



ISSN: 1979-4940  
E-ISSN: 2477-0124

**Editorial Office:** Faculty of Law, Islamic University Of Kalimantan,  
Jalan Adhyaksa No. 2 Kayutangi Banjarmasin, Kalimantan Selatan, Indonesia (70123)  
**Email:** al\_adl@uniska-bjm.ac.id  
**Web:** http://ojs.uniska-bjm.ac.id

## TINDAK PIDANA PENCUCIAN TERHADAP UANG VIRTUAL *MONEY LAUNDERING ON VIRTUAL MONEY*

**Suci Utami**

**Fakultas Hukum Universitas Islam Kalimantan MAB**  
Jl. Adhyaksa No. 2 Kayutangi, Banjarmasin, Kalimantan Selatan  
Email: suci.utami.law@gmail.com

Submitted : 25 Januari 2021  
Revised : 27 Januari 2021  
Accepted : 29 Januari 2021  
Published : 30 Januari 2021

### **Abstract**

*Globalization and technological advances have influenced the development of money laundering which was once conventional crime, now money laundering practiced virtually where it's increase the difficulty to detect and the national regulations hardly applied to prosecute it in blurred virtual world jurisdiction. This has become a major issue in the process of implementing Indonesian law against virtual money laundering, which has caused huge losses for Indonesian national financial system. The purpose of this research is to describe virtual money laundering in current criminal law, especially in Indonesian law and ways of dealing with it in the future. This study uses normative research methods and uses related legal materials. The research method uses a statutory approach and a conceptual approach. The results of this study are due to virtual characteristics, virtual money laundering has become a part of cyber crime, and several popular methods are using virtual / digital anonymous exchange rates that are used on the Online Games site. From the results of the reviewed legal materials, it is concluded that several Indonesian laws can categorize virtual money laundering as a criminal act according to Law no. 8/2010 supported by cyber regulation Law no. 19/2016. Technological law enforcement as a penal effort is needed as important as we increase non-penal measures such as strict supervision in national financial transactions in Indonesia.*

**Keywords :** Money Laundering, Virtual Money, Cyber Space

### **Abstrak**

Perkembangan globalisasi dan kemajuan teknologi mempengaruhi perkembangan pencucian uang yang dulunya kejahatan konvensional kini pencucian uang dapat dilakukan secara virtual sehingga semakin sulit dideteksi dan jangkauan payung hukum nasional sulit pengusutannya dalam yurisdiksi dunia virtual yang semakin kabur. Hal ini menjadi isu utama terhadap proses implementasi hukum Indonesia terhadap pencucian uang virtual yang memberi kerugian besar bagi sistem keuangan nasional Indonesia. Tujuan dari penelitian ini adalah untuk mendeskripsikan pencucian uang virtual dalam hukum kriminal saat ini khususnya dalam hukum Indonesia dan cara penanggulangan ke depannya. Penelitian ini menggunakan metode penelitian normative dan menggunakan bahan hukum terkait. Untuk metode penelitian menggunakan menggunakan pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian ini adalah karena karakteristik yang virtual, pencucian uang virtual

menjadi bagian dari kejahatan siber, dan beberapa metode yang populer adalah menggunakan virtual/digital kurs anonim yang digunakan dalam situs Games Online. Dari hasil bahan hukum yang dikaji disimpulkan bahwa beberapa hukum Indonesia, dapat mengategorikan pencucian uang virtual sebagai perbuatan kriminal sesuai UU No. 8/2010 didukung dengan regulasi siber UU No. 19/2016. Penegakan hukum secara teknologi sebagai upaya penal diperlukan sama pentingnya dengan kita meningkatkan upaya non penal seperti pengawasan ketat dalam transaksi keuangan nasional di Indonesia.

**Kata Kunci** : Pencucian Uang, Uang Virtual, Dunia Maya

## PENDAHULUAN

Hukum terus berkembang dalam pergerakan sistem dunia yang dinamis. Perbuatan yang semula bersifat konvensional dengan terlingkup dalam ranah hukum yang mengaturnya mulai memiliki banyak celah sehingga lepas dari jeratan dan semakin merajalela akibat hukum yang masih tertatih-tatih mengikuti perkembangan dinamis dunia untuk merangkulnya kembali dalam ketentuan yang mengatur. Kemajuan teknologi sebagai bagian dari globalisasi dan perkembangan peradaban manusia menjadi aspek yang sangat mempengaruhi masyarakat dalam menjalankan aktifitasnya.

Kemajuan dan perkembangan revolusi industri membawa perubahan secara ekonomi dan sosial. Istilah “perkembangan” membawa dampak pada “revolusi” yang menunjukkan cepatnya perkembangan tersebut. Pada umumnya ini merupakan tantangan bagi hukum untuk mampu mengikuti perkembangan tersebut.<sup>1</sup> Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Salah satu kejahatan yang menjadi semakin canggih dalam pelaksanaannya adalah tindak pidana pencucian uang atau *money laundering*.

Pada awalnya pencucian uang hanyalah bersifat fisik, dimana tindakan tersebut berjalan mengenai seni menyembunyikan keberadaan sumber ilegal maupun aplikasi ilegal dengan membuatnya menjadi uang sah dengan dibatasi oleh kemampuan kreatif untuk memanipulasi dunia fisik. Kemudian keadaan ini mulai mengikis dengan kecenderungan penggunaan sarana elektronik untuk mempertipis kemungkinan deteksi terhadap uang kotor tersebut yang marak digunakan oleh hampir semua pencuci uang sekarang. Modus pencucian uang sekarang tidak terbatas pada perbuatan konvensional yang berlangsung dalam dunia nyata untuk diusut dan ditegakkan hukum terhadapnya. Karena sifatnya yang virtual maka kemudian pencucian uang mengarah ke konteks kejahatan teknologi informasi yang kini

---

<sup>1</sup> Yati Nurhayati, Ifrani, A.H. Barkatullah, M. Yasir Said, (2019), “The Issue of Copyright Infringement in 4.0 Industrial Revolution: Indonesian Case”, *Jurnal Media Hukum*, Vol. 26, No.2, Desember 2019, hlm. 122-130.

makin marak di dunia. Hal ini dikarenakan karena telah terjadi pergeseran dari sarana kejahatan yang sudah menggunakan sarana elektronik. Hingga penggunaan hukum yang diterapkan pun sudah mengacu kepada aturan siber. Kaburnya jarak nyata dalam berbagai transaksi pencucian uang menjadi salah satu isu sehingga bentuk dan jangkauan luar negeri yang dimaksud pada pasal 3 dan pasal 4 di Undang-Undang RI Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang patut diperjelas dengan payung hukum yang menaungi dunia siber lebih jelas lagi, karena kaburnya batas ruang dan waktu dunia siber ini sendiri dapat mempengaruhi jangkauan 'wilayah luar negeri' yang ditentukan.

Dalam melakukan pencucian uang, pelaku tidak terlalu mempertimbangkan hasil yang akan diperoleh, dan besarnya biaya yang harus dikeluarkan, karena tujuan utamanya adalah untuk menyamarkan atau menghilangkan asal-usul uang sehingga hasil akhirnya dapat dinikmati atau digunakan secara aman. Sekalipun terdapat berbagai macam tipologi atau modus operandi pencucian uang, namun pada dasarnya proses pencucian uang dapat dikelompokkan ke dalam tiga tahap kegiatan yaitu *placement*, *layering* dan *integration*. Dalam praktiknya ketiga kegiatan tersebut dapat terjadi secara terpisah atau simultan, namun pada umumnya dilakukan secara tumpang tindih.

Sementara itu terdapat tiga metode umum yang digunakan dalam pencucian uang yaitu *Buy and Sell Conversions*, *Offshore Conversions*, dan *Legitimate Business Conversions*. Dari berbagai metode ini modus yang berkembang cepat seiring dengan perkembangan teknologi adalah dengan mengonversi mata uang riil menjadi mata uang digital di dunia maya. Salah satu kasus yang paling terkenal adalah layanan mata uang digital Costa Rica yang disebut Liberty Reserve. Cara cuci uang lain adalah melalui *online gaming*. Pada sejumlah *online game*, orang bisa mengonversi uang dari dunia real menjadi layanan barang virtual atau uang virtual. Nantinya uang atau barang virtual bisa dikonversi balik ke uang asli.

Menurut kepala PPATK Kiagus Ahmad Badaruddin mengatakan penggunaan virtual currency dapat mempertinggi risiko kejahatan keuangan, yakni pendanaan terorisme dan juga pencucian uang. Perkembangan teknologi digital saat ini juga dapat memicu berbagai upaya pencucian uang. Bahkan, ia menyebut dunia tengah memasuki 'era *digital money laundering*'. Kiagus memaparkan, bahwa pendapatan yang dihasilkan dari 11 kejahatan transnasional, seperti perdagangan narkoba, perdagangan gelap senjata hingga perdagangan manusia diperkirakan berkisar antara US\$1,6 triliun hingga US\$2,2 triliun per tahun. Aliran dana ilegal lintas negara (*Illicit Financial Flows/IFF*) yang berasal dari aktivitas kejahatan

ekonomi antarnegara juga meningkat. Terlebih, dengan hadirnya virtual asset seperti *cryptocurrency* yang sulit dilacak. Saat ini nilai dari IFF berkisar sekitar 2 persen hingga 5 persen dari GDP Global.<sup>2</sup>

Dengan demikian, pelaku kejahatan kini tidak lagi melakukan kejahatan keuangan dalam bentuk uang tunai ataupun berbagai jenis aset. Melainkan, dengan memanfaatkan teknologi informasi yang berfungsi untuk mengelola dana ilegal tersebut. Karena sifatnya yang virtual maka kemudian pencucian uang mengarah ke konteks kejahatan teknologi informasi yang kini makin marak di dunia. Secara internasional hukum yang terkait kejahatan teknologi informasi digunakan istilah hukum siber atau *cyber law*. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara. Sejalan dengan istilah tersebut Barda Nawawi Arief menyatakan : ”tindak pidana mayantara”, identik dengan ”tindak pidana di ruang siber (”*cyber space*”)” atau yang biasa juga dikenal dengan istilah ”*cybercrime*”.<sup>3</sup>

Dalam konsep kejahatan siber sendiri terdapat dua hal yang menjadi fokus utama, yakni menggunakan teknologi siber sebagai sarana dalam melakukan kejahatan dan yang kedua adalah menjadikan siber itu sendiri sebagai obyek kejahatan. Hingga penggunaan hukum yang diterapkan pun menjadikan aturan siber sebagai salah satu payung hukum dalam mendukung penegakan hukum atas kejahatan yang dilakukan. Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang yang diharapkan (*ius constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan Internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.<sup>4</sup> Misalnya saja praktik pencucian uang dalam bentuk uang virtual dalam sebuah platform situs digital yang dapat menyebabkan situs tersebut ditutup dan menghasilkan kerugian besar. Kegiatan dalam dunia virtual yang tidak terbatas sangat beragam sehingga terkadang jangkauan hukum untuk pengaplikasiannya masih harus diperluas lagi dan saling melengkapi.

Pencucian uang tidak lepas dari sistem perbankan sebagai tempat keluar masuknya aliran dan atau investasi. Perkembangan sistem perbankan yang pada masa kini sudah canggih

---

<sup>2</sup> Adhi Wicaksono. 22 Januari 2020. *PPATK Sebut 'Virtual Currency' Bisa Mendanai Terorisme*. [www.cnnindonesia.com](http://www.cnnindonesia.com). Diakses 14 Januari 2021.

<sup>3</sup> Barda Nawawi Arief. (2006). *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia*. PT.Rajagrafindo Persada :Jakarta, hlm. 1.

<sup>4</sup> *Ibid*, hlm. 34.

seperti adanya *e-money* (*electronic money*/ uang elektronik) menjadi wajah baru yang berbeda dari bentuk konvensional uang yang pernah ada. Uang elektronik ini tidak hanya disimpan dalam bentuk *chip* ataupun kartu, namun juga tersimpan dalam media elektronik yang sifatnya tidak nyata sehingga penggunaan uang elektronik inipun hanya dapat digunakan di dunia maya saja atau transaksi *on-line*. Peraturan Bank Indonesia Nomor 16/8/PBI/2014 tentang Perubahan Atas Peraturan Bank Indonesia Nomor 11/12/PBI/2009 Tentang Uang Elektronik (*Electronic Money*), menetapkan persyaratan mengenai ketentuan penyelenggaraan atas uang elektronik tersebut sebagai dukungan upaya pemerintah dalam pencegahan pencucian uang seperti batasan nominal, jenis kurs, hingga penerapan prinsip mengenal nasabah (*know your customer principles*).

Namun jika dalam hal uang elektronik ini ditransaksikan ke dalam website online yang memiliki kurs nya sendiri, seperti situs *second life* dengan Linden Dollarnya, yang mana kita melakukan kegiatan harian dalam suatu dunia virtual dengan transaksi yang tidak jauh berbeda dari kehidupan nyata yang memiliki aturan hukumnya sendiri, hal ini menjadi problematika dalam penegakan hukum atas pencucian uang yang menggunakan metode *layering* dengan sifat virtual.

Menurut Massimo Nardo, isu memerangi kejahatan ekonomi dan keuangan di tingkat global telah menjadi semakin penting dalam arena internasional selama puluhan tahun yang menandai transisi dari abad kedua puluh ke abad dua puluh satu. Nardo menunjukkan bahwa pekerjaan masa lalu di bidang kejahatan keuangan di dunia maya sebagian besar telah difokuskan pada struktur dan pendekatan metode dan bukan kerja sosial-hukum kejahatan. Dia menyatakan, tampaknya karena itu berguna untuk meningkatkan analisis dengan membuka upaya untuk aspek ekonomi dan sosiologis.<sup>5</sup> Kejahatan ekonomi virtual mungkin tampak kecil dibandingkan dengan kejahatan terlarang lainnya seperti perdagangan narkoba, namun sekarang muncul bahwa ada hubungan yang kuat antara kejahatan terorganisir di dunia nyata dan kejahatan ekonomi melalui internet.<sup>6</sup> Pencucian uang akan berfokus sebagai kegiatan kriminal utama dalam dunia maya, tapi tidak untuk mengatakan bahwa itu adalah satu-satunya kejahatan keuangan yang terjadi. Para kriminal yang melakukan kejahatan ekonomi menggunakan internet sebagai cara memperoleh, memasukan, dan menggunakan

---

<sup>5</sup> Massimo Nardo. (2011). *Economic crime and illegal markets integration: a platform for analysis*. Journal of Financial Crime, Vol. 18, No. 1, hlm.47 - 62

<sup>6</sup> Clare Chambers-Jones, (2012), *Virtual Economies and Financial Crimes*, Edward Elgar Publishing Limited: United Kingdom, hlm. 1.

informasi berharga.<sup>7</sup> Pencucian uang virtual ini yang merupakan bentuk dari kejahatan dimensi baru dengan penggunaan sarana yang baru berkembang. Perkembangan hukum sendiri diupayakan dapat mengikuti perkembangan bentuk kejahatan dimensi baru namun tidak gegabah dalam merumuskan aturan yang mengaturnya agar tidak terjadi tumpang tindih aturan atau perumusan aturan yang kurang matang.

### RUMUSAN MASALAH

Beranjak dari latar belakang di atas, dengan tujuan untuk menjelaskan kejahatan pencucian uang pada uang virtual dalam hukum pidana sekarang dan penanggulangan kejahatan pencucian uang terhadap uang virtual di masa yang akan datang maka rumusan masalah penelitian ini adalah :

1. Bagaimanakah kejahatan pencucian uang pada uang virtual dalam hukum pidana Indonesia saat ini?
2. Bagaimanakah penanggulangan kejahatan pencucian uang terhadap uang virtual?

### METODE PENELITIAN

Dalam pembuatan sebuah karya ilmiah terutama karya ilmiah penelitian hukum diharuskan menggunakan metode penelitian hukum. Ilmu hukum berusaha untuk menampilkan hukum secara integral sesuai dengan kebutuhan kajian ilmu hukum itu sendiri, sehingga metode penelitian dibutuhkan untuk memperoleh arah penelitian yang komprehensif.<sup>8</sup> Sebenarnya ilmu hukum mempunyai ciri-ciri sebagai ilmu yang bersifat preskriptif dan terapan. Dalam preskriptif, ilmu hukum mempelajari tujuan hukum, nilai-nilai keadilan dalam suatu hukum, baik buruk suatu aturan hukum, konsep-konsep dan norma hukum. sedangkan dalam ilmu terapan, ilmu hukum menetapkan suatu prosedur, ketentuan-ketentuan dan batasan-batasan dalam menegakan suatu aturan hukum.<sup>9</sup>

Metode penelitian yang digunakan adalah tipe penelitian berupa penelitian hukum normatif; pendekatan masalah menggunakan pendekatan perundang-undangan (*statute aproach*), pendekatan konseptual (*conceptual aproach*); sifat penelitian ini adalah deskriptif analisis; bahan hukum yang digunakan adalah bahan hukum primer berupa perundangan-undangan terkait dengan tindak pidana pencucian uang, khususnya Undang-Undang Nomor 8

---

<sup>7</sup> *Ibid.*

<sup>8</sup> Yati Nurhayati, (2013), "Perdebatan Metode Normatif dengan Metode Empirik Dalam Penelitian Ilmu Hukum Ditinjau Dari Karakter, Fungsi dan Tujuan Ilmu Hukum", *Jurnal Al Adl*, Vol. 5, No. 10, hlm. 15.

<sup>9</sup> Yati Nurhayati, (2020), *Pengantar Ilmu Hukum*, Bandung: Nusa Media, hlm. 9.

Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, dan juga menggunakan bahan hukum sekunder berupa artikel hukum dan lainnya; dalam pengumpulan bahan hukum yang akan digunakan, penulis akan menginventarisir dan mengklasifikasinya melalui studi kepustakaan sesuai masalah yang dibahas dengan menggunakan sistem kartu, yakni bahan hukum yang berhubungan dengan masalah yang dibahas dipaparkan, disistematisasi, kemudian dianalisis untuk menginterpretasikan hukum yang berlaku; pengolahan dan analisis dalam penelitian yaitu bahan-bahan hukum yang dikumpulkan untuk menjawab masalah hukum yang dirumuskan di rumusan masalah, kemudian menganalisisnya dengan menggunakan penalaran ilmiah deduktif, yaitu perumusan analisis dari hal-hal yang umum kepada penyimpulan yang lebih khusus.

## PEMBAHASAN

### **Kejahatan Pencucian Uang Pada Uang Virtual dalam Hukum Pidana Sekarang**

Oleh sifatnya yang terorganisir, pencucian uang merupakan tindak pidana di bidang ekonomi yang pada intinya memberikan gambaran terhadap hubungan langsung bahwa kriminalitas merupakan suatu kelanjutan dari kegiatan dan pertumbuhan ekonomi. Fenomena pencucian uang bukan permasalahan nasional lagi tetapi sudah internasional, sehingga sangat penting ditempatkan pada sentral pengaturan hukum. Hampir semua kejahatan ekonomi dilakukan dengan motif keuntungan. Oleh karena itu untuk membuat pelaku jera atau mengurangi tindak pidana itu dengan cara mencari fakta kejahatan supaya pelaku tidak dapat menikmati dan kejahatan juga sirna. Hal ini juga sangat membantu dalam pengembalian kerugian negara.

Kejahatan pencucian uang merupakan delik berganda dan berkait, yang artinya delik itu tidak akan ada bila tidak ada delik lainnya sebagai asal terjadinya delik.<sup>10</sup> Berdasarkan pasal 2 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Pencucian Uang, menyebutkan hasil tindak pidana yang merupakan harta kekayaan dari berbagai tindak pidana asal seperti korupsi, perdagangan obat terlarang, perdagangan orang, dan lain sebagainya. Pencucian uang sebagai suatu kejahatan yang berdimensi internasional merupakan hal baru di banyak negara termasuk Indonesia. Sebegitu besar dampak negatif terhadap perekonomian suatu negara yang dapat ditimbulkannya, mendorong negara-negara di dunia dan organisasi internasional menaruh perhatian serius dan khusus terhadap

---

<sup>10</sup> Paku Utama. (2013). *Memahami Asset Recovery dan Gatekeeper*. Jakarta Selatan: Indonesian Legal Roundtable, hlm. 102.

pengecahan dan pemberantasan masalah ini. Hal ini turut pula menjadi perhatian serius di Indonesia sebagai negara berkembang yang tengah menjalankan pembangunan nasional karena permasalahan *money laundering* dapat menimbulkan masalah domestik, seperti mempersulit pengendalian moneter, dan juga mengurangi pendapat negara. Tak hanya itu, pencucian uang juga mempertinggi risiko negara (*country risk*), sehingga berpotensi menciptakan instabilitas sistem keuangan ataupun perlambatan pertumbuhan ekonomi. Untuk itu peran PPATK sebagai lembaga sentral yang mengoordinasikan pelaksanaan upaya pencegahan dan pemberantasan pencucian uang di Indonesia sangat penting.

Berdasarkan buletin statistik PPATK bulan Oktober 2020 lalu, dalam lingkup nasional terdapat tiga besar dugaan tindak pidana asal yang dilaporkan pada Laporan Transaksi Keuangan Mencurigakan (LTKM) yaitu penipuan, narkoba, dan korupsi. Pergerakan aliran dana yang diawasi dan dilaporkan adalah bahwa secara keseluruhan jumlah LTKM yang diterima oleh PPATK sejak Januari 2003 s.d. Oktober 2020 telah mencapai sebanyak 558.933 LTKM atau bertambah 10,9 persen dibandingkan jumlah kumulatif LTKM pada akhir Desember 2019. Peningkatan pelaporan LTKM, terutama terjadi sejak diberlakukannya UU TPPU tanggal 22 Oktober 2010. Jumlah LTKM yang telah diterima PPATK sejak Januari 2011 s.d. Oktober 2020 tercatat sebanyak 495.009 LTKM, atau secara rata-rata tahunan meningkat 530,0 persen dibandingkan periode sebelum diberlakukannya UU TPPU.<sup>11</sup> Dalam pelaksanaan penegakan hukum terhadap pencucian uang, terdapat 540 perkara TPPU yang telah diputus oleh Pengadilan sejak Januari 2005 s.d. Oktober 2020 dengan hukuman maksimal penjara seumur hidup dan denda maksimal Rp32 Miliar. Selama periode tersebut, sebagian besar Putusan Pengadilan terkait TPPU diputus oleh Pengadilan (mencakup Pengadilan Negeri/Tipikor, Pengadilan Tinggi, dan atau Mahkamah Agung) di wilayah DKI Jakarta, yaitu sebanyak 173 putusan atau 32 persen. Putusan yang telah diputus oleh Pengadilan terkait TPPU adalah hukuman maksimal selama seumur hidup dan denda maksimal sebesar Rp32 Miliar. Sebagian besar putusan Pengadilan perkara TPPU terkait dengan tindak pidana asal Narkoba, yakni sebanyak 137 putusan atau 25,4 persen dari total keseluruhan putusan TPPU. Di posisi kedua tindak pidana asal pencucian uang adalah korupsi, sebanyak 104 putusan atau 19,3 persen dari total keseluruhan putusan TPPU.<sup>12</sup> Berdasarkan data yang tersebut dalam buletin ini dapat terlihat bahwa saat ini penegakan

---

<sup>11</sup> PPATK. 2020. *Buletin Statistik: Anti Pencucian Uang dan Pendanaan Teroris*, Volume 128/THN X/2020, hlm. 4

<sup>12</sup> *Ibid*, hlm. 45-46

pencucian uang di Indonesia belum cukup luas untuk menjangkau praktik pencucian uang yang terjadi dibawah radar praktik konvensional, misalnya saja *digital money laundering* atau pencucian uang virtual. Sehingga untuk Indonesia harus meningkatkan kerja sama internasional sebagai upaya pemberantasan pencucian uang.

Dengan perkembangan globalisasi dan teknologi yang cepat kini membuat kejahatan pencucian uang yang dulunya konvensional menjadi tingkatan yang berbeda sehingga penanganan yang diperlukan sendiri menjadi khusus. Hal ini salah satunya adalah karena pelaksanaan pencucian uang itu sendiri yang dilaksanakan di dunia maya atau virtual. Pencucian ini tentu saja berbeda dengan proses pencucian yang menggunakan sistem transfer dana elektronik maupun pengubahan aset yang berputar dan acak yang jalurnya masih bisa dilacak oleh jaringan sistem lembaga keuangan.

Namun kesulitan menjadi jauh sangat kentara ketika proses pencucian dilakukan di dunia virtual dimana bahkan uang rill dapat ditukarkan dengan barang virtual yang memiliki nilai tertentu dan perputaran atas barang virtual tersebut di dunia maya yang tidak dinaungi oleh lembaga terdaftar di dunia nyata. Disebutkan oleh FATF bahwa pencucian uang sekarang semakin jarang terjerat, namun mereka menambahkan apakah disebabkan karena perbuatan ini yang semakin langka atau justru para pencucinya yang semakin canggih hingga lepas dari endusan para penegak hukum. Kemajuan teknologi sekarang telah menjadi tombak penting dimana pencucian uang yang merupakan *white collar crime* ini dapat main akal-akalan dalam menyiasati pelegalan uang haramnya. Seperti yang disebutkan pada tinjauan pustaka mengenai faktor maraknya pencucian uang bahwa kemajuan di bidang teknologi-informasi menyebabkan kejahatan terorganisir dapat lintas negara dengan mudah hingga hukum sulit dalam pencapaian perbuatan pidana tersebut untuk dijerat dan diadili. Di Indonesia sendiri *cyber/ digital/ virtual money laundering* bukan kata yang umum untuk didiskusikan, kebanyakan hanya mengetahui sebatas pencucian uang tapi kurang yakin dengan pencucian uang berbasis telematika. Dari kajian komprehensif oleh penulis menyimpulkan bahwa unsur-unsur *money laundering* meliputi unsur *person*, unsur objektive yang melibatkan sistem elektronik, dan unsur subjektive. Ketiga tahapan pencucian uang pada dasarnya dilakukan dalam dunia siber atau virtual untuk menciptakan "*disassociation*" antara uang atau harta hasil kejahatan dengan si penjahat serta tindak pidananya, sehingga proses hukum konvensional akan mengalami kesulitan dalam melacak si penjahat dan menemukan jenis tindak pidananya.

Pencucian uang virtual ini dapat dijelaskan lebih lanjut sebagai berikut. *Launderer* bergabung dengan membuka akun pada situs dunia virtual 3D. Dalam situs para pemain bisa bergabung dengannya, menciptakan pribadi baru dan aspek fisik baru, cara berjalan, terbang, bersenang-senang dengan teman, bisa membeli lahan, dan bisa juga bertransaksi dengan uang

virtual yang bisa dikonversi ke uang sesungguhnya, dan semua ini dimainkan secara online. Pada tahap *placement*, para *launderer* dapat membeli kurs virtual tersebut dengan mentransfer pada rekening milik perusahaan situs virtual tersebut. Contoh situs yang terkenal dengan banyak praktik *money laundering* dalam permainan tersebut adalah Second Life oleh Linden Research, Inc. yang mana terdapat berbagai profesi aktif yang bisa dijalankan secara virtual dan secara 'sah' dapat menerima bayaran besar dari profesi yang dilaksanakannya di dunia virtual tersebut, mulai dari pengusaha sukses yang tinggal di mansion mewah virtual, penyanyi yang mengadakan konser virtual besar, hingga berbagai jasa dan konsultan misalnya psikolog hingga pengecara. Praktik umum yang dipraktikkan dalam situs tersebut adalah agen real estate yang menawarkan berbagai lahan virtual yang bisa jadi sangat mahal untuk kebanyakan pengguna. Dalam tahap *layering* seorang pemain dapat membeli lahan itu dan akan membuat pembayaran dengan transfer uang virtual antar pemain yang kemudian diubah menjadi uang sebenarnya. Tetapi semenjak pemindahan uang dalam jumlah besar bisa beresiko, transaksinya akan dibagi-bagi ke dalam beberapa transfer uang dalam jumlah kecil. Uang yang sangat banyak dipindahkan dari seorang pemakai ke pemakai lain dalam angka kecil, sebuah medium yang baik untuk pencucian uang, dengan perdagangan menggunakan kurs virtual antar pemain. Pencairan dana besar dari akun pemain yang melakukan permainan secara 'sah sesuai aturan yang diberlakukan situs' tersebut merupakan tahap integrasi pencucian uang yakni mengoversi uang virtual tersebut ke dalam dunia nyata.

Transaksi aset virtual dengan uang rill yang sudah dikonversikan ke kurs privat khusus situs tersebut sehingga menjadi uang virtual yang bukan merupakan mata uang digital resmi, menyebabkan transaksi dengan penggunaan mata uang tersebut tidak terlacak oleh badan resmi. Jika situs tersebut terdaftar di Indonesia, maka transaksi keuangan berada dalam pengawasan OJK. Namun hal ini tentu berbeda jika situs luar negeri yang bukan berada dalam pengawasan OJK. Seperti situs Second Life tersebut yang bebas diakses dan pelaksanaan transaksinya berada ditengah milyaran transaksi antar pemain yang tidak diawasi secara ketat. Karena uang virtual sendiri hanya dapat ditransaksikan secara elektronik dan virtual pula, menjadikan nilai ekonomis dari kurs virtual tersebut tidak semuanya yang terpayungi oleh hukum di dunia nyata dalam pelaksanaan transaksinya. Transaksi tersebut akan bertebaran dengan acak dalam dunia virtual dengan triliun transaksi sehingga untuk penggalian data dan penemuan bukti sulit dilakukan. Apalagi dengan tujuan penegakan hukum terhadap pencucian uang sendiri adalah khususnya untuk pengembalian aset yang merugikan negara sekaligus, termasuk semua keuntungan hasil kejahatan tersebut. Hal ini terkait dengan pelaksanaan

transaksi bisnis virtual yang berlangsung di dunia virtual, dimana kasus pencucian uang virtual masih banyak yang sulit ditelusuri oleh penegak hukum karena kerumitan dunia virtual itu sendiri sementara aset tersebut bisa diuangkan kembali ke dunia nyata untuk dimanfaatkan nilai ekonomisnya.

Uang virtual sebagai objek pencucian uang virtual, merupakan harta kekayaan yang menjadi unsur dalam kriminalisasi pencucian uang. Peraturan BI Nomor 16/8/PBI/2014 mengatur tentang uang elektronik, namun tidak memayungi terhadap uang elektronik yang tidak terdaftar atau dalam pengawasan lembaga keuangan resmi. Maka untuk penjeratan terhadap pencucian uang virtual tetap berkiblat kepada undang-undang Nomor 8 Tahun 2010 yang menyebutkan bahwa harta kekayaan yang dicuci dapat merupakan barang yang tidak berwujud dan dapat Penulis analogikan ke uang virtual.

Salah satu tren terbaru dalam pencucian uang melibatkan mata uang digital. Banyak orang yang hanya mulai belajar tentang meningkatnya penggunaan cryptocurrency virtual independen, seperti Bitcoins, Litecoins, Zen dan Namecoins. Tetapi kenyataannya adalah transaksi online dan alternatif mata uang ada di banyak tempat, dari Dolar Linden yang digunakan dalam game online Second Life, dan Justice Poin di World of Warcraft, hingga Berkshares, mata uang alternatif yang dibuat oleh lima bank untuk mempromosikan bisnis lokal di Berkshire wilayah Massachusetts Barat. Di mana ada kesempatan untuk menukar uang riil dengan uang online, maka pencucian uang juga bisa eksis. Beberapa mata uang virtual benar-benar anonim, tidak seperti transaksi kartu kredit atau cek pribadi, yang dapat dikaitkan dengan seseorang atau entitas tertentu. Mata uang virtual tidak seperti rupiah, dolar, yen atau euro karena tidak ada pemerintah atau badan pengawas pusat yang mengatur nilai mereka atau penggunaan. Mereka dipertukarkan secara bebas dan anonim pada jaringan *peer-to-peer* di seluruh dunia.<sup>13</sup>

Teknik yang paling banyak digunakan adalah dengan mengonversi mata uang riil menjadi mata uang digital di dunia maya. Salah satu kasus yang paling terkenal adalah layanan mata uang digital Costa Rica yang disebut Liberty Reserve. Dengan cara uang Dollar atau Euro dikonversi ke sebuah mata uang digital yang disebut dollar Liberty Reserve dollars atau Euro Liberty Reserve. Mata uang digital Liberty Reserve ini kemudian bisa dikirimkan dan diterima secara anonim. Penerimaannya bisa mengonversi mata uang Liberty Reserve kembali ke uang tunai dengan membayar sejumlah kecil uang jasa. Pada Mei tahun 2013,

---

<sup>13</sup> Cindy Williamson dkk. (2013). *Technology In The Fight Against Money Laundering In The New Digital Currency Age*. hlm. 7. E-Book : Thompson Reuters.

pihak berwenang AS telah menutup layanan tersebut. Pendiri Liberty Reserve dan beberapa orang lain didakwa dengan tuduhan mencuci uang. Namun menurut Richet, penutupan Liberty Reserve tidak akan menghentikan praktik cuci uang. Sebab ada banyak alternatif lain, seperti WebMoney, Bitcoins, Paymer, dan PerfectMoney.<sup>14</sup> Yang menjadi tantangan besar adalah pencucian uang melalui *online gaming*. Pada sejumlah *online game*, orang bisa mengonversi uang dari dunia real menjadi layanan barang virtual atau uang virtual. Nantinya uang atau barang virtual bisa dikonversi balik ke uang asli. Menurut Richet, game Second Life dan World of Warcraft adalah game yang paling sering digunakan.

Bagi sebagian akademisi, pencucian uang melalui banyaknya game online multiplayer sebagian besar telah diabaikan oleh penegak hukum untuk waktu yang lama karena dianggap terlalu rumit. Hal ini dikarenakan dunia virtual terpisah dari dunia nyata sehingga dunia virtual menjadi *lawless* dan *unregulated*. Sementara bagi sebagian yang lain berpendapat bahwa dunia virtual dan dunia nyata melebur sehingga hukum di dunia nyata dapat diberlakukan di dunia virtual. Yang menjadi permasalahan adalah terkait yurisdiksi yang sesuai dalam pengusutan, pengaturan, dan darimana untuk di kontrol.<sup>15</sup> Game online ini, dan *Deep Web* pada umumnya, bisa sangat mengintimidasi. Apalagi banyak penjahat yang canggih dengan penggunaan kode komputer dan teknologi yang maju dan kompleks dalam pencucian uang virtual. Ini bukan hanya subkultur asing, tetapi ukuran itu semua bisa terasa luar biasa. Dengan triliunan transaksi, banyak di komunitas penegakan hukum bahkan tidak bisa membayangkan di mana untuk memulai. Pencucian uang online pada dasarnya tidak jauh berbeda dengan pencucian uang offline. Pada kebanyakan kasus, pencucian uang virtual merupakan kombinasi dan terintegrasi dengan pencucian uang offline. Hanya saja keunikan pada pencucian uang virtual adalah dunia virtual itu sendiri. Keunikan di dunia virtual tersebut antara lain yaitu : Anonimitas tinggi; Kerahasiaan tinggi; Banyak kesulitan dalam penegakan hukum, artinya banyak pengamanan yang dapat dikelokan karena kurangnya pengaturan; Biaya dan upaya rendah; serta Kecepatan transaksi. Hal ini yang menyebabkan pencucian uang virtual sulit untuk dideteksi.

Tantangan tersendiri bagi Indonesia adalah Indonesia masih harus meningkatkan kerjasama internasional yang lebih baik untuk bisa melakukan pengusutan dan pemulihan aset pencucian uang yang beredar di dunia virtual dan lintas negara yang mana belum dipayungi

---

<sup>14</sup> Wiwiek Juwono. (2013). *Ini Dia Empat Praktek Cuci Uang di Internet*. <http://www.pcplus.co.id>. Diakses tanggal 20 Desember 2020.

<sup>15</sup> Clare Chambers-Jones. *Op.cit.* hlm. 103-113.

oleh hukum nasional Indonesia sehingga perlu penerapan hukum internasional. Namun patut diketahui hingga per Januari 2021 menurut Menteri Keuangan Sri Mulyani dalam pertemuan PPATK tahunan secara virtual, Indonesia adalah satu-satunya negara di antara negara G20 yang belum bergabung dengan FATF (*Financial Action Task Force*) yang merupakan gerakan anti pencucian uang global, sehingga saat ini Indonesia belum bisa menerapkan aturan pencucian uang internasional. Upaya Indonesia untuk bergabung sebagai anggota pada FATF telah dilaksanakan sejak tahun 2017 dengan memenuhi berbagai persyaratan dan direncanakan pada 1-17 Maret 2021, akan ada evaluasi yang dilakukan untuk menjadi anggota FATF. Indonesia akan mengikuti evaluasi ini sehingga diharapkan bisa segera menjadi anggota FATF di akhir 2021. Harapannya setelah itu dapat menerapkan hukum internasional dan membangun kebijakan nasional terhadap penanggulangan pencucian uang yang lebih baik di Indonesia, selain itu diharapkan Indonesia bisa menjadi negara yang cukup tinggi terkait pencegahan TPPU dan TPPT. Kepala PPATK juga menekankan bahwa keberhasilan menjadi anggota FATF menuntut kerja ekstra keras dari seluruh pihak, bahkan dukungan penuh dari segenap komponen bangsa, termasuk kalangan pers. Menjadi anggota FATF akan bernilai strategis sebagai bentuk pengakuan dunia internasional terhadap integritas sistem keuangan RI, sekaligus diharapkan mendorong Indonesia yang terus berproses memajukan perekonomiannya<sup>16</sup>

Berdasarkan hal tersebut diatas, maka untuk saat ini penulis akan menarik hukum pidana indonesia untuk implementasi dalam dunia virtual dan mengupas unsur-unsur pencucian uang menurut Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Pencucian Uang terhadap uang virtual meliputi unsur *person*, unsur objektive yang melibatkan sistem elektronik, dan unsur subjektive yang dapat terpenuhi. Selanjutnya perlu ditopang Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk mencengkram Pencucian uang terhadap uang virtual. Dari hasil pengkajian bahan hukum tersebut, maka hukum pidana Indonesia saat ini dapat mengategorikan pencucian uang virtual sebagai perbuatan pidana dan dapat menjerat pelakunya maupun terkait jangkauan hukum pencucian uang terhadap ruang siber dan kegiatan maupun aset yang ada di dalamnya. Hal ini dijelaskan sebagai berikut:

### 1. Unsur Person

---

<sup>16</sup> Lidya Julita Sembiring. 14 Januari 2021. *Masih Banyak Kasus Pencucian Uang, Kapan RI Join FATF?*. [www.cnbcindonesia.com](http://www.cnbcindonesia.com). Diakses 14 Januari 2021.

Undang-Undang ini menyebutkan ‘Setiap Orang’ sebagai subjeknya. Pada pasal 1 menerangkan bahwa yang dimaksud ‘Setiap Orang’ ini adalah orang perseorangan atau korporasi (korporasi adalah kumpulan orang dan/atau kekayaan yang terorganisasi, baik merupakan badan hukum maupun bukan badan hukum). Unsur ini sesuai untuk pencucian uang siber yang merupakan kejahatan terorganisir. Tapi kembali pada persoalan sifat kejahatan yang transnasional, unsur pelaku ini kurang merinci karakteristik netizen yang menjadi seorang *cyber launderer* yang menggunakan pemanfaatan sarana elektronik dalam proses pencuciannya.

Maka untuk menopang kepentingan unsur *person*, penulisan berpendapat untuk digunakannya Undang-Undang Nomor Nomor 19 tahun 2016 yang menentukan bahwa orang adalah orang perseorangan, baik WNI, WNA, maupun Badan Hukum yang melakukan transaksi elektronika dengan penyelenggaraan sistem elektronik seperti yang disebutkan bagi pasal-pasal nya. Menurut Undang-Undang ITE ini, *cyber launderer* sebagai seorang netizen baik WNI maupun WNA dapat dijerat karena melakukan kejahatan yang menggunakan sarana elektronik dalam proses perbuatannya. Unsur person pada pencucian uang siber dapat ditopang oleh ketentuan dari Undang-Undang ITE. Meski begitu pengusutan *person* yang terlibat pencucian uang di dunia virtual harus benar-benar mewujudkan bukti yang dapat dinyatakan secara nyata, sehingga dalam investigasi siber ataupun dalam forensik siber penting bagaimana peran kerjasama dunia internasional untuk proses penggalian data siber ini.

## 2. Unsur Objektif

Dalam Undang-Undang Nomor 8 Tahun 2010 ini merumuskan perbuatan pencucian uang dalam 3 jenis kepada pelakunya, yaitu :

1. Pencuci yang menempatkan, mentrasfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa keluar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga dengan tujuan menyembunyikan atau menyamarkan asal-usul;
2. Penyembunyi atau Penyalur yang menyembunyikan, mengaburkan, menyamarkan asal usul, sumber, lokasi, peruntukan, pengalihan hak-hak atau kepemilikan yang sebenarnya; dan
3. Penadah yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan, Atas harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana yang disebutkan oleh pasal 2 Undang-Undang ini. Harta kekayaan yang dimaksudkan oleh Undang-Undang ini adalah semua benda bergerak atau benda tidak

bergerak, baik yang berwujud maupun tidak berwujud, yang diperoleh baik secara langsung maupun tidak langsung. Undang-Undang ini juga dapat melingkupi objek *cyber laundering* yang bersifat digital dengan ditopang oleh UU ITE. Misalnya transaksi uang virtual dalam tukar menukar rumah ataupun pulau virtual, yang jika aset rumah atau pulau virtual itu di konversikan akan menghasilkan nilai dalam bentuk uang yang memiliki nilai ekonomis di dunia nyata.

Undang-Undang Nomor 8 Tahun 2010 menerangkan tentang transaksi yaitu kegiatan yang menimbulkan hak dan/atau kewajiban yang menyebabkan timbulnya hubungan hukum antara dua pihak atau lebih. Meskipun pada poin lain menyebutkan dokumen yang terekam secara elektronik, namun hal transaksi tersebut tidak disebutkan sebagai transaksi elektronika, sebagaimana yang disarankan oleh *cyber launderer*. Menurut pasal 82 Undang-Undang Nomor 3 Tahun 2011 bahwa salah satu kejahatan dalam transfer dana adalah penerima yang dengan sengaja menerima atau menampung, baik untuk diri sendiri maupun untuk orang lain, suatu Dana yang diketahui atau patut diduga berasal dari Perintah Transfer Dana yang dibuat secara melawan hukum. Untuk menunjang hal ini, Undang-Undang ITE difungsikan untuk menambal kelemahan ini dengan memuat ketentuan bahwa transaksi elektronika adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya, sehingga transaksi keuangan yang dilakukan secara elektronik pada *cyber laundering* dapat terjerat oleh ketentuan pasal pada Undang-Undang Nomor 8 Tahun 2010 ini.

Meski begitu masih diributkan khalayak banyak mengenai transfer dana sebagai salah satu transaksi keuangan yang ditopang oleh Undang-Undang ITE. Memang hal ini dengan luas memasung pelaku pencucian uang yang utamanya menggunakan sistem transfer dana dalam mengalirkan dana haramnya, namun tetap saja dirasa perlu untuk tambahan perundangan lain untuk semakin menyempurnakan penjeratan *cyber launderer*.

Undang-Undang ITE pada sekarang ini difungsikan sebagai norma bagi masyarakat siber, namun aturan pidana yang dimuatnya sejauh ini terfokus pada kejahatan komputer berupa larangan terhadap jenis-jenis kejahatan seperti *hacking*, *cracking*, *phising*, *piracy*, *cybersex*, penghinaan, perjudian, pemerasan, HOAX, hingga ujaran kebencian. Maka untuk menghadapi pencucian uang terhadap uang virtual yang merupakan hasil dari *electronic funds transfer crime* dan *cyber crime*, Undang-

Undang ITE tidak dapat membantu banyak dalam menggarap *cyber launderer* sekalipun memang memuat ketentuan mengenai transaksi elektronik namun tidak menyebutkan tentang transaksi keuangan online seperti kejahatan pada transfer dana.

### 3. Unsur Subjektif

Tentu saja undang-undang ini sebagai Undang-Undang pencucian uang memuat se jelasnya unsur subjektif dari tindak pencucian uang. Undang-Undang ini kembali menjelaskan bahwa yang dimaksud dengan ‘patut diduganya’ adalah suatu kondisi yang memenuhi setidaknya-setidaknya pengetahuan, keinginan, atau tujuan pada saat terjadinya transaksi yang diketahuinya yang mengisyaratkan adanya pelanggaran hukum, dengan poin kedua yaitu dengan maksud menyembunyikan atau menyamarkan.

Seperti yang dipaparkan sebelumnya, *Mens rea* yang harus dibuktikan yaitu *knowledge* (mengetahui atau patut menduga) dan *intended* (bermaksud). Kedua hal tersebut berkaitan bahwa terdakwa mengetahui dana tersebut berasal dari hasil kejahatan dan pelaku mengetahui tentang atau maksud untuk melakukan transaksi. Namun pembuktian inipun sulit ketika *launderer* telah sedemikian rupa hebatnya untuk menyembunyikan hasil kejahatannya terlebih dengan penggunaan sarana internet yang semakin berkembang praktis dan canggih. Meski kesulitan untuk pembuktian pada poin menyembunyikan yang ditransaksikan di dunia siber namun pasal kriminalisasi dalam Undang-Undang Nomor 8 Tahun 2010 ini membantu dengan pemuatan poin ‘menyamarkan’ sehingga perbuatan yang menyesatkan pelacakan terhadap keilegalan harta haram didunia siber tetap dapat dipidana. Penulis berpendapat bahwa unsur subjektif pada pasal ini memiliki pasung yang kuat dan luas dalam menjerat *cyber launderer*.

### Penanggulangan Kejahatan Pencucian Uang Terhadap Uang Virtual

Pada awalnya, Yurisdiksi merupakan konsekuensi logis dari kedaulatan negara atas wilayahnya. Yurisdiksi negara atas individu, benda dan lain-lain dalam batas wilayahnya (teritorial daratan, laut dan udara) pada akhirnya dapat berkembang/meluas melalui batas-batas negara (perluasan atas individu dan benda-benda yang terletak dinegara lain). Hal ini merupakan salah satu dampak/akibat dari semakin terbukanya hubungan internasional dan perdagangan internasional yang ada. Di sinilah perlu ada kesepakatan bersama. Adanya

proses yang berlangsung/berkembang melalui kesepakatan bersama tersebut, hukum internasional menyusun aturan yang mengikat.

Sebagaimana sering terlihat, kedaulatan yang dimiliki suatu negara, kadang-kadang, menimbulkan konflik antar negara yang ada. Hal ini banyak terkait dengan adanya kewenangan/yurisdiksi yang dimiliki oleh satu negara terhadap individu, benda, dan lain-lain, misalnya seorang warga negara dari suatu negara melakukan kejahatan di banyak negara, dapat berkembang menjadi masalah pula di negara lain, persoalan tersebut masuk dalam lingkup yurisdiksi. Meskipun yurisdiksi berkaitan erat dengan wilayah, namun keterkaitan ini tidaklah mutlak sifatnya. Negara-negara lain pun dapat mempunyai yurisdiksi untuk mengadili suatu perbuatan yang dilakukan di luar negeri. Di samping itu, ada beberapa orang (subyek hukum) tertentu memiliki kekebalan terhadap yurisdiksi wilayah suatu negara meskipun mereka berada di dalam negara tersebut. Berdasarkan kedudukan negara dalam hukum internasional, yurisdiksi dapat dibedakan menjadi:<sup>17</sup>

1. Yurisdiksi teritorial. Menurut prinsip yurisdiksi teritorial, negara mempunyai yurisdiksi terhadap semua persoalan dan kejadian di dalam wilayahnya. Prinsip ini adalah prinsip yang paling mapan dan penting dalam hukum internasional. Menurut Hakim Lord Macmillan suatu negara memiliki yurisdiksi terhadap semua orang, benda, perkara-perkara pidana atau perdata dalam batas-batas wilayahnya sebagai pertanda bahwa negara tersebut berdaulat.
2. Yurisdiksi Personal. Menurut prinsip yurisdiksi personal, suatu negara dapat mengadili warga negaranya karena kejahatan yang dilakukannya di mana pun juga. Sebaliknya, adalah kewajiban negara untuk memberikan perlindungan diplomatik kepada warga negaranya di luar negeri. Ketentuan ini telah diterima secara universal.
3. Yurisdiksi menurut Prinsip Perlindungan. Berdasarkan prinsip yurisdiksi perlindungan, suatu negara dapat melaksanakan yurisdiksinya terhadap warga-warga asing yang melakukan kejahatan di luar negeri yang diduga dapat mengancam kepentingan keamanan, integritas, dan kemerdekaan negara. Penerapan prinsip ini dibenarkan sebagai dasar untuk penerapan yurisdiksi suatu negara. Latar belakang pembenaran ini adalah perundang-undangan nasional pada umumnya tidak mengatur atau tidak menghukum perbuatan yang dilakukan di dalam suatu negara yang dapat mengancam atau mengganggu keamanan, integritas, dan kemerdekaan orang lain.
4. Prinsip Yurisdiksi Universal. Menurut prinsip ini, setiap negara mempunyai yurisdiksi terhadap tindak kejahatan yang mengancam masyarakat internasional. Yurisdiksi ini lahir tanpa melihat di mana kejahatan dilakukan atau warga negara yang melakukan kejahatan. Lahirnya prinsip yurisdiksi universal terhadap jenis kejahatan yang merusak terhadap masyarakat internasional sebenarnya juga disebabkan karena tidak adanya badan peradilan internasional yang khusus mengadili kejahatan yang dilakukan orang-perorang (individu).

---

<sup>17</sup> Leonard Marpaung. 2017. *Yurisdiksi Negara Menurut Hukum Internasional*. <https://diskumal.tnial.mil.id>. Diakses tanggal 28 Desember 2020.

*Cyber space* adalah media yang tidak mengenal batas. Baik batas-batas wilayah maupun batas kenegaraan. Sehubungan dengan adanya unsur-unsur internasional dari kejahatan di dunia maya (*cyber crime*) tentunya akan menimbulkan masalah tersendiri, khususnya berkenaan dengan masalah yurisdiksi. Kejahatan Pencucian Uang, karena metode, sarana yang digunakan, dan/atau objek perbuatan tersebut merupakan bentuk digital di dunia virtual, maka pencucian uang terhadap uang virtual dikategorikan sebagai kejahatan siber (*cyber crime*). Untuk penegakan hukum pencucian uang terhadap uang virtual yang dilakukan di domain situs luar negeri, mengikuti prinsip yurisdiksi berdasarkan prinsip hukum internasional berlaku.

Internet memiliki 3 (tiga) level regulasi, yang ketiganya diatur langsung oleh infrastruktur internet itu sendiri; regulasi aktivitas yang bisa dilakukan hanya melalui internet; dan regulasi aktivitas yang dapat, tapi tidak harus, dilakukan melalui internet. Berikut 3 level dari regulasi yang diatur langsung oleh infrastruktur internet itu sendiri menurut Froomkin, yaitu<sup>18</sup> :

1. Lingkup Pertama adalah Komunikasi standar; Peralatan yang digunakan untuk menyediakan dan mengakses komunikasi internet; dan Perantara yang terlibat dalam penyediaan komunikasi internet, seperti ISP.
2. Lingkup Kedua, berhubungan dengan pengaturan kegiatan yang dapat dilakukan hanya melalui internet dan yang tidak memiliki analog pengunjung signifikan.
3. Lingkup Ketiga adalah di mana ada pengaturan kegiatan yang mungkin saja atau tidak dilakukan melalui internet, misalnya *e-commerce* untuk sebuah barang berwujud maupun tidak berwujud.

Penanggulangan kejahatan seringkali dimaknai hanya sebatas pendekatan penal yang berkaitan dengan masalah kriminalisasi yaitu perbuatan apa yang dijadikan tindak pidana dan penalisasi yaitu sanksi apa yang sebaiknya dikenakan pada si pelaku tindak pidana. Sementara pendekatan penal tersebut memiliki keterbatasan-keterbatasan. Sehingga, diperlukan upaya lain (non-penal) yang dilakukan untuk menanggulangi kejahatan. Oleh karena itu dalam menanggulangi kejahatan idealnya ditempuh dengan pendekatan integral, secara “penal” dan “non-penal”.<sup>19</sup>

Dalam hal penanggulangan tindak pidana internasional seperti kasus pencucian uang, dikenal asas “*au dedere au judicare*”, yang berarti “Setiap Negara berkewajiban untuk menuntut dan mengadili pelaku tindak pidana internasional dan berkewajiban untuk

---

<sup>18</sup> Clare Chambers-Jones. *Op.Cit.*, hlm 177

<sup>19</sup> Ifrani & M. Yasir Said, (2020), “Kebijakan Kriminal Non-Penal Ojk Dalam Mengatasi Kejahatan Cyber Melalui Sistem Peer To Peer Lending”, *Al-Adl Jurnal Hukum*, Vol.12, No.1, Januari 2020, hlm.61-76

bekerjasama dengan negara lain di dalam menangkap, menahan dan menuntut serta mengadili pelaku tindak pidana internasional.” Dalam kegiatan *cyber space*, Darel Manthe menyatakan yuridiksi di *cyber space* membutuhkan prinsip-prinsip yang jelas yang berakar dari hukum internasional. Selanjutnya Manthe menyatakan hanya melalui prinsip-prinsip yuridiksi ini, maka negara-negara dapat dihimbau untuk mengadopsi pemecahan yang sama terhadap pernyataan mengenai yuridiksi internet. Yuridiksi *cyber space* oleh Manthe yang berlaku di Amerika Serikat ini yaitu : <sup>20</sup>

1. *Theory of The Uploader and the Downloader*, Teori ini menekankan bahwa dalam dunia cyber terdapat 2 (dua) hal utama yaitu uploader (pihak yang memberikan informasi ke dalam cyber space) dan downloader (pihak yang mengakses informasi)
2. *Theory of Law of the Server*, Dalam pendekatan ini, penyidik memperlakukan server di mana halaman web secara fisik berlokasi tempat mereka dicatat atau disimpan sebagai data elektronik.
3. *Theory of International Space*, Menurut teori ini, cyber space dianggap sebagai suatu lingkungan hukum yang terpisah dengan hukum konvensional di mana setiap negara memiliki kedaulatan yang sama.

Beberapa hal tersebut di atas patut menjadi hal yang dipertimbangkan dalam penyusunan kebijakan nasional dan penegakan hukum terkait pencucian uang virtual yang transnasional. Hal ini juga dapat dibagi dalam kategori, misalnya beberapa versi internet dari suatu kegiatan dapat diatur dengan cara yang berbeda dari versi online atau di mana peraturan khusus dibuat karena penggunaan internet membuat aturan yang ada tidak mungkin untuk diimplementasikan. Oleh karena itu sangat sulit untuk menuju ke arah kesepakatan nasional maupun internasional tentang apa yang harus atau tidak harus dilaksanakan untuk mengatur kegiatan internet jika terdapat ketidaksetaraan atau keseriusan dalam penanggulangan pencucian uang virtual secara global. Hal ini dikarenakan setiap negara memiliki kerangka hukum, administrasi dan operasional yang beragam serta sistem keuangan yang berbeda, sehingga tidak dapat mengambil semua tindakan yang identik untuk melawan ancaman ini. Kegiatan kontraktual penting di sini karena ini adalah di mana sebagian besar undang-undang ditemukan karena ekspansi bisnis dan perdagangan melalui internet.

Satu cara pemerintah dapat mengontrol akses orang-orang terhadap internet dan pengetahuan terhadap itu adalah melalui penegakan hukum secara teknologi dan pembatasan. Reidenberg mendemonstrasikan asumsi logik bahwa melalui penggunaan teknologi yang berkembang pemerintah bisa menggunakan keuntungan dalam teknologi untuk mengontrol dan menjaga penegakan hukum. Dengan memiliki pembatasan teknologi untuk semua atau

---

<sup>20</sup> Radian Adi. 2 April 2012. *Cara Pembuktian Cyber Crime Menurut Hukum Indonesia*. [www.hukumonline.com](http://www.hukumonline.com) diakses 14 Januari 2020.

sebagian internet, pemerintah bisa mengontrol dan membatasi apa yang orang-orang bisa lihat dan gunakan di internet dan jika pelanggaran terjadi, maka mereka memiliki yuridiksi terhadap orang-orang mereka. Banyak negara menggunakan metode pembatasan ini sebagai jalan untuk menjaga yuridiksi.<sup>21</sup> Di Indonesia sendiri, transaksi keuangan dalam situs *game online* maupun aplikasi yang resmi masuk Indonesia saat ini juga sudah banyak yang berpayung resmi dibawah pengawasan Otoritas Jasa Keuangan, namun belum menjangkau secara ketat jika seorang *launderer* membuka akun internasional dan melakukan transaksi uang virtual pada situs luar negeri.

Kemudian penegakan hukum secara teknologi diperlukan sebagai salah satu cara untuk tetap mengimbangi pesatnya kecanggihan berbagai metode pencucian uang virtual sekarang. Tujuan akhir adalah untuk mencegah pencucian uang virtual dan kejahatan ekonomi terjadi, karenanya sebuah sistem harus dirancang untuk mencegah ini. Oleh karena itu, sementara pembatasan teknologi harus dilaksanakan sebagai reaksi terhadap masalah, perlu dipikirkan dengan baik tentang penggabungan strategi. Banyak pertimbangan yang perlu di ambil seperti yang sudah disebutkan sebelumnya, namun kembali penulis tegaskan sekali lagi bahwa pertimbangan-pertimbangan yang perlu diberikan adalah mengenai apakah setiap negara secara individual menerapkan yurisdiksi dan memantau serta mengendalikan situasi dalam batas-batas mereka sendiri atau apakah ada yang disepakati secara internasional terhadap rencana untuk memerangi kejahatan ekonomi global. Bergabung dengan FATF merupakan salah satu strategi yang bagus untuk meningkatkan penanggulangan kejahatan ekonomi virtual di Indonesia. FATF sendiri adalah badan antar-pemerintah yang didirikan pada tahun 1989 oleh para Menteri dari yurisdiksi Anggota. Mandat FATF adalah untuk menetapkan standar dan untuk mempromosikan implementasi yang efektif dari langkah-langkah hukum, peraturan dan operasional untuk memerangi pencucian uang, pendanaan teroris dan pembiayaan proliferasi, dan ancaman terkait lainnya terhadap integritas sistem keuangan internasional. Bekerja sama dengan pemangku kepentingan internasional lainnya, FATF juga bekerja untuk mengidentifikasi kerentanan tingkat nasional dengan tujuan melindungi sistem keuangan internasional dari penyalahgunaan. FATF mengeluarkan update rekomendasi terbaru yang rilis pada Oktober 2020 lalu. Secara garis besar berisi tentang penjabaran langkah-langkah penting yang harus dimiliki negara untuk :

1. mengidentifikasi risiko, dan mengembangkan kebijakan dan koordinasi domestik;
2. mengejar pencucian uang, pendanaan teroris dan pembiayaan proliferasi;

---

<sup>21</sup> Clare Chambers-Jones. *Op.cit.* hlm. 187

3. menerapkan tindakan pencegahan untuk sektor keuangan dan sektor lain yang ditunjuk;
4. menetapkan kekuasaan dan tanggung jawab untuk otoritas yang kompeten (misalnya, investigasi, penegakan hukum dan otoritas pengawas) dan tindakan kelembagaan lainnya;
5. meningkatkan transparansi dan ketersediaan informasi *Beneficial Ownership* dari badan hukum dan pengaturan; dan
6. memfasilitasi kerjasama internasional.

Sehingga dengan bergabungnya Indonesia dalam FATF akan menunjang upaya non penal lebih baik maupun penegakan upaya penal secara lebih luas. Di Indonesia sendiri sudah membentuk lembaga Otoritas Jasa Keuangan berdasarkan UU No. 21 tahun 2011 tentang Otoritas Jasa Keuangan yang berfungsi menyelenggarakan sistem pengaturan dan pengawasan yang terintegrasi terhadap keseluruhan kegiatan di dalam sektor jasa keuangan. OJK secara umum merupakan Lembaga Pengawas dan Pengatur (LPP) yang menetapkan ketentuan prinsip mengenali Pengguna Jasa (nasabah) dan melaksanakan pengawasan kepatuhan Pihak Pelapor dalam menerapkan prinsip mengenali nasabah. Pelaksanaan penerapan program APU PPT yang dilakukan melalui pengawasan dan pemeriksaan di masing-masing sektor pengawasan, yaitu perbankan, pasar modal, dan IKNB (Industri Keuangan Non-Bank) dalam bentuk pengawasan *offsite & onsite*. Sejalan dengan manajemen risiko, pengawasan terhadap APU PPT (Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme) di sektor jasa keuangan didasarkan atas penilaian 5 (lima) aspek manajemen risiko APU PPT terhadap keseluruhan proses (*end to end business process*) kegiatan identifikasi, verifikasi dan pemantauan nasabah yaitu: Pengawasan Aktif Direksi dan Dewan Komisaris; Kebijakan dan Prosedur; Pengendalian Intern; Sistem Informasi Manajemen, dan Sumber Daya Manusia dan Pelatihan.<sup>22</sup> Hal ini juga didukung dengan menggunakan sarana dan prasarana yang bersifat non penal yang mendukung dalam investigasi dan identifikasi perbuatan tersebut. Salah satu upaya tersebut adalah dengan peningkatan disiplin etik dan integritas para *gatekeeper* yaitu para profesional khusus yang dapat membantu klien dalam transaksi keuangan nasional maupun internasional, misalnya saja pengacara, notaris, akuntan, auditor, agen real estate, dan sebagainya.<sup>23</sup>

Berkaca pada aturan beberapa negara terhadap pencucian uang terhadap uang virtual, penulis berfokus kepada negara Inggris, Amerika Serikat, dan China yang dapat dijadikan

---

<sup>22</sup> OJK. (2016). *Penguatan Penerapan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU PPT) di Sektor Jasa Keuangan dan Kesiapan Sektor Jasa Keuangan dalam Menghadapi Penilaian Mutual Evaluation Review terhadap Indonesia*. hlm. 5-15.

<sup>23</sup> Paku utama. *Op.cit.* hlm. 142

acuan sebagai bahan pertimbangan penyusunan kebijakan penanggulangan pencucian uang virtual. Inggris menggunakan aturan siber mereka sebagai negara hingga juga dapat memayungi dalam tindakan pencucian uang terhadap uang virtual yang berlaku di dunia maya. Selanjutnya adalah Amerika Serikat menjadi salah satu negara yang paling berkembang pesat dalam upaya-upaya penegakan hukum terhadap pencucian uang khususnya terhadap pencucian uang terhadap uang virtual yang saat ini marak terjadi. Selain meregulasi tentang tindak pidana pencucian uang, mereka juga menggunakan aturan *cyber law* dalam mempertegas penegakan hukum terhadap *cyber launderer*. Kemudian China, dalam salah satu penangkapan terbesar oleh kepolisian di China adalah terhadap seorang penipu pengusaha kecil \$48 Juta. Penjahat tersebut tidak menggunakan uang kejahatannya tersebut untuk membeli jam swiss mahal atau properti mahal, melainkan kredit atau chips di situs game online dan menukarkannya dengan berbagai barang virtual untuk akun avatar mereka yang terdaftar di game online tersebut.<sup>24</sup> Penjahat tersebut bermaksud mencuci uang kejahatan tersebut dalam bentuk lain yang tidak terdeteksi oleh pemerintahan. China juga memberlakukan undang-undang siber mereka yang menyebutkan bahwa siapapun yang mengakses komputer (internet) dengan maksud menyimpang dan kriminal akan di penjara selama 5 tahun. Dapat disimpulkan dari ketiga negara bahwa regulasi siber sangat penting untuk menunjang penegakan hukum pencucian uang virtual. Dimensi transnasional yang melekat pada teknologi ini sangat menguntungkan pelaku kejahatan. Pelaku kejahatan dapat melakukan kejahatannya pada korban di negara manapun korban berada. Keuntungan yang lain bagi pelaku adalah perbedaan aturan berkaitan dengan tindak pidana siber di setiap negara. Bahkan masih banyak negara yang belum memiliki hukum yang mengatur khusus mengenai tindak pidana siber. Hal ini tentu memudahkan pelaku bisa dengan leluasa melakukan aktifitasnya tanpa terjerat hukum.

Berbagai cara dilakukan oleh negara-negara untuk menyelesaikan permasalahan yurisdiksi, namun apabila pelaku *cyber launderer* berada di luar wilayah negara yang terkena dampak paling besar, maka harus dipikirkan bagaimana cara membawa pelaku tersebut ke negara tersebut. Cara yang biasa ditempuh oleh negara-negara adalah melalui jalur kerja sama internasional untuk membawa pelaku *cyber launderer* agar dapat diadili di negaranya, yaitu Ekstradisi dan Deportasi serta Bantuan Timbal Balik (*Mutual Legal Assistance*). Hambatan terbesar dalam memerangi pencucian uang virtual adalah data besar (*Big Data*). Secara

---

<sup>24</sup> Christopher Mims. (2012). *Chinese cyber-criminals caught laundering \$48 mln through online games*. <http://qz.com>. Diakses tanggal 28 Desember 2020.

harfiah triliunan transaksi melalui sistem keuangan dunia. Di situlah teknologi akan membantu dalam pertarungan ini. Pencarian melalui gedung pengadilan negara untuk catatan publik telah diganti dengan perangkat penggalian data (*data mining*) yang kuat yang memungkinkan lembaga penegak hukum untuk menelusuri lebih dalam dan lebih luas untuk mendapatkan informasi tentang kegiatan kriminal yang mencurigakan dan orang-orang berkepentingan.

Penanggulangan kejahatan ekonomi virtual, khususnya pencucian uang terhadap uang virtual, di masa yang akan datang adalah dengan meningkatkan kemampuan baik dari sarana dan prasarana maupun sumber daya manusia. Upaya non penal menduduki posisi kunci dan strategis dalam menanggulangi sebab-sebab kejahatan dan kondisi-kondisi yang menyebabkan kejahatan, yaitu dengan cara Pencegahan tanpa pidana (*prevention without punishment*), termasuk di dalamnya penerapan sanksi administrative dan sanksi perdata; dan mempengaruhi pandangan masyarakat mengenai kejahatan dan pembinaan lewat media massa (*influencing views of society on crime and punishment*). Chambers-Jones mengutip Interpol menyebutkan bahwa untuk menghadapi kejahatan ekonomi virtual ini dibutuhkan aksi internasional oleh pemerintah. Terdapat empat aspek yang harus dipertimbangkan, yaitu :<sup>25</sup>

1. Badan penegak hukum perlu mengetahui secara langsung dimana lokasi basis *server* tempat kejahatan ekonomi tersebut terjadi. Mungkin terjadi di berbagai negara yang berbeda yang mana menjadi masalah ketika mencari lokasi hukum yang bisa diambil.
2. Badan penegak hukum harus memberi pengaruh legislator terkait kejahatan ekonomi virtual di masa depan dalam menyusun kebijakan baru. Pertimbangan butuh diberikan tidak hanya untuk pengusutan tetapi juga untuk perolehan kembali aset dan informasi dari masing-masing kejahatan virtual yang dilakukan.
3. Batasan diantara badan penegak hukum dan industri harus dijebol untuk memastikan akuntabilitas jaringan pertukaran data.
4. Badan penegak hukum harus belajar dan menguasai investigasi kejahatan virtual.

Berdasarkan hal tersebut di atas, penanggulangan terhadap pencucian uang terhadap uang virtual, khususnya di Indonesia, untuk selanjutnya dapat menggunakan penegakan hukum dengan mengintegrasikan aturan undang-undang tentang pencucian uang dan regulasi siber. Kementerian terkait harus dengan jeli menyaring dan memberi ijin untuk akses terhadap situs maupun aplikasi yang melakukan penyelenggaraan keuangan sehingga setiap transaksi dalam pengawasan. Kerjasama internasional akan sangat membantu dalam investigasi siber dan pelacakan sebaran transaksi pencucian sehingga diharapkan pemulihan uang haram

---

<sup>25</sup> Clare Chambers-Jones. *Op.cit.* hal 114.

tersebut bisa diperoleh dengan optimal dan dapat menutupi kerugian yang disebabkan oleh kejahatan tersebut.

## PENUTUP

### Kesimpulan

1. Untuk saat ini, penjeratan terhadap pencucian uang virtual tetap berkiblat kepada undang-undang Nomor 8 Tahun 2010 dan didukung oleh regulasi siber Undang-Undang Nomor 19 Tahun 2016 yang menyebutkan bahwa harta kekayaan yang dicuci dapat merupakan barang yang tidak berwujud dan dapat dianalogikan ke uang virtual.
2. Dalam penanggulangan kejahatan pencucian uang terhadap uang virtual, yuridiksi siber terhadap kejahatan di dunia virtual menggunakan yuridiksi hukum yang berlaku karena dunia virtual yang tidak terbatas maka penegakan hukum dapat dilakukan dengan ketentuan pembagian yuridiksi berdasarkan kedudukan negara dalam hukum internasional. Sehingga sangat diperlukan kerjasama internasional yang baik dalam penanggulangan pencucian uang virtual yang global. Penegakan hukum secara teknologi diperlukan sebagai salah satu cara untuk tetap mengimbangi pesatnya kecanggihan berbagai metode pencucian uang virtual sekarang. Penanggulangan kejahatan ekonomi virtual, khususnya pencucian uang terhadap uang virtual, di masa yang akan datang tidak hanya menggunakan sarana penal dalam penegakan hukumnya, namun juga menggunakan upaya non penal dalam pencegahannya.

### Saran

1. Perluasan payung hukum yang lebih baik dan detail agar mampu menjerat penjahat siber, khususnya *cyber launderer*, dalam aktifitas kejahatan di dunia virtual yang terselubung dalam. Menjalin jaringan kerja sama internasional dalam penanganan berbagai kasus pencucian uang khususnya yang menggunakan kurs virtual di berbagai situs dunia yang tidak terdeteksi oleh lembaga hukum sah.
2. Penerapan yang efisien dan efektif upaya non penal dalam pencegahan pencucian uang virtual, dengan pengembangan wawasan kepada masyarakat luas dan pemangku kepentingan khususnya para pebisnis, profesional *gatekeeper* maupun penyelenggara jasa keuangan untuk kontrol yang lebih ketat dalam pengawasan berkelanjutan yang dinamis. Serta meningkatkan kesadaran masyarakat untuk taat dan memiliki integritas hukum.

3. Peningkatan kualitas sumber daya manusia bagi profesional mandiri maupun di lembaga dan badan yang terkait, sehingga dalam forensik siber, khususnya dalam penambangan data (*data mining*), dapat mengumpulkan bukti-bukti secara fakta nyata yang detail. Hal ini diharapkan dapat secara optimal memulihkan kekayaan virtual yang tidak terdeteksi untuk dapat dikonversi kembali nilai ekonomisnya di dunia nyata sehingga bisa menutupi kerugian pihak (negara) yang dirugikan.

## DAFTAR PUSTAKA

### Buku

- Chambers-Jones, Clare. 2012. *Virtual Economies and Financial Crimes*. Edward Elgar Publishing Limited : United Kingdom
- Halim, Pathorang. 2013. *Penegakan Hukum Terhadap Kejahatan Pencucian Uang di Era Globalisasi*. Yogyakarta : Total Media.
- Hiariej, Eddy O.S. 2009. *Pengantar Hukum Pidana Internasional*. Jakarta : Penerbit Erlangga.
- Makarim, Edmon. 2005. *Pengantar Hukum Telematika*. Jakarta : PT. Raja Grafindo Persada.
- Menthe, Darrel. 1998. *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 Mich. Telecomm. & Tech. L. Rev. 69.
- Soesilo, R. 1991. *Kitab Undang-Undang Hukum Pidana, serta Komentar- Komentar Lengkap Pasal Demi Pasal*. Bogor : Politeia.
- Sunarso, Siswnto. 2009. *Hukum Informasi dan Transaksi Elektronik : Studi Kasus Prita Mulyani*. Jakarta: Rineka Cipta.
- Sutarman. 2007. *Cyber Crime Modus Operandi dan Penanggulangannya*. Jogjakarta : LaksBang Pressindo.
- Utama, Paku. 2013. *Memahami Asset Recovery dan Gatekeeper*. Jakarta Selatan : Indonesian Legal Roundtable, hal. 102.
- Widodo. 2013. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law) Telaah Teoritik dan Bedah Kasus*. Yogyakarta : Aswaja Pressindo.
- , 2013. *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta : Aswaja Pressindo.
- Yati Nurhayati, 2020. *Pengantar Ilmu Hukum*, Nusa Media, Bandung.

### Peraturan Perundang-Undangan

Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 8 tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Republik Indonesia.

Undang-Undang Nomor 3 tahun 2011 tentang Transfer Dana.

Peraturan Bank Indonesia Nomor 16/8/PBI/2014 tentang Perubahan Atas Peraturan Bank Indonesia Nomor 11/12/PBI/2009 Tentang Uang Elektronik (*Electronic Money*)

Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

### Jurnal dan Publikasi Lainnya

Effros, Robert C. (Ed). *Current Legal Issues Affecting Central Banks. Vol. 2* Washington : International Monetary Fund.

FATF. 2020. *The FATF Recommendation: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.*

Ifrani & M. Yasir Said, (2020), "Kebijakan Kriminal Non-Penal Ojk Dalam Mengatasi Kejahatan Cyber Melalui Sistem Peer To Peer Lending", *Al-Adl Jurnal Hukum*, Vol.12, No.1, Januari 2020, hlm.61-76

Nardo, Massimo. 2011. *Economic crime and illegal markets integration: a platform for analysis. Journal of Financial Crime*, Vol. 18 Iss: 1.

OJK. 2016. *Penguatan Penerapan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU PPT) di Sektor Jasa Keuangan dan Kesiapan Sektor Jasa Keuangan dalam Menghadapi Penilaian Mutual Evaluation Review terhadap Indonesia.*

PPATK. 2020. *Buletin Statistik: Anti Pencucian Uang dan Pendanaan Teroris*, Volume 128/THN X/2020.

Williamson, Cindy dkk. 2013. *Technology In The Fight Against Money Laundering In The New Digital Currency Age*. E-Book : Thompson Reuters.

Yati Nurhayati, Ifrani, A.H. Barkatullah, M. Yasir Said, 2019, "The Issue of Copyright Infringement in 4.0 Industrial Revolution: Indonesian Case", *Jurnal Media Hukum*, Vol. 26, No.2, Desember 2019, hlm. 122-130

Yati Nurhayati, 2013. "Perdebatan Metode Normatif dengan Metode Empirik Dalam Penelitian Ilmu Hukum Ditinjau Dari Karakter, Fungsi dan Tujuan Ilmu Hukum", *Jurnal Al Adl*, Volume 5 Nomor 10.

**Internet**

Adhi Wicaksono. 22 Januari 2020. *PPATK Sebut 'Virtual Currency' Bisa Mendanai Terorisme*. [www.cnnindonesia.com](http://www.cnnindonesia.com). Diakses 14 Januari 2021.

Wiwiek Juwono. 2013. *Ini Dia Empat Praktek Cuci Uang di Internet*. <http://www.pcplus.co.id>. Diakses tanggal 20 Desember 2020.

Lidya Julita Sembiring. 14 Januari 2021. *Masih Banyak Kasus Pencucian Uang, Kapan RI Join FATF?*. [www.cnbcindonesia.com](http://www.cnbcindonesia.com). Diakses 14 Januari 2021.

Leonard Marpaung. 2017. *Yurisdiksi Negara Menurut Hukum Internasional*. <https://diskumal.tnial.mil.id>. Diakses tanggal 28 Desember 2020.

Radian Adi. 2 April 2012. *Cara Pembuktian Cyber Crime Menurut Hukum Indonesia*. [www.hukumonline.com](http://www.hukumonline.com) diakses 14 Januari 2020.

Christopher Mims. 2012. *Chinese cyber-criminals caught laundering \$48 mln through online games*. <http://qz.com>. Diakses tanggal 28 Desember 2020.