Journal of International Relations, Volume 8, Nomor 3, 2022, hal *280-288*
Online di http://ejournal-s1.undip.ac.id/index.php/jihi

The Deception of Art : Analisis Potensi Ancaman *NFTs* (*Non-Fungible Tokens*) Terhadap Keamanan Nasional Indonesia

Yosafat Caesar Sinurat, Ika Riswanti Putranti, Marten Hanura
Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro
Jalan Prof. H. Soedarto, SH., Tembalang, Kota Semarang
Website: http://www.fisip.undip.ac.id Email: fisip@undip.ac.id

ABSTRACT

Technological developments have brought world civilization to a time where everything relies heavily on technology. This development greatly affects all aspects of human life. We can see this from the daily life of humans who are very dependent on the digital world and the internet. The use of the digital world can be seen in vital aspects such as the world of banking, transactions, even in the creative industry. The use of NFT as a way for creative industry activists is a new way to gain and appreciate the work they produce. Aspects that are affected, not only make it easier for humans to do work, but the development of this technology is also used as a gap by criminals to commit crimes. Money laundering crimes and terrorism financing are no longer carried out conventionally, but have penetrated into the digital world. This study aims to find loopholes in the use of NFT as a medium in committing money laundering and terrorism financing crimes, and why it can become a national threat if there is no securitization of the issue. This study uses constructivism theory with the concept of securitization. This study also found that the anonymity feature in NFT transactions can make it easier for criminals to commit money laundering and terrorism financing crimes that can threaten the national security of a country.

Keywords*: NFT, money laundering, terrorism financing, economic securitization.*

PENDAHULUAN

Kemajuan teknologi telah membawa dunia dalam tingkatan yang berbeda. Segala hal dalam segala aspek sudah memasuki era digitalisasi. Mulai dari transaksi, komunikasi, informasi, bahkan hiburan sudah merambah ke dunia digital. Hal ini membuat akses terhadap segala hal menjadi lebih mudah. Kita bisa berkomunikasi dengan orang yang jaraknya ribuan mil hanya dalam hitungan detik. Kita bisa mengakses informasi secepat mungkin. Hiburan-hiburan dari belahan dunia lain juga dapat kita akses dengan mudah.

Internet sudah menjadi bagian dari hidup kita sehari-hari. Segala lini dalam kehidupan kita tidak bisa dilepaskan dari internet. Salah satunya adalah cara bertransaksi dalam membeli suatu barang, sekarang terjadi perpindahan uang di internet dalam bentuk virtual (Filipkowski, 2008). Hal ini juga termasuk dalam mendapatkan hiburan-hiburan yang banyak tersedia dari internet. Dalam hal ini, hiburan-hiburan tersebut diantaranya adalah film, *game*, musik, dan hiburan-hiburan lain secara gratis maupun berbayar. Hal ini membuat banyak *entertainment creator* berlomba-lomba membuat konten dengan baik dan laku di pasar. Hal ini tentu saja ditujukan agar *creator-creator* tersebut mendapatkan minat dari pasar untuk membeli apa yang telah mereka buat. Sebagai konsumen, kita juga dapat mengunduh hiburan-hiburan tersebut dan menikmatinya.

Salah satu fitur dalam internet, yang dapat menjadi media dari tindak kejahatan yang dapat mengancam keamanan nasional adalah transaksi NFT *(Non-Fungible Tokens)*. NFT merupakan sebuah bentuk penggunaan *cryptocurrency* yang berasal dari mata uang *crypto* yang bernama Ethereum (Wood, 2015). NFT pertama kali diusulkan dalam Ethereum Improvement Proposals (EIP)-721 (Entriken, Shirley, Evans, & Sachs, 2018) dan dikembangkan lebih lanjut di EIP-1155. NFT berbeda dari cryptocurrency klasik (Shirole, Darisi, & Bhirud, 2019) seperti Bitcoin dalam fitur bawaannya. Bitcoin adalah koin standar, di mana semua koin setara dan tidak dapat dibedakan. Sebaliknya, NFT bersifat unik yang tidak dapat dipertukarkan (setara, *non-fungible*), sehingga cocok untuk mengidentifikasi sesuatu atau seseorang dengan cara yang unik. Untuk lebih spesifiknya, dengan menggunakan NFT pada sebuah karya seni, pencipta dapat dengan mudah membuktikan keberadaan dan kepemilikan aset digital dalam bentuk video, gambar seni, dll. Pembuat NFT dapat juga mendapatkan royalti setiap kali karya yang diciptakannya berpindah tangan di pasar NFT mana pun atau dengan pertukaran *peer-to-peer*. Riwayat perdagangan yang lengkap, likuiditas yang mudah, dan pengoperasian yang mudah memungkinkan NFT menjadi solusi perlindungan kekayaan intelektual (IP) yang menjanjikan. Meskipun pada dasarnya NFT mewakili lebih dari sekadar kode, tetapi kode bagi pembeli telah memberikan nilai ketika mempertimbangkan kelangkaan komparatifnya sebagai objek digital. Hal ini mengamankan harga jual produk terkait kekayaan intelektual ini dengan baik untuk aset virtual yang tidak dapat dipertukarkan.

Laporan dari Non-Fungible.com menyatakan bahwa meskipun *NFT* mengalami kelesuan dari tahun 2018 ke 2019, lonjakan terjadi pada tahun selanjutnya, dimana pada tahun 2019 ke 2020 terjadi peningkatan sebanyak 97.09% pada *wallet* yang aktif, 66,94% pada jumlah pembeli aktif, 24,7% pada jumlah *creator* ataupun penjual, dan peningkatan sebesar 299% pada jumlah uang yang berputar. Hal ini mengarah pada sebuah kesimpulan dimana pasar *NFT* mengalami lonjakan yang sangat pesat, dan pada laporan tersebut, juga disebutkan bahwa pada tahun 2021 terjadi lonjakan, meskipun tidak signifikan, namun akan tetap menjadi ladang yang subur, apalagi bila terkait dengan tindak kriminal (NonFungible.com, 2020).

NFT sendiri memiliki berbagai bentuk dan wujud. *NFT* dalam hal ini dapat berupa barang koleksi seperti *CryptoKitties, CryptoPunks, SoRare* dan masih banyak barang-barang koleksi digital yang berupa *NFT*. Selain itu, *NFT* juga dapat berupa permainan video seperti *Axie Infinity, Gods Unchained, MyCryptoHeroes*. Dunia virtual seperti *Decentraland, Somnium Space,* dan *Cryptovoxels* juga dapat dijadikan sebagai aset *NFT*.

Namun, hal ini datang tentunya bukan tanpa tantangan. Mudahnya akses yang tersedia di internet, tentunya juga mempermudah dan mempermulus tindak kriminal yang terjadi di ruang siber. Dalam hal ini, adalah tindak kejahatan yang dilakukan melalui ruang siber menjadi fokus utama. Para pelaku tindak kejahatan menggunakan internet sebagai media untuk melancarkan tindak kejahatan mereka. Dengan itu, apabila hal ini terjadi, internet sebagai media kejahatan mereka merupakan sebuah bahaya yang laten bagi keamanan ekonomi dunia internasional. Hal inilah yang disebut dengan *Cyber Laundering*. Selain *cyber laundering*, tindak kejahatan yang dilakukan melalui dunia siber khususnya NFT adalah pendanaan terorisme atau *terrorism financing*.

Pencucian uang via dunia siber menggunakan fitur-fitur yang disediakan di internet, dan mengkonversikan uang di dunia nyata menjadi mata uang *virtual*. *Cyber Laundering* adalah cara terbaru dalam teknik pencucian uang (Levi & Reuter, 2006). Ketika pencucian uang dilakukan melalui ruang siber, maka kecepatan proses dari pencucian uang akan meningkat pesat. Hal ini juga didukung oleh kondisi internet yang sedikit luput dari kekuatan hukum yang bersifat mengikat, adanya sifat anonimitas dari internet tanpa harus melibatkan kontak fisik, jangkauan yang luas, serta kecepatan transaksi yang cepat. Dengan begitu, hal ini akan menambah probabilitas atas peningkatan tindak kejahatan pencucian uang yang dilakukan melalui ruang siber.

Selain *cyber laundering*, ancaman lain yang dapat mengancam keamanan nasional Indonesia adalah *terrorism financing.* Bagaimana teroris memeroleh uang, dan bagaimana ini bisa dicegat, sering diabaikan. Sebaliknya, para pembuat kebijakan sering berfokus pada sumber pendanaan konvensional teroris atau hal-hal yang digunakan teroris untuk menghabiskan uang, seperti senjata dan serangan itu sendiri. Namun pergerakan uang merupakan langkah perantara yang penting. Kelompok teroris sering mengumpulkan uang di tempat yang berbeda dari tempat mereka berada dan berbeda dari tempat serangan mungkin terjadi. Agar kelompok teroris efektif, mereka harus bisa memindahkan uang dari asalnya ke wilayah operasional yang membutuhkan. Transfer uang ini merupakan titik lemah potensial yang dapat ditargetkan oleh negara untuk lebih efektif menghentikan organisasi teroris dan operasinya.

Untuk menemukan bagaimana NFT berpotensi menjadi sebuah ancaman bagi keamanan nasional Indonesia, penelitian ini akan menggunakan konsep keamanan nasional. Keamanan nasional adalah bentuk dari keamanan dan pertahanan negara yang berdaulat, termasuk warga negara, ekonomi, dan institusinya, yang dianggap sebagai tugas pemerintah (Baldwin, 1997). Konsep ini awalnya dipahami sebagai perlindungan terhadap serangan militer, namun setelah adanya perubahan dari kondisi dunia internasional, keamanan nasional secara luas dipahami mencakup juga dimensi non-militer, termasuk keamanan dari terorisme, minimalisasi kejahatan, keamanan ekonomi, keamanan energi, keamanan lingkungan, keamanan pangan, dan keamanan siber (Romm, 1993). Demikian pula, risiko keamanan nasional termasuk, selain tindakan negara-bangsa lain, tindakan oleh aktor non-negara oleh kartel narkotika, dan oleh perusahaan multinasional, dan juga dampak dari bencana alam. Keamanan Nasional merupakan sebuah konsep yang dinamis, yang berarti konsep ini sangat sering mengalami perubahan mengikuti konstelasi politik internasional. Ketika berbicara tentang definisi dari keamanan nasional, adalah sangat sulit untuk mendefinisikan keamanan nasional tersebut. Namun, dalam kerangka hukum internasional, definisi dari keamanan nasional ini sendiri diserahkan kepada masing-masing negara untuk membuat definisi dari keamanan nasional sendiri, selama definisi ini tidak melanggar dan menyalahi konsepsi negara demokratis (Amaritasari, 2015).

Keamanan nasional sendiri memiliki beberapa dimensi sebagai fokus dari konsep tersebut. Beberapa dimensi studi dari konsep keamanan nasional diantaranya adalah tindakan oleh negara lain (serangan militer atau siber), aktor kekerasan non-negara (serangan teroris), kelompok kriminal terorganisir seperti kartel narkotika, dan juga dampak bencana alam (banjir, gempa bumi), pemicu ketidakamanan sistemik, yang mungkin transnasional, termasuk perubahan iklim, ketidaksetaraan dan marginalisasi ekonomi, pengucilan politik, dan militerisasi (Rogers, 2010). Dalam jangkauan yang lebih luas, keamanan suatu negara memiliki beberapa dimensi, antara lain keamanan ekonomi, keamanan energi, keamanan fisik, keamanan lingkungan, keamanan pangan, keamanan perbatasan, dan keamanan siber. Dimensi ini berkorelasi erat dengan unsur-unsur kekuatan nasional.

PEMBAHASAN

Dalam keberjalanan perkembangan tindak kejahatan, akan selalu ada cara-cara dan modus-modus baru yang akan digunakan demi memperlancar keberjalanan tindak kejahatan tersebut. Keberadaan dari regulasi dan peraturan yang dibuat untuk mencegah serta memberantas tindak kejahatan tersebut juga akan selalu berubah, mengikuti modus-modus baru tindak kejahatan tersebut. Adanya sinkronisasi antara modus baru dan peraturan baru ini haruslah berimbang mengikuti satu sama lain, terutama dari sisi peraturan. Ketiadaan perubahan dari regulasi tersebut tentunya akan memperparah dampak dari tindak kejahatan tersebut dan dapat mengancam keamanan dan stabilitas nasional sebuah negara.

Hal ini berlaku pula pada tindak kejahatan pencucian uang dan pendanaan terorisme.

Ditemukannya modus-modus baru selalu diikuti dengan adanya perubahan aturan demi mencegah serta memberantas tindak kejahatan tersebut. Tindak pidana pencucian uang dan pendanaan terorisme selalu mengalami perubahan dari waktu ke waktu. Penggunaan jasa binatu swadaya yang digunakan oleh Al Capone pada awal tahun 1930 yang pada saat itu merupakan metode yang cukup baru, dengan cepat ditangani oleh pemerintah Amerika Serikat dengan adanya perubahan pada peraturan AML/CFT pada tahun 1932. Hal ini juga berlaku pada NFT.

NFT hadir sebagai salah satu sarana untuk mempermudah transaksi terutama pada seniman dan kreator dari setiap NFT yang ada di *marketplace*. Namun, dibalik kemudahan itu terdapat celah yang dapat digunakan oleh oknum-oknum yang tidak bertanggung jawab untuk melakukan tindak pidana pencucian uang serta pendanaann terorisme. Dalam hal regulasi, beberapa negara sudah menerapkan peraturan mengenai transaksi pada *marketplace* penyedia NFT untuk mencegah tindak pidana pencucian uang dan pendanaan terorisme. Secara garis besar, bab ini akan berusaha untuk menjelaskan mengenai potensi ancaman baru bagi keamanan nasional Indonesia yang dapat ditimbulkan oleh NFT, serta penanganan oleh negara-negara lain dalam mencegah dan memberantas tindak pidana pencucian uang dan pendanaan terorisme.

NFT sebagai Teknologi Nano dalam Tindak Pidana Pencucian Uang

Pencucian uang telah lama menjadi masalah di dunia seni rupa, dan tidak sulit untuk mengetahui alasannya. Seperti yang ditunjukkan oleh salah satu artikel 2019 dari National Law Review, karya seni seperti lukisan mudah dipindahkan, memiliki harga yang relatif subjektif, dan mungkin menawarkan keuntungan pajak tertentu (Hardy, 2019). Oleh karena itu, pelaku kejahatan dapat membeli barang seni dengan dana yang diperoleh secara tidak sah, kemudian menjualnya kembali, dan mereka memiliki uang bersih yang tidak ada hubungannya dengan kegiatan kriminal. Latar belakang ini membuat banyak orang bertanya-tanya apakah NFT rentan terhadap kejahatan serupa. Namun, pencucian uang dalam seni fisik sulit untuk diukur, dapat membuat perkiraan pencucian uang berbasis NFT yang lebih andal berkat transparansi yang melekat pada blockchain.

Meskipun setiap detail dari setiap transaksi dicatat, terdapat fitur anonimitas yang disediakan oleh banyak *marketplace* untuk melindungi identitas asli dari pengguna. Dengan kata lain, setiap orang dapat menggunakan identitas palsu untuk melakukan transaksi pada *marketplace* terkait. Hal ini dapat terjadi karena banyak *marketplace* tidak menerapkan prinsip KYC (*Know Your Customer*) untuk mendapatkan identitas riil dari pengguna tersebut. Sebagai contoh, jika kita ingin membuat akun pada *marketplace* OpenSea, identitas yang dibutuhkan hanya alamat *email*, serta nomor *wallet* dari *cryptocurrency* yang sudah dibuat sebelumnya untuk melakukan transaksi. Pengguna dapat saja memalsukan identitas deengan membuat alamat *email* palsu, serta menggunakan identitas palsu dalam pembuatan *wallet cryptocurrency* dan kemudian pengguna dapat melakukan transaksi dengan bebas. Hal ini dapat menjadi berbahaya, apabila seseorang membuat banyak akun untuk melakukan transaksi, bahkan transaksi dengan akun palsu lainnya yang dibuat secara mandiri.

Penggunaan fitur anonimitas ini memunculkan sebuah sifat baru dalam tindak pidana pencucian uang, yaitu sifat nano yang artinya pencucian uang dapat dilakukan dalam skala yang jauh lebih kecil. Pencucian uang yang dilakukan dengan metode konvensional dan non-digital, memerlukan bantuan dari pihak kedua untuk membantu pelaku dalam melakukan tindak kejahatannya. Sebagai contoh, pencucian uang dengan transaksi jual beli karya seni, properti, dan lain-lain memerlukan pelaku sebagai pihak pembeli, dan pihak kedua sebagai penjual maupun sebaliknya. Transaksi ini sangat mudah dilacak, karena adanya kejelasan mengenai pihak yang bertransaksi dan identitas asli dari para pelaku transaksi tersebut. Hal ini juga berlaku dengan metode penukaran uang pada gerai *money changer* atau pada bank.

Catatan-catatan mengenai setiap transaksi dengan jelas tercatat menggunakan identitas asli. Hal lain yang perlu dicatat, adalah transaksi yang terjadi pada pasar pelelangan tersebut tidak menggunakan mata uang resmi negara manapun. Transaksi yang dilakukan oleh pihak tersebut menggunakan *cryptocurrency*, dimana penggunaan alat tukar tersebut menambah lapisan baru yang menambah rumit pelacakan jejak dari uang ilegal tersebut.

Menurut data yang dihimpun dari *Chainalysis,* jumlah uang yang dikirimkan dari alamat *blockchain* yang terkait dengan tindakan kriminal meningkat pesat pada tahun 2021, seiring dengan meningkatnya tren NFT. Jumlah uang yang dikirim ke pasar NFT oleh alamat yang terdeteksi pernah terkait dengan tindak kriminal, melonjak secara signifikan pada kuartal ketiga tahun 2021, dengan jumlah cryptocurrency senilai 1 juta US Dollar. Angka tersebut tumbuh lagi pada kuartal keempat, mencapai 1,4 juta US Dollar. Di kedua kuartal, sebagian besar aktivitas ini berasal dari alamat terkait penipuan yang mengirimkan dana ke pasar NFT untuk melakukan pembelian. Kedua kuartal juga mendeteksi sejumlah besar dana curian yang dikirim ke pasar NFT. Mungkin yang paling memprihatinkan, pada kuartal keempat, Chainalysis mendeteksi cryptocurrency senilai sekitar $284.000 yang dikirim ke pasar NFT dari alamat dengan transaksi mencurigakan (Chainalysis, 2022).

Tindak pidana pencucian uang dengan menggunakan metode *NFT* ini dapat digolongkan berbahaya. Beberapa ahli menyebutkan bahwa, ada banyak kemungkinan yang diberikan oleh metode ini, yang tidak hanya terbatas pada tindak pidana pencucian uang. Metode ini juga dapat memberikan sebuah celah pada tindak pidana kejahatan keuangan lainnya seperti penghindaran dan penggelapan pajak, penggelapan uang, dan tindak kejahatan keuangan lainnya. Hal ini dikarenakan selain menggunakan alat tukar yang tidak lazim, fitur anonimitas dari transaksi-transaksi tersebut sangat mempersulit pelacakan transaksi yang terjadi, sehingga penelusuran dan rekam jejak dari transaksi-transaksi tersebut hampir mustahil untuk dilakukan. Enkripsi yang diterapkan pada beberapa penyedia jasa transaksi virtual tersebut, bahkan tidak memungkinkan untuk diakses, bahkan oleh penyedia jasa tersebut sekalipun.

Anonimitas NFT dalam Pendanaan Terorisme

Fitur anonimitas merupakan fitur yang memungkinkan seorang pengguna untuk tidak menggunakan identitas asli mereka dalam menjelajah internet dan meakukan transaksi di Internet. Jika dibandingkan dengan jasa keuangan konvensional seperti bank, gerai penukaran uang, dan jasa-jasa lainnya, penggunaan identitas asli dari pelaku transaksi merupakan salah satu prinsip utama dari KYC (*Know Your Customer*). Hal ini dilakukan demi mencegah adanya tindakan-tindakan yang mencurigakan yang dapat mengarah pada tindak kejahatan.

Fitur anonimitas ditawarkan oleh banyak *marketplace* sebagai solusi atas keamanan data dari setiap pelaku transaksi. Jika ditilik dari sisi positif, penggunaan fitur anonimitas sangat melindungi privasi dan keamanan data dari sesorang. Data tersebut bisa saja digunakan untuk tindak kejahatan lain seperti pemalsuan identitas, dan kejahatan lainnya. Solusi yang ditawarkan oleh banyak *marketplace* ini merupakan sebuah fitur yang solutif, namun tidak dapat dipungkiri bahwa fitur ini dapat disalahgunakan oleh orang-orang yang memiliki niat untuk melakukan tindak kejahatan. Penggunaan fitur anonimitas yang melindungi identitas asli dari pendana tindak terorisme ini jika digunakan oleh pelaku tersebut, dapat melindungi pelaku tindak pidana pendanaan terorisme dari aturan-aturan yang berlaku.

Penggunaan fitur anonimitas juga tidak terbatas pada tindak pidana pencucian uang. Fitur ini dapat pula digunakan dalam tindak pidana pendanaan terorisme. Dalam metode konvensional, tindak pidana pendanaan terorisme dilakukan dengan penggunaan uang tunai, baik dengan perpindahan uang tunai tersebut melewati batas negara untuk kemudian digunakan oleh jaringan terorisme dalam mebiayai kegiatan terornya, maupun transaksi jual beli oleh pemberi dana terhadap jaringan terorisme tersebut. Seperti contoh yang sudah dipaparkan pada

bab II, jaringan Mujahidin Indonesia Timur kelompok Santoso mendapatkan dana dari ISIS dalam bentuk uang tunai yang diangkut dari Turki ke Indonesia, maupun melalui transaksi aset milik WNI yang sedang berada di Suriah dan kemudian dibeli oleh ISIS. Metode konvensional ini juga sudah dapat ditangkal dengan aturan-aturan yang dibuat oleh pihak yang berwenang.

NFT memberikan banyak kemudahan bagi pelaku tindak pidana pendanaan terorisme untuk mengalirkan dana bagi kelompok teroris yang membutuhkan. Dibandingkan dengan metode konvensional, NFT menawarkan banyak kemudahan pada kedua belah pihak (pendana dan teroris). Fitur anonimitas yang digunakan dapat menyamarkan identitas asli dari pemberi dana, dan kelompok teroris itu sendiri. Pendanaan terorisme dapat menjadi lebih mudah dengan adanya fitur ini.

Selain itu, pendana tindak terorisme dapat dipecah menjadi bagian-bagian yang sangat kecil. Hal ini dapat pula dilakukan oleh penerima dana yaitu kelompok teroris itu sendiri. Pemecahan dana kedalam akun-akun kecil yang nantinya akan dikumpulkan menjadi satu bertujuan untuk mempersulit pelacakan dana yang akan digunakan untuk mendanai terorisme itu sendiri. Dengan demikian, aparat penegak hukum semakin sulit pula untuk menelusuri asal dari dana tersebut.

Dalam pengaplikasiannya, pihak pendana dan teroris dapat secara anonim mendaftarkan *wallet* yang akan mereka gunakan untuk bertransaksi. Kemudian, pihak teroris dapat mendaftarkan *NFT* yang nantinya akan dibeli oleh pihak pendana menggunakan akun anonim mereka, dan memindahkan sejumlah uang dari akun pendana menuju akun teroris. Identitas mereka akan tetap terjaga dengan adanya fitur anonimitas dari *marketplace* yang mereka gunakan.

Sebagai contoh, jika A ingin melakukan pendanaan terhadap organisasi Al-Qaeda, A akan menyuruh pihak Al-Qaeda untuk mendaftarkan sebuah *Kitties* pada *marketplace CryptoKitties*. A kemudian akan melakukan pembelian terhadap *kitties* tersebut, dengan harga sesuai dengan yang dibutuhkan oleh Al-Qaeda. Uang tersebut kemudian berpindah dari *wallet* A ke *wallet* dari Al-Qaeda, yang kemudian akan dicairkan melalui metode yang tersedia pada *CryptoKitties*.

Penggunaan NFT ini hampir sama dengan metode konvensional yang sudah pernah digunakan sebelumnya. Namun, dengan munculnya sifat anonimitas dalam setiap transaksi pada *marketplace*, semakin memudahkan dan semakin menyamarkan identitas asli dari setiap pelaku transaksi dalam marketplace tersebut.

KESIMPULAN

Dalam perkembangan teknologi informasi dan komunikasi, ada banyak perkembangan yang terjadi. Salah satunya merupakan kemunculan NFT sebagai tren terbaru dalam perdagangan digital. Hal ini, tentunya merupakan sebuah terobosan baru dalam dunia digital. Namun, hal ini juga dapat menjadi celah dalam melakukan tindak kejahatan pencucian uang dan pendanaan terorisme.

Fitur anonimitas dan sifat nano yang ditimbulkan yang disediakan oleh banyak tempat penjualan NFT menjadi salah satu kunci penting dalam melakukan tindak kejahatan pencucian uang dan pendanaan terorisme dengan menggunakan NFT sebagai medianya, sementara belum ada regulasi yang dikeluarkan oleh pemerintah untuk mengatur dan meregulasi transaksi NFT yang terjadi.

Dalam penelitan terdahulu, disebutkan bahwa masalah utama dari pencucian uang via NFT dan *cryptocurrency* adalah kurangnya pemahaman tentang peran *cryptocurrency* dalam kejahatan keuangan (Matherson, 2021). Selama ketidakpahaman ini tidak ditangani, maka potensi penggunaan NFT sebagai metode baru dalam kejahatan keuangan akan meningkat tajam hinggan membahayakan keamanan nasional. Meskipun penyelidik kriminal menggunakan teknologi untuk memecahkan kejahatan kripto, terdapat kekurangan sumber

daya untuk membongkar operasi ilegal tersebut. Sistem peradilan pidana harus menegakkan hukuman terhadap organisasi kriminal untuk mencegah kejahatan tambahan. Masalah spesifiknya adalah banyaknya *cryptocurrency* yang digunakan di pasar gelap. Koin-koin dan NFT yang digunakan memungkinkan transaksi anonim yang menimbulkan kesulitan bagi penegak hukum untuk menyelidiki kejahatan yang berkaitan dengan mata uang digital.

Selain itu, saat ini hanya terdapat sedikit undang-undang dan peraturan yang berfokus pada masalah pencucian uang melalui dunia siber, dan peraturan-peraturan tersebut juga bergantung pada batas keuangan dan geografis yang ditentukan (Nathalie, 2022). Pemerintah kemudian harus mempertimbangkan perkembangan teknologi terkini, bersama dengan peraturan lintas yurisdiksi, sambil membangun kebijakan pencucian uang baru yang merangkup dunia siber. Penegakan hukum, badan pengatur, dan sektor swasta jelas memiliki peran dalam proses pembuatan kebijakan. Pihak-pihak ini harus berkumpul untuk membahas masalah yang menjadi perhatian bersama, dan mengembangkan tindakan yang efektif untuk mencegah dan mendeteksi kejahatan keuangan *online* tanpa menghalangi keuntungan komersial dan konsumen dari teknologi baru.

Hasil penelitian ini didapat menggunakan konsep keamanan nasional. Konsep ini menyatakan bahwa masalah keamanan tidak hanya berasal dari aspek militer, namun juga dapat berasal dari aspek-aspek non-tradisional seperti keamanan siber, keamanan ekonomi, dan lain-lain. Penggunaan NFT sebagai metode baru dalam melakukan tindak kejahatan pencucian uang dan pendanaan terorisme dapat menjadi salah satu ancaman terhadap keamanan ekonomi Indonesia. Penggunaan fitur anonimitas dan pemecahan transaksi pada tingkat nano menambah tingkat kerusakan yang dapat dihasilkan oleh para pelaku pencucian uang dan pendanaan terorisme.

Beberapa negara sudah mengeluarkan regulasi mengenai transaksi dunia kripto dan NFT untuk mencegah terjadinya hal ini untuk menjaga keamanan nasional dan menutup celah-celah yang dapat digunakan oleh para pelaku tindak kejahatan pencucian uang dan pendanaan terorisme. Hal ini dapat menjadi ancaman serius terhadap keamanan nasional, apabila tidak ada pihak berwenang yang mengambil langkah yang serius dalam menangani celah-celah dalam transaksi mengenai NFT. Hal ini menjadi sebuah ancaman yang semakin serius, mengingat fenomena NFT sedang menjadi tren baru-baru ini.

UCAPAN TERIMA KASIH

Dalam hal ini, penulis ingin mengucapkan apreasiasi yang sebesar-besarnya dan rasa terima kasih kepada Ibu Ika Riswanti Putranti, A.Md.Ak., S.H., M.H., Ph.D sebagai Dosen Pembimbing I dan Bapak Marten Hanura, S.IP M.P.S sebagai Dosen Pembimbing II yang telah meluangkan waktunya untuk memberikan bimbingan dan motivasi kepada penulis. Lebih dari itu, penulis dengan segala hormat juga ingin mengucapkan terima kasih banyak kepada seluruh tenaga pendidik Departemen Hubungan Internasional Universitas Diponegoro untuk semua ilmu dan wawasan yang telah diberikan kepada penulis. Singkat kata, semoga segala tanggung jawab yang diberikan kepada Ibu Ika, Bapak Marten, dan semua tenaga pendidik Departemen Hubungan Internasional dapat dimudahkan dan dilancarkan.

REFERENSI

Amaritasari, I. (2015). Keamanan Nasional dalam Konsep dan Standar Internasional. *Jurnal Keamanan Nasional*, 153-174.

Baldwin, D. A. (1997). The Concept of Security. *Review of international studies*, 5-26.

Chainalysis. (2022). *Crypto Crime Report.* Chainalysis.

Entriken, W., Shirley, D., Evans, J., & Sachs, N. (2018). Erc-721 non-fungible token standard. *Ethereum Standard*.

Filipkowski, W. (2008). Cyber Laundering: An Analysis of Typology and Techniques. *International Journal of Criminal Justice Sciences*.

Hardy, P. D. (2019, 3 20). *The World of Fine Art and Money Laundering*. Diambil kembali dari National Law Review: https://www.natlawreview.com/article/art-and-money-laundering

Kibar Kaloka, M. (2018). Cyber Laundering melalui Online Games: Potensi Ancaman Keamanan Ekonomi. *Journal of International Relations 1.1*, 31-40.

Levi, M., & Reuter, P. (2006). Money Laundering. *Crime And Justice*, 289-375.

Matherson, N. (2021). The Driving Force of Cryptocurrency and Money Laundering. Dalam N. Matherson, *The Driving Force of Cryptocurrency and Money Laundering* (hal. 1-9). ProQuest Dissertations Publishing.

Nathalie, R. (2022). Cyber Laundering. *International Conference on Cybersecurity and Cybercrime*, (hal. 77-82).

NonFungible.com. (2020). *Non-Fungible Tokens Yearly Report.* L'Atelier BNP Paribas.

Rogers, P. (2010). *Losing Control: Global security in the 21st century.* London: Pluto Press.

Romm, J. J. (1993). *Defining national security: the nonmilitary aspects.* Council on Foreign Relations.

Shirole, M., Darisi, M., & Bhirud, S. (2019). Cryptocurrency Token: An Overview. *IC-BCT*, 133-140.

Wood, G. (2015). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*.