: A Review of Extant Literature. *Studies in Economics and Finance*, *37*(1), 71–88. https://doi.org/10.1108/SEF-07-2019-0270.
Santucci, L. (2018). Quantifying Cyber Risk in the Financial Services Industry. *FRB of*

Philadelphia Payment Cards Center Discussion Paper No. 18-3, 1–30.
Şcheau, M. C. (2017). Methods of Laundering Money Resulted from Cyber-Crime. *Economic Computation and Economic Cybernetics Studies and Research*, *51*(3), 299–315.
Sharma, N. (2019). Banking and FinTech (Financial Technology) Embraced with IoT Device. *Advances in Intelligent Systems and Computing*, *1042*, 197–211. https://doi.org/10.1007/978-981-32-9949-8_15.
Shekar, B., & Prabha, A. (2020). Impacts of Cyber Crime on the Victims. *UGC Care Journal*, *40*(50), 2731–2737. https://digital.wings.uk.barclays/for-everyone/milestone/impacts-of-cyber-crime/.
Shekar, M. C., & Kumaran, R. (2019). Fintech - An Exploratory Study and Its Applications. *The Management Accountant*, 51–54.
Singh, P., & Rajput, R. S. (2019). Cybersecurity Analysis in the Context of Digital Wallets. *International Journal of Advanced Studies of Scientific Research*, *4*(3), 522–525.
Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity Policy in ASEAN Countries. *Information Institute Conferences*, 1–8.
Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review. *Information*, *11*(12), 1–20. https://doi.org/10.3390/info11120590.
Teigland, R., Siri, S., Larsson, A., & Puertas, A. M. (2018). *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*. Routledge. New York: Third Avenue.
Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and Financial System Vulnerability: A Synthesis of Literature. In *Risk Management* (Vol. 22, Issue 4). Palgrave Macmillan UK. https://doi.org/10.1057/s41283-020-00063-2.
Uman, L. S. (2011). Systematic Reviews and Meta-Analyses. *Journal of the Canadian Academy of Child and Adolescent Psychiatry*, *20*(1), 57–59. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3024725/.
Vedral, B. (2021). The Vulnerability of the Financial System to a Systemic Cyberattack. *13th International Conference on Cyber Conflict (CyCon)*, 95–110. https://doi.org/10.23919/CyCon51939.2021.9468291.
Wang, J. S. (2021). Exploring Biometric Identification in FinTech Applications Based on the Modified TAM. *Financial Innovation*, *7*(42), 1–24. https://doi.org/10.1186/s40854-021-00260-2.
Wibawa, I. (2017). Cyber Money Laundering (Salah Satu Bentuk White Collar Crime abad 21). *Jurnal Pemikiran Hukum Dan Hukum Islam*, *8*(2), 240–254. https://doi.org/10.21043/yudisia.v8i2.3238.
Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 1–20. https://doi.org/10.1177/0739456X17723971.
Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995.
Zavolokina, L., Dolata, M., & Schwabe, G. (2016). The FinTech Phenomenon: Antecedents of Financial Innovation Perceived by the Popular Press. *Financial Innovation*, *2*(16), 1–16. https://doi.org/10.1186/s40854-016-0036-7.