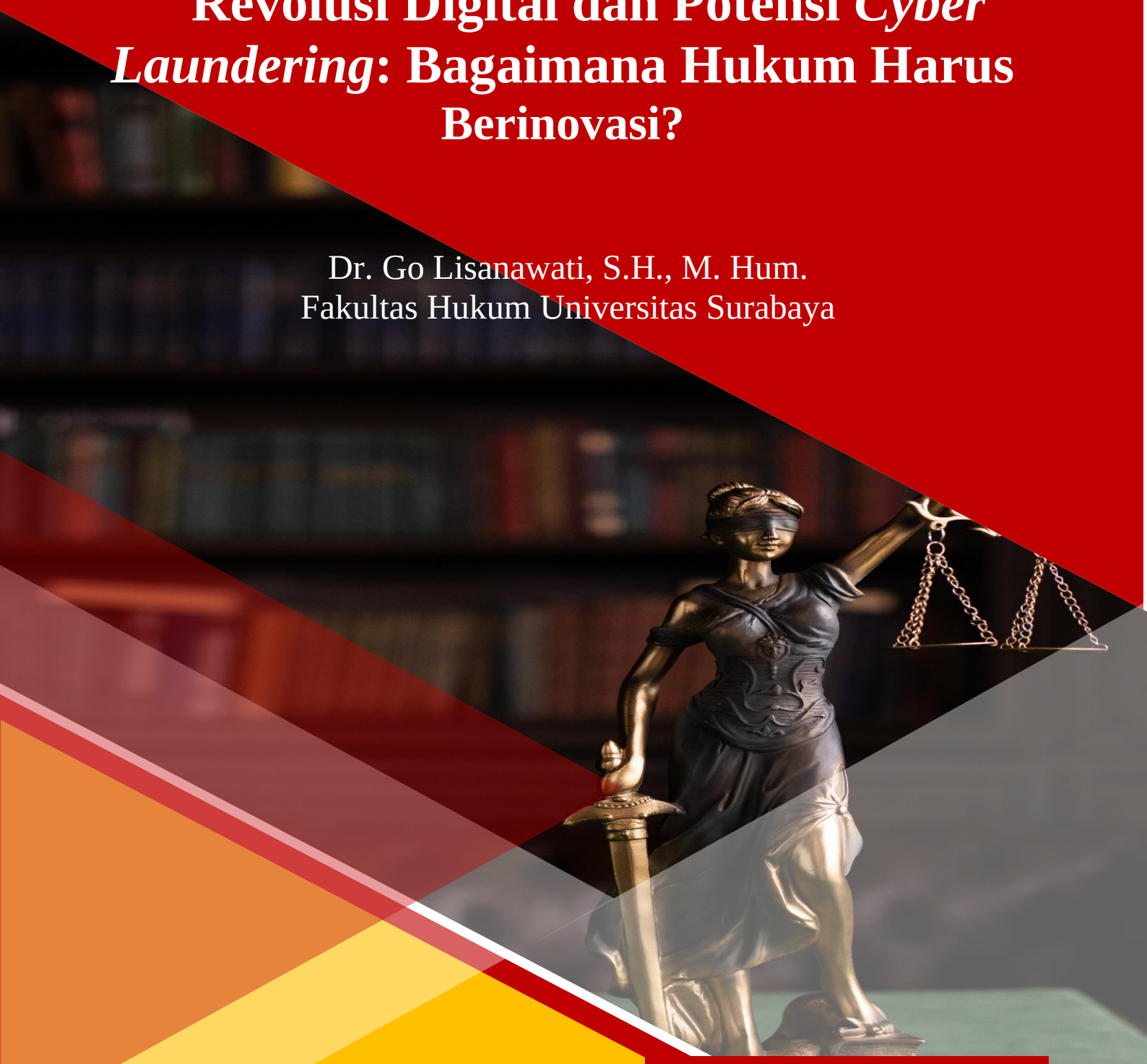
Revolusi Digital dan Potensi *Cyber Laundering*: Bagaimana Hukum Harus Berinovasi?

Dr. Go Lisanawati, S.H., M. Hum.
Fakultas Hukum Universitas Surabaya



ORASI ILMIAH
DIES NATALIS KE-55
11 Maret 2023

Disampaikan pada:
Rapat Terbuka Senat
Universitas Surabaya dalam rangka
Dies Natalis ke-55 Universitas Surabaya

ORASI ILMIAH

Disampaikan pada Rapat Terbuka Senat Universitas Surabaya
Dalam rangka Dies Natalis ke-55 Universitas Surabaya

Revolusi Digital dan Potensi *Cyber Laundering*: Bagaimana Hukum Harus Berinovasi?

Oleh: Dr. Go Lisanawati, S.H., M. Hum.
Fakultas Hukum
Universitas Surabaya

2023

Revolusi Digital dan Potensi *Cyber Laundering*: Bagaimana Hukum Harus Berinovasi?

Go Lisanawati*

1. Pendahuluan

Marc Goodman dalam pengantar bukunya yang berjudul *Future crimes* pada intinya menegaskan mengenai *how our technology can be used to help us or hurt us. To build a society where everything is connected, and technology makes us more vulnerable to people who know how to use our technology*.[1] Manusia menjadi bergantung pada teknologi baik saat ini maupun ke depan. Goodman kemudian juga menekankan bahwasanya tekonologi memunculkan kerentanan-kerentanan yang dapat merugikan manusia. Goodman menambahkan penjelasan tentang *how computers are taking over the lives of people and how people become too dependent on them. The more complicated the systems become, the more people who can understand them and find new ways to use them. This is hurting us all, but some groups are doing better than others at managing these complexities.*[2] Hal tersebut yang menyebabkan Goodman merasa sangat khawatir. Kerentanan-kerentanan tersebut tidak saja karena munculnya kejahatan, pemerintahan yang manipulatif, tetapi juga perusahaan-perusahaan dan organisasi-organisasi yang mengandalkan perlindungan, ternyata juga memunculkan kerentanan karena organisasi dan perusahaan tersebut akan mengendalikan kode-kode yang akan menjalankan hidup manusia.[3]

Sagwandi Mabunda menyatakan: *"An old saying goes 'for every level there's a new devil" and technology has taken society to a new level where it appears that cybercrime is the new devil that must be contended with*.[4] Pernyataan ini sesungguhnya menunjukkan bagaimana teknologi akan membawa masyarakat pada sebuah level baru yang juga diikuti dengan risiko kejahatan yang harus dihadapi dan ditundukkan. Adagium lama yang digaungkan oleh Cicero yaitu *Ubi Societas Ibi Ius*, di mana ada

*Fakultas Hukum Universitas Surabaya, Email: go_lisanawati@staff.ubaya.ac.id

[1] Marc Goodman. 2015. Future Crimes: Inside the *Digital* Underground and the Battle for Our Connected World. Canada: Anchor Canada 3

[2] Ibid 4

[3] Ibid. 53

[4] Sagwadi Mabunda, 'Cryptocurrency: The New Face of Cyber Money Laundering' [2018] 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, icABCD 2018 1.

masyarakat di situ ada hukum menjadi relevan untuk mengingatkan bagaimana hukum harus menjadi pemimpin di dalam perkembangan zaman. Karya Thomas Hobbes[5] dengan judul *De Cive* (1651) yang pada intinya menjelaskan bahwa semua orang dalam keadaan alami memiliki keinginan untuk menyakiti, tetapi penyebabnya tidak sama. Hal tersebut bergantung pada bagaimana manusia memandang dirinya atas orang lain.

Pada pandangan ini tepatlah apa yang dikemukakan oleh Thomas Hobbes: "*That Man to Man is a kind of God; and that Man to Man is an errant wolf."*[6] Pada masyarakat akan selalu terjadi kecenderungan manusia menjadi serigala dan pemangsa atas kebebasan manusia, kecuali hutan yang menampung manusia digerus akarnya. Dengan demikian, masyarakat akan selalu memerlukan hukum mengingat kecendurungan manusia yang menjadi ancaman bagi sesamanya, sekalipun di pihak lainnya, manusia dapat menjadi sahabat bagi sesamanya.

Penyebaran teknologi informasi berbasis komputer dan peralatan komunikasi serta digitalisasi di masing-masing dan semua bidang kehidupan telah mengaburkan batas-batas dan ekonomi dan infrastruktur nasional yang saling berhubungan. *Trend* tersebut telah menyebabkan munculnya lingkungan informasi global terintegrasi di mana setiap orang dapat mengakses informasi dalam dimensi lintas ruang dan waktu, menandatangani kontrak dengan rekanan asing tanpa kontak tatap muka, dan lain sebagainya. Pada saat yang sama, lingkungan informasi telah menjadi tempat dan instrumentalitas kejahatan. Pelaku hanyalah memerlukan komputer dan akses ke sistem informasi.

Berbagai kejahatan dan serangan di bidang dunia maya pada hakikatnya mencakup setiap kejahatan yang dengan perangkat komputer, dan perangkat canggih lainnya. Kejahatan siber bermanifestasi menjadi berbagai macam kejahatan, seperti manifestasi kejahatan siber terkait sistem komputer, keamanan komputer, harta kekayaan, ketertiban umum, identitas dan manifestasi-manifestasi lainnya. *Phishing*, penipuan secara daring, maupun perjudian secara daring juga masuk ke dalam kejahatan siber yang hasilnya dilakukan pencucian uang.

---

[5] WRC, 'Table of Contents Table of Contents ازسیرتاپیازمصاحبه‌دکتری' [2012] European University Institute 2 <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT%0Ahttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:pt:NOT>.

[6] ibid.

Trend peningkatan Tindak Pidana Pencucian Uang (TPPU) dan kejahatan keuangan di Indonesia sesungguhnya juga menunjukkan tantangan di dalam implementasi UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (disebut UU Pencucian Uang) dan aturan hukum terkait dengan kejahatan keuangan di Indonesia itu sendiri. Sektor perbankan masih menjadi target utama TPPU dan kejahatan-kejahatan di bidang keuangan lainnya, dan untuk hal tersebut Pemerintah Indonesia telah melakukan berbagai upaya penguatan rezim anti pencucian uang (APU).

Indonesian FIU (PPATK), dalam pertemuan dengan UNODC pada 19 – 20 April 2022, memberikan perhatian pada risiko pencucian uang secara elektronik *(electronic money laundering/cyber laundering)* dan pendanaan terorisme muncul dari *new payment methods*.[7] Indonesia sendiri telah memasuki era *digital transformation* dengan segala kebijakannya, dan memerlukan penegakan hukum yang mampu memitigasi risiko yang ditimbulkan oleh potensi *digital innovation* yang berasosiasi dengan kejahatan. Perkembangan penggunaan teknologi dalam layanan keuangan, termasuk di dalamnya adalah menyangkut teknologi finansial (Tekfin), yang di dalam bahasa asing digunakan adalah *Financial Technology (Fintech)*. Fintech (Artikel ini akan menggunakan istilah Fintech apabila tidak disebut secara khusus sebagai Tekfin oleh literatur yang dirujuk) dan perdagangan krypto, sesungguhnya memiliki karakter yang rentan dimanfaatkan oleh pelaku kejahatan terorganisir *(organized crime)*. Teknologi memberikan kemudahan dalam berbagai hal, seperti *non face to face*, *speedy transaction*, dan *real time privacy*. PPATK melaporkan bahwa modus penipuan terus menunjukkan peningkatan setiap tahunnya.

Berdasarkan laporan tahun 2021[8], PPATK menjelaskan dalam grafis sebagai berikut:

[7] https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2022/03-assessing-*digital*-financial-threat-landscape-indonesia.html, akses pada 20 Desember 2022.
[8] PPATK. 2021. Laporan Tahunan 2021: Indonesia Maju Tanpa Pencucian Uang dan Pendanaan Terorisme, PPATK, 32

Grafis 1: Hasil Analisis Risiko TPPU oleh PPATK

Penjelasan tersebut didasarkan pada hasil analisis risiko yang dilakukan oleh PPATK tersebut merupakan suatu langkah yang penting dan relevan untuk dilakukan, sebagai suatu respon atas perkembangan kebutuhan nasional dan internasional. Pada penilaian risiko tersebut dinyatakan bahwa terdapat ancaman yang muncul (*emerging threat)* berupa digunakannya cara atau *new payment system* dalam TPPU, di samping penggunaan identitas palsu, *nominees* (nama pinjaman), *trusts*, anggota keluarga atau pihak ketiga, properti/*real estate* termasuk pula peran agen properti, *Smurfing*, *Structuring*, penggunaan jasa profesi, pemanfaatan korporasi *(legal person)*, serta pemanfaatan sekrot yang tidak terregulasi dengan baik.[9] Hal ini dinyatakan sebagai tipe *high risks money laundering*. PPATK[10] juga melaporkan bahwasannya kemajuan teknologi yang diikuti dengan meningkatnya kompleksitas penjahat, memunculkan ancaman-ancaman terkait pencucian uang. Ancaman tersebut di antaranya:

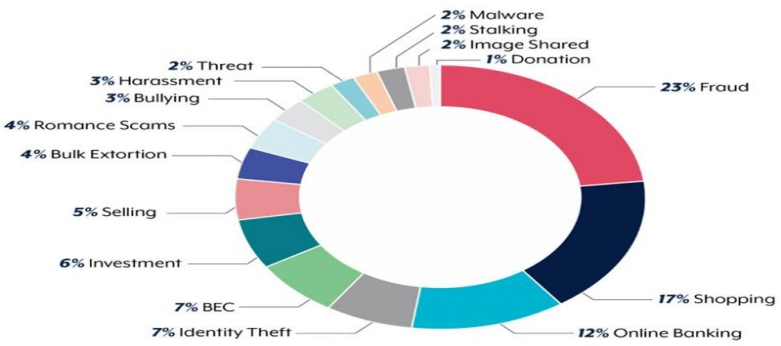
- terjadinya transaksi jual-beli oleh sindikat, serta penggunaan nama pihak lain atas suatu rekening;
- Disalahgunakannya kegiatan e-*commerce* untuk mentransaksikan hasil-hasil tindak pidananya; serta
- Beroperasinya *Fintech P2P lending* yang tidak memiliki izin.

[9] Tim Pelaksana Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang. 2021. Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang, Jakarta: PPATK x
[10] Ibid, xi

Selain itu, hasil analisis PPATK menunjukkan bahwa *fraud* di Indonesia terus meningkat, dari 9.801 laporan tindakan mencurigakan terkait *fraud* pada 2019 menjadi 13.338 pada 2020, menjadi sekitar 23.000 pada 2021. Mulai Februari 2022, penipuan – termasuk penipuan berbasis dunia maya dan pelanggaran undang-undang transaksi elektronik – telah menjadi jenis kejahatan paling umum yang memicu laporan tindakan mencurigakan.[11] Berdasarkan data tersebut, dapat dipahami bahwasanya *fraud* mendominasi pada proses munculnya pencucian uang, termasuk juga *fraud* yang dilakukan *cyber based fraud* dan juga pelanggaran undang-undang ITE lainnya.

Australian Cyber Security Center - Australia memberikan laporan tahun 2020 – 2021 bahwa selama tahun fiskal 2020 – 2021, lebih dari 67,000 laporan *cybercrime* mengalami kenaikan sekitar 13% dari tahun fiskal sebelumnya.[12] Kategori *cybercrime* dengan laporan terbanyak adalah jenis *cybercrime* yang terjadi ketika komputer dipergunakan sebagai sarana yang memfasilitasi kejahatan seperti penipuan daring *(Online Fraud)* ataupun *Online child sexual and exploitation*. Sementara itu, *Ransomware* tetap menjadi ancaman *cybercrime* yang paling serius, dalam hal ini pada bidang keuangan, dan menimbulkan gangguan bagi korban dan masyarakat.

Secara grafik, macam-macam serangan *cybercrime* tersebut adalah sebagaimana digambarkan sebagai berikut:

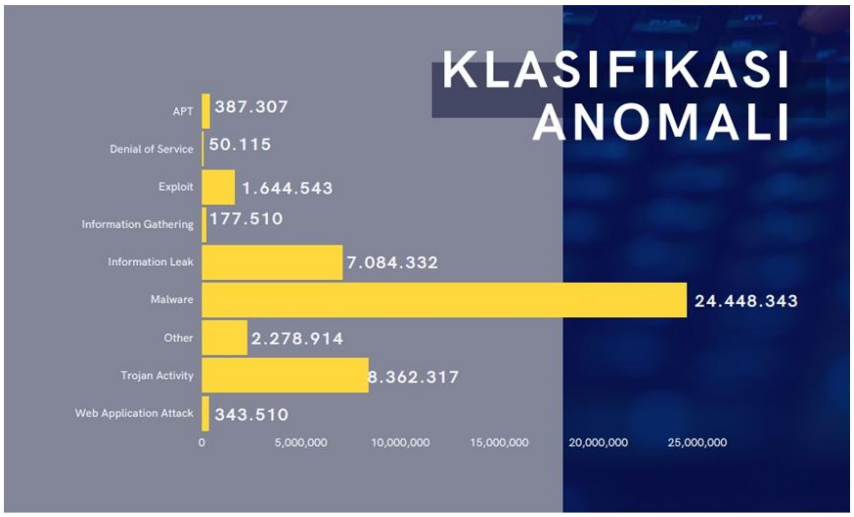


Gambar 1: Laporan *cybercrime* Tahun Fiskal 2020 – 2021

Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Agustus 2022, Badan Siber dan Sandi Negara (BSSN), menjelaskan terjadinya Anomali Trafik, dan puncak

[11] https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2022/03-assessing-*digital*-financial-threat-landscape-indonesia.html, akses pada 20 Desember 2022
[12] ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021, p. 15

tertinggi adalah pada tanggal 3 Agustus 2022 sebanyak 3.103.770 anomali trafik.[13] Perbandingannya, pada 2021, BSSN menyatakan anomali trafik yang masuk ke Indonesia tercatat 1.637.937.022 serangan yang didominasi oleh Botnet.[14] Laporan tersebut sebagai berikut:



Gambar 2: Statistik Klasifikasi Anomali

Serangan siber melalui anomali trafik menunjukkan kerentanan siber di Indonesia. Salah satu kejahatan yang banyak dilakukan adalah terkait *Phishing*. *Phishing* merupakan manifestasi kejahatan siber terhadap identitas. *Phishing* ini berusaha memperoleh informasi terkait data dengan teknik untuk mengelabui korban. Objek dari *phishing* ini biasanya data pribadi seperti nama, alamat, data akun termasuk kata sandi, data kartu, data akun bank, nomor *handphone*. *Phishing* memancing korban untuk memberikan informasi pribadinya tanpa sadar, yang apabila informasi tersebut didapatkan maka data tersebut akan disalahgunakan untuk melakukan kejahatan. Teknik yang banyak digunakan dalam *Phishing* adalah dengan *social engineering* (rekayasa sosial). Teknik ini akan memanipulasi korban maupun calon korban melalui tautan-tautan yang diberikan, padahal tautan tersebut tidak benar. Selain *Phishing*, *Ransomware* masih menjadi ancaman utama bagi sektor publik, rumah sakit maupun tempat yang melayani kesehatan, pabrik/perusahaan, maupun organisasi-organisai yang memiliki nilai tinggi. *Malware* ini akan meminta korban melakukan pelunasan ataupun pembayaran atas data yang dicurinya karena dikunci oleh *cybercriminals*, dengan ancaman bahwa apabila tidak melakukan yang diminta, maka data penting tersebut akan

[13] Badan Siber dan Sandi Negara. 2022. Laporan Bulanan Publik Hasil Monitoring Keamanan Siber. Sumber: https://www.bssn.go.id
[14] M.cyberthreat.id

rusak dan tidak dikembalikan. Pada praktiknya, *ransomware* ini banyak meminta tebusan dalam bentuk *bitcoin*. Tidak dapat dipungkiri ancaman siber ini semakin marak karena semua orang saat ini menjadi bergantung dengan aktivitas di dunia maya. Semua bergantung dengan kecanggihan teknologi. Salah satu yang berkembang saat ini misalnya penggunaan *Non Fungible Tokens, metaverse*, transaksi aset kripto dan adopsi investasi.

Artikel ini hendak menganalisis bagaimana hukum anti pencucian uang harus melakukan inovasi untuk merespon revolusi *digital* yang memungkinkan dieksplorasi oleh pelaku kejahatan dunia maya untuk melakukan *cyber laundering*. Artikel ini merupakan tipe artikel analisis dengan menekankan pada konsep dan bahan hukum yang berupa peraturan hukum yang terkait dan relevan dengan permasalahan. Penelitian ini menggunakan metode penelitian hukum yang yuridis normatif, yang merupakan penelitian yang mendasarkan pada penggunaan bahan hukum primer, dalam hal ini beberapa aturan hukum dalam bentuk undang-undang sebagai hukum positif di Indonesia dan aturan hukum lainnya, serta berdasarkan bahan hukum sekunder.

2. Revolusi *Digital*: Teknologi Finansial, *Digital Currency*, dan *Digital Onboarding*

a. Teknologi Finansial *(Financial Technology)*

Revolusi *digital* memunculkan berbagai macam inovasi di segala aspek kehidupan manusia. Muchsin Al-Fikri[15] memberikan pemikiran bahwasanya perkembangan *digital* mendorong terjadinya *Industrial Revolution* 4.0 sehingga memberikan kemungkinan manusia mempelajari hal baru tanpa banuan dari operator. Pada fase ini, muncul berbagai penggunaan *artificial intelligence* (kecerdasan buatan). Era *digital* juga ditandai dengan hadirnya masyarakat internet (*internet society*). Eksistensi teknologi yang digital ini menyebabkan munculnya masa yang dikenal sebagai era disruptif, yaitu melalui beragai inovasi, yang secara cepat memenuhi kebutuhan manusia. Kehadiran teknologi ini semakin vital. Revolusi *digital* tidak dapat dipungkiri telah menempatkan hukum pada suatu keharusan untuk berinovasi agar hukum tetap menjadi panglima di dalam perubahan di segala bidang. Salah satu penetrasi terbesar di bidang revolusi *digital* adalah pada bidang perbankan, perusahaan-perusahaan *start up* yang jelas

[15] H Muchsin Al-Fikri, 'Peluang Dan Tantangan Perguruan Tinggi Menghadapi Revolusi Digital Di Era Society 5.0' (2021) 3 Prosiding Seminar Nasional Pendidikan 350 <https://mail.prosiding.unma.ac.id/index.php/semnasfkip/article/view/621>.

mengandalkan teknologi di dalam mendukung aktivitasnya. Penetrasi tersebut sekaligus memunculkan permasalahan-permasalahan hukum. Perkembangan teknologi mempengaruhi kehadiran kehidupan yang serba digital, serta hadirnya Fintech.

Revolusi *digital* yang membawa inovasi juga menyentuh pada penggunaan alat pembayaran baru. Permasalahan mengenai *new payment system* tersebut muncul dengan berbagai nama yang hampir sama, tetapi memiliki karakteristik dan penggunaan yang berbeda-beda. Namun demikian memiliki kesamaan yaitu memunculkan potensi yang merugikan dan disalahgunakan oleh penjahat. Berbagai nama seperti mata uang virtual, mata uang digital, mata uang kripto, aset digital, *Stable Coin*, *Fiat Currency*, dan lainnya dengan berbagai inovasinya. Pemerintah dalam hal ini perlu segera memberikan respon/reaksi berupa pelarangan atau pengaturan terkait mata uang-mata uang tersebut, sekalipun mungkin sesuai karakter tidak sesuai dengan karakter sebagai mata uang. Inovasi ini menjadi rentan atas eksplotasi dari pelaku kejahatan dalam hal ini para *cyber-offender* dan *launderer*.[16]

Otoritas Jasa Keuangan mengatur mengenai Inovasi Keuangan Digital di Sektor Jasa Keuangan, yaitu berupa Peraturan Otoritas Jasa Keuangan 13/POJK.02/2018, sesungguhnya menunjukkan bahwa Pemerintah Indonesia telah melakukan berbagai inovasi. Inovasi tersebut adalah Inovasi Keuangan *Digital* (IKD). Pada konsiderans menimbang, Otoritas Jasa Keuangan (OJK) menegaskan bahwa inovasi keuangan *digital* perlu diarahkan untuk menghasilkan IKD yang memiliki tanggung jawab, aman, melindungi konsumen, dan mengelola risiko yang harus dikelola dengan baik. Aspek penting lain yang harus diperhatikan adalah aspek Perlindungan Data. Pada dasarnya, IKD itu merupakan kegiatan pembaharuan yang meliputi:

- *business process*
- *business model*, dan
- *financial instrument*

ketiga hal tersebut memberikan nilai lebih baru di sektor jasa keuangan, dengan ekosistem *digital* (lihat pada Pasal 1 angka 1).

Merujuk pada definisi tersebut, IKD ini diarahkan untuk memperkuat sektor jasa keuangan agar mampu bersaing dengan nilai tambah baru. Salah satu yang menjadi perhatian adalah IKD ini akan memiliki makna yang berarti untuk memberikan

[16] Go Lisanawati and Erly Aristo, 'Urgensi Pengaturan Hukum Central Bank *Digital* Currency Dalam Dimensi Anti Pencucian Uang' (2022) 8 Jurnal Ilmiah Hubungan Internasional 49.

dukungan bagi servis jasa keuangan menjadi bertambah cepat, juga murah, mudah, serta meluas sehingga hadir pula pada daerah yang jauh dari teknologi, sekaligus pula untuk memperkecil jurang perbedaan yang sangat tajam di bidang ekonomi di seluruh daerah di Indonesia. IKD akan mengandalkan pada kehadiran dan percepatan teknologi. Teknologi ini harus hadir untuk mendorong terwujudnya servis di bidang jasa keuangan sehingga menjadi bertambah efisien, sekaligus memenuhi kebutuhan bagi masyarakat Indonesia.

Merujuk pada bagian penjelasan umum dari peraturan OJK tentang IKD ini, didapatkan pemahaman bahwa perkembangan dan inovasi selalu memiliki dua bagian yang berseberangan. Terkait hal ini adalah sisi kebermanfaatan, tetapi sekaligus juga disrupsi yang mengganggu sisi pemberian pelayanan pada jasa keuangan yang tradisional. Dengan demikian perlu dikedepankan *good governance* yang baik sehingga sisi manfaat dan disrupsi ini tetap dapat bermanfaat bagi seluruh masyarakat[17]

Perkembangan pembangunan ekosistem keuangan digital harus selalu inovatif, dan yang pada akhirnya harus saling menguntungkan. Dari sudut pandang filsafat, hal ini yang menjadi kebijakan sosial, yang harus selalu mengarah pada kesejahteraan masyarakat. Negara kemudian harus memberikan respon terhadap inovasi tersebut, dan yang harus diimplementasikan melalui peraturan hukum, dan pengawasan dilakukan dalam kaitannya dengan kegiatannya dan kelembagaannya.

Salah satu perkembangan yang pesat adalah Fintech. Kehadiran Fintech diatur di dalam Peraturan Bank Indonesia 19/12/PBI/2017 terkait penyelenggaraan teknologi finansial. Berikutnya Peraturan OJK 77/POJK.01//2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. Ketentuan Peraturan OJK ini kemudian diubah dengan Peraturan OJK 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi. Pada intinya PBI 19/12/PBI/2017 ini menyebutkan mengenai 5 bidang Teknologi Informasi, yaitu sistem pembayaran, pendukung pasar, manajemen investasi, dan manajemen risiko, pinjaman, pembiayaan dan penyediaan modal dan jasa finansial lainnya.[18] Sementara itu Peraturan OJK 77/POJK.01/2016 merupakan peraturan lebih lanjut mengenai Fintech yang bergerak pada jenis atau

[17] Otoritas Jasa Keuangan, 'Peraturan OJK No. 13/POJK.02/2018 Tentang Inovasi Digital Di Sektor Jasa Keuangan' [2018] Otoritas Jasa Keuangan 1 <http://www.ojk.go.id/id/kanal/iknb/regulasi/lembaga-keuangan-mikro/peraturan-ojk/Documents/SAL-POJK PERIZINAN FINAL F.pdf>.

[18] Agus DW Martowardojo, 'Penyelenggaraan Teknologi Finansial' [2017] Peraturan Bank Indonesia 1 <https://www.bi.go.id/id/sistem-pembayaran/fintech/Contents/default.aspx>.

bidang peminjaman, pembiayaan, dan penyediaan modal. Peraturan OJK No. 77/POJK.01/2016 tersebut menjadi landasan atas kegiatan *Peer to peer lending* di Indonesia. Namun Peraturan OJK No. 77/POJK.01/2016 tersebut telah dicabut dan diganti dengan Peraturan OJK 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI).

Perkembangan Fintech ini secara hakikat ditujukan sebagai penggunaan teknologi dalam sistem keuangan yang menghasilkan produk, layanan, teknologi dan/atau model bisnis baru serta berdampak pada stabilitas moneter, stabilitas sistem keuangan, dan/atau efisiensi, kelancaran, keamanan, dan keandalan sistem pembayaran.[19] Berdasarkan hal inilah Fintech akan terus mengalami perkembangan, dan tidak menafikan bahwasanya akan memungkinkan dieksploitasinya Fintech oleh pencuci uang juga pelaku pendanaan terorisme. Fintech memiliki kecepatan dan kedinamisan teknologi. Hal inilah yang memungkinkan dilakukannya eksploitasi oleh pelaku kejahatan. Fintech mempunyai tujuan untuk mempermudah pemenuhan kebutuhan masyarakat di dalam banyak aspek yang memungkinkan *non face to face* dan mudah.

Berdasarkan Pasal 1 angka 1 PBI 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial menjelaskan bahwa Fintech adalah penggunaan teknologi dalam sistem keuangan yang menghasilkan produk, layanan, teknologi, dan/atau model bisnis baru serta dapat berdampak pada stabililitas moneter, stabilitas sistem keuangan, dan/atau efisiensi, kelancaran, keamanan, dan keandalan sistem pembayaran. Fintech juga dapat dipahami melalui pendapat beberapa ahli sebagai: suatu pemanfaatan perkembangan teknologi informasi di bidang keuangan.[20] Fintech juga sebagai industri keuangan baru yang menerapkan teknologi untuk mengembangkan aktivitas keuangan.[21] Leong and Sung selanjutnya menjelaskan *Fintech* sebagai *"any innovative ideas that improve financial service processes by proposing technology solutions according to different business situations while the ideas could also lead to new business models or even new businesses"*[22] Lebih jauh, Fintech meliputi *start-ups*, penggunaan teknologi informasi dan komunikasi untuk layanan keuangan, dan industri

[19] ibid.
[20] Clarisa Permata Hariono Putri and Go Lisanawati, 'Peran Teknologi Finansial Dalam Pencegahan Pendanaan Terorisme' (2023) 30 70.
[21] Patrick Schueffel, 'Taming the Beast: A Scientific Definition of Fintech' (2016) 4 Journal of Innovation Management 32.
[22] Kelvin Leong, 'FinTech (Financial Technology): What Is It and How to Use Technologies to Create Business Value in Fintech Way?' (2018) 9 International Journal of Innovation, Management and Technology 74.

start-ups yang berkolaborasi dengan layanan keuangan tradisional.[23] Dengan demikian Fintech dapat dipahami sebagai suatu pemanfaatan teknologi dalam sistem keuangan, dan merupakan inovasi dalam menghasilkan produk-produk, dan juga sebagai bentuk baru bisnis untuk berbagai macam sistem pembayaran dan kegiatan bisnis lainnya. Tujuan dengan berkembangnya Fintech haruslah ditujukan untuk kemanfaatan bagi masyarakat melalui pemanfaatan teknologi.

Pada hakikatnya *Fintech* mewajibkan dilakukannya pendaftaran dan perolehan izin usaha dari Otoritas Jasa Keuangan, tetapi di dalam praktik banyak muncul aplikasi-aplikasi Fintech ilegal. Fintech yang ilegal ini sangat rentan menjadi instrumen *money laundering* dan *terrorist financing*. Hal ini memerlukan pengawasan atas keberadaan semua *Fintech* serta kontrol atasnya. Regulator harus dapat memaksa Fintech untuk tunduk pada rezim APU/PPT.

Fintech ini memadukan teknologi dengan fitur keuangan dengan model bisnis yang berbeda. Fintech tidak hanya meliputi sistem pembayaran, tetapi juga pemberian pinjaman, penyediaan modal, serta produk dan jasa finansial lainnya. Fintech jelas ditujukan untuk mempermudah pemenuhan kebutuhan masyarakat di dalam berbagai aspek tanpa harus bertatap muka, dan dengan proses yang lebih mudah. Namun demikian Fintech tidak terlepas dapat dijadikan sarana pencucian uang maupun pendanaan terorisme. Fintech sangat mudah, cepat dan dinamis. Industri ini sangat rentan disalahgunakan oleh para pelaku tindak pidana, secara khusus terkait di sini adalah pencucian uang dan pendanaan terorisme.

Karakteristik berupa kemudahan, kecepatan dan dinamisasi industri fintech, banyak bermunculan perusahaan *fintech* yang tidak terdaftar dan tidak berizin oleh OJK dan BI sesuai peraturan perundang-undangan yang berlaku. Pada prinsipnya, penyelenggara *Fintech Lending* harus mendapatkan tanda telah terdaftar sebelum memulai kegiatan operasional dan mengajukan izin dari OJK paling lambat satu tahun kemudian. Penyelenggara kredit fintech terdaftar dan/atau berlisensi dapat beroperasi maksimal satu tahun setelah menerima merek dagang terdaftar, setelah itu mereka harus mengajukan izin. Manakala *fintech lending* tidak mengajukan izin, maka penyelenggara harus mengembalikan nomor tanda daftarnya ke OJK. Merek berlisensi dari penyedia layanan pinjaman fintech yang disetujui tidak memiliki tanggal kedaluwarsa

[23] Ryan Randy Suryono, Indra Budi and Betty Purwandari, 'Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review' (2020) 11 Information (Switzerland) 1.

Pada kenyataannya, ketentuan tentang Fintech ini masih memiliki kelemahan dengan tidak dapat membendung kemunculan perusahaan fintech ilegal. OJK sendiri telah berkoordinasi dengan Kementerian Komunikasi dan Informatika, juga Satgas Waspada Investasi dengan menerbitkan informasi bahwa sejak awal tahun 2018 hingga September 2019 terdapat 1.350 operator fintech ilegal dan diblokir oleh Satgas Waspada Investasi.[24]

Kementerian Komunikasi dan Informatika memberikan penjelasannya bahwasanya banyak *Fintech* dari China yang menjadikan Indonesia sebagai sasaran empuk. Data OJK menunjukkan bahwa sebanyak 227 perusahaan *Fintech* peer-to-peer lending berstatus ilegal. Kemudahan untuk menemukan *Fintech* ilegal tersebut cukup dengan mengakses pada search engine Google, ataupun mengakses *play store* dan *app store*. Kemudahan *Fintech* China beroperasi di Indonesia tetapi ilegal tersebut sebenarnya dipicu oleh ketatnya kebijakan terkait *Fintech* di Negara China sendiri. Hal tersebut menyebabkan banyak perusahaan *Fintech* beroperasi di Indonesia dengan menggunakan dua atau tiga platform dalam bahasa Indonesia. OJK tidak dapat mengetahui profil *Fintech* ilegal tersebut, tetapi diyakini banyak memiliki member atau nasabah karena jumlah pengunduh aplikasi tersebut ribuan.[25] Selanjutnya, telah dijelaskan pada bagian sebelumnya, *fintech* ilegal rentan menimbulkan efek negatif, dan penyalahgunaan oleh penjahat terkait pendanaan terorisme, pencucian uang, maupun penyalahgunaan informasi berupa data pribadi.

Melalui Putusan Nomor 577/Pid.Sus/2020/PN.JKT.TIM dan Putusan Nomor 600/Pid.Sus/2020/PN.JKT.TIM yang terjadi di Indonesia terkait dengan penyalahgunaan Fintech untuk mendanai kegiatan terorisme, terdapat hal yang harus menjadi perhatian yaitu terkait dengan mekanisme penerapan CDD dan EDD atas nasabah. Hal tersebut dalam hal ini adalah pengajuan pinjaman. Ketentuan mengenai Pihak Pelapor ini hanya dimuat dalam hal pencucian uang, sementara pada pendanaan terorisme, belum dinyatakan secara tegas. Namun demikian rezim APU/PPT sebenarnya merupakan rezim yang saling menyatu, sekalipun akan selalu memungkinkan terjadinya perbedaan pendapat pada bagaimana hukum harus beranjak dan berakhir, apakah hanya memperhatikan kepastian hukum, kemanfaatan hukum, ataukah keadilan hukum.

[24] www.ojk.go.id FAQ *Fintech* Lending, diakses pada 12 Desember 2022, pukul 22.00 WIB
[25] *Fintech* China tumbuh subur di Indonesia, diakses dari https://www.kominfo.go.id/content/detail/13681/*Fintech*-china-serbu-indonesia/0/sorotan_media

Pendapat dan pandangan tersebut tidak akan mungkin dapat diakhiri sekalipun para ahli hukum tidak selalu membedakan begitu saja.

Fintech menjadi salah satu instrumen dan solusi baru bagi perusahaan-perusahaan dan konsumen, seperti kredit Online, platform trading, dan juga berbagai *Artificial Intelligent* lainnya. Fintech sebagai salah satu perkembangan teknologi akan diikuti pula dengan risiko, yang pastinya memerlukan pengaturan baik berupa perundangan maupun kebijakan yang bersifat khusus, dan harus mampu memitigasi risiko. Pembuat peraturan dan kebijakan mengidentifikasi risiko utama bagi penyedia layanan *Fintech* tersebut, dan harus memperlengkapi dengan kerangka aturan yang kuat. Salah satu kelemahannya yang kemudian dapat diidentifikasi adalah bahwasanya layanan Fintech masih memiliki celah dieksploitasi sebagai alat/instrumen melakukan tindak pidana.

Fintech memiliki risiko sebagai target kejahatan siber (*cybercrime*), yang dapat dipandang sebagai hasil dari perkembangan teknologi sendiri. Pembayaran melalui *mobile (mobile payments)* menimbulkan kerentanan atas *data breaches* dan masalah keamanan jaringan *(network security)*. *Fintech* juga berisiko rentan atas *Fraud* dan pencucian uang mengingat jumlah pembayaran yang sangat besar dan banyak, serta ekspansi yang sangat cepat. *Fintech* menjadi sangat berisiko secara signifikan atas keterlibatan *financial crimes*. Cara yang efektif untuk memitigasi risiko adalah dengan menerapkan program kepatuhan APU/PPT. Oleh karenanya, kepatuhan yang ketat atas program APU/PPT perlu diterapkan.

b. Digital Currency

Permasalahan mengenai *digital currencies* dan/atau *cryptocurrencies* membawa dampak pada eksistensi uang dan sistem pembayaran yang selama ini dilaksanakan oleh suatu negara. Sistem pembayaran meliputi pemahaman mengenai berbagai kerangka aturan, kelembagaan, serta mekanisme di dalam proses pemindahan dana, instrumen-instrumen pembayaran, mulai dari proses kliring sampai dengan penyelesaian akhir. Terkait dengan kelembagaan maka Bank Indonesia selaku lembaga yang memiliki kewenangan atas pengaturan sekaligus menjaga kelancaran pelaksanaan sistem pembayaran di Indonesia, menentukan lembaga-lembaga lainnya.

Pelaksanaan kebijakan sistem pembayaran harus memperhatikan berbagai aspek, dengan salah satunya adalah terkait masalah melindungi konsumen. Permasalahan mengenai *virtual (digital) currency* banyak dikaitkan dengan ketiadaannya untuk memberikan kepastian mengenai perlindungan bagi konsumen, sebagaimana dinyatakan oleh Bank Indonesia di dalam pernyataan pers sebagaimana disebut sebelumnya.

Risiko *money laundering* di dalam sistem keuangan yang modern *(modern financial systems)* sangat besar. Suatu sistem finansial yang semakin modern rentan memunculkan kemungkinan tereksploitasi oleh para penjahat. John McDowell memberikan penekanan bahwasannya di dalam suatu sistem finansial yang canggih, penjahat dapat dengan mudah memberikan perintah transfer jutaan dolar secara instan melalui akses komputer dan satelit. Sementara penjahat dapat memilih untuk mencuci uang sepenuhnya berdasarkan kreativitasnya sendiri, juga bergantung pada jenis operasional dan sistem finansial yang ada.[26]

Terkait dengan ancaman dari keberadaan *new payment* tersebut, *money laundering* atau pencucian uang menjadi salah satu macam kejahatan yang akan mendapatkan kesempatan untuk semakin berkembang. *The Financial Action Tasks Force Recommendation* Tahun 2012 dengan update terakhir pada Maret 2022 (FATF), Rekomendasi 15 yang terkait dengan bagaimana negara harus melakukan identifikasi dan penilaian atas risiko pencucian uang dan pendanaan terorisme atas perkembangan *New Products and new business practices*, yang termasuk di dalamnya adalah masalah *delivery mechanism* yang baru, serta penggunaan teknologi baru maupun yang berkembang.[27] Pada intinya rekomendasi 15 menjelaskan:

- Setiap negara dan Lembaga keuangan harus melakukan identifikasi dan menilai risiko pencucian uang dan pendanaan terorisme yang mungkin muncul karena:
    - Perkembangan praktik bisnis dan produk-produk baru, termasuk juga adalah mekanisme baru terkait dengan proses pengirimannya;
    - Penggunaan teknologi baru maupun perkembangannya, maupun produk-produk yang sudah ada sebelumnya.

[26] John Mc Dowell and Gary Novis, ***'The consequences of Money Laundering and Financial Crime'***, Economic Perspective: The Fight Against Money Laundering. Electronic Journal of the Office of International Information Program (IIP), U.S Department of State, 2001, p. 5

[27] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' [2012] FATF, Paris, France 1 <www.fatf-gafi.org/recommendations.html>.

- Lembaga keuangan harus mengambil tindakan yang tepat untuk mengelola dan memitigasi risiko yang muncul. Oleh karenanya penilaian atas risiko harus ditempatkan paling utama terkait dengan diluncurkannya produk-produk baru, praktik-praktik bisnis baru, maupun teknologi baru dan perkembangannya.
- Negara-negara juga harus memastikan bahwa *Virtual Asset Service Providers (VASP)* telah diregulasikan sesuai dengan tujuan APU/PPT, harus memiliki lisensi atau teregistrasi. VASP juga terikat pada sistem monitoring dan memastikan tingkat kepatuhan yang relevan dengan Rekomendasi-rekomendasi FATF. Hal ini dimaksudkan sebagai upaya untuk mengelola dan memitigasi risiko yang muncul karena VASP.

Pada hakikatnya, Rekomendasi FATF sudah memberikan penekanan-penekanan pada munculnya *New Technology* yang menjadi *threat* bagi rezim APU/PPT. Terkait dengan dieksploitasinya teknologi oleh penjahat, telah banyak kasus yang terjadi. Sinergitas pencuci uang dan kejahatan dunia maya dilihat dari adanya virus Wannacry yang eksis pada tahun 2017, dan menggunakan yang tebusan yang diminta dalam bentuk bitcoin.

Terkait dengan pencucian uang dan teknologi ini, M. Arief Amrullah menambahkan bahwasanya tidak dipungkiri bahwa pencucian uang telah menjadi salah satu kegiatan utama dari organisasi kriminal internasional yang mencari keuntungan.[28] Nahid Joveda et.al juga menegaskan kemajuan teknologi dan globalisasi keuangan memudahkan dilakukannya transfer uang secara ilegal, dan dalam hal inilah muncul istilah *cyber laundering*.[29] Hasil yang diperoleh secara ilegal tersebut diletakkan pada sistem keuangan global sehingga muncul sebagai hasil yang sah. Pelaku *Cyber laundering* ini memanifestasikan dirinya dalam sistem pembayaran baru, yang pengembangannya menggunakan teknologi yang terintegrasi dengan pasar dan sistem finansial. Bruce Nikkel[30] menggunakan istilah *online money laundering*, dengan memberikan penjelasan yang intinya *Once funds are stolen, criminals hire money transfer operators to cover their tracks and launder money… In hopes of part-time work, financial intermediaries hire as mules through online job portals or spam*

[28]Arief Amrullah, Tindak Pidana Pencucian Uang Money Laundering: Reorientasi kebijakan Penanggulangan dan Kerjasama Internasional. Malang, Bayumedia Publishing, 2004, hlm. 32

[29] Nahid Joveda, Md Tarek Khan and Abhijit Pathak, 'Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of Financial Information' (2019) 11 International Journal of Economics and Finance 54.

[30] Bruce Nikkel, 'Fintech Forensics: Criminal Investigation and *Digital* Evidence in Financial Technologies' (2020) 33 Forensic Science International: *Digital* Investigation 1.

campaigns. It will be... if the money is stolen, it will be transferred to a mule account and expected to withdraw cash and keep the agreed portion. Transfer the rest to another recipient (usually via a cash transfer service).

Salah satu pendekatan rezim anti pencucian uang adalah mengembangkan kepatuhan melalui pihak yang dikenal sebagai pihak pelapor anti pencucian uang. Bank Indonesia yang masih melarang semua jenis *virtual currency* tidak menguntungkan dalam hal anti pencucian uang, karena masyarakat justru sangat antusias terhadap penggunaan berbagai *virtual currency*.

Munculnya berbagai istilah juga sangat mempengaruhi bagaimana kebijakan negara di dalam merespon mengenai keberadaan dan urgensi mata uang yang dikeluaran oleh bank sentral itu sendiri. Penggunaan istilah mengenai *Cryprocurrencies* dan *digital currency* harus dipertegas, walaupun di dalam praktik selama ini dipergunakan dengan persamaan makna lebih jauh sebagai *virtual currency*. Kemunculan *bitcoin* telah memotong keseluruhan sistem finansial secara global dengan sebuah digital, jaringan pembayaran yang tidak dapat dipercayai *(trustless)*, tetapi *Bitcoin* memberikan kekuasaan seseorang untuk menyimpan, mengirim, dan menerima uang melampaui waktu, ruang, dan skala.

Tentu saja, setiap mata uang digital memiliki kekuatan dan kelemahan, tetapi setiap mata uang digital dapat memiliki kelemahan dan kekuatan. Beberapa isu tersebut antara lain apakah ada pihak yang bertanggung jawab terhadap negara, bagaimana bertindak jika terjadi kesalahan atau pembatalan, masalah kerahasiaan, data yang diretas atau pengiriman data dalam sistem tersebut, kerentanan terhadap penipuan.

Pada setiap perkembangan pasti diikuti risiko. Namun demikian, karena perkembangan yang semakin global dan tingkat ancaman kejahatan yang semakin kompleks, negara harus mempertimbangkan dan memutuskan apakah akan berpartisipasi atau tidak dalam mengatur, apakah akan melanjutkan perkembangan atau menolaknya. *Cryptocurrency*, mata uang digital, atau mata uang virtual, ataupun mata uang lainnya yang akan muncul sudah berada pada tahap yang tidak dapat diabaikan melalui melakukan pelarangan saja. Hal ini disebabkan karena keberadaan mata uang-mata uang dan perkembangannya tersebut dirasakan menguntungkan penggunanya.

Ketiadaan otoritas yang bertanggung jawab atas mata uang virtual bukan satu-satunya aalasan dibalik pelarangan oleh Bank Indonesia. Larangan yang dilakukan

didasari oleh ketiadaan *underlying asset* yang menjadi dasar penentuan harga *virtual currency*. Harga mata uang virtual sangat fluktuatif sehingga tidak dapat dijadikan sebagai acuan untuk menentukan nilai konversi mata uang tersebut. Hal tersebutlah yang menimbulkan kerentanan atas risiko nilai yang menggelembung, dan dapat digunakan sebagai alat pencucian uang dan pendanaan teroris. Bank Indonesia melarang penggunaan virtual currency sebagai alat pembayaran atau tidak diakui sebagai mata uang di Indonesia dikarenakan ketidakjelasan penyedia jasa yang bertanggung jawab atas *virtual currency* tersebut. Atas hal tersebut, Bank Indonesia akan meluncurkan Digital Rupiah sebagai *Central Bank Digital Currency*.

c. Digital Onboarding

Adanya migrasi ke arah *digital* membawa konsekuensi perubahan yang dapat menimbulkan kesulitan bagi masyarakat sebagai pengguna *digital* itu sendiri. Masyarakat sebagai pengguna belum mengetahui bagaimana cara menyikapi segala transisi kehidupan yang sudah menjadi *digital* ini Salah satu aspek terbesar yang harus segera melakukan penyesuaian atas migrasi secara *digital* adalah dunia perbankan (dan lembaga keuangan). Terkait hal ini, Miren Karmele (2022) menambahkan pendapat yang pada hakikatnya menyatakan: *"In recent years, the financial sector has been experiencing a digital revolution in which traditional institutions have seen the need to become digital service providers in order to remain competitive. This process of digital transformation is driving not only the development of new products and services, but also the progress and implementation of the very technology that supports them and which also enables innovation in the development of customer interaction with financial entities"*[31]. Hal tersebut memang menunjukkan bahwasanya sektor keuangan merupakan salah satu jalan paling cepat untuk melihat migrasi digital.

Perubahan pola hidup di dalam masyarakat, terkait secara khusus adalah dalam hal penggunaan teknologi informasi dan *gadget*, terus mendorong masyarakat untuk menyesuaikan dengan perubahan yang terjadi. Perubahan tersebut meliputi berbagai aspek sektor kehidupan, usaha, serta layanan yang dilakukan oleh sektor keuangan dan ekonomi, salah satunya adalah transaksi keuangan non tunai. Saat ini di Indonesia telah muncul layanan yang disebut dengan Layanan Keuangan *Digital* (LKD). LKD tersebut merupakan aktivitas pemberian layanan di sektor jasa sistem pembayaran yang

[31] Miren Karmele García and others, '*Digital* Onboarding in Finance: A Novel Model and Related Cybersecurity Risks' (2022) 1 Open Research Europe 149.

mempergunakan teknologi yang berbasis mobile dan web, serta jasa pihak ke tiga. LKD diharapkan dapat memberikan manfaat kepada masyarakat untuk lebih mudah berbelanja online, termasuk transfer uang sehingga menjadi lebih cepat dan nyaman. Transfer uang melalui LKD ini mempersingkat waktu karena *customer* tidak perlu untuk mendatangi kantor secara fisik untuk melakukan transaksi-transaksi yang diperlukan. LKD ini dikenal sebagai layanan keuangan inklusif. Berbagai layanan keuangan *digital* menunjukkan adanya peningkatan akseptasi dan preferensi masyarakat untuk melakukan belanja secara daring, mengakui kemudahan sistem pembayaran *digital*, sekaligus akselerasi perbankan secara daring.

Laporan Bank Indonesia mencatat nilai transaksi perbankan digital meningkat 38,38% menjadi Rp. 5.184,1 Triliun pada Oktober 2022. Pada saat yang sama, nilai transaksi elektronik juga meningkat sebesar Rp. 20,19% menjadi Rp. 35,1 triliun pada tahun yang sama.[32] Dengan data tersebut, masyarakat sudah mendukung sepenuhnya akan penggunaan layanan *digital banking* tersebut, sekaligus menunjukkan bahwa sektor keuangan *digital* memiliki arti kehadiran sebagai platform keuangan digital yang dapat mendukung percepatan dan pemulihan ekonomi negara.

Untuk mencapai pertumbuhan yang kuat melalui berbagai perkembangan dan inovasi keuangan digital, dengan didukung oleh ekosistem keuangan dan keuangan digital yang berdaya bersaing, serta mengikuti perkembangan teknologi, Pemerintah Indonesia terus mengembangkan industri fintech dan ikut mendorong ekonomi digital sambil melakukan imovasi layanan, termasuk *digital onboarding*. Pemerintah juga terus mewujudkan kepastian dan pemberian perlindungan hukum, termasuk jaminan keamanan siber.

Digital onboarding tidak sama dengan layanan *mobile banking* pada umumnya. *Digital onboarding* mengacu pada proses pengajuan pembuatan rekening melalui website ataupun aplikasi telepon genggam. Hal tersebut berarti bahwa semenjak pembuatan rekening baru, atau deposito, investasi, dan lain-lain termasuk di dalamnya *Top up e-wallet* maupun *e-money* yang dapat dilakukan dengan *digital onboarding*. Hal tersebut memudahkan karena nasabah tidak harus datang ke bank. Keamanan sistem layanan *digital onboarding* juga semakin memberikan rasa aman kepada penggunanya,

[32] CNN Indonesia "Nilai Transaksi *Digital* Banking Tembus Rp5.184,1 T pada Oktober 2022", diakses dari https://www.cnnindonesia.com/ekonomi/20221117164404-78-875191/nilai-transaksi-*digital*-banking-tembus-rp51841-t-pada-oktober-2022 pada tanggal 10 Januari 2023

kecuali data yang masih relatif rentan disalahgunakan. Pada *digital onboarding* menggunakan sistem keamanan dengan sidik jari maupun *faceID*. Teknologi *digital onboarding* meminimalisir proses yang panjang, rumit, dan lama karena juga harus antri di bank.

Selain keuntungan yang diberikan oleh *digital onboarding*, terdapat pula tantangan dan ancaman yang dimunculkan. Terkait dengan *threat* dan *challenges* dengan adanya *Digital Onboarding* ini, Varun Mittal et.al menjelaskan bahwasanya tantang yang dihadapi oleh lembaga keuangan terkait *onboarding* adalah:

- *Time-consuming process leading to poor consumer experience*
- *Resource intensive*
- *Geographically inconvinient*
- *Limited customer outreach and engagement*
- *Need for physical offices for operators and customer services*
- *Identifying fraud and security risks*.[33]

Penekanan yang dapat digarisbawahi terkait dengan munculnya kejahatan adalah pada permasalahan penipuan pada saat proses identifikasi dan risiko keamanan. Reza Soltani dan Uyen Treng Nguyen[34] menegaskan proses KYC *(Know Your Customer)* dalam hal *onboarding* ini sebagai*: the process of having financial institutes engage with their prospective clients to verify the customer's identity. Through this process, financial organizations obtain better insight about their clients, and establish a rapport by which they gain a better understanding of how their clients' funds are obtained, accessed and withdrawn. KYC is a necessary process to prevent money laundering and terrorism financing.* KYC merupakan proses yang penting di dalam upaya mencegah pencucian uang dan pendanaan teroris. Pihak PJK ataupun lembaga keuangan harus memastikan klien, dan melakukan verifikasi. KYC ini harus ditaati dan dipatuhi oleh seluruh pihak pelapor, sekaligus memitigasi risiko. KYC menjadi sangat relevan bila dikaitkan dengan berbagai perbuatan hukum baru yang terjadi di ruang maya.

Lebih lanjut, Bank Indonesia merilis *Blueprint* Sistem Pembayaran Indonesia (BPSI) 2025, yang pada intinya menekankan bahwasanya digitalisasi telah menghadirkan model dan pemain baru, serta mengubah perilaku konsumen, juga

[33] Arab Monetary Fund, '*Digital* Customer On-Boarding, e-KYC and *Digital* Signatures'.
[34] Reza Soltani, 'Self-Sovereign Identity and Distributed Ledger' [2018] 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) 1129.

lanskap ekonomi dan keuangan. Model bisnis yang baru tersebut menekankan pada keramahan bagi pengguna, sehingga dengan cepat diterima oleh publik. Kemunculan pemain baru juga mulai mengubah kondisi industri, sehingga model bisnisnya terjadi transformasi digital. Hal ini menjadi pilihan yang strategis bagi perusahaan mampu berhadapan dengan konsumen yang menuntut layanan baru yang cepat, mudah, dan terjangka di platform digital. Digitalisasi juga membawa paradigma baru dalam kaitannya dengan data, yang tidak hanya dilihat sebagai inisiator inovasi dan efisiensi, tetapi juga sebagai kontribusi penting dalam proses produksi barang dan jasa. Perubahan mendasar ini menghadirkan tantangan politik, yaitu menemukan keseimbangan antara mengoptimalkan peluang inovasi digital dan memitigisi risiko baru.[35] Dengan demikian perubahan tatanan akibat inovasi digital telah mengubah proses interaksi yang lebih berorientasi pada demokratisasi ekonomi dan bertujuan untuk meningkatkan efisiensi dengan meningkatkan akses dan kapasitas eksploitasi pelaku ekonomi.

Setiap perkembangan selalu diikuti dengan adanya risiko dan tantangan. Bank Indonesia[36] menambahkan beberapa hal sebagai berikut:

- Munculnya *shadow banking*. Risiko ini muncul ketika industri perbankan tidak diatur dan diawasi secara memadai. Risiko ini berdampak negatif terhadap stabilitas sektor keuangan.
- Teknologi *digital* terancam oleh impor besar-besaran, khususnya barang konsumsi, risiko dunia maya, bentuk penipuan, persaingan tidak sehat, juga penyalahgunaann data milik konsumen.
- Persoalan kedaulatan ekonomi dan sulitnya melindungi kepentingan nasional yang menjamin kesinambungan ekonomi jangka panjang, menjadi problematis karena model bisnis digital yang bersifat tidak terbatas *(borderless)*.
- Adanya risiko dari segelintir pihak yang menguasai informasi berpotensi menyebabkan gangguan pasar dan membatasi kemampuang untuk mengintegrasikan layanan dan produk, yang dapat menghambat inklusi ekonomi dan keuangan.

[35] Departemen Komunikasi, 'Inovasi Untuk Integrasi Ekonomi Keuangan *Digital*' (2020) 7 Laporan Perekonomian Indonesia 2019 1292.
[36] ibid.h.101

- Salah satu tantangan yang muncul adalah adanya persyaratan bahwa otoritas publik harus mampu menyeimbangkan kegiatan inovasi dengan tindakan untuk memitigasi risiko.

Salah satu upaya untuk mendukung keuangan *digital* yang kondusif diperlukan penyelarasan dan penguatan regulasi dan peraturan hukum. Sebagai suatu otoritas sistem pembayaran, Bank Indonesia juga mendorong pertukaran informasi yang setara antara Bank dengan fintech melalui sistem open banking. Pendekatan ini dilakukan untuk mendorong transformasi digital sektor perbankan secara keseluruhan dan membangun hubungan antara bank dan fintech. Dengan demikian, *Fintech* juga harus melaksanakan keterbukaan data demi terwujudnya kolaborasi yang akan memenuhi kebutuhan konsumen. Penekanan yang harus dilakukan adalah bagaimana kolaborasi tersebut tidak membahayakan data konsumen yang menjadi ancaman terbesar sampai hari ini yaitu terkait dengan masalah perlindungan data.

Masalah perlindungan data sendiri telah diatur oleh negara melalui Undang Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang diundangkan pada 17 Oktober 2022, dan dinyatakan berlaku semenjak 17 Oktober 2022 (disebut sebagai UU PDP). Secara filosofis, undang-undang ini diletakkan pada adanya pengakuan bahwasanya Perlindungan data pribadi adaah hak asasi semua orang. Oleh karena itu, Pemerintah Indonesia harus membuat landasan hukum untuk melindungi data pribadi berdasaran undang-undang Dasar Republik Indonesia Tahun 1945. Pengundangan UU ini tidak menafikan adanya peranan perkembangan teknologi informasi dan komunikasi yang semaking berkembang dengan pesat tersebut telah memberikan peluang sekaligus tantangan bagi pelaksanaan hukum itu sendiri. Permasalahan ini sendiri telah diatur dengan berbagai regulasi, namun demikian perlu diatur dalam aturan tersendiri, dalam hal ini UU PDP guna meningkatkan implementasi perlindungan data pribadi di Indonesia. Tantangan yang dimunculkan perkembangan digitalisasi ini sekaligus memunculkan berbagai macam *threat*, termasuk di dalamnya masalah data. Pada era digitalisasi ini, data telah menjadi *new oil* yang kemudian dipergunakan untuk akselerasi dan integrasi sistem ekonomi dan keuangan *digital* sebagaimana telah dijelaskan pada bagian sebelumnya. Selain data, *threat* lain yang muncul adalah risiko atas serangan siber.

3. *Cyber laundering*: Permasalahan hukum yang dihadapi

Pencucian uang telah berkembang dengan sangat cepat. Pencucian uang menjadi salah satu tujuan penjahat di dalam menyembunyikan hasil kejahatannya. Pada prinsipnya pelaku harus berusaha menyamarkan atau mengaburkan atau menyembunyikan asal usul harta kekayaan hasil kejahatannya. Cara ini membuat pelacakan aset menjadi sulit atau tidak mungkin dilakukan oleh penegak hukum. Go Lisanawati (2018) menjelaskan bahwasanya tindak pidana pencucian uang adalah luas dan rumit prosesnya. Penanda karakteristik tindak pidana pencucian uang pada hakikatnya meliputi upaya *Placement, Layering, dan Integration*, yang dilakukan dengan bentuk kesalahan berupa kesengajaan (baik yang meliputi pengetahuan, menghendaki, maupun menjadikan sebagai tujuan) agar orang dan/atau aparat penegak hukum tidak mengetahui bahwa harta itu dihasilkan dari kejahatan.[37] Pencucian uang merupakan proses yang sangat rumit dan berlapis-lapis, dan dilakukan dengan berbagai cara demi satu tujuan yaitu membuat supaya uang hasil kejahatan yang dilakukannya tampak seolah-olah bukan merupakan hasil kejahatan.

Cyber laundering dapat dimaknai oleh Asset Arthadik[38] sebagai *a combination of the use of computer technology and criminal money laundering itself. The process of moving, transforming, or taking some action on an asset. Questions are obfuscated while cyber focuses on the culture of computers, information technology, and virtual reality. Cyber laundering* pada hakikatnya merupakan penetrasi teknologi *(cyber)* yang bermanfestasi menjadi sarana kejahatan *(crime)*, dan secara khusus kejahatan siber tersebut dieksploitasi untuk melakukan kegiatan pencucian uang *(money laundering)*. Terminologi *cyber laundering* ini juga banyak yang menyebut sebagai *electronic money laundering*, yang dewasa ini banyak merujuk pada perkembangan digitalisasi terkait dengan munculnya *digital assets, crypto currencies, virtual currencies, financial technology*, dan beberapa hal lain, yang secara khusus ditujukan untuk melakukan kegiatan pencucian uang. Lebih lanjut, Alessio Faccia et al mengemukakan poin penting terkait dengan *electronic money laundering*, yaitu bahwasanya *cryptocurrency exchanges take place on unregulated platforms and many thefts occur without users being able to defend their rights.* Lebih lanjut ditambahkan bahwa *on the subject of*

[37]Go Lisanawati. 2018. Eksistensi dan Peranan Lembaga Pengawas dan Pengatur (LPP) dalam Rezim Anti Pencucian Uang, Yogyakarta: Graha Ilmu, 13.

[38] Asset Arthadik. "Cyber Laundering: Risk and Future Threats of Virtual Currency in Indonesia" in Tackling Financial Crimes: Various International Perspectives. 2017. Yogyakarta: Genta Publishing 314

money laundering, the untraceability of cryptocurrencies has made possible the movement of dubious assets targeted by authorities. Exchange channels allow bypassing approved financial intermediaries and transaction are become not secure.[39] Penekanan yang diberikan oleh Alessio Faccia tersebut adalah pada kemunculan *cryptocurrencies* dengan sifat anonim-nya yang menjadi incaran pencuci uang di dalam melakukan pencucian uang. Helen Tunnicliffe menambahkan pada ekploitasi Fintech oleh Pencucian uang yaitu: *"Fintechs, by their very nature, are not encumbered by legacy systems. They are generally more streamlined and less complex in terms of their operations, products and services and therefore should be able to quickly implement cutting edge solutions to combat growing fraud and money laundering."*[40]

Pencucian Uang merupakan tindak pidana yang sulit dipahami mengingat sifat dan batasannya yang masih abstrak, terlebih pula mengenai eksistensinya. Pencucian Uang juga telah dipahami sebagai suatu tindak pidana yang berdiri sendiri *(Sui Generis)*, sekalipun dalam pemahamannya tindak pidana pencucian uang adalah sebagai suatu *proceeds of crime* suatu tindak pidana asal.

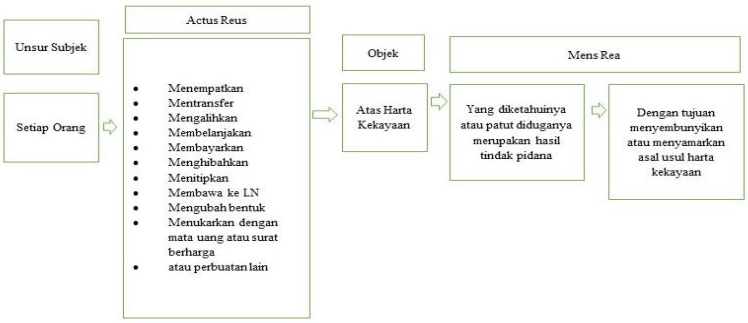
Pencucian uang didefinisikan oleh Undang Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (selanjutnya disebut sebagai UU Pencucian uang) sebagai: "segala perbuatan yang memenuhi unsur-unsur tindak pidana sesuai dengan ketentuan dalam Undang-Undang ini" (Pasal 1 angka 1 UU Pencucian Uang).

Pencucian Uang memiliki 3 (tiga) element penting sebagaimana dikemukakan oleh Stephen R. Kroll[41], yaitu: Perbuatan (*act*), yang meliputi beberapa perbuatan atas aset atau property; Pengetahuan (*knowledge*) bahwa aset atau properti tersebut dihasilkan dari satu atau lenih jenis kegiatan *underlying criminal*; Tujuan (*objective*), pencucian uang selalu bertujuan untuk mengaburkan asal usul aset yang berasal dari kegiatan kriminal.

Ketentuan Pasal 3 sampai dengan Pasal 5 ayat (1) UU PPTPPU kemudian mengatur mengenai kriminalisasi pencucian uang, yang kemudian dikenal sebagai delik utama pencucian uang. Secara skema dijelaskan delik utama pencucian uang sebagaimana dikriminalisasikan dalam UU Pencucian Uang, Pasal 3:

[39] Alessio Faccia and others, 'Electronic Money Laundering, the Dark Side of Fintech: An Overview of the Most Recent Cases' [2020] ACM International Conference Proceeding Series 29.
[40] Helen Tunnicliffe, 'On the Frontline' [2011] Chemical Engineer 52.
[41] J.E. Sahetapy. "Business" Uang Haram (2003), paper, 2

Skema 1: Pasal 3 UU Pencucian Uang



Ketentuan Pasal 3 UU Pencucian Uang hanya dapat dilakukan oleh pelaku *initial crime* sebagaimana diatur di dalam Pasal 2 UU Pencucian Uang, yang sekaligus menjadi melakukan pencucian uang. Ketentuan Pasal 3 ini dikenal dengan Tindak Pidana Pencucian Uang aktif.

Kriminalisasi selanjutnya adalah dalam Pasal 4, yang merupakan tindak pidana pencucian uang aktif, tetapi pelaku bukanlah pelaku *initial crime*. Namun pihak-pihak ini memfasilitasi terjadinya tindak pidana pencucian uang. *Mens Rea* di dalam Pasal 4 ini jelas adalah suatu kesengajaan. Secara skema, dijabarkan Pasal 4 sebagai berikut:

Skema 2: Pasal 4 UU Pencucian Uang

Pasal 5 ayat (1) UU PPTPPU dibedakan secara hakikat dari ketentuan Pasal 3 dan Pasal 4. Pasal 5 ayat (1) ini dikenal sebagai bentuk tindak pidana pencucian uang pasif, mengingat pasal ini memberikan larangan kepada orang-orang yang di dalam kategorinya secara pasif menerima atau menguasai atas penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan. Namun demikian mengenai *mens rea*, tetap dikehendaki suatu konstruksi kesengajaan, dalam bentuk yang diketahuinya atau patut diduganya merupakan hasil

tindak pidana. Ketentuan Pasal 5 ayat (1) ini memunculkan kesulitan untuk dipahami dan diterima secara akal sehat, tetapi sesungguhnya tetap dapat dijelaskan secara akal sehat atas hal-hal yang *upnormal* yang tidak boleh diterima sebagai sesuatu yang dinormalkan. Atas ketentuan Pasal 5 ayat (1) ini harus tetap diberikan rambu-rambu dan konstruksi penerapan pasalnya yang objektif dan *reasonable*. Tidak perlu dipertentangkan, tetapi tetap harus dipahami bahwa undang-undang pencucian uang ini juga justru ingin melindungi yang tidak bersalah, dan memberikan keadilan serta kepastian dan kemanfaatan hukum sebagaimana dirumuskan sebagai tujuan hukum. Lebih lanjut Pasal 5 tersebut dapat dipahami melalui skema sebagai berikut:

Skema 3: Pasal 5 UU Pencucian Uang

Ketentuan Pasal 5 ayat (1) UU Pencucian Uang ini sangat krusial karena setiap orang diberikan standar untuk dapat mengetahui atau patut menduga bahwasanya harta kekayaan yang diterima atau dikuasainya karena penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan atas harta kekayaan tersebut bukanlah harta kekayaan yang berasal dari tindak pidana. Hukum mengharuskan setiap Orang mengetahui atau paling tidak patut menduga sebelum menerima atau menguasai atau menggunakan harta kekayaan yang ditempatkan, ditransfer, dibayarkan, dihibahkan, disumbangkan, dititipkan, atau ditukarkan. Namun demikian sesungguhnya UUPPTPPU tetap memiliki ditujukan untuk memberikan perlindungan kepada korban ataupun *potential victim*. Hukum harus ditujukan untuk kesejahteraan manusia dan hukum adalah untuk manusia. Secara limitatif, Pasal 5 ayat (1) UU PPTPPU tidak berlaku bagi Pihak Pelapor telah melaksanakan kewajiban

pelaporan sebagaimana ditentukan oleh UU PPTPPU. Dengan demikian kewajiban pelaporan menjadi salah satu indikator untuk melepaskan diri dari tanggung jawab atas risiko penerapan Pasal 5 ayat (1) UU PPTPPU.

Dalam konsep hukum anti pencucian uang, pelaku dan hasil tindak pidana dapat diketahui melalui penelusuran, dan selanjutnya akan dilakukan perampasan oleh negara, dan dikembalikan kepada yang berhak. Penelusuran Harta Kekayaan hasil tindak pidana pada umumnya dilakukan oleh lembaga keuangan, yang dalam hal ini memiliki peranan khusus untuk menerapkan Prinsip Mengenali Pengguna Jasa (PMPJ), dan melaporkan Transaksi-transaksi yang memenuhi indikator-indikator sebagaimana ditentukan oleh Undang-Undang kepada Otoritas *(Financial Intelligence)*, dalam hal ini adalah PPATK melalui Lembaga Pengawas dan Pengatur (LPP).

UU PPTPPU memberikan indikator pencucian uang berdasarkan Transaksi Keuangan Mencurigakan (TKM), Transaksi Keuangan Tunai (TKT), dan Transaksi Keuangan Transfer Dana dari dan ke luar negeri (TKTD). Mengenai Transaksi Keuangan Mencurigakan, terdapat 4 hal sebagai berikut:

- Transaksi keuangan yang berbeda dengan profil, karakteristik, atau pola transaksi yang biasa dilakukan pengguna jasa yang bersangkutan;
- Transaksi keuangan yang dilakukan oleh pengguna jasa yang diduga wajar telah terjadi, untuk menghindari pelaporan transaksi yang relevan, yang harus dipatuhi oleh pihak pelapor;
- Transaksi keuangan yang dilakukan atau dibatalkan dengan menggunakan Harta kekayaan yang diduga berasal dari hasil tindak pidana; atau
- Transaksi keuangan yang dimintakan kepada pihak pelapor untuk dilaporkan pada PPATK karena menyangkut harta kekayaan yang diduga hasil tindak pidana.

Selain TKM terdapat juga TKT sebagai indikator pencucian uang. TKT ini merupakan transaksi dengan menggunakan uang kertas maupun uang logam (vide Pasal 1 angka 6 UU Pencucian Uang). Berdasarkan hal ini, uang masih terbatas bentuknya yaitu dalam bentuk uang kertas ataupun logam. Selanjutnya adalah TKTD yang berupa kegiatan transfer dari dan ke luar negeri termaktub di dalam ketentuan Pasal 23 UU Pencucian Uang, yang tentu saja mengenai transfer dana tunduk pada aturan Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana. Dengan demikian hakikat pencucian uang

itu dilakukan atas sebuah transaksi. Transaksi ini yang akan memunculkan hubungan hukum dan memunculkan hak dan kewajiban antara dua pihak atau lebih.

Tindak Pidana Pencucian Uang sendiri berkembang dengan sangat meluas. N.H.T Siahaan menjelaskan mengenai sifat pencucian uang, yang intinya karena pencucian uang merupakan salah satu aspek kejahatan yang dihadapi oleh individu, bangsa dan negara, maka sifat pencucian uang menjadi universal dan melampaui batas yurisdiksi negara sehingga permasalahannya tidak hanya bersifat nasional tetapi juga regional, serta internasional. Pencucian uang dapat dilakukan seseorang tanpa harus bepergian ke luar negeri. Hal ini dapat dicapai melalui perkembangan teknologi informasi di dunia maya, di mana pembayaran dapat dilakukan melalui elektronik *(cyber payment)*.[42]

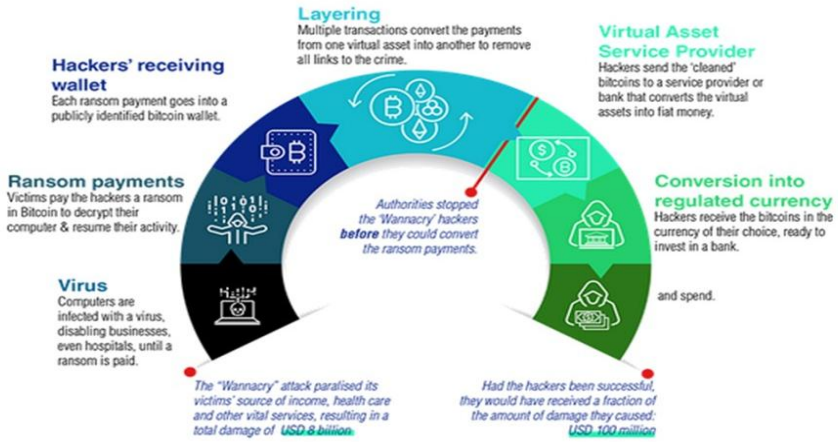
Selanjutnya Christoph Wronka[43] memberikan penekanannya bahwasannya with *a new era of technological advancement, it was only a matter of time before criminals started using the internet for money laundering purposes. This criminal money laundering practices in cyberspace known as cyber-laundering*. Hal tersebut menandakan bahwa kemajuan teknologi hanyalah sebagai *trigger* atas kemunculan tujuan pencucian yang lebih canggih untuk menghindari deteksi oleh penegak hukum. Internet memungkinkan tercapainya hal tersebut. Hal ini yang kemudian disebut dengan *Cyber laundering.*

Permasalahan-permasalahan perkembangan teknologi membawa permasalahan-permasalahan kompleks dalam penegakan hukum, khususnya penegakan hukum atas tindak pidana pencucian uang yang menggunakan kemajuan teknologi informasi, dan berbagai *emerging threat*-nya. Penyidik harus memiliki kemampuan bagaimana memperoleh bukti-bukti elektronik untuk menguji kasus-kasus yang harus disidiknya, bagaimana menggunakan analisis forensik untuk merespon agar permasalahan *criminal justice* dapat terus direspon dengan baik. Penyidik perlu memahami mitigasi risiko atas praktik-praktik *cyber laundering (electronic money laundering practices)*. Fithriadi Muslim dari PPATK dalam presentasinya menjelaskan tiga area yang menjadi prioritas perhatian PPATK terkait dengan 3 praktik *electronic money laundering*[44], sebagai berikut:

[42] N.H.T Siahaan. 2008. Money Laundering dan Kejahatan Perbankan. Jakarta: Jala 3.
[43] Christoph Wronka, '"Cyber-Laundering": The Change of Money Laundering in the *Digital* Age' (2022) 25 Journal of Money Laundering Control 330.
[44]https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2022/03-assessing-*digital*-financial-threat-landscape-indonesia.html

- *The first group is the financial services sector, where digital transformation requires enhanced information security on both the provider and customer side. It is essential because criminals can exploit it through identity theft and scams.*
- *Business email compromises are becoming more common in retail transactions, with criminals intercepting communications and attempting to transfer funds from victims to criminals. The criminals often pretend to sell goods, both domestically and internationally.*
- *Trade-Based Money Laundering (TBML) contributes to Indonesia's informal economy, where transactions occur without government knowledge or supervision.*

Financial Action Task Force (selanjutnya disebut sebagai FATF) di dalam kajiannya menjelaskan kerentanan pencucian uang atas perkembangan *virtual Assets* dalam kasus serangan siber *wannacry* adalah sebagaimana digambarkan di dalam bagan berikut ini:



Gambar 3 Serangan Siber Wannacry

(Sumber data: The Financial Action Tasks Force)

Virus yang disebut "*wannacry*" ini mulai menginfeksi ke komputer-komputer yang terkena menjadi korban dengan disertai permintaan sejumlah bitcoin untuk tebusan. Virus *wannacry* ini menyebabkan komputer-komputer, yang ada dipergunakan untuk kegiatan bisnis termasuk juga rumah sakit, menjadi tidak dapat berfungsi sampai uang tebusan yang diminta tersebut dibayarkan. Virus ini berkembang dengan begitu cepat, yang menyebabkan keresahan, karena ada banyak data yang harus dilindungi. Sebagian korban melakukan pembayaran tebusan. Pada tahap *Ransom payments* ini,

korban akan membayarkan sejumlah tebusan berupa sejumlah bitcoin yang diminta oleh *hackers* untuk mendekripsikan komputer-komputer tersebut dan melanjutkan aktivitas kembali. Selanjutnya para *hackers* tersebut menerima *bitcoin* sebagai uang tebusan tersebut dimasukkan ke dalam *bitcoin wallets* yang dapat diidentifikasi secara publik. Pada hakikatnya proses ini dapat terjadi manakala terdapat dua orang yang terlibat dalam perjanjian yang seorang mengirimkan *bitcoin* atau *cryptocurrencies* yang lainnya, maka para pihak akan saling mengungkapkan alamat publik. Setelah proses tersebut, satu tahap di dalam pencucian uang yang disebut dengan *Layering* terjadi. Beberapa transaksi mengkonversi pembayaran dari satu *virtual asset* ke *virtual asset* lainnya untuk menghilangkan tautan ke kejahatannya. Di sini kerentanan penggunaan metode dalam pencucian uang untuk menghilangkan jejak asal usul harta kekayaannya tersebut. Proses serangan siber dalam bentuk virus wannacry ini berhenti karena otoritas berhasil menghentikan sebelum para *hacker* berhasil mengkonversikan uang tebusan pembayaran tersebut lebih jauh. Peran *Virtual Asset Service Provide* (VASP) menjadi sangat penting untuk untuk dapat mengidentifikasi *"seems legal"* bitcoin yang dikirimkan oleh *hacker* kepada *service provider* atau bank yang akan mengkonversi aset menjadi *fiat money* (uang yang nilainya berasal dari regulasi atau hukum suatu negara). *Hacker* yang menerima bitcoin dalam bentuk mata uang yang dipilihnya tersebut kemudian dipersiapkan untuk diinvestasikan ke dalam suatu bank. Jadi terjadi konversi ke mata uang yang diregulasi oleh suatu negara. Serangan siber berupa Virus *Wannacry* ini melumpuhkan sumber penghasilan para korbannya, kesehatan dan bidang jasa-jasa penting dan vital lainnya. Kerugian total yang diakibatkan oleh serangan ini adalah USD$ 8 Billion.

Marc Goodman menjelaskan: *"Technology is enabling new forms of money, and the growing digital economy holds great promise to provide new financial tools. These emerging virtual currencies are often anonymous, and non have received quite as much as Bitcoin, a decentralized peer-to-peer digital form of money*."[45] Anonimiti tersebut yang masih menjadi permasalahan dan ancaman bagi para penegak hukum karena *anonymous transaction* ini dieksploitasi oleh para penjahat atau para pencuci uang.

Di India, telah terjadi kasus pencucian uang dengan memanfaatkan Fintech. *Enforcement Directorate* (ED) Pencucian Uang India melakukan penyidikan atas 365

[45] Marc Goodman. Opcit. P. 264

Perusahaan Fintech dan mitra perusahaan keuangan non-perbankan (*non-banking financial companies*) karena menemukan dugaan lebih dari Rs 800 Crore sebagaimana dijelaskan oleh *Federal Agency* sebagai dana hasil kejahatan, dan melanggar aturan dari *the Reserve Bank of India* (RBI) ketika beroperasi di India. Penyidikan yang dilakukan oleh ED menemukan perusahaan-perusahaan Fintech mencairkan pinjaman lebih dari Rs 4.000 Crore, yang kemudian berusaha mendapatkan kembali jumlah yang dipinjamkan tersebut melalui telepon. Selanjutnya perusahaan yang termasuk mitra perusahaan keuangan non-perbankan yang sudah tidak beroperasi, yang diduga memberikan lisensi yang dikeluarkan oleh *the Reserve Bank of India* untuk pembagian keuntungan mulai dari 0.5% hingga 1%. Menurut berita, penyidik mengungkapkan bahwa platform fintech tersebut sebagian besar didukung oleh uang dari negara China, dan warga negara China telah mengambil kendali operasional dari perusahaan Fintech tersebut, dan menyediakan uang untuk menjalankan aplikasinya. Hal ini dirasakan mengkhawatirkan. Berdasarkan pinjaman yang didistribusikan, lebih dari Rs 700 Crore dikembalikan di awal oleh platform pinjaman *digital* ini, dengan alasan sebagai biaya pemrosesan dan lebih dari Rs 85 crore dalam bentuk bunga dan denda. Modal Fintech dimasukkan di rekening perusahaan keuangan non-perbankan (*non-banking financial companies*) dalam bentuk simpanan antar perusahaan atau jaminan kinerja. *Non-Banking Financial Companies* ini sendiri tidak pernah mendapatkan persetujuan dari *the Reserve Bank of India* sebelum menerima simpanan dari para pelaku Fintech sehingga melanggar norma. Hal tersebut juga ditambahkan bahwa perusahaan Fintech dan *Non-banking financial companies* ini membebankan sekitar 0.5% dari pembayaran melalui aplikasi seluler atau komitmen minimum setiap bulan. *Non-banking financial companies* dalam hal ini tidak menginvestasikan satu rupee pun.[46] Sumber berita lain menambahkan bahwa modus operandi aplikasi pinjaman instan *(Instant Loan Apps)* dimulai dengan permintaan aplikasi kepada mitra *non-banking financial companies* untuk membuat ID pedagang *(Merchant ID)* dengan *gateway* pembayaran. Hal tersebut akan memungkinkan aplikasi pinjaman untuk menyalurkan pencairan dan pemulihan pinjaman dari *non-banking financial companies partners* melalui *payment gateway* ini. *Payment Gateway* tersebut tidak dapat menolak entitas yang terdaftar di *the Reserve Bank of India*, dan *non-banking financial companies* membuat beberapa akun *virtual*

[46] ttps://www.timesnownews.com/business-economy/industry/ed-unearths-over-rs-800-crore-crime-proceeds-in-fintech-nbfc-money-laundering-probe-article-93754032, retreived 5 Januari 2023,

untuk aplikasi pinjaman dari mitra-mitranya, sekaligus di dalam aplikasi tersebut juga tertera klausula persetujuan yang menyebutkan bahwa *non-banking financial companies* tersebut tidak terlibat dalam aktivitas bisnis apapun dari aplikasi pinjaman tersebut. *The Enforcement Directorate* menetapkan bahwa aplikasi tersebut dipinjamkan dari uang jaminan dan menggunakan lisensi *non-banking financial companies*. Perusahaan-perusahaan tersebut memberikan pinjaman jangka pendek dengan jangka waktu mulai dari tujuh hari sampai dengan dua bulan, membebankan suku bunga yang sangat tinggi, biaya pemrosesan dan biaya GST. Kepolisian telah menangkap Direktur dan CEO di bawah undang-undang pencegahan pencucian uang 2002, dan ditemukan bahwasanya Direktur dan CEO tersebut tidak memiliki aplikasi peminjaman sendiri, tetapi bekerja dengan berbagai aplikasi pinjaman.[47]

Mendasarkan pada terjadinya pencucian uang di sektor Fintech di India tersebut, Indonesia juga harus berhati-hati. Sebagaimana dijelaskan pada bagian sebelumnya, OJK telah melaporkan banyaknya perusahaan-perusahaan Fintech yang masih tidak teregistrasi maupun tidak berizin. Hal ini harus menjadi kehati-hatian bersama oleh penegak hukum.

Terkait dengan *cyber laundering* lainnya, FATF juga memberikan *red flags indicators*, yang meliputi permasalahan *Virtual assets*. Melalui *Red Flags* ini, FATF meminta negara-negara memastikan bahwa *red flags* ini diterapkan di dalam sistem monitoring transaksi yang ada. VASP harus menggunakan enam kategori yang ditekankan pada laporan tersebut sebagai kerangka untuk memulai proses identifikasi atas kegiatan yang terkait dengan *ML/TF risks*. 6 kategori tersebut meliputi:

- Transaksi
- Pola Transaksi
- Anonimitas
- Pengirim atau Penerima
- Sumber dana atau kekayaan
- Risiko wilayah geografi.[48]

Selain itu perlu juga diperhatikan apa yang menjadi perhatian dari *the US Financial Crimes Enforcement Networks* dengan contoh-contoh sebagai berikut:

[47] https://inc42.com/buzz/ed-uncovers-proceeds-crime-inr-800-cr-loan-apps-money-laundering-probe/, retrieved 5 Januari 2023.
[48] Ms. Francisca Fernando. and others, 'Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1)'.

- Seorang nasabah atau pengguna jasa yang menerima serangkaian setoran dari sumber yang berbeda, yang secara agregat, jumlahnya hampir identik dengan jumlah transfer dana ke platform pertukaran mata uang virtual yang dikenal dalam waktu yang singkat;
- Transaksi dari nasabah atau pengguna jasa yang bermuila dari alamat IP yang tidak terpercaya, atau dari negara-negara yang tidak dapat dipercaya, atau alamat-alamat IP yang sebelumnya telah ditandai sebagai alamat yang mencurigakan;
- Nasabah atau pengguna jasa yang memberikan identitas atau kredensial akun seperti kata sandi yang non-standar, alamat IP, maupun *flash cookies*) yang dibagikan oleh akun lain;
- Alamat dompet umum yang dibagikan antar nasabah/pengguna jasa
- Seorang nasabah/pengguna jasa yang melakukan beberapa penjualan dengan cepat antara beberapa mata uang virtual tanpa tujuan yang jelas, yang mungkin merupakan indikasi sebagai upaya untuk memutus mata rantai blockchain yang ditahan atau lebih jauh untuk mengaburkan transaksi.[49]

Cyber laundering pada hakikatnya menuntut kehati-hatian lebih dari para pihak terkait, seperti penegak hukum dan pihak pelapor.

4. Inovasi Hukum Anti Pencucian Uang di Era Digital

Hukum dalam berinteraksi dengan teknologi dan digitalisasi harus tetap mewujudkan tujuan hukum untuk masyarakat. Hukum di dalam masyarakat tentu diatur berdasarkan norma-norma dan peraturan yang ditujukan untuk mengatur kehidupan masyarakat. Hukum dalam pandangan ini harus mampu memberikan perlindungan sekalipun masyarakat berubah. Samsir Salam menegaskan mengenai makna perubahan sosial yang memiliki arti terlibatnya orang banyak di dalam kegiatan-kegiatan kelompok, serta dalam hubungan-hubungan kelompok yang berbeda. Hubungan yang berubah tersebut dapat terjadi karena situasi baru yang dihadapi dan harus direspon oleh kelompok masyarakat tersebut, yang merefleksikan faktor-faktor seperti teknologi, inovasi baru, serta nilai-nilai baru.[50]

Teknologi dan berbagai inovasi baru sebagai pemicu perubahan sosial di era *digital* ini harus direspon oleh hukum. Hukum tidak dapat menafikan untuk bertransformasi dan berinovasi. Menilik asal kata Inovasi, Kamus Besar Bahasa Indonesia mendefinisikan inovasi sebagai 1. pemasukan atau pengenalan hal-hal yang

[49] ibid.
[50] Samsir Salam, 'Hukum Dan Perubahan Sosial (Kajian Sosiologi Hukum)' (2015) 11 STAI DDI Pangkep Sulawesi Selatan 107.

baru; pembaharuan, 2. Penemuan baru yang berbeda dari yang sudah ada atau yang sudah dikenal sebelumnya (gagasan, metode, atau alat).[51]

Pertanyaan yang muncul kemudian adalah adalah bagaimana hukum dapat berinovasi? Dalam hal apa hukum harus berinovasi? Pertanyaan kontempelasi ini membawa konsekuensi logis mengingat hukum berkembang dengan berbagai madzhab-nya. Hukum tidak selalu dimaknai sebagai institusi keadilan, atau sebagai pranata sosial saja, tetapi dalam pandangan hukum juga selalu dimaknakan sebagai sistem peraturan. Hukum berjalan dalam makna norma dan kaidah. Norma hukum dimaknai sebagai perintah dan penilaian, sekaligus sebagai suatu peraturan hukum. Hukum harus dilihat dari tujuannya, dan selalu memperhatikan bagaimana cara memecahkan masalah yang terjadi. Masalah-masalah hukum inilah yang berubah seiring dengan dorongan kuat karena inovasi di bidang teknologi yang tidak mungkin tidak untuk direspon oleh masyarakat dan negara. Winda Wijayanti, mengutip pendapat Mochtar Kusumaatmadja, menegaskan secara umum fungsi hukum adalah:

a. memelihara ketertiban dalam masyarakat,
b. menjamin kepastian hukum,
c. sebagai pengayom masyarakat,
d. pelerai perselisihan-perselisihan dalam masyarakat,
e. membagi kekuasaan dan kewenangan dalam negara dan pemerintahan,
f. menegakkan keadilan[52]

Perspektif tujuan hukum inilah yang harus selalu dipegang. Hukum dalam keadaan bagaimanapun harus dapat menjadi panglima atas perkembangan masyarakat demi terwujudnya tujuan-tujuan hukum. Hukum juga harus memiliki pandangan yang progresif, yang di dalam penjelasannya, Satjipto Rahardjo[53] menegaskan bahwasanya hukum progresif ingin melindungi masyarakat dari cita-cita hukum, menolak *status quo* dan menjadikan hukum sebagai institusi moral daripada teknologi yang tidak memiliki nurani.

Hukum pada hakikatnya harus ditujukan untuk manusia. Perubahan sosial yang terjadi karena digitalisasi dan segala macam inovasinya harus diadopsi oleh hukum, dengan mengukur bagaimana masyarakat sebagai subjek hukum akan terus dapat

[51]Kamus Besar Bahasa Indonesia, akses dari https://kbbi.web.id/inovasi
[52] Winda Wijayanti, 'Eksistensi Undang-Undang Sebagai Produk Hukum Dalam Pemenuhan Keadilan Bagi Rakyat (Analisis Putusan Mahkamah Konstitusi Nomor 50/PUU-X/2012)' (2016) 10 Jurnal Konstitusi 179.
[53] Satjipto Rahardjo. Hukum Progresif: Sebuah Sintesa Hukum Indonesia (2009). Yogyakarta: Genta Publishing.1-2

mengikuti perkembangan tersebut, tetapi dilindungi oleh hukum dan peraturan-peraturannya. Hukum yang berinovasi tidak sekedar dibuat dalam bentuk kaidah aturan hukum yang berisikan segala macam aturan adopsi atas perubahan teknologi tersebut, tetapi lebih jauh juga hendak meletakkan kewajiban kepada subjek hukum untuk melaksanakan kewajiban hukumnya tersebut.

Hukum harus bertransformasi, dan harus selalu menjadi panglima atas seluruh perubahan masyarakat. Oleh karenanya inovasi hukum harus melampaui dari inovasi di bidang teknologi itu sendiri. Hukum tidak lagi berdiri di belakang perubahan sosial. *Het recht hink aachter de feiten aan* harus berubah. Revolusi Digital yang akan terus berkembang memacu hukum harus berinovasi melebihi dari inovasi teknologi itu sendiri.

Hukum dalam era *digitalisasi* ini memberikan tantangan sekaligus ancaman yang berupa munculnya masalah-masalah hukum, secara khusus dalam kaitannya dengan kejahatan dunia maya yang membawa pengaruh pula pada tantangan atas hukum pencucian uang, yang dalam hal ini dibahas adalah *cyber laundering* pada rezim *anti money laundering*. Ifrany dan Djoni S. Gozali[54] menambahkan catatannya pada permasalahan: *the increase in money laundering crimes, which use the financial systems to hide and conceal the origin money from criminal activities, has particularly negative impact on economic sectors. The impact of money laundering is immense and even threatens the country's economic stability*.

Hukum anti pencucian uang yang berlaku di Indonesia merupakan hukum yang bertransformasi dan berinovasi khususnya dengan munculnya banyak ancaman yang telah diingatkan oleh FATF maupun *inter-governmental agencies* lainnya dengan standar-standar dan rekomendasinya. Salah satu kekuatan yang harus diakui di dalam hukum anti pencucian uang saat ini diletakkan pada peran aktif dari pihak pelapor. Masyarakat Internasional telah mengembangkan berbagai pendekatan seperti melalui pendekatan berbasis risiko (*risk based approach)* atas keterlibatan pihak pelapor dalam upaya maksimalisasi pencegahan dan pemberantasan tindak pidana pencucian uang dan pendanaan terorisme. Kondisi tindak pidana pencucian uang semakin hari semakin

[54] Ifrany dan Djoni S. Gozali. Assesing Money Laundering in the *Digital* Era: The High Potential of Cyber Laundering on the Revolution of Financial Technology, paper, International conference on Wetland and Multidiciplinary Research 2019

berkembang dengan adanya penetrasi dari berbagai pihak dan keadaan.[55] Peranan pihak pelapor menjadi penting, dan memiliki korelasi yang sangat besar untuk terus diupayakan kepatuhannya *(Compliance)*.

Teknologi finansial muncul sebagai sebuah sektor yang memiliki kekuatan dengan perkembangan yang mengalami perkembangan cepat. Pemerintahan di seluruh dunia harus melihat dan memanfaatkan kekuatan tersebut. Namun demikian kekuatan teknologi keuangan yang semakin inovatif membawa pada risiko munculnya *fraud*. *Fraud* dan kejahatan lainnya harus dapat dicegah. Teknologi harus dapat dimanfaatkan pula untuk mencegah kejahatan, di samping perlunya membangun pengetahuan dan pemahaman lebih mendalam mengenai Fintech, meminta pihak-pihak terkait untuk melakukan mitigasi risiko dengan selalu mendorong sektor swasta untuk mengembangkan dan menggunakan *Regulation Technology* (*Regtech*).

Rezim APU/PPT menekankan pada peran penting dari peran Pihak Pelapor yang secara aktif melaporkan dan patuh pada penerapan Prinsip Mengenali Pengguna Jasa (PMPJ) atau yang dikenal sebagai *Customer Due Diligence* dan *Enhance Due Diligence* (CDD-EDD). Berdasarkan ketentuan Pasal 17 UU PPTPPU, dan lebih lanjut diatur di dalam Peraturan Pemerintah No. 43 Tahun 2015 sebagaimana diubah dengan Peraturan Pemerintah No. 61 Tahun 2021 tentang Pihak Pelapor dalam pencegahan dan pemberantasan tindak pidana pencucian uang, Fintech akhirnya dimasukkan sebagai pihak pelapor. Pihak Pelapor memiliki peranan penting, yang melibatkan kewajiban untuk menerapkan CDD/EDD dan melaporkan kepada otoritas yang melaksanakan pengawasan (PPATK dan/atau Lembaga Pengawas Pengatur yang ditetapkan lebih lanjut) sebagai suatu kewajiban di dalam pencegahan pencucian uang.

Pada konsiderans menimbang huruf a dari Peraturan Pemerintah No. 61 Tahun 2021 menegaskan semakin berkembangnya layanan jasa keuangan berbasis teknologi informasi yang berpotensi dipergunakan sebagai sarana pencucian uang hasil tindak pidana oleh pelaku, dan sekaligus diperlukannya perlindungan oleh penyelenggara layanan jasa keuangan berbasis teknologi dari risiko tindak pidana pencucian uang, diperlukan pengaturan bagi penyelenggara layanan jasa keuangan tersebut sebagai pihak pelapor dalam pencegahan dan pemberantasan tindak pidana pencucian uang. Peran penyelenggara Fintech sangatlah penting di dalam rezim anti pencucian uang dalam

[55] Go Lisanawati dan Njoto Benarkah. Hukum Money Laundering (Pencucian Uang) Dalam Dimensi Kepatuhan (2018) Malang: Setara Press 43

masa revolusi digital seperti saat ini, sehingga menjadikan Fintech sebagai pihak pelapor yang harus tunduk pada mekanisme *compliance* (kepatuhan) sebagaimana diatur di dalam UU Pencucian Uang.

Peran Lembaga Pengawas dan Pengatur juga penting, yang juga akan turut mendukung terciptanya mekanisme kepatuhan yang baik dari Pihak Pelapor melalui pengawasan dan penetapan sanksi bila Pihak Pelapor tidak patuh. Oleh karenanya semua perusahaan Fintech baik besar ataupun kecil, harus melarang setiap orang untuk menggunakan jasa maupun barangnya untuk mencuci uang maupun mendanai kegiatan pencucian uang. Penggunaan layanan perusahaan teknologi keuangan sebagai kemungkinan taktik kejahatan oleh organisasi kriminal mengharuskan bisnis Fintech mampu mengatasi kejahatan keuangan dengan secara efisien. Oleh karenanya Fintech harus memenuhi kewajiban dan kepatuhan pada program Anti Pencucian Uang.

Sebagaimana telah dijelaskan pada bagian sebelumnya, masalah perlindungan data pribadi juga menjadi permasalahan utama yang ditemui dalam kerangka digitalisasi ini. Salah satu inovasi oleh Pemerintah Indonesia, yaitu UU Perlindungan Data Pribadi, yang secara hakiki melakukan penyatuan aturan-aturan terkait dengan perlindungan data pribadi yang tersebar di berbagai peraturan perundang-undangan seperti Undang Undang No. 11 Tahun 2008 jo. Undang Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, kemudian peraturan menteri telekomunikasi dan informasi, serta beberapa peraturan perundangan lainnya. Undang Undang ini menjadi salah satu terobosan yang telah diambil oleh pemerintah mengingat perkembangan dunia *digital*. Namun demikian, undang-undang ini masih diperlukan pembuktian keefektifannya mengingat kebaruan yang dilakukan. Selain itu, Bank Indonesia juga merilis *blueprint* tentang penerapan *Central Bank Digital Currency* yaitu berupa Rupiah *Digital* Currency. Hal ini diharapkan dapat memberikan perlindungan kepada pemain krypto, tetapi di saat yang bersamaan harus memikirkan bagaimana memberikan edukasi kepada masyarakat mengenai penggunaan Rupiah *Digital* Currency tersebut, yang berarti di dalamnya juga menyangkut pada literasi atas penggunaan teknologi kepada seluruh lapisan masyarakat.

Salah satu tantang terbesar bagi hukum di era *digital* ini adalah masalah penegakan hukum sebagaimana dijelaskan pula pada bagian sebelumnya. Fadil Zumhana, Wakil Jaksa Agung untuk Kejahatan Umum Kejaksaan Agung, menjelaskan

bahwasanya kompleksitas teknologi baru dapat menjadi halangan bagi instansi penegak hukum. Fadil Zumhana merefleksikan tantangan tersebut terkait dengan pencucian uang, dan menjelaskan bahwa penyidik perlu diperlengkapi dengan keahlian untuk memperoleh dokumen-dokumen elektronik untuk menguji kasus-kasus, dan untuk melakukan analisis forensik. Dengan demikian sistem peradilan pidana dapat terus mengikuti ancaman-ancaman yang muncul.[56] Permasalahan penegak dan penegakan hukumnya menjadi permasalahan yang penting untuk dilakukan, dan oleh karenanya penegak hukum juga diharapkan melakukan inovasi.

Salah satu *tools* di dalam keberhasilan pencegahan tindak pidana pencucian uang adalah pada kepatuhan pihak pelapor untuk melakukan *Customer Due Diligence* (CDD) maupun *Enhanced Due Diligence* (EDD). Mengingat perkembangan *Digital Onboarding* yang semakin pesat maka harus pula diikuti kemampuan untuk melakukan e-CDD dan/atau e-EDD. CDD/EDD sebenarnya merupakan standar yang ditetapkan dalam Rekomendasi nomor 10 (yang semula merupakan Rekomendasi 5) FATF Revisi Tahun 2012 sebagaimana diupdate Maret 2022, yang sebenarnya mengatur larangan bagi lembaga keuangan untuk menyimpan rekening tanpa nama (anonim) maupun rekening yang nyata-nyata menggunakan nama fiktif. Lembaga keuangan diminta untuk melakukan langkah-langkah mengenali Pengguna Jasa (CDD) pada saat:

i. membangun hubungan bisnis;
ii. melakukan transaksi yang tidak bersifat kontinyu: (i). di atas batas yang ditentukan yang berlaku (USD/Euro 15,000); atau (ii). Merupakan *wire tranfer* dalam keadaan yang dipersyaratkan dalam *Interpretative Note* atas Rekomendasi 16
iii. terdapat dugaan pencucian uang atau pendanaan terorisme; atau
iv. lembaga keuangan meragukan kebenaran dan kecukupan identifikasi data Pengguna jasa yang telah didapatkan.

Ketentuan tersebut telah diadopsi oleh Undang Undang Nomor 8 Tahun 2010, yang meletakkan kewajiban untuk mengenali pengguna jasa, yaitu pada saat:

a. terdapat hubungan usaha antara pihak pelapor dengan Pengguna jasa
b. terdapat transaksi keuangan yang menggunakan mata uang Indonesia maupun mata uang asing, dengan nila transaksi minimum Rp, 100.000.000,00

[56] https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2022/03-assessing-*digital*-financial-threat-landscape-indonesia.html

c. diketahui terdapat TKM yang terkait dengan pencucian uang dan pendanaan teroris
d. adanya keraguan dari Pihak pelapor atas kebenaran informasi yang disampaikan oleh Pihak Pelapor. (vide Pasal 18 ayat (3) UU Pencucian Uang)

Merujuk pada pengaturan CDD dalam FATF dan Pasal 18 ayat (3) UU Nomor 8 Tahun 2010 tersebut maka perlu diberi penekanan pada beberapa hal, antara lain:

- Penyesuaian batas *treshold* yang diperkenankan. FATF 2012 Update Maret 2022 telah menaikan batas transaksi semula USD 10,000 menjadi USD/Euro 15,000. Sementara UU Nomor 8 Tahun 2010 menetapkan transaksi keuangan dengan mata uang Rupiah dan/atau asing minimal atau setara dengan Rp. 100.000.000,00. Sekalipun setiap negara diperbolehkan menentukan sendiri, tetapi perubahan dari rekomendasi FATF ini akan menimbulkan gap antar negara.
- Penekanan dari lingkup pengaturan pada UU No. 8 Tahun 2010 adalah pada terdapatnya Transaksi Keuangan Mencurigakan yang terkait dengan pencucian uang dan pendanaan terorisme, sementara FATF hanya menekankan pada adanya dugaan pencucian uang dan pendanaan terorisme. Hal ini juga dapat menjadi gap. Indonesia sendiri mengenal mekanisme transaksi keuangan meliputi Transaksi Keuangan Mencurigakan, Transaksi Keuangan Tunai, dan Transaksi Keuangan Transfer Dana. Penekanan CDD haruslah pada keseluruhan transaksi, sepanjang ada dugaan terkait tindak pidana pencucian uang dan pendanaan terorisme. Tentu saja hal ini membutuhkan inovasi di dalam penerapannya di Indonesia, khususnya di dalam menghadapi era digital ini.

Selanjutnya FATF memberikan penekanan bahwa setiap lembaga keuangan harus menerapkan CDD yang harus diatur oleh hukum. Setiap negara dapat menentukan bagaimana pemberlakuan kewajiban CDD tertentu, baik melalui hukum ataupun cara penegakannya. Langkah CDD[57] yang harus diambil antara lain:

- Mengidentifikasi nasabah/pengguna jasa dan melakukan verifikasi atas data diri nasabah dengan menggunakan sumber dokumen, data atau informasi yang terpercaya dan mandiri,

[57] FATF (n 27).

- Melakukan identifikasi atas penerima manfaat, dan melakukan langkah yang *reasonable* untuk melakukan verifikasi atas identitas dari Penerima manfaat, bahwa lembaga keuangan harus merasa yakin telah mengetahui penerima manfaat tersebut. Atas korporasi dan pengaturannya harus mencakup bagaimana lembaga keuangan memahami struktur kepemilikan dan penguasaan nasabah
- Memahami perolehan informasi tentang tujuan dan sifat hakikat dari hubungan bisnis yang dilakukan
- Melakukan *due diligence* yang berkelanjutan dari hubungan bisnis dan pemeriksaan transaksi yang dilakukan selama hubungan bisnis tersebut berlangsung untuk memastikan bahwa transaksi tersebut dilakukan secara konsisten melalui pemahaman institusi tentang nasabah/pengguna jasa, profil bisnis, dan risikonya, termasuk sumber dana apabila dibutuhkan.

Sementara melalui Pasal 18 ayat (5) UU Pencucian uang, setidaknya Prinsip Mengenali Pengguna Jasa (PMPJ) meliputi:

- Identifikasi dari pengguna jasa
- Verifikasi atas identifikasi tersebut
- Memantau Transaksi dari Pengguna Jasa

Sementara pada poin ke dua dari ketentuan FATF di atas, diatur secara tersendiri di dalam Peraturan Presiden No. 13 Tahun 2018 tentang Prinsip Mengenai Pemilik Manfaat dari Korporasi dalam Rangka Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Sementara kewajiban CDD pada butir c dan d dari ketentuan rekomendasi FATF tersebut juga harus terus dilaksanakan oleh seluruh Pihak Pelapor. Hal tersebut harus dijelaskan agar memiliki kesamaan persepsi di antara seluruh Pihak Pelapor.

Peranan CDD sangat penting. Proses identifikasi pengguna jasa menjadi sangat penting di dalam upaya pencegahan tindak pidana pencucian uang. Sementara *Enhanced Due Diligence* (EDD) merupakan penerapan CDD secara ketat kepada pihak-pihak dengan keadaan tertentu, dalam hal ini yang terkait dengan *Politically Exposed Persons* (PEPs).

Terkait dengan era *digital* ini, salah satu inovasi yang harus dilakukan adalah menciptakan sistem e-CDD/e-KYC dan e-EDD sehingga upaya-upaya pencegahan tindak pidana pencucian uang dan pendanaan terorisme juga dapat dimutakhirkan.

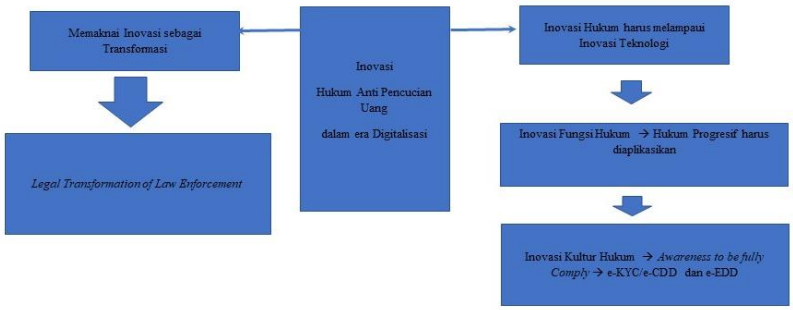
Untuk itu perlu dikembangkan software yang dapat dipergunakan oleh Pihak Pelapor, sehingga secara efektif dapat mencegah terjadinya pencucian uang atau pendanaan terorisme. Peran pihak Pelapor menjadi sangat dominan, dan oleh karenanya masalah penerapan *crypto currency* juga harus diperhatikan. Bank Indonesia tidak dapat meletakkan hanya pada norma himbauan berupa larangan yang diberikan oleh Bank Indonesia, tetapi ada ketegasan bahwa krypto dilarang, kecuali *Rupiah Digital Currency* yang akan diberlakukan. Pada saat yang bersamaan pemerintah juga harus menyiapkan sarana dengan menetapkan siapa pihak yang bertanggungjawab dengan krypto ini sehingga dapat diberi beban dan tanggung jawab sebagai Pihak Pelapor. Dengan demikian harus tunduk pada semua aturan hukum yang berlaku.

Mengenai e-KYC atau e-CDD dan e-EDD ini memiliki makna bahwa upaya melakukan pengenalan nasabah/pengguna jasa dilakukan secara elektronik, yaitu dengan menggunakan sistem yang *compatible* sehingga melalui proses tersebut tidak memerlukan kehadiran atau kontak secara fisik dengan nasabah atau pengguna jasa, dan proses akan lebih mudah. Pelaksanaan e-KYC/e-CDD dan e-EDD ini harus didukung dengan sistem pengamanan dan pengenalan yang komprehensif, karena kunci di dalam melakukan upaya pencegahan pencucian uang diletakkan pada kekuatan metode KYC/CDD nya. Dengan e-KYC/e-CDD ini diharapkan pihak pelapor memitigasi risiko pencucian uang yang mengikuti, dan juga selalu melakukan *risk-based approach* atas usaha yang dilaksanakannya. Melalui e-KYC/e-CDD dan e-EDD ini, pengguna jasa wajib memberikan informasi yang benar, sekaligus pihak pelapor akan melakukan penggalian atas kemungkinan dieksploitasinya rekening atau aplikasi digital tersebut untuk kegiatan pencucian uang dan pendanaan terorisme. Mengingat bahwa KYC/CDD ini dilakukan tanpa kontak dengan pengguna jasa maka pihak pelapor harus berhati-hati dan melakukan pemeriksaan yang benar atas profil nasabah atau calon pengguna jasa tersebut. Konsekuensinya apabila pihak pelapor tidak melaksanakan dengan baik kewajiban tersebut, risiko akan reputasi dari perusahaan dipertaruhkan, di samping risiko penjatuhan sanksi bila terbukti terlibat dalam pencucian uang. Lebih jauh yang diharapkan dengan dilaksanakannya e-KYC/e-CDD dan e-EDD dengan cermat maka risiko kerugian negara akibat pencucian uang ini dapat diminimalisir.

Inovasi lainnya adalah membangun mekanisme *Public-Private Partnerships*, yang sebenarnya sudah dilaksanakan oleh PPATK sebagai Indonesian Focal Point dan

Financial Intelligent Units dengan beberapa lembaga dan institusi baik publik dan privat. Namun demikian masih terdapat keterbatasan karena masih diterapkan dengan beberapa pihak saja, belum secara menyeluruh. Dinamika *digital* ini menjadi penting untuk dicarikan solusi, dan dicegah bersama-sama oleh seluruh elemen masyarakat Indonesia. Melalui *Public-Private partnership* ini akan mendorong kesadaran hukum seluruh masyarakat mengenai potensi risiko pencucian uang, secara khusus dengan pesatnya perkembangan teknologi dan revolusi digital, yang tidak lagi memungkinkan masyarakat memilih untuk tetap bertahan dengan kehidupan yang lama tetapi harus mengikuti perubahan itu sendiri. Masyarakat harus menyadari kerentanan dan risiko atas ketidaktahuan atau ketidakengganan untuk mengetahui apa dan bagaimana pencucian uang, akan menempatkan dirinya sebagai *potential victims* maupun *potential offender* itu sendiri.

Dengan demikian inovasi yang dapat dilakukan hukum anti pencucian uang dapat dijelaskan melalui gambar sebagai berikut:



Gambar 4: Bagan Inovasi Hukum Anti Pencucian Uang dalam Era Digitalisasi

5. Penutup

Risiko *cyber laundering* dalam era revolusi *digital* ini sangat tinggi, sehingga hukum anti pencucian uang harus juga berinovasi. Inovasi ini harus bersinergi dengan teknologi itu sendiri. Secara khusus, peraturan hukum yang berlaku saat ini, harus terus dilaksanakan secara konsisten, dan harus dapat menumbuhkan kesadaran hukum masyarakat Indonesia, di dalam hal ini secara khusus bagi Pihak Pelapor, Penegak Hukum, Pihak Regulator, serta masyarakat harus memiliki pemahaman yang sama untuk pencapaian program anti pencucian uang dan pendanaan terorisme di Indonesia menjadi efektif.

Berbagai pihak yang diharapkan berperan aktif di dalam upaya pencegahan dan pemberantasan tindak pidana pencucian uang tersebut harus mampu melakukan berbagai transformasi sekaligus inovasi agar mampu mengikuti perkembangan teknologi yang akan semakin maju di masa yang akan datang, dan di saat yang bersamaan menyadari risiko pencucian uang dan pendanaan terorisme, ancaman kejahatan siber lainnya agar dapat bertindak penuh kehati-hatian.

Sumber Referensi

ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021

Arthadik A. "Cyber Laundering: Risk and Future Threats of Virtual Currency in Indonesia" in Tackling Financial Crimes: various International Perspectives [2017] Yogyakarta: Genta Publishing

Al-Fikri HM, 'Peluang Dan Tantangan Perguruan Tinggi Menghadapi Revolusi Digital Di Era Society 5.0' (2021) 3 Prosiding Seminar Nasional Pendidikan 350 <https://mail.prosiding.unma.ac.id/index.php/semnasfkip/article/view/621>

Amrullah, A, Tindak Pidana Pencucian Uang Money Laundering: Reorientasi kebijakan Penanggulangan dan Kerjasama Internasional [2004] Malang, Bayumedia Publishing

Arab Monetary Fund, 'Digital Customer On-Boarding, e-KYC and Digital Signatures'

Faccia A and others, 'Electronic Money Laundering, the Dark Side of Fintech: An Overview of the Most Recent Cases' [2020] ACM International Conference Proceeding Series 29

Badan Siber dan Sandi Negara, Laporan Bulanan Publik Hasil Monitoring Keamanan Siber [2022] Sumber: https://www.bssn.go.id

CNN Indonesia "Nilai Transaksi *Digital* Banking Tembus Rp5.184,1 T pada Oktober 2022", diakses dari https://www.cnnindonesia.com/ekonomi/20221117164404-78-875191/nilai-transaksi-*digital*-banking-tembus-rp51841-t-pada-oktober-2022 pada tanggal 10 Januari 2023

FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' [2012] FATF, Paris, France 1 <www.fatf-gafi.org/recommendations.html>

García MK and others, 'Digital Onboarding in Finance: A Novel Model and Related Cybersecurity Risks' (2022) 1 Open Research Europe 149

Goodman, M, Future Crimes: Inside the *Digital* Underground and the Battle for Our Connected World [2015] Canada: Anchor Canada

https://inc42.com/buzz/ed-uncovers-proceeds-crime-inr-800-cr-loan-apps-money-laundering-probe/, retrieved 5 Januari 2023.

https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2022/03-assessing-*digital*-financial-threat-landscape-indonesia.html, akses pada 20 Desember 2022.

Ifrany dan Gozali D.S. Assesing Money Laundering in the *Digital* Era: The High Potential of Cyber Laundering on the Revolution of Financial Technology, paper [2019] International conference on Wetland and Multidiciplinary Research

Joveda N, Khan MT and Pathak A, 'Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of

Financial Information' (2019) 11 International Journal of Economics and Finance 54
Kamus Besar Bahasa Indonesia, akses dari https://kbbi.web.id/inovasi
Komunikasi D, 'Inovasi Untuk Integrasi Ekonomi Keuangan Digital' (2020) 7 Laporan Perekonomian Indonesia 2019 1292
Leong K, 'FinTech (Financial Technology): What Is It and How to Use Technologies to Create Business Value in Fintech Way?' (2018) 9 International Journal of Innovation, Management and Technology
Lisanawati G, Eksistensi dan Peranan Lembaga Pengawas dan Pengatur (LPP) dalam Rezim Anti Pencucian Uang [2018] Yogyakarta: Graha Ilmu
Lisanawati G and Aristo E, 'Urgensi Pengaturan Hukum Central Bank Digital Currency Dalam Dimensi Anti Pencucian Uang' (2022) 8 Jurnal Ilmiah Hubungan Internasional
Lisanawati G dan Benarkah N. Hukum Money Laundering (Pencucian Uang) Dalam Dimensi Kepatuhan [2018] Malang: Setara Press
m.cyberthreat.id
Mabunda S, 'Cryptocurrency: The New Face of Cyber Money Laundering' [2018] 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, icABCD 2018
Martowardojo ADW, 'Penyelenggaraan Teknologi Finansial' [2017] Peraturan Bank Indonesia 1 <https://www.bi.go.id/id/sistem-pembayaran/fintech/Contents/default.aspx>
Ms. Francisca Fernando. and others, 'Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1)'
Nikkel B, 'Fintech Forensics: Criminal Investigation and Digital Evidence in Financial Technologies' (2020) 33 Forensic Science International: Digital Investigation 1

Otoritas Jasa Keuangan, 'Peraturan OJK No. 13/POJK.02/2018 Tentang Inovasi Digital Di Sektor Jasa Keuangan' [2018] Otoritas Jasa Keuangan 1 <http://www.ojk.go.id/id/kanal/iknb/regulasi/lembaga-keuangan-mikro/peraturan-ojk/Documents/SAL-POJK PERIZINAN FINAL F.pdf>
PPATK. Laporan Tahunan 2021: Indonesia Maju Tanpa Pencucian Uang dan Pendanaan Terorisme [2021] PPATK
Putri CPH and GL, 'Peran Teknologi Finansial Dalam Pencegahan Pendanaan Terorisme' (2023)
Rahardjo S, Hukum Progresif: Sebuah Sintesa Hukum Indonesia [2009] Yogyakarta: Genta Publishing
Sahetapy J.E. "Business" Uang Haram (2003), paper
Salam S, 'Hukum Dan Perubahan Sosial (Kajian Sosiologi Hukum)' (2015) 11 STAI DDI Pangkep Sulawesi Selatan
Schueffel P, 'Taming the Beast: A Scientific Definition of Fintech' (2016) 4 Journal of Innovation Management
Siahaan N.H.T. Money Laundering dan Kejahatan Perbankan [2008] Jakarta: Jala
https://www.timesnownews.com/business-economy/industry/ed-unearths-over-rs-800-crore-crime-proceeds-in-fintech-nbfc-money-laundering-probe-article-93754032 retrieved 5 January 2023
Soltani R, 'Self-Sovereign Identity and Distributed Ledger' [2018] 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social

Computing (CPSCom) and IEEE Smart Data (SmartData)
Suryono RR, Budi I and Purwandari B, 'Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review (2020) 11 Information (Switzerland)
Tim Pelaksana Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang, Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang [2021] Jakarta: PPATK
Tunnicliffe H, 'On the Frontline' [2011] Chemical Engineer
Wijayanti W, 'Eksistensi Undang-Undang Sebagai Produk Hukum Dalam Pemenuhan Keadilan Bagi Rakyat (Analisis Putusan Mahkamah Konstitusi Nomor 50/PUU-X/2012)' (2016) 10 Jurnal Konstitusi
WRC, 'Table of Contents Table of Contents از سیر تا پیاز مصاحبه دکتری' [2012] European University Institute 2 <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT%0Ahttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:pt:NOT>
Wronka C, '"Cyber-Laundering": The Change of Money Laundering in the Digital Age (2022) 25 Journal of Money Laundering Control 330
www.ojk.go.id FAQ Fintech Lending, diakses pada 12 Desember 2022, pukul 22.00 WIB
Fintech China tumbuh subur di Indonesia, diakses dari https://www.kominfo.go.id/content/detail/13681/Fintech-china-serbu-indonesia/0/sorotan_media

Universitas Surabaya
Jalan Ngagel Jaya Selatan 169 Surabaya
Email: rektorat@unit.ubaya.ac.id
www.ubaya.ac.id