Technology and Economics Law Journal

Volume 1 | Number 1 Article 5

2-11-2022

PERKEMBANGAN KEJAHATAN TINDAK PIDANA PENCUCIAN UANG DAN TINDAK PIDANA PENDANAAN TERORISME (TPPU DAN TPPT) DI MASA PANDEMI COVID-19

LYDIA ANGGUN
Faculty of Law University of Indonesia, anggunlydia83@gmail.com

TELJ
Technology And Economic Law Journal
Vol.1 No.1

PERKEMBANGAN KEJAHATAN TINDAK PIDANA PENCUCIAN UANG DAN TINDAK PIDANA PENDANAAN TERORISME (TPPU DAN TPPT) DI MASA PANDEMI COVID-19

LYDIA ANGGUN
Mahasiswa Pascasarjana Ilmu Hukum Universitas Indonesia
korespondensi anggunlydia83@gmail.com

kata Kunci :
Pencucian Uang, Pendanaan Terorisme, Pandemi COVID-19

ABSTRAK
Pandemi COVID-19 yang muncul pada awal tahun 2020 lalu telah mengakibatkan krisis multidimensi di berbagai bidang seperti ekonomi, sosial, budaya, politik dan lain sebagainya yang belum pernah terjadi sebelumnya. Kondisi ini memaksa Pemerintah dan dunia global lebih fokus untuk menangani dan menyelesaikan dampak pandemi terhadap aspek perekonomian, kesehatan maupun sosial budaya masyarakat. Hal ini tentunya berdampak terhadap kemampuan pemerintah dan sektor swasta dalam penerapan kewajiban Anti Pencucian Uang dan Pecegahan Pendanaan Terorisme (APU dan PPT) di berbagai bidang termasuk pengawasan, regulasi, dan kebijakan. reformasi, pelaporan transaksi mencurigakan dan kerjasama internasional. Ketidakpastian akibat pandemi COVID-19 telah dimanfaatkan oleh para pelaku kejahatan untuk memuluskan aksi kejahatan mereka. FATF melaporkan adanya peningkatan kejahatan seperti penipuan, kejahatan dunia maya, eksploitasi dana pemerintah atau bantuan keuangan internasional yang menciptakan sumber pendapatan baru bagi pelaku kejahatan di masa pandemi COVID-19. Pandemi COVID-19 telah menyebabkan perubahan pada tindak pidana asal dan perubahan aktivitas pencucian uang dan pendanaan terorisme. Penelitian ini akan membahas mengenai bagaimana kondisi pandemi COVID-19 telah berdampak pada peningkatan risiko TPPU dan TPPT dan perkembangan pola-pola kejahatan serta bagaimana upaya-upaya yang dilakukan dalam rangka pencegahan dan pemberantasan TPPU dan TPPT dimasa Pandemi COVID-19. Metode penelitian hukum yang digunakan adalah normatif-empiris yaitu dengan menggabungkan kajian norma hukum dan penerapan atau implementasi hukum normatif pada peristiwa hukum tertentu.

PENDAHULUAN

A. Latar Belakang

Virus Corona COVID-19 telah dinyatakan sebagai pandemi global oleh Organisasi Kesehatan Dunia WHO pada 11 Maret 2020 [1]. Pandemi yang diakibatkan virus COVID-19 ini telah menimbulkan gejolak di berbagai bidang seperti ekonomi, sosial, budaya, politik dan sebagainya yang belum pernah terjadi sebelumnya. Gejolak ekonomi global akibat pandemi COVID-19 telah menimbulkan ketidakpastian ekonomi yang ditandai dengan pengangguran yang tinggi, kepailitan bisnis, dan gangguan dalam pola perdagangan global. Banyak perusahaan menutup bisnisnya sehingga berdampak pada berkurangnya lapangan kerja, bertambahnya pengangguran dan meningkatnya kemiskinan. Hal ini turut berdampak pada meningkatnya kejahatan di masa pandemi COVID-19.

Serangkaian kebijakan dan tindakan dilakukan oleh Pemerintah di berbagai negara dalam menangani gejolak akibat Pandemi COVID-19 ini seperti memberlakukan kebijakan *lockdown* untuk mengatasi

[1] Archived: WHO Timeline - COVID-19, diakses dari https://www.who.int/news/item/27-04-2020-who-timeline---covid-9, pada tanggal 16 Juni 2021, pk.00:12 WIB.

penyebaran COVID 19, memberikan stimulus dan insentif untuk menggerakkan perekonomian, memberikan bantuan COVID-19 dan berbagai kebijakan lain yang membuka peluang bagi para pelaku kejahatan yang memanfaatkan kondisi pandemi ini melakukan tindakan melawan hukum.

Pandemi COVID-19 membuat dunia berfokus untuk merespons langkah-langkah perbaikan terhadap kondisi kesehatan, ekonomi dan sosial masyarakat dunia. Hal ini berdampak pada kemampuan pemerintah dan sektor swasta untuk menerapkan kewajiban anti pencucian uang dan pencegahan pendanaan terorisme (APU PPT) di berbagai bidang termasuk pengawasan, regulasi, dan kebijakan, reformasi, pelaporan transaksi mencurigakan dan kerjasama internasional.[2] Hal ini menyebabkan munculnya risiko dan kerentanan diantaranya yaitu penjahat menemukan cara untuk melewati langkah-langkah *Customer Due Diligence* (CDD), melakukan penyalahgunaan layanan keuangan online dan aset virtual untuk memindahkan dan menyembunyikan dana haram, memanfaatkan langkah-langkah stimulus ekonomi dan skema kepailitan sebagai sarana bagi perorangan dan badan hukum untuk menyembunyikan dan mencuci dana gelap, meningkatkan penggunaan sektor keuangan yang tidak diatur sehingga menciptakan peluang tambahan bagi penjahat untuk mencuci dana terlarang, penyalahgunaan bantuan keuangan domestik dan internasional dan bantuan dana darurat, serta memanfaatkan COVID-19 dan penurunan ekonomi untuk beralih ke lini bisnis padat uang dan likuiditas tinggi baru di negara berkembang[3].

Menurut Financial Action Task Force (FATF), Badan Internasional yang menetapkan Standar Internasional tentang Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU PPT) serta pelaporan lainnya, pandemi COVID-19 turut menyebabkan perubahan signifikan dalam pola perilaku keuangan pemerintah, bisnis, dan orang-orang di berbagai belahan dunia sehingga berdampak pada peningkatan ancaman dan risiko TPPU dan TPPT dengan pola-pola atau modus yang berkembang [4].

Kebijakan *lockdown* atau pembatasan dalam rangka pencegahan penyebaran virus COVID-19 telah menyebabkan sebanyak kurang lebih 300 juta pekerja kantor di seluruh dunia bekerja dari rumah[5]. Sejumlah sekolah termasuk di Indonesia juga masih memberlakukan pembelajaran *online*. Masyarakat semakin beralih kepada *platform-platform* online dalam kegiatan sehari-hari. Penutupan aktivitas bisnis juga turut andil dalam peningkatan penjualan *online* dan penggunaan alat pembayaran digital. Peningkatan transaksi *online* ini menimbulkan tantangan tersediri bagi perbankan dan lembaga keuangan lain untuk tetap dapat memenuhi aspek APU/PPT.

Pelaporan dari anggota FATF, pengamat, dan sumber terbuka menunjukkan bahwa para penjahat telah berusaha mengambil untung dari pandemi COVID-19 melalui peningkatan aktivitas penipuan seperti penipuan investasi, pemalsuan barang medis, penggalangan bantuan palsu, maupun penipuan berbasis online. Selain itu, terjadi peningkatan tajam terkait serangan *cyber*, khususnya *email* phishing dan pesan seluler (SMS) serta serangan *ransomware*.[6]

Di Indonesia sendiri terjadi peningkatan transaksi keuangan mencurigakan selama masa pandemi COVID-19. Hal ini berdasarkan laporan pada Buletin Statistik Anti Pencucian Uang dan Pendanaan Terorisme Edisi Desember 2020 yang dikeluarkan oleh Pusat Pelaporan Analisis dan Transaksi Keuangan (PPATK), yang melaporkan adanya peningkatan pada Laporan Transaksi Keuangan Mencurigakan (LKTM) yang terkait dengan berbagai kejahatan seperti korupsi, penipuan, perjudian online, tindak pidana perpajakan dan pasar modal [7]. Peningkatan laporan transaksi keuangan mencurigakan tersebut mengindikasikan adanya peningkatan risiko TPPU dan TPPT. Terkait hal tersebut, diperlukan respon kebijakan dari otoritas terkait dan sinergi dari seluruh pihak sebagai upaya pencegahan dan pemberantasan TPPU dan TPPT di Indonesia khususnya di masa pandemi COVID-19 seperti saat ini.

[2] FATF (2020), "*COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*", diakses dari https://www.fatf-gafi.org/publications/methodsandtrends/documents/covid-19-ml-tf.html, tanggal 16 Juni 2021 pk. 01:05 WIB.

[3] FATF, *op.cit.*

[4] Rose, Liana W (2020), *"COVID-19 and Emerging Global Patterns of Financial Crime"*, Congressional Research Service, hal.1

[5] Crisanto, Juan Carlos dan Jermy Prenio (2020), "*Financial Crime in Times of Covid-19 - AML and Cyber Resilience Measures*", Bank of International Settlement Publication.

[6] FATF (2020), "*COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*", FATF Publication, hal.4-7.

[7] Buletin Statistik Anti Pencucian Uang dan Pendanaan Terorisme Edisi Desember 2020

B. Rumusan Masalah

Rumusan masalah dalam makalah ini sebagai berikut:

1. Bagaimana perkembangan kejahatan TPPU dan TPPT di masa pandemi COVID-19?
2. Bagaimana upaya pencegahan dan pemberantasan TPPU dan TPPT di masa Pandemi COVID-19?

C. Metode Penelitian

Metode penelitian hukum yang digunakan adalah normatif-empiris yaitu dengan menggabungkan kajian norma hukum dan penerapan atau implementasi hukum normatif pada peristiwa hukum tertentu dan hasilnya yang dikaji secara komprehensif analitis, dan hasil kajiannya dipaparkan secara lengkap, rinci, jelas, dan sistematis. Adapun data yang digunakan dalam penelitian ini berupa data sekunder yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Dari bahan-bahan yang sudah ada kemudian dianalisis secara deskriptif, komparatif, kualitatif kemudian dideduksi untuk menjawab permasalahan yang diteliti.

PEMBAHASAN DAN ANALISIS

A. Perkembangan Kejahatan TPPU dan TPPT di Masa Pandemi COVID-19 (Contoh Kasus dari Berbagai Yurisdiksi).

A.1Perkembangan pada Tindak Pidana Asal (*Predicate Crime*)

Tindak Pidana Pencucian Uang (TPPU) bertujuan untuk melindungi atau menutupi suatu aktivitas kriminal yang menjadi sumber dana atau uang yang akan "dibersihkan". Dengan demikian, pemicu dari kejahatan pencucian uang yang sebenarnya adalah suatu tindak pidana atau aktivitas kriminal. Kegiatan pencucian uang memungkinkan pelaku kejahatan menyembunyikan asal usul sebenarnya dari suatu dana atau uang hasil kejahatan yang dilakukan dan pelaku dapat menikmati dan menggunakan hasil kejahatannya secara bebas seolah-olah tampak sebagai hasil kegiatan yang sah atau legal.[8].

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU) Pasal 2 ayat (1) UU TPPU telah mengatur mengenai jenis-jenis tindak pidana asal (*predicate crime*) yang dapat dikenakan pidana pencucian uang yaitu antara lain tindak pidana : korupsi, penyuapan, narkotika, psikotropika, penyelundupan tenaga kerja, penyelundupan migran, di bidang perbankan, di bidang pasar modal, di bidang perasuransian, kepabeanan, cukai, perdagangan orang, terorisme, penculikan, pencurian, penggelapan, penipuan, pemalsuan uang, perjudian, prostitusi, di bidang perpanjakan, di bidang kehutanan, di bidang kelautan, di bidang lingkungan hidup, di bidang kelautan dan perikanan atau tindak pidana lain pidana penjara 4 (empat) tahun atau lebih, yang dilakukan di wilayah Negara Kesatuan Republik Indonesia atau di luar wilayah Negara Kesatuan Republik Indonesia dan tindak pidana tersebut juga merupakan tindak pidana menurut hukum Indonesia[9].

Namun demikian, terdapat perbedaan yang mendasar dari *predicate crime* untuk tindak pidana terorisme. Dalam tindak pidana terorisme, uang yang diduga akan digunakan secara langsung atau tidak langsung untuk kegiatan terorisme dapat dikenakan pidana pencucian uang, walaupun uang tersebut bukan diperoleh dari suatu tindak pidana.[10] Aturan terkait hal ini terdapat pada Pasal 2 ayat (2) UU TPPU sebagai sebagai berikut:

Pasal 2 ayat (2) :

"Harta Kekayaan yang diketahui atau patut diduga akan digunakan dan/atau digunakan secara

[8] Husein, Yunus (2007), *Bunga Rampai Anti Pencucian Uang*, (Penerbit : BooksTerrace & Library: Cetakan Pertama 2007), hal 26
[9] Wiyono, R (2014), Pembahasan UU Pencegahan dan Pemberantasan TPPU, (Jakarta : Sinar Grafika), hal. 41
[10]Wiyono, R, *ibid,* hal. 41-53

langsung atau tidak langsung untuk kegiatan terorisme, organisasi teroris, atau teroris perseorangan disamakan sebagai hasil tindak pidana sebagaimana dimaksud pada ayat (1) huruf n".

Adapun setiap negara memiliki ketentuan yang berbeda terkait jenis tindak pidana yang dikategorikan sebagai *predicate crime.*

Sehubungan dengan kondisi Pandemi COVID-19 saat ini dan pengaruhnya terhadap perkembangan *predicate crime*, hasil analisa FATF menunjukkan bahwa penjahat terus mengeksploitasi peluang yang diciptakan akibat pandemi COVID-19 di seluruh dunia, dengan meningkatnya kasus pemalsuan uang, barang medis, penipuan investasi, penipuan kejahatan *cyber crime*, dan penyalahgunaan stimulus ekonomi dari pemerintah dan penipuan amal. Selain itu, terdapat contoh eksploitasi anak secara online karena peningkatan waktu yang dihabiskan untuk aktifitas *online*, peningkatan kejahatan properti karena properti tidak berpenghuni, dan korupsi sehubungan dengan kontrak pasokan barang-barang medis[11].

Sejumlah yurisdiksi telah melaporkan peningkatan dramatis dalam jumlah jenis kasus tertentu. Peningkatan kejahatan ini terkait dengan jenis penipuan seperti pemalsuan barang medis dan penyalahgunaan tindakan stimulus ekonomi atau korupsi yang berkaitan dengan kontrak publik. Berikut ini beberapa contoh peningkatan kejahatan tertentu dari berbagai yurisdiksi sebagai akibat dari pandemi COVID-19.

I. Kejahatan Terorganisir dan Tindak Pidana Asal

Kasus di Brasil - COVID-19 Memicu Meningkatnya Kejahatan Terorganisir dan Tindak Pidana Asal[12]

Dalam periode bulan April dan November 2020, Polisi Federal Brazil melakukan 56 operasi polisi di 17 negara bagian Federasi yang berbeda terkait dengan tindakan korupsi atau penyalahgunaan sumber daya publik dan pencucian uang. Operasi ini menghasilkan 133 penangkapan, 985 perintah penggeledahan dan penyitaan dan perintah penyitaan dalam berbagai kasus penipuan kontrak publik, dengan total nominal berjumlah sekitar 1,9 miliar Brazilian Real atau sekitar USD 360 juta. Adapun kasus-kasus yang terjadi adalah terkait adanya *mark up* penjualan peralatan medis, pembelian peralatan medis tanpa izin, penyimpangan dalam kontrak penawaran, penipuan umum dalam tender publik dan penggelapan dana yang ditujukan untuk memerangi COVID-19.

Investigasi yang dilakukan termasuk investigasi pencucian uang, penyalahgunaan sumber daya publik, korupsi, penipuan, penggelapan dan kemungkinan tindak pidana asal lainnya. Praktik pencucian uang melibatkan penggunaan rekening bank pihak ketiga dan perusahaan, penyembunyian nilai tunai, investasi di pasar ternak, serta praktik lainnya.

II. Kasus Penipuan

Pandemi COVID-19 telah memicu tingginya angka kasus penipuan baik di Amerika Serikat maupun belahan negara lainnya. Bentuk umum dari penipuan terkait pandemi COVID-19 antara lain penipuan produk medis (misalnya, penipuan *non delivery*, penipuan harga, penimbunan barang, serta penjualan produk palsu, di bawah standar, tidak disetujui, dan penjualan merk yang salah); penipuan investasi dan sekuritas (misalnya, perdagangan orang dalam, penipuan investasi, dan penipuan akun pensiun; dan penipuan bantuan/amal palsu. Di tengah krisis COVID-19, menurut Organisasi Polisi Eropa (EUROPOL), masker bedah palsu merupakan produk medis yang paling banyak dijual secara online. Organisasi Polisi Kriminal Internasional (Interpol) telah mengeluarkan Purple Pemberitahuan tentang skema COVID-19 dan penipuan yang melibatkan pola pembayaran keuangan transnasional.[13]

Interpol, Europol, dan lainnya, menganggap pemalsuan barang medis, seperti obat palsu, dan pakaian pelindung, sebagai ancaman yang signifikan. Rentang studi kasus menunjukkan bahwa pemalsuan barang medis terus menjadi pelanggaran yang sangat umum, dan yurisdiksi dari

[11] FATF (Desember : 2020), "*Update: COVID-19-related Money Laundering and Terrorist Financing*", FATF Publication, hal. 6-7.
[12] FATF, *ibid* hal.7
[13] Rose, Liana W, *ibid.* hal 2

setiap wilayah di seluruh dunia melaporkan adanya peningkatan. Dampak dari kejahatan ini sangat signifikan. Bahan medis yang salah atau tidak diatur berpotensi menyebabkan kerusakan fisik pada individu yang menggunakannya.[14]

a. Interpol – Penipuan COVID-19 Internasional[15]

Pada bulan Maret, otoritas kesehatan Jerman mengontrak dua perusahaan di Zurich dan Hamburg untuk membeli masker wajah senilai EUR 15 juta. Akibat adanya kekurangan pasokan medis yang terjadi secara global, sulit di lakukan pengadaan dengan jalur yang biasa. Pembeli kemudian mencari vendor baru dan menemukan alamat email dan situs web yang tampaknya terkait dengan sebuah perusahaan di Spanyol. Tanpa sepengetahuan mereka, situs itu palsu dan alamat email di dalamnya telah disusupi. Perusahaan awalnya mengklaim memiliki 10 juta masker, namun untuk pengiriman mengalami kegagalan. Hal itu kemudian merujuk pembeli ke *dealer* di Irlandia yang menempatkan mereka berhubungan dengan pemasok di Belanda.

Kesepakatan untuk pengiriman awal sebanyak 1,5 juta masker dibuat dengan pemasok Belanda, membutuhkan uang muka pembayaran sebesar EUR 1,5 juta. Tepat sebelum tanggal pengiriman, pembeli diberitahu bahwa diperlukan transfer lebih lanjut sebesar EUR 880.000. Ketika pembeli menyadari bahwa mereka ditipu, mereka menghubungi bank mereka di Jerman, yang kemudian menghubungi unit Kejahatan Keuangan Interpol. Bank, unit intelijen keuangan dan otoritas peradilan, serta mitra, organisasi Europol dan Eurojust, bergabung dengan Interpol dalam penyelidikan. Intervensi segera memungkinkan mereka untuk membekukan EUR 1,5 juta dan mengidentifikasi Perusahaan Irlandia yang terlibat. Pihak berwenang Belanda melacak EUR 880.000 yang telah ditransfer dari bank Jerman. Sebesar kurang lebih EUR 500.000 sudah telah dikirim ke Inggris, yang semuanya ditujukan untuk akun di Nigeria.

Berkat peringatan yang diajukan oleh penyelidik, bank Inggris dapat menarik kembali secara penuh atas dana tersebut yang kini telah dikembalikan ke Belanda dan dibekukan oleh otoritas. Operasi tersebut telah menyebabkan penangkapan dan hukuman terhadap dua orang tersangka di Belanda. Sesuai dengan temuan investigasi saat ini, kedua pelaku bertindak atas nama tersangka utama, yang ditangkap pada bulan Agustus di Nigeria.

b. Hong Kong, Tiongkok - Penipuan Alat Pelindung Diri[16]

Pada bulan Januari 2020, seseorang memasang iklan di berbagai *platform e-commerce* yang mengklaim memiliki sejumlah besar masker bedah dan alkohol sanitiser untuk dijual. Dalam periode Januari s.d Maret 2020, sebanyak lebih dari 200 korban membeli barang-barang ini secara lokal dan membayarnya dengan menyetor uang tunai atau membuat transfer dana elektronik. Total dana sebesar HKD 1,4 juta (USD 180.630) telah disetorkan ke tiga rekening bank Hong Kong dan empat dompet elektronik yang dipegang oleh pasangan dan rekan mereka.

Pada awal Maret 2020, para korban melaporkan bahwa mereka belum

menerima barangnya dan tidak dapat menghubungi salah satu individu yang terlibat. Investigasi mengungkapkan bahwa uang itu ditarik dengan cepat setelah korban menyetorkannya ke rekening bank dan dompet elektronik yang ditunjuk. Penegak hukum menangkap empat orang pada April 2020. Pada saat publikasi laporan ini (Desember 2020), individu belum didakwa dan penyelidikan tetap berlangsung.

III. Cyber Crime

Pergeseran aktivitas kearah online selama pandemi COVID-19 telah memicu peluang bagi

[14] FATF, ibid hal 8-9
[15] FATF, ibid hal 8-9
[16] FATF, *ibid.* hal 11.

penjahat *cyber* untuk menargetkan individu dan bisnis. Ketergantungan yang lebih besar pada *platform* jarak jauh dan virtual selama pandemi telah semakin mengekspos kerentanan dunia maya, termasuk kerentanan sistem keuangan dan perawatan kesehatan. Penjahat dunia maya menggunakan kembali skema yang diketahui (misalnya, kampanye phishing, distribusi *malware*, dan skema kompromi email bisnis) untuk menargetkan korban dengan umpan terkait COVID-19. FinCEN melaporkan bahwa pencucian uang kejahatan dunia maya terutama melibatkan mata uang virtual. Menurut INTERPOL, telah terjadi peningkatan domain berbahaya dan berisiko tinggi yang terdaftar dengan kata kunci terkait COVID-19. EUROPOL lebih lanjut melaporkan peningkatan serangan *cyber* selama pandemi dan periode yang lebih pendek antara infeksi *ransomware* awal dengan aktivasi serangannya, serta penggunaan berkelanjutan *platform* web gelap yang untuk mendistribusikan barang dan layanan terlarang.[17]

Sejumlah besar yurisdiksi dari berbagai wilayah di seluruh dunia melaporkan adanya peningkatan terus-menerus dalam penipuan terkait *cyber*, khususnya skema phishing email dan SMS, penipuan kompromi email bisnis dan juga serangan *ransomwar*e. Karena tindakan pemerintah dan kepentingan individu telah berubah selama enam bulan terakhir, skema SMS dan email phishing terkait COVID-19 telah berubah. Hal ini termasuk juga email dengan tautan palsu ke paket stimulus pemerintah, bank yang mendistribusikan bantuan, peta tingkat infeksi, dan situs web yang menjual masker. Satu yurisdiksi melaporkan kasus di mana penjahat mengirim email yang mengancam tidak hanya untuk membocorkan data pribadi korban, tetapi juga menginfeksi mereka dan keluarga mereka dengan virus corona jika mereka tidak membayar penjahat. [18]

a. Spanyol - Phishing Email[19]

Dalam kasus email phising di Spanyol, Departemen *Cyber Crime* dari Kepolisian Nasional Spanyol menerima peringatan dari serangan phishing yang melibatkan sejumlah besar email yang meniru perusahaan pengecer online terkenal. Serangan phishing ini berfokus untuk mendapatkan informasi identifikasi korban dan nomor kartu kredit mereka. Data diperoleh dari para korban kemudian dapat dijual ke organisasi kriminal lain atau digunakan dalam kegiatan penipuan lebih lanjut.

Kejadian ini terjadi pada akhir Maret 2020, selama periode *lockdown* pertama, terjadi peningkatan volume pembelian online yang mengakibatkan peningkatan serangan phishing. Isi pesan email menunjukkan bahwa akun pribadi pelanggan di perusahaan yang disebutkan telah diblokir dan untuk alasan keamanan karena kemungkinan akses yang tidak sah. Tautan ke halaman web yang menyamar sebagai perusahaan ritel online juga disertakan dalam email dengan tujuan untuk mendapatkan informasi secara curang.

Aktivitas terlarang itu terdeteksi melalui analisis informasi dan data transaksi yang dikembangkan oleh unit polisi *cybercrime* khusus. Akibat adanya peningkatan aktivitas online selama periode *lockdown*, dilakukan peningkatan pemantauan atau yang disebut “patroli dunia maya.

b. Indonesia - Penipuan Business Email Compromise [20]

Modus Penipuan dengan menggunakan Business Email Compromise di tengah pandemi COVID-19, aktivitas kriminal dengan memanfaatkan ketidakhati-hatian berbagai negara yang mengalami kepanikan karena kekurangan persediaan alat kesehatan, terus meningkat. Modus yang dilakukan melalui Business Email Compromise-BEC yaitu dengan mengirimkan perintah melalui email ke perusahaan pembeli agar mengalihkan rekening tujuan pembayaran ke rekening bank lain di negara lain.

Berdasarkan data PPATK, terdapat kasus penipuan dengan modus BEC yang dilakukan warga negara Indonesia yang merugikan sebuah perusahaan dibidang manajemen dan pemeliharaan

[17] Rose, Liana W, *ibid.* hal 3
[18] FATF, *ibid.* hal 11.
[19] FATF, *ibid.* hal 11.
[20] PPATK (2020), Laporan PPATK Semeseter 1/2020, hal. 56

peralatan medis di Italia. Perusahaan di Italia melakukan kontrak kerjasama pembelian 1.500 lung ventilators dan 5.000 multi-parameter monitors dengan perusahaan di China total nilai EUR17.011.980,-. Modus yang dilakukan pelaku adalah dengan mendirikan beberapa perusahaan palsu yang bergerak dibidang perdagangan alat laboratorium, farmasi dan kedokteran dengan nama yang hampir sama dengan counterpart bisnis perusahaan Italia yang berada di China tersebut. Pelaku juga membuka rekening atas nama perusahaan palsu di salah satu bank di Indonesia yang dipersiapkan untuk menampung pembayaran dari perusahaan pembeli. Selanjutnya, dengan menggunakan domain email palsu yang mirip dengan domain email perusahaan di China, pelaku mengirimkan informasi perubahan rekening bank pembayaran dengan alasan situasi COVID-19, sehingga menyebabkan perusahaan di Italia mengirimkan dananya ke rekening perusahaan palsu di Indonesia total sebesar Rp58,8 miliar dalam tiga kali transaksi Incoming SWIFT. Pada periode yang berdekatan, dari total dana masuk tersebut sebesar Rp2,7 miliar ditransfer ke beberapa rekening perusahaan tempat penampungan dana dan ditransfer ke banyak pihak individu dalam 72 kali transaksi untuk selanjutnya dilakukan transaksi penarikan dana tunai hingga hanya meninggalkan saldo minim dalam rekening. Sementara, sisa dana sebesar Rp56,1 miliar berhasil diselamatkan dengan melakukan penundaan transaksi oleh Bank dan dilanjutkan dengan penghentian sementara transaksi.

c. Thailand- Pencurian Identitas

Para pelaku kejahatan menawarkan peluang kerja kepada pencari kerja melalui situs web. Setelah pendaftaran di situs web, para pencari kerja diminta untuk mengisi data pribadi mereka termasuk nomor rekening bank. Para pelaku kemudian menggunakan informasi ini untuk melakukan pencurian identitas dengan cara meretas rekening bank korban dan/atau akun Facebook mereka dan kemudian meminta uang dari teman korban. Kegiatan penipuan ini dilakukan oleh jaringan pelaku. Hasil kejahatan, sekitar 200.000 Baht (USD6.460) kemudian ditransfer ke dompet elektronik mereka. Setelah penangkapan beberapa pelaku, hasil kejahatan berjumlah sekitar 105.000 Baht (USD3.390) dikembalikan kepada para korban.

IV. Penipuan Investasi

Yurisdiksi sebagian besar wilayah terus melaporkan risiko penipuan investasi yang melibatkan iklan penipuan dari perusahaan yang diduga mengembangkan apa yang disebut “obat ajaib” untuk COVID-19. Pelaku *Scammers* berusaha menarik korban dengan membuat klaim palsu bahwa investasi mereka akan tumbuh secara eksponensial nilainya sebagai akibat dari pandemi, kemudian dana ditarik dan dicuci oleh penjahat yang mengoperasikan skema.[21]

Kasus di California, USA - Penipuan Investasi [22]

Pada Juni 2020, seorang pria di California didakwa atas tuduhan penipuan yang menyatakan bahwa dia meminta orang-orang di seluruh negeri untuk berinvestasi di perusahaan yang akan memasarkan pil yang dia klaim akan mencegah infeksi virus corona dan menghasilkan obat suntik bagi mereka yang sudah menderita COVID-19. Terdakwa secara melawan hukum mengklaim telah mengembangkan obat untuk virus COVID-19 dan perawatan yang mencegah seseorang terinfeksi oleh COVID-19 virus melalui pesan teks, video, dan pernyataan yang dikirim ke calon investor dan diposting di internet.

Surat dakwaan menuduh bahwa dia secara curang meminta investasi di dua perusahaan dengan serangkaian janji palsu, termasuk hasil ajaib dari produk pencegahan dan pengobatannya, serta “*return*” besar atas investasi yang bebas risiko dan dijamin 100%. Untuk mendukung klaim, terdakwa menyatakan bahwa ada pihak yang tidak disebutkan namanya di Dubai telah menawarkan untuk membeli dua perusahaan seharga USD 10 miliar, dan mengklaim penawaran ini akan

[21] FATF, *ibid.* hal 12-13
[22] FATF, *ibid.* hal 12-13

mengamankan investasi investor korban di kedua perusahaan, dan dia telah mendapatkan dana dari tujuh investor yang masing-masing telah menginvestasikan antara USD 750ribu dan USD 1juta.

FBI menangkap terdakwa pada Maret 2020 setelah dia memberikan pil yang diklaim merupakan pengobatan untuk mencegah infeksi virus corona kepada agen rahasia yang menyamar sebagai investor. Pelaku didakwa dengan 11 tuduhan penipuan yang berasal dari permintaan yang diduga dibuat untuk calon investor di Nevada, New York, Texas dan Colorado. Dua dari dakwaan terkait dengan komunikasi dengan agen yang menyamar. Catatan: Di Amerika Serikat, surat dakwaan berisi tuduhan bahwa terdakwa telah melakukan kejahatan. Setiap terdakwa dianggap tidak bersalah sampai dan kecuali terbukti bersalah di luar batas wajar keraguan.

V. Penggalangan Dana Palsu - Penipuan Amal

Fraud melalui penggalangan dana untuk program amal palsu terus berlanjut selama pandemi. Dalam skema ini, *scammers* menghubungi individu, menggambarkan bahwa mereka mencari dana untuk *non existing charity* sendiri, dengan menggunakan platform sosial media untuk meminta dana. Dalam beberapa kasus, penipu telah menipu korban dengan bertindak seolah-olah mereka adalah perwakilan dari badan amal global yang terkenal, dan dalam kasus lain mereka telah membuat program amal palsu.[23]

Kasus di China - Penipuan Amal [24]

Contoh kasus di China, Mr. W, mengklaim telah menyumbang untuk memerangi COVID-19. Ybs mempublikasikan informasi terkait pengalangan donasi bagi yang dilakukan dengan kode QR dan dipublikasikan di media online. Selama pandemi, lebih dari 100 orang dari wilayah China telah melakukan donasi dengan memindai kode QR yang disedikan. Sebagian besar dengan nominal kelipatan RMB 10 (USD 1,50) atau RMB 100 (USD 15). Nilai total donasi melebihi RMB 100.000 (USD 14.960). Tak lama setelah dana tersebut dikreditkan, kemudian dana ditransfer ke rekening bank pribadi atas nama Tn. W. Tidak ada catatan donasi yang dapat dipertanggung jawabkan. Kasusnya sudah dilaporkan ke pihak kepolisian untuk diselidiki. Belum ditemukan hubungan antara pelaku dan kelompok criminal yang terorganisir.

VI. Penyalahgunaan Program Stimulus Ekonomi

Penyalahgunaan program stimulus ekonomi terus berkembang. Selama beberapa bulan terakhir, negara-negara telah menerapkan peningkatan jumlah dan skala program stimulus. Hal ini telah memberikan peluang bagi para penjahat baik individu, perusahaan, atau kelompok kriminal terorganisir mencoba untuk memanipulasi dana pemerintah.[25]

a. Washington DC, Amerika Serikat – Penyalahgunaan Program Stimulus Ekonomi dan Pencucian Uang

Pada Juli 2020, seorang eksekutif teknologi di negara bagian Washington didakwa dengan satu dakwaan *wire fraud* dan satu tuduhan pencucian uang sehubungan dengan dugaan pengajuan setidaknya delapan Program Perlindungan *Paycheck* palsu, aplikasi pinjaman atas nama enam perusahaan berbeda untuk diasuransikan secara federal pada lembaga keuangan. Pengajuan tersebut untuk mendapatkan pinjaman sebersar lebih dari USD 5,5 juta. Dalam mendukung pengajuan pinjaman palsu tersebut, tersangka diduga membuat banyak pernyataan palsu dan menyesatkan tentang operasi bisnis perusahaan masing-masing dan biaya penggajiannya. Pengaduan pidana lebih lanjut menuduh bahwa ia menyerahkan dokumen palsu yang telah diubah, termasuk pengajuan pajak federal palsu dan dokumen penggabungan yang telah diubah.

[23] FATF, *ibid.* hal 13.
[24] FATF, *ibid.* hal 13-14.
[25] FATF, *ibid.* hal 14.

Contohnya, tersangka telah mengeluarkan pernyataan tidak benar bahwa salah satu perusahaannya memiliki puluhan karyawan dan membayar jutaan dolar dalam bentuk upah dan pajak gaji. Dalam kenyataannya, perusahaan dimaksud dibeli di internet pada Mei 2020, tidak memiliki karyawan dan tidak ada aktivitas bisnis pada saat pembelian. Tersangka juga diduga mentransfer setidaknya USD 231.000 dalam pinjaman yang diperoleh secara curang ke akun pialang pribadinya untuk keuntungan pribadinya. Kasus ini diselidiki oleh otoritas terkait di Amerika Serikat. Catatan: Di Amerika Serikat, pengaduan pidana hanyalah tuduhan dan semua terdakwa adalah dianggap tidak bersalah sampai terbukti bersalah tanpa keraguan di pengadilan.

b. Swiss – Penipuan Permohonan Pinjaman COVID-19 [26]

Pada pertengahan Juni 2020, sebuah lembaga keuangan memberikan pinjaman COVID-19 sebesar CHF 90.000 (EUR 98.500) untuk perusahaan yang aktif dalam sektor konstruksi. Beberapa hari kemudian, lembaga keuangan diberitahu bahwa perusahaan tersebut mencari pinjaman tambahan dari lembaga keuangan lain. Sementara, diketahui bahwa sebagian besar pinjaman telah ditarik tunai dan dihabiskan untuk biaya konsumsi sehari-hari. Oleh karena itu, lembaga keuangan melaporkan hal tersebut sebagai laporan kegiatan mencurigakan kepada FIU Swiss. Kasus telah diteruskan ke otoritas penegak hukum Swiss yang kompeten dan proses pidana telah berlangsung.

c. Italia - Kejahatan Terorganisir dan Penyalahgunaan Program Stimulus Ekonomi[27]

Investigasi yang berakhir pada Juli 2020 mengungkapkan bahwa anggota kelompok kriminal, terkait dengan kelompok kejahatan terorganisir bergaya mafia, sedang menjalankan bisnis yang konon terlibat dalam perdagangan logam di Italia. Namun, bisnis yang sebenarnya adalah terkait dengan sejumlah tindak pidana asal yang berkaitan dengan COVID-19. Tindak pidana asal yang terlibat menghasilkan pernyataan pajak palsu atau menyesatkan, yang kemudian digunakan untuk menipu dan mendapatkan pengembalian PPN. Dana itu kemudian dicuci via bank dan sebagian dikirim ke perusahaan yang berlokasi di negara asing di Eropa, dan sebagian lainnya dikirim ke negara asing di luar negeri, kemudian para penjahat menerima koresponden sejumlah uang tersebut secara tunai melalui koresponden di Italia.

Penipuan PPN menghasilkan omset palsu bagi perusahaan yang terlibat dalam skema ini. Dalam konteks pandemi COVID-19, terdapat persyaratan untuk mendapatkan hibah publik yang tidak perlu dibayar kembali. Skema kriminal juga digunakan untuk mencoba meminta dukungan ekonomi tambahan. Penyelidikan lebih lanjut mengungkapkan bahwa tersangka utama menggunakan omset palsu yang dihasilkan dari penipuan PPN dan membenarkan kerugian akibat pandemi, agar dapat menerima hibah yang tidak dikembalikan sebagai insentif akibat pandemi COVID-19 untuk tiga perusahaan yang termasuk dalam skema kriminal. Berdasarkan iInvestigasi, terdeteksi pula bahwa penjahat berusaha untuk mendapatkan keuntungan dari pinjaman yang diberikan negara dalam rangka pemulihan sistem ekonomi akibat dampak COVID-19. Otoritas penegak hukum menyita senilai hampir EUR 7,5 juta aset dan sumber daya keuangan dan serta menangkap 10 tersangka.

VII. Penyalahgunaan Dana Bantuan

Selain penyalahgunaan dana pemerintah yang melibatkan penipuan pinjaman perusahaan, aplikasi hibah dan aplikasi asuransi pengangguran, sejumlah yurisdiksi juga menyatakan keprihatinan atas kemungkinan penyalahgunaan bantuan internasional yang diterima untuk tujuan memerangi pandemi. Selain itu, beberapa yurisdiksi juga melaporkan kasus korupsi yang melibatkan penyalahgunaan dana pemerintah yang ditujukan untuk penggunaan peralatan medis atau kontrak yang didanai publik.[28]

[26] FATF, *ibid.* hal 14-16.
[27] FATF, *ibid.* hal 16.
[28] FATF, *ibid.* hal 17.

Tunisia – Penyalahgunaan Bantuan

Pada bulan Oktober 2020, unit intelijen keuangan Tunisia (CTAF) menerima laporan transaksi mencurigakan dari lembaga keuangan yang menunjukkan bahwa Warga negara Tunisia (Mr. X) menguangkan cek bank sebesar TND 2 juta (kira-kira. USD 724.000) ke dalam rekening perusahaannya, Perusahaan C. Tuan X mengklaim bahwa dana itu berasal dari konsulat negara asing yang mengeluarkan cek kepadanya yang dimaksudkan membantu 2.000 warga asing yang terdampar di Tunisia selama periode penahanan dengan menyediakan akomodasi, obat-obatan, persediaan, dan tes COVID-19. Pada hari yang sama ketika Tuan X mencairkan cek, dia mentransfer seluruh uang tersebut ke rekening yang berbeda-beda milik perorangan, klinik dan firma saudaranya (Perusahaan A). Tak lama kemudian, CTAF menerima laporan transaksi mencurigakan lainnya dari lembaga keuangan yang berbeda, yang dipicu oleh fakta bahwa rekening Perusahaan A menerima lima transfer identik dari Perusahaan C pada hari yang sama dengan total TND 400.000 (USD 145.000).

Analisis lebih lanjut menunjukkan bahwa dalam rentang waktu yang singkat (kurang dari 6 bulan setelahnya) membuka rekening) Perusahaan C menerima enam transfer hanya dari konsulat dimaksud dengan jumlah total hampir TND 7 juta (USD 2,5 juta). Tak lama setelah itu, sebesar TND 500.000 (USD 182.000) ditarik tunai dan TND 2,5 juta (USD 910.000) ditransfer ke Perusahaan B rekening (milik Tuan X), serta TND 700.000 (USD 255.000) ditransfer ke rekening pribadi Tuan X.

Dalam kenyataannya, Tuan X hanya menghabiskan 15% dari jumlah yang diterima dari konsulat asing untuk hotel, klinik dan apotek. Kontrak antara konsulat dan Perusahaan C, tidak tidak mendefinisikan jenis layanan, harga, atau pajak yang terkait dengan transaksi. Selanjutnya, Perusahaan C tidak memiliki rekening bank atau kegiatan ekonomi lain. Sementara itu, transfer yang dikirim ke Perusahaan A ditemukan berdasarkan penipuan faktur, berisi harga yang sangat tinggi dibandingkan dengan yang seharusnya dibebankan. Akibatnya, CTAF menyimpulkan bahwa Tuan X menggunakan perusahaan cangkang (Perusahaan C), perusahaan keluarga dan faktur palsu untuk menyesatkan bantuan publik yang diberikan oleh negara asing untuk warganya terdampar di Tunisia karena pandemi COVID-19. CTAF memerintahkan pembekuan rekening perusahaan A, B dan C, dan rekening bank Mr. X. sebagai tindakan pencegahan dan mengirim pengungkapan spontan ke unit intelijen keuangan asing serta mengirimkan laporan kepada Jaksa. Investigasi telah berlangsung.

A.2 Peningkatan Risiko Tindakan Pencucian Uang dan Pendanaan Terorisme

Secara umum dapat dikatakan bahwa aktifitas pencucian uang merupakan suatu perbuatan memindahkan, menggunakan atau melakukan perbuatan lainnya atas hasil suatu tindak pidana yang kerap dilakukan organisasi kejahatan maupun individu yang melakukan tindak pidana seperti korupsi, penyuapan, perdagangan narkotia, pembalakan liar dan sebagainya.[29] Kegiatan pencucian uang melibatkan aktifitas uang sangat kompleks.[30] Pada dasarnya kegiatan tersebut terdiri dari 3 langkah yang masing-masing berdiri sendiri, tetapi seringkali dilakukan secara bersama-sama yaitu : *placement, layering* dan *integration*[31]. Secara umum pencucian uang melibatkan 3 (tiga) metode yang bertujuan untuk manipulasi dan mengubah status dana ilegal menjadi dana legal. Ketiga metode tersebut adalah : (1) schemes to *buy and sell assets*, *goods or services*; (2) *offshore conversion schemes*; and (3) *legitimate business conversion schemes*.[32]

Sebagaimana telah diuraikan sebelumnya, pandemi COVID-19 menyebabkan adanya perubahan pola-pola kejahatan awal (*predicate crime*). Berdasarkan studi FATF ditemukan adanya peningkatan pada kasus penipuan, *cybercrime*, penyalahgunaan program stimulus ekonomi, penggalangan donasi palsu

[29] PPATK (2007), "*Rezim Anti Pencucian Uang Indonesia : Perjalanan 5 Tahun*", Penerbit : PPATK, hal. 10

[30] TURNER, Jonathan E (2011), "*Money Laundering Prevention : Detering, Detecting and Resolving Financial Fraud*", Willey, p.1

[31] *Money Laundering : A Banker's Guide To Avoiding Problem*, occ.treas.gov/launder/org.h.htm, p.2 sebagaimana dikutip dari Husein, Yunus (2007), "*Bunga Rampai Anti Pencucian Uang*", Bandung : Books Terrace & Library.

[32] *Tracing Illegal Proceeds Workbook,* E.R. Burke, Investigation Training Institute, Copyright 2001, p.15.

dan lain sebagainya yang berpotensi di"bersih"kan dengan ketiga pola diatas yaitu pembelian dan penjualan aset, pengalihan dana ilegal ke wilayah *tax haven money laundering center* maupun pemindahan/ penempatan dana hasil kejahatan pada bisnis atau kegiatan usaha yang sah.

Pergeseran pola perilaku keuangan masyarakat ke arah transaksi *online* serta volatilitas keuangan akibat kontraksi ekonomi global sebagai dampak pandemi COVID-19 telah meningkatkan risiko terjadinya pencucian uang. FATF juga mencatat adanya peningkatan dalam penggunaan aset-aset virtual yang memberikan tantangan tersendiri bagi lembaga keuangan untuk mendeteksi transaksi-transaksi yang anomali.

I. Perubahan Perilaku Masyarakat[33]

Tindakan pembatasan sosial yang diterapkan oleh pemerintah dalam rangka memutus mata rantai penyebaran COVID-19 membuat aktivitas masyarakat beralih menjadi serba *online*. Hal ini turut menyulitkan bagi lembaga-lembaga keuangan untuk mengidentifikasi terjadinya transaksi-transaksi anomali. Di beberapa negara, entitas pelapor belum terbiasa memfasilitasi transaksi atau menawarkan layanan *online* sehingga mereka mengalami kesulitan dalam melakukan prosedur APU dan PPT seperti uji tuntas pelanggan (CDD) yang efektif dan/atau pemantauan berkelanjutan.

Dalam beberapa kasus, *Work From Home* juga telah berdampak pada efektivitas pelaporan oleh entitas pelapor, yang disebabkan Staf Kepatuhan tidak dapat menjalankan fungsinya dengan efisien seperti saat sebelum pandemi. Penggunaan teknologi yang efektif menjadi lebih penting karena perubahan perilaku pelanggan dan langkah-langkah pembatasan sosial berarti bahwa interaksi tatap muka tidak selalu memungkinkan. Indikator risiko perlu diperbarui secara berkala, komunikasi berkelanjutan perlu disesuaikan, serta *sharing* informasi yang efektif antara sektor publik dan swasta sangat diperlukan karena risiko yang terus berubah dari waktu ke waktu.

Kasus : Ethiopia – Penyalahgunaan Rekening *Dormant*[34]

Seorang pegawai bank secara illegal menarik sebesar ETB 3 juta (EUR 68.300) dari sebuah rekening nasabah yang tidak aktif dan dipinjamkan kepada temannya tanpa jaminan apapun. Ketika auditor internal bank menemukan penarikan uang secara illegal dari rekening yang tidak aktif, mereka melaporkan kasus tersebut ke Ethiopian Financial Pusat Intelijen sebagai transaksi mencurigakan. Pusat Intelijen kemudian melakukan analisis dan mengirimkan hasilnya ke aparat penegak hukum untuk dilakukan tindak lanjut penyelidikan. Baik karyawan bank maupun individu yang menerima uang sedang diselidiki. Mereka didakwa melakukan korupsi dan kejahatan keuangan terkait lainnya dan untuk sementara dibebaskan dari tahanan dengan jaminan. Kasusnya masih aktif.

Penyelewengan yang dilakukan oleh pegawai bank ini terjadi ketika diumumkan adanya keadaan darurat COVID-19 di Ethiopia yang mengakibatkan kebijakan *Work From Home* bagi sebagian pegawai. Hanya sebanyak 50% pegawai yang masuk sementara sisanya bekerja dari rumah. Hal ini memungkinkan karyawan untuk mengeksploitasi sistem dan melakukan kejahatan. Sistem kontrol di lembaga keuangan juga melemah akibat berkurangnya jumlah karyawan yang hadir secara fisik di bank untuk melakukan identifikasi dan verifikasi terhadap nasabah, Selain itu, akibat dari pandemi COVID-19 banyak bisnis yang terpaksa tidak aktif secara terus menerus sepanjang masa keadaan darurat.

II. Peningkatan Volatilitas Keuangan dan Kontraksi Ekonomi[35]

[33] FATF, *ibid.* hal 18-20.
[34] FATF, *ibid.* hal 18-20.
[35] FATF, Ibid, hal 19-20

Banyak yurisdiksi menghadapi kontraksi ekonomi yang turut mengakibatkan kerentanan pencucian uang. Salah satu risikonya adalah dana dari sumber gelap dapat digunakan untuk mengeksploitasi bisnis yang sedang menghadapi kesulitan. Kerentanan ini dihadapi berbagai sektor bisnis seperti *real estate*, konstruksi, industry *cleaning*, dan sektor transportasi, serta usaha kecil dan menengah pada umumnya. Sementara itu, kekhawatiran tentang ekonomi telah menyebabkan peningkatan penarikan tunai dan pertumbuhan jumlah uang tunai yang beredar. Kombinasi antara kebijakan penutupan perbatasan dan pembatasan sosial yang dikeluarkan telah meningkatkan uang beredar yang kemudian oleh kelompok kriminal digunakan untuk aktifitas pencucian uang.

Peningkatan volatilitas keuangan juga menimbulkan kerentanan untuk terjadinya *insider trading.* Terkait dengan peningkatan volatilitas keuangan, terdapat pula kerentanan tambahan terkait dengan penyalahgunaan aset virtual (VA) dalam skema terkait pandemi (misalnya, VA dapat digunakan untuk pembayaran dalam skema penipuan terkait pandemi).

Otoritas yang kompeten mencatat kekhawatiran lebih lanjut seputar VA, termasuk penipuan "*money mule*" uang yang menargetkan orang yang baru saja menganggur atau cuti. Dalam suatu tipologi, penjahat menyamar sebagai pemberi kerja palsu, dan mendekati korban dan menawarkan mereka untuk menerima donasi ke rekening bank mereka sendiri. Selanjutnya mereka diminta untuk menyetor dana ke kios kripto. Jika dana donasi yang diterima tersebut merupakan dana haram, maka tanpa disadari korban telah menjadi bagian dalam praktek pencucian uang dan bertindak sebagai pelaku "*money mule*". Adapun definisi "*money mule*" adalah kejahatan dengan mentransfer sejumlah uang dalam jumlah kecil ke sejumlah penerima, yang akan mendapatkan komisi jika mentransfer kembali ke penerima lain.[36]

Hong Kong, China : Aset Virtual dan Penipuan COVID-19.

Pada periode Februari sampai dengan awal Maret 2020, pemilik perusahaan perdagangan produk layanan kesehatan di Hong Kong, Cina melihat iklan di internet termasuk di platform media sosial utama yang diposting oleh beberapa penjual masker bedah dan peralatan medis. Ketika dia mencoba untuk membeli peralatan, dia ditipu hingga mentransfer sejumlah HKD 450 000 (USD 58.000) ke berbagai rekening bank di Hong Kong, Cina, dan negara Eropa Timur dan mengubah nilai yang setara dengan HKD 3,96 juta (USD 510.000) menjadi Bitcoin. Untuk melakukannya, korban menarik uang tunai dari rekening bank pribadinya dan menyetorkan uang tunai ke ATM Bitcoin yang ditunjuk di mana dana tersebut ditransfer ke akun Bitcoin yang ditunjuk. Secara total terdapat tiga bank yang terletak di dua yurisdiksi (Hong Kong, Cina dan yurisdiksi Eropa Timur) yang terlibat. Lima transfer senilai mulai dari USD 47.250 hingga USD 235.830 Bitcoin ditransfer ke akun yang dimiliki oleh pelakunya. Seluruh pelaku penipuan berhenti menanggapi korban setelah menerima pembayaran.

B. Upaya Pencegahan dan Pemberantasan TPPU dan TPPT di Masa Pandemi COVID-19.

B.1Respon dan Rekomendasi Kebijakan FATF

Menghadapi krisis multidimensi akibat pandemi COVID-19 yang dampaknya tidak hanya pada bidang ekonomi, melainkan hampir seluruh aspek kehidupan, FATF telah menyampaikan respon mengenai potensi risiko TPPU/TPPT dan rekomendasi kebijakan bidang penanganan program APU PPT yang perlu diperhatikan dan diwaspadai di tengah kondisi pandemi *Covid*-19 antara lain khususnya untuk memberantas *Illicit Financing* dan juga Organisasi Nirlaba.[37] Adapun respon kebijakan dari PPATK dimaksud antara lain [38]:

[36] Despian Nurhidayat, "*Money Mule, Tren Fraud dalam Sistem Pembayaran Digital RI*", diakses pada https://mediaindonesia.com/ekonomi/382560/money-mule-tren-fraud-dalam-sistem-pembayaran-digital-ri, tanggal 17 Juni 2021 pk. 20:32WIB.

[37] OJK(2020), Webinar "*Mengelola Risiko Pencucian Uang dan Pendanaan Terorisme di Masa Pandemi Covid-19" oleh PT Pegadaian (Persero)*", diakses pada https://www.ojk.go.id/apu-ppt/id/berita-dan-kegiatan/info-terkini/Pages/webminar-pegadaian.aspx, tanggal 17 Juni 2021 pk. 22:10 WIB.

[38] FATF (2020) : "*Statement by the FATF President: COVID-19 and measures to combat illicit financing"*, FATF Publication

a. Mendorong pemerintah untuk bekerja dengan lembaga keuangan dan bisnis lain untuk menggunakan pendekatan berbasis risiko FATF dalam menghadapi tantangan yang ditimbulkan oleh COVID-19 sambil tetap waspada terhadap risiko keuangan baru dan yang muncul.

b. Meminta otoritas nasional dan badan internasional untuk memperingatkan warga dan bisnis tentang bahaya *fraud* di masa pandemi, yang mencakup penipuan investasi dan produk, serta perdagangan orang dalam terkait dengan COVID-19. Seperti penjahat, teroris juga dapat memanfaatkan peluang ini untuk mengumpulkan dana.

c. Meminta regulator, pengawas, unit intelijen keuangan, dan lembaga penegak hukum agar terus berbagi informasi dengan sektor swasta untuk memprioritaskan dan mengatasi risiko utama TPPU, terutama yang terkait dengan penipuan, dan risiko TPPT yang terkait dengan COVID-19.

d. Dalam rangka penyaluran bantuan terkait COVID-19, otoritas nasional dan lembaga keuangan diminta untuk menerapkan pendekatan berbasis risiko. FATF mendorong negara-negara untuk bekerja dengan NPO yang relevan guna memastikan bahwa bantuan yang sangat dibutuhkan sampai ke penerima yang dituju secara transparan.

e. Mendorong penggunaan teknologi, termasuk Fintech, Regtech, dan Suptech semaksimal mungkin. FATF baru-baru ini merilis Panduan tentang ID Digital, yang men*highlight* manfaat penggunaan identitas digital yang dipercaya dapat meningkatkan keamanan, privasi, dan kenyamanan melakukan identifikasi terhadap orang secara jarak jauh dalam rangka mengatasi risiko TPPU dan TPPT.

B.2. Respon Otoritas Terkait di Indonesia atas Rekomendasi FATF sehubungan Peningkatan Risiko TPPU dan TPPT di masa Pandemi COVID-19

B.2.1Respon PPATK[39]

PPATK telah melakukan serangkaian riset terkait pandemi COVID-19 dengan hasil bahwa Penipuan, Korupsi, dan Narkotika memiliki potensi risiko paling besar terhadap TPPU selama masa pandemi COVID-19; DKI Jakarta, Jawa Barat, dan Jawa Timur wilayah paling berisiko TPPU selama masa pandemi dan DKI Jakarta, Jawa Barat, Jawa Tengah, Jawa Timur, dan Aceh wilayah paling berisiko TPPT selama masa pandemi ; Pengusaha/wiraswasta, pegawai swasta, pedagang, PNS, pejabat lembaga legislatif dan pemerintahan berisiko tinggi melakukan TPPU selama masa pandemi dan Pengusaha/wiraswasta, ibu rumah tangga, pedagang, pelajar/mahasiswa berisiko tinggi menjadi sasaran TPPT selama masa pandemi ; Bank Umum berisiko tinggi digunakan untuk TPPU dan TPPT selama masa pandemi ; Tipologi TPPT yang berisiko tinggi selama pandemi adalah melalui Penyedia Jasa Keuangan.

Adapun rekomendasi atas Riset Risiko TPPU dan TPPT terkait Pandemi Covid-19 dimaksud anatara lain : (1) Melakukan pendidikan dan pelatihan secara virtual terkait kebijakan Pedoman Prinsip Mengenal Pengguna Jasa/*Customer Due Diligence* (CDD) yang didalamnya terdapat pedoman CDD elektronik dengan menerapkan prinsip APU PPT; (2) Menyusun pedoman yang memungkinkan kegiatan pengawasan/pemeriksaan dilakukan secara *on-line/virtual/remote* dengan memanfaatkan penggunaan TI; (3) Koordinasi secara intensif antar otoritas untuk fokus melakukan pengawasan pada penyelenggara yang dianggap berisiko tinggi selama pandemi COVID-19; dan (4) Mengoptimalkan proses pemantauan transaksi khususnya bagi pengguna jasa yang dianggap berisiko tinggi selama pandemi COVID-19.

Dalam rangka peningkatan efektifitas upaya pencegahan dan pemberantasan TPPU dan TPPT di Indonesia, PPATK telah mengintesifkan kerjasama dengan lembaga dan otoritas internasional terutama terkait pertukaran data. Di dalam negeri, PPATK secara intensif melakukan sinergi dengan Lembaga Pengatur dan Pengawas serta seluruh entitas pelapor.

B.2.2Respon OJK[40]

[39] PPATK (2020), "Laporan Tahunan PPATK 2020"
[40] OJK (2020), *op.cit.*

Sejalan dengan rekomendasi kebijakan FATF terkait peningkatan risiko TPPU dan TPPT di masa Pandemi COVID-19, OJK telah melakukan langkah-langkah diantaranya dengan optimalisasi pemanfaatan sarana elektronik, penggunaan digital ID dalam proses CDD, CDD Sederhana, penerimaan nasabah sebelum verifikasi diselesaikan, verifikasi *non face to face*, penerapan pengawasan APU PPT berbasis risiko, kajian khusus terkait risiko TPPU/TPPT akibat *Covid*-19 dan peningkatan penerapan *Risk Based Approcah* (RBA) di Sektor Jasa Keuangan.

Sebagai bagian dari upaya pencegahan dan pemberantasan TPPU dan TPPT di masa pandemi COVID-19, OJK juga telah mengeluarkan rekomendasi penerapan program APUPPT di masa pandemi COVID-19 bagi Penyedia Jasa Keuangan yaitu antara lain :

a. Peningkatan kewaspadaan atas timbulnya risiko TPPU dan TPPT akibat kondisi pandemi COVID-19.
b. Peningkatan kewaspadaan dalam menyikapi peningkatan aktivitas usaha Yayasan atau Lembaga amal (*non profit organization*).
c. Mengoptimalkan penggunaan CDD sederhana terhadap calon nasabah atau transaksi yang tingkat risiko terjadi TPPU dan TPPT-nya tergolong rendah.

B.2.3 Respon Bank Indonesia[41]

Dalam rangka pencegahan tindak pidana pencucian uang dan pendanaan terorisme yang memanfaatkan lembaga keuangan dibawah pengawasan Bank Indonesia, BI selaku Lembaga Pengawas dan Pengatur telah mengadakan serangkaian edukasi dan himbauan kepada Penyelenggara Jasa Sistem Pembayaran Selain Bank (PJSP SB) dan Kegiatan Usaha Penukaran Valuta Asing Bukan Bank (KUPVA BB) agar tetap waspada dalam masa pandemik COVID-19.

Isi dari Bank Indonesia tersebut antara lain : (1) *Awareness* : memahami risiko TPPU dan TPPT sebagai dampak dari COVID-19 terhadap usaha Penyelenggara tersebut; (2) *Adapt* : melakukan asesmen dampak dari COVID-19 terhadap kebijakan APU PPT Penyelenggara sesuai dengan rekomendasi FATF, seperti perluasan pembayaran berbasis digital dan pemberlakuan prinsip mengenal pengguna jasa/pelanggan yang berbasis elektronik ; (3) *Action* : melakukan pendekatan berbasis risiko dalam melakukan kebijakan APU PPT dan melakukan koordinasi dengan aparat terkait serta Pengawas Bank Indonesia.

PENUTUP

A. Kesimpulan

1. Pandemi COVID-19 telah menimbulkan krisis multidimensi di berbagai bidang terutama bidang ekonomi, kesehatan dan sosial. Pemerintah di banyak negara merespon kondisi pandemi dengan mengeluarkan berbagai kebijakan seperti kebijakan pembatasan sosial, pemberian stimulus ekonomi, dan berbagai kebijakan lain. Kondisi ini telah menyebabkan perkembangan dan pergeseran pola-pola kejahatan pada tindak pidana asal (*predicate crime*) dan pada akhirnya berdampak terhadap peningkatan risiko TPPU dan TPPT.

2. Kebijakan pembatasan sosial yang diterapkan pemerintah menyebabkan adanya pergeseran perilaku masyarakat ke arah serba *online*, baik itu dalam hal bekerja, sekolah, berbelanja maupun bertransaksi keuangan semua dilakukan secara *online*. Pola-pola transaksi *online* ini memunculkan sejumlah ancaman *cyber crime* dan menjadi tantangan bagi lembaga keuangan dalam melakukan identifikasi dan verifikasi yang diperlukan terhadap pengguna jasa. Selain itu pandemi juga menyebabkan peningkatan penggunaan aset-aset virtual yang beresiko tingi dimanfaatkan pelaku TPPU dan TPPU sebagai sarana untuk melakukan kejahatan.

[41] Bank Indonesia , diakses dari https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/anti-pencucian-uang-dan-pencegahan-pendanaan-terrorisme/default.aspx, tanggal 18 Juni 2020, pk. 21.19 WIB.

3. Gejolak ekonomi akibat pandemi COVID-19 telah memukul perekonomian dan memaksa banyak bisnis untuk menutup usahanya sehingga berdampak terhadap berkurangnya sumber pendapatan dan lapangan kerja. Pemerintah merespon dengan mengeluarkan berbagai kebijakan stimulus dan insentif untuk menggerakkan ekonomi. Berbagai stimulus ekonomi ternyata memicu pelaku kejahatan untuk melakukan berbagai aksi manipulasi dan penipuan yang merugikan pemerintah.

4. Kebutuhan akan barang-barang medis meningkat tajam akibat Pandemi COVID-19. Hal ini ternyata dimanfaatkan oleh oknum pelaku kejahatan untuk melakukan berbagai kejahatan seperti penipuan, penjualan barang palsu, dan kejahatan lain.

5. Selain itu, kejahatan lain yang marak di masa pandemi COVID-19 adalah terkait penggalangan dana palsu, korupsi dan penyalahgunaan dana bantuan COVID-19, Penyelewenangan dana hasil donasi, dan lain sebagainya.

6. Menanggapi peningkatan risiko TPPU dan TPPT di masa pandemi COVID-19, FATF telah menyampaikan respon kebijakan dan himbauan yang secara garis besar dapat disimpulkan sebagai berikut : (1) Peningkatan koordinasi domestik terutama dalam menilai dampak COVID-19 pada risiko dan sistem APU PPT, (2) Memperkuat komunikasi dengan sektor swasta, (3) Mendorong penuh pendekatan berbasis risiko untuk pelaksanaan CDD (*Customer Due Dilligence*) terhadap pengguna jasa dan (4) Mendukung opsi pembayaran elektronik dan digital.

B. **Saran**

Perkembangan TPPU dan TPPT dimasa Pandemi COVID 19 harus direspon oleh otoritas terkait dengan mengambil langkah-langkah kebijakan yang sesuai dan efektif dimasa pandemi COVID-19. Diperlukan sinergi dan kerjasama yang baik antara otoritas dengan entitas pelapor agar kebijakan yang ada dapat berjalan efektif. Otoritas Pengawas perlu mengintensifkan edukasi dan sosialisasi kepada entitas pelapor terutama terkait kebijakan e-KYC atau e-CDD yang merupakan pintu pertama bagi entitas pelapor untuk melakukan identifikasi dan verifikasi terhadap pengguna jasa secara jarak jauh dan mengidentifikasi risiko kejahatan TPPU/TPPT.

DAFTAR PUSTAKA

Buku

Bank Indonesia (2019), "*Sectoral Risk Assesment On Money Laundering and Terrorism Financing*"

Husein, Yunus (2007), *Bunga Rampai Anti Pencucian Uang*, Penerbit : BooksTerrace & Library: Cetakan Pertama 2007.

PPATK (2007), "*Rezim Anti Pencucian Uang Indonesia : Perjalanan 5 Tahun*", Penerbit : PPATK

TURNER, Jonathan E (2011), "*Money Laundering Prevention : Detering, Detecting and Resolving Financial Fraud*", Willey : New Jersey

Tracing Illegal Proceeds Workbook, E.R. Burke, Investigation Training Institute, Copyright 2001

Wiyono, R (2014), Pembahasan UU Pencegahan dan Pemberantasan TPPU, Jakarta: Sinar Grafika.

Jurnal, Paper, Makalah, Publikasi

Crisanto, Juan Carlos dan Jermy Prenio (2020), "*Financial Crime in Times of Covid-19 - AML and Cyber Resilience Measures*", Bank of International Settlement Publication.

FATF (2020), "*COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*",

FATF Publication, hal.4-7.

FATF (Desember : 2020), "*Update: COVID-19-related Money Laundering and Terrorist Financing*", FATF Publication, hal. 6-7.

FATF (2020) : "*Statement by the FATF President: COVID-19 and measures to combat illicit financing"*, FATF Publication

PPATK (2020), Buletin Statistik Anti Pencucian Uang dan Pendanaan Terorisme Edisi Desember 2020

PPATK (2020), Laporan PPATK Semester 1 2020

Rose, Liana W (2020), *"COVID-19 and Emerging Global Patterns of Financial Crime"*, Congressional Research Service.

Peraturan Perundang-Undangan dan Peraturan Lain

Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, UU No. 8 Tahun 2010, LN No. 122 Tahun 2010, TLN No. 5164.

Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme, UU No. 9 Tahun 2013, LN No. 50 Tahun 2013, TLN No. 5406.

Peraturan Bank Indonesia tentang Penerapan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Bagi Penyelenggara Jasa Sistem Pembayaran Selain Bank dan Penyelenggara, PBI No. 19/10/PBI/2017, LN No. 207 Tahun 2017, TLN No. 6121.

Peraturan Otoritas Jasa Keuangan tentang Perubahan atas Peraturan Otoritas Jasa Keuangan tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan, POJK Nomor 12/POJK.01/2017, LN No.178 tahun 2019, TLN No.6394.

Sumber Elektronik

https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/anti-pencucian-uang-dan-pencegahan-pendanaan-terorisme/default.aspx

https://www.ojk.go.id/apu-ppt/id/berita-dan-kegiatan/info-terkini/Pages/webminar-pegadaian.aspx

https://mediaindonesia.com/ekonomi/382560/money-mule-tren-fraud-dalam-sistem-pembayaran-digital-ri

https://www.fatf-gafi.org/publications/methodsandtrends/documents/covid-19-ml-tf.html

https://www.who.int/news/item/27-04-2020-who-timeline---covid-9,