



**Cyber Laundering melalui Online Games:
Potensi Ancaman Keamanan Ekonomi**

Muchamad Kibar Kaloka
Departemen Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Diponegoro
Jalan Prof. H. Soedarto, SH, Tembalang, Semarang, Kontak Pos 1269
Website: <http://www.fisip.undip.ac.id> Email: fisip@undip.ac.id

ABSTRACT

The development of money laundering modus has begun to move into the digital and the internet world, which triggers the emerging of potential of new threats. One of these potentials is the potential threat of cyber laundering through online games. The world of entertainment market, especially in the field of online games that continues to grow has the potential to invite potential money launderers. In Indonesia, this market still does not have a strong regulation. It creates a gap for cyber laundering. This research seeks to see how big the potential threat is and whether the Indonesian government has realized about the potential threat, and how are the chances of the issue to be securitized by the Indonesian government. The research method used is quantitative and qualitative by collecting data and analyzing them to find out how big the potential of the threat and the securitization opportunities of the threat. The result of this research shows that there is a lack of securitization from the Indonesian government due to the related parties in the field of gaming and the government itself has not realized the potential of this threat, so there are gaps that can be entered by potential money launderers.

Keywords: *Indonesia, cyber laundering, online games, securitization*

Pendahuluan

Internet merupakan sarana pertukaran informasi yang sangat luas. Informasi apapun bisa diakses kapan saja dengan mudah dan cepat. Dalam perkembangannya, internet sudah mulai menjadi salah satu kebutuhan hidup bagi masyarakat modern. Banyak layanan yang mulanya hanya dapat diperoleh di kehidupan nyata yang mulai bermunculan di internet dengan proses yang lebih mudah dan singkat. Sebagai contoh adalah adanya transaksi belanja dan *online banking* di mana terjadi perpindahan dana di dalam internet dalam bentuk uang virtual (Filipkowski, 2008). Masyarakat dapat bertransaksi lintas negara dengan lebih mudah dan cepat. Dengan adanya transaksi ini dan adanya aliran dana di internet, ekonomi dapat berkembang dengan cepat.

Namun di sisi lain, ada pihak-pihak yang berniat untuk menggunakan kemudahan-kemudahan yang tersedia di internet ini untuk melakukan tindakan-tindakan ilegal, salah satunya adalah *money laundering*. Penyalahgunaan internet untuk upaya pencucian uang oleh pihak-pihak tersebut merupakan sebuah ancaman yang potensial bagi keamanan ekonomi internasional (Solicitor General Canada, 1998). Tindakan ini dikenal dengan istilah *cyber laundering*.

Cyber laundering memanfaatkan layanan-layanan dan media-media finansial *online* yang tersedia di dalam internet yang menggunakan uang virtual. Pencucian uang melalui internet dipercaya merupakan sebuah teknik terbaru dan termutakhir dalam metode pencucian uang (Levi dan Reuter, 2006). Dengan *cyber laundering*, proses pencucian uang

menjadi lebih cepat. Dengan keadaan internet yang masih belum dipenuhi dengan aturan hukum, menambah kemungkinan akan banyaknya pelaku yang berpindah dari pencucian uang secara konvensional menuju ke *cyber laundering* dapat semakin meningkat sebagai akibat dari anonimitas yang ada, tidak adanya kontak fisik, kecepatan transaksi dan jangkauan yang lebih luas di dalam layanan internet. (Filipkowski, 2008).

Salah satu media yang menggunakan layanan finansial di internet yang dijadikan sebagai sarana *cyber laundering* adalah *online games*. Media permainan ini menyediakan layanan berbayar secara virtual bagi jutaan pemainnya yang berasal dari berbagai negara. Dengan jumlah pemain tersebut, para pencuci uang dapat dengan mudah membuka banyak akun palsu untuk bertransaksi, misalnya dengan menjual uang virtual yang mereka beli dengan uang ilegal kemudian dijual kembali kepada para pemain melalui transaksi *online* agar uang tersebut menjadi legal (Richet, 2013).

Dengan terus berkembangnya pasar *online games*, kemungkinan ancaman *cyber laundering* menjadi semakin besar. Hampir setiap tahunnya, pasar *online games* selalu meningkat jumlah profitnya (Versace, 2014; Newzoo, 2014; Newzoo, 2015). Peningkatan tersebut dapat menjadi ladang pencucian uang yang besar dan luas jika dibiarkan begitu saja. Atas dasar adanya potensi ancaman ini, penulis memutuskan untuk meneliti fenomena ancaman *cyber laundering* di internet melalui online game. Penulis akan meneliti bagaimana potensi dan kemungkinan proses sekuritisasi terhadap *cyber laundering* melalui *online games* dilakukan dan ancaman-ancaman yang dapat muncul dari pencucian tersebut. Penulis juga akan mengkaji mengenai ancaman lanjutan dari ancaman *cyber laundering* tersebut bagi keamanan ekonomi apabila dibiarkan tanpa adanya regulasi dari pihak yang berwenang di Indonesia.

Pembahasan

Cyber laundering adalah perkembangan dari tindak pencucian uang tradisional. Tindakan pencucian uang (*money laundering*) yang prosesnya tidak lagi dilakukan dalam bentuk nyata atau fisik. *Cyber laundering* melibatkan perubahan wujud dari wujud legal yang sah menuju ke wujud virtual dan kemudian dicuci dalam bentuk tersebut di dalam internet untuk kemudian dijadikan menjadi wujud legalnya kembali dengan transaksi yang sah melalui internet. Transaksi di internet dapat dilakukan dengan menggunakan layanan seperti *micro-payment*, *online banking*, dan *smart cards* (Filipkowski, 2008). Layanan ini digunakan untuk transaksi jual beli di dalam internet, biasanya pada situs belanja ataupun *online games* (Strauss, 2013). Dalam perkembangannya, *cyber laundering* diperkirakan memiliki potensi untuk menggunakan sejumlah layanan internet yang berkaitan dengan pembayaran, jual-beli, dan transaksi keuangan lain. (Tropina, 2014)

Layanan-layanan tersebut antara lain adalah *online banking*, layanan dari berbagai bank yang ada di internet. Fasilitas yang ada di *online banking* sama dengan fasilitas yang ada di bank nyata. Pemilik akun bank dapat melakukan transaksi pembayaran, mentransfer, mendepositkan uang ke rekening lain atau akun bank lain, dan juga menyetorkan uang ke rekening sendiri. Kelebihan dari *online banking* adalah segala transaksi dapat dilakukan secara cepat dimanapun dan kapanpun selama terhubung dengan internet. Dalam kasus-kasus pencucian uang penggunaannya kurang lebih sama dengan transfer biasa melalui ATM atau bank. Kedua, *mobile banking*, layanan ini memiliki layanan dan proses yang sama seperti dengan *online banking*. Perbedaannya terletak pada peralatan yang digunakan. *Mobile banking* dilakukan dengan menggunakan peralatan genggam (*gadget*) seperti telepon genggam, misalnya dengan membeli aplikasi. *Mobile banking* dapat dilakukan di mana saja selama telepon genggam tersambung dengan layanan internet. Ketiga, situs-situs *online games*, dengan memasukkan uang ilegal dari hasil kejahatan ke dalam permainan dan mengubahnya menjadi bentuk mata uang yang berlaku di dalam

permainan dapat menyamakan asal muasal uang tersebut, termasuk dengan mengubahnya menjadi barang dalam permainan dan kemudian ditransaksikan dengan pemain lain yang tersebar di berbagai negara (Trend Micro, 2016).

Keempat, layanan jual-beli *online* dan *e-commerce*. Dengan membelanjakan uang yang telah di-*placement* ke dalam layanan jual beli internet maka uang akan dapat berpindah tangan dengan cepat dan berubah bentuk menjadi barang atau jasa yang dibeli, yang kemudian dapat diubah kembali menjadi uang, dan keluar sebagai dana yang legal dari hasil jual beli yang sah (Trend Micro, 2016). Kelima, pembajakan akun dan situs game. Dengan menggunakan jasa *hacker*, akun-akun dan situs game dapat dibajak dan diubah datanya sehingga menjadi menguntungkan bagi pelaku (Trend Micro, 2016).

Sementara itu, *online games* adalah sebuah permainan yang dimainkan dengan memanfaatkan jaringan internet, dapat dimainkan melalui computer (PC), laptop, serta perangkat lain yang memadai untuk tersambung dengan internet. Pada umumnya, permainan ini dimainkan oleh banyak pemain, yang diwakilkan secara *digital* dengan sebuah karakter di dalam permainan tersebut. Pemain yang berada di dalam permainan berasal dari berbagai negara (Steinkuehler dan Williams, 2006) untuk menyelesaikan suatu tujuan yang telah ditetapkan dalam permainan tersebut bersama, atau bersaing satu sama lain. Di beberapa judul, pemain berusaha untuk mencapai skor/nilai atau menyelesaikan tugas tertentu yang ditentukan dan kemudian dibandingkan dengan pemain lainnya (Keegan, 2010).

Online game hadir di Indonesia dimulai pada tahun 2001, (Basitt, t.thn.) yang kemudian mulai menarik perhatian banyak pengguna komputer dalam mencari alternatif hiburan baru, dengan sebuah sajian yang disebut "*Online games*", di mana banyak pemain dapat memainkan game ini secara bersamaan dari berbagai tempat yang berbeda melalui koneksi internet. Pada sekitar tahun 2009-2014 terjadi pertumbuhan (Basitt, t.thn.) pesat pemain yang memainkan *online game* diiringi dengan masuknya lebih dari 20 judul *online game* dengan berbagai macam genre.

Online games memiliki layanan yang berbeda di setiap judulnya, tergantung dari kebijakan pengembangnya. Beberapa permainan akan meminta pemain untuk membayar biaya dalam jumlah tertentu dan pemain baru akan dapat bermain ketika biaya tersebut telah dibayarkan. Dengan layanan seperti ini, pemain akan diberikan sebuah masa langganan untuk memainkan permainan tersebut. Bentuk layanan lain adalah dengan memberikan pemain kesempatan untuk bermain dan mengakses semua konten permainan yang disediakan secara gratis. Namun, pihak pengembang menyediakan barang-barang berbayar di dalam permainan, di mana barang-barang tersebut akan membantu pemain dalam permainannya (Oh dan Ryu, 2007). Sebagai contoh, sebuah barang dapat memberikan pemain kemudahan dalam menyelesaikan sebuah misi atau tujuan di dalam permainan tersebut dengan menguatkan karakter pemain .

Bantuan, keistimewaan, barang-barang dan perlakuan khusus yang didapat dari pembelian layanan ini dapat juga disebut sebagai aset di dalam game yang dimiliki oleh pemain di dalam game. Tetapi, pada dasarnya, meskipun aset tersebut milik para pemain di dalam akun mereka masing-masing, pihak perusahaan pemilik game tersebutlah yang berkuasa atas aset tersebut karena akun dari para pemain tersebut dipegang oleh pihak perusahaan dan dapat dirubah, digunakan, atau dihilangkan sewaktu-waktu, karena sumber utama dari barang-barang tersebut berasal dari *online games* milik perusahaan, dan disimpan dalam sistem milik perusahaan, mulai dari desainnya, modelnya, hingga ide atau konsep dari barang tersebut (Oh dan Ryu, 2007).

Barang-barang tersebut dapat dibeli melalui mata uang khusus yang berlaku di dalam permainan yang dapat dibeli dengan melakukan transaksi pembelian dengan uang nyata kepada pihak pengembang, umumnya melalui sebuah kode yang disediakan oleh

pengembang. Pemain dapat mengunjungi halaman situs dari pengembang dan membelinya dari halaman tersebut, atau melalui perantara lain yang ditunjuk oleh pihak pengembang (Oh dan Ryu, 2007). Layanan penyediaan barang ini juga terdapat pada permainan dengan layanan berlangganan dan membayar sebelum bermain.

Keberlangsungan online games sendiri tidak lepas dari peran aset-aset yang digunakan di luar *online games*. Aset di luar *online games* lebih melibatkan pihak dari luar selain dari pemain. Pihak yang terlibat dalam aset ini berupa penyedia jasa, produk, maupun dana yang berkaitan dengan upaya penjagaan keberlangsungan game dan pemasarannya menuju ke pasar yang lebih luas (Marchand dan Thurau, 2013). Cara yang sering dilakukan adalah dengan memproduksi aset berupa *merchandise* yang berkaitan dengan *game*. *Merchandise* ini seringkali berupa barang yang dapat dikoleksi oleh para pemain dan diproduksi dalam jumlah terbatas, dengan harapan agar pemain tertarik untuk membeli dan mencari tahu mengenai *game* yang diiklankan melalui *merchandise* tersebut dan hasil penjualannya dapat digunakan untuk mengembangkan *game*.

Selain menggunakan aset berupa *merchandise*, perusahaan juga menawarkan aset berupa lisensi kepada pihak-pihak yang menawarkan jasa sebagai distributor perusahaan tersebut ke wilayah lain, seringkali ke suatu negara lain (Marchand dan Thurau, 2013). Selain distribusi game lintas wilayah, penawaran lisensi yang diberikan oleh perusahaan juga dapat diarahkan ke alternatif lain berupa adaptasi. Adaptasi yang dimaksud adalah membuat game menjadi bentuk media hiburan yang berbeda, seperti film, animasi, komik, dan juga novel. Selain cakupan pasar yang lebih luas dan beragam, adaptasi memberi kemudahan bagi para calon pemain baru mengetahui dan mengakses mengenai keberadaan game.

Dalam dinamika *online games*, pemain merupakan sumber pemasukan bagi *game* atau perusahaan *game* tersebut. Perputaran dana dan transaksi yang terjadi di dalam *game* berasal dari pemain. Berdasar hal tersebut, penulis melakukan survei untuk melihat seberapa sering pemain memainkan *online games*, seberapa besar dana yang berputar dan seberapa tinggi intensitas transaksi yang terjadi di dalam permainan.

Dari hasil yang penulis dapatkan dari 346 responden, 209 orang menghabiskan lebih dari 8 jam, 65 orang menghabiskan antara 6-8 jam, 52 orang menghabiskan antara 4-6 jam, 16 orang menghabiskan antara 2-4 jam, dan 4 orang sisanya menghabiskan dalam penggunaan internet mereka per harinya. Dengan data ini, dapat dilihat bahwa waktu penggunaan internet rata-rata mulai dari 4 hingga lebih dari 8 jam per harinya. Dari lamanya penggunaan internet per harinya, 42 orang menghabiskan lebih dari 8 jam, 66 orang menghabiskan antara 6-8 jam, 97 orang menghabiskan antara 4-6 jam, 94 orang menghabiskan 2-4 jam, dan 47 orang menghabiskan kurang dari 2 jam dari total penggunaan internet mereka per harinya untuk bermain *online games*. Dengan data ini, ada rata-rata waktu antara 2 hingga 6 jam dari waktu penggunaan internet digunakan untuk bermain *online games*. Waktu bermain tersebut digunakan oleh para responden untuk memainkan beberapa judul *online games* yang berbeda. 146 orang memainkan lebih dari 6 judul, 34 orang memainkan 4-6 judul, 118 orang memainkan 2-4 judul, dan 48 orang sisanya memainkan 1 judul *online games* dari waktu bermain mereka per harinya. Hal ini menunjukkan bahwa terdapat aktivitas penggunaan internet yang besar untuk bermain *online games* per hari dari para responden.

Sebagian besar responden juga menjawab bahwa mereka sering melakukan transaksi pembelian di dalam permainan. 12 orang mengaku mereka melakukan pembelian lebih dari Rp. 1.000.000,00, 18 orang melakukan pembelian sebesar Rp. 500.000,00 – Rp. 1.000.000,00, 44 orang melakukan pembelian sebesar Rp. 300.000,00 – Rp. 500.000,00, 122 orang melakukan pembelian sebesar Rp. 100.000,00 – Rp. 300.000,00, dan 100 orang melakukan pembelian di bawah Rp. 100.000,00. Para responden sebagian besar melakukan

pembelian dengan nominal rata-rata antara Rp. 100.000,00 - Rp. 500.000,00 di setiap pembeliannya. Diikuti dengan responden yang melakukan pembelian di bawah Rp. 100.000,00 dan beberapa yang melakukan pembelian di atas Rp. 1.000.000,00. Pembelian tersebut dilakukan dengan intensitas rata-rata 1 hingga 4 kali per bulannya. Beberapa responden juga menjawab bahwa mereka melakukan transaksi pembelian lebih dari 10 kali per bulan.

Data-data tersebut menunjukkan adanya transaksi yang berjumlah besar yang terjadi setiap bulannya di dunia *online games* Indonesia. Berdasar hasil survei, mulai dari waktu yang dihabiskan dalam bermain, dana yang dikeluarkan dan intensitas transaksi, penulis memperkirakan setidaknya setiap bulannya terdapat jumlah transaksi paling rendah dengan nilai antara Rp. 1.000.000,00 – Rp. 9.000.000,00 per pembeliannya, yang berasal hanya dari 100 orang yang melakukan pembelian di bawah Rp. 100.000,00 dengan 1 kali pembelian per bulannya, dan transaksi paling tinggi antara Rp. 12.200.000,00 - Rp. 36.600.000,00 yang berasal hanya dari 122 pemain yang menghabiskan antara Rp. 100.000,00 – Rp. 300.000,00 dengan pembelian 1 kali pembelian per bulannya di dalam *online games* yang aktif dilakukan oleh para pemain dengan penggunaan waktu yang banyak di internet dan *online games* setiap hari dki setiap bulannya. Jumlah ini pun belum termasuk dengan beberapa pemain yang menghabiskan lebih dari Rp. 500.000,00 atau bahkan Rp. 1.000.000,00 dan jumlah pembelian di atas 1 kali per bulannya yang dapat membuat total transaksi tertinggi dapat melampaui Rp. 40.000.000,00.

Keaktifan dan intensitas transaksi pemain ini dapat memberikan *online games* potensi untuk digunakan sebagai sarana *cyber laundering*. Fakta lain yang penulis dapatkan adalah transaksi yang dilakukan oleh para pemain Indonesia seringkali berada di luar pengawasan pihak perusahaan game dan bukan transaksi resmi untuk *game* tersebut. Transaksi ini dinamai RMT (*Real Money Transaction*). Transaksi ini merupakan sebuah transaksi menggunakan uang nyata untuk membeli aset di dalam *game*, di mana seharusnya aset tersebut hanya boleh diperjualbelikan melalui mata uang yang berlaku di dalam *game*. Berdasar survei, hampir separuh mengaku pernah melakukan RMT. Hal ini dapat menjadi celah bagi *online games* karena pemain sendiri seringkali melakukan transaksi di luar pengawasan perusahaan yang memiliki *game* tersebut.

Hasil dari survei penulis menunjukkan bahwa dari 346 responden yang menjawab, 239 responden mengaku tidak mengetahui apa yang dimaksud dengan *cyber laundering*. Sementara itu, 90 responden mengaku hanya sekedar mengetahui istilah tersebut dan 17 responden mampu menjawab pertanyaan penulis dengan cukup baik, menunjukkan bahwa mereka memang benar memahami istilah *cyber laundering*, dengan beberapa diantaranya mampu menjelaskan pandangan mereka sendiri terhadap potensi *cyber laundering* melalui *online games*.

Hasil tersebut menunjukkan bahwa kesadaran pemain mengenai potensi *cyber laundering* masih rendah dan dapat menjadi celah karena pemain tidak mengetahui apa dan bagaimana praktik *cyber laundering* dilakukan. Ditambah dengan fakta tingginya perkiraan angka transaksi yang terjadi di dalam *online games* dan banyaknya pemain yang menghabiskan sebagian besar waktu mereka untuk bermain setiap harinya, lalu lintas pemain yang tinggi ini dapat dijadikan sarana untuk *cyber laundering*.

Bagaimana dengan kesadaran pemerintah dan perusahaan *online games*? Di Indonesia, transaksi yang dilakukan pemain lebih mengarah kepada transaksi terhadap aset di dalam *game*. Hal ini dikarenakan karena perusahaan-perusahaan game di Indonesia hanya bertindak sebagai distributor yang membeli lisensi dari perusahaan pemilik asal *online games* tersebut diciptakan untuk dipasarkan di Indonesia. Sebagai hasilnya, perusahaan-perusahaan yang berada di Indonesia memiliki kemampuan dan kekuasaan

yang terbatas dalam produksi aset di luar game seperti *merchandise* dan adaptasi ke media lain.

Hasil pengamatan penulis terhadap kebijakan-kebijakan yang diterapkan oleh perusahaan-perusahaan *online games* di Indonesia menunjukkan bahwa mereka menerapkan aturan dan kebijakan yang cenderung sama. Semua perusahaan mewajibkan pemain untuk memberikan identitas yang dijamin kerahasiaannya oleh perusahaan yang biasanya berupa alamat email yang aktif dan beberapa data tambahan seperti nama dan tanggal lahir agar dapat memainkan game. Semua tindakan yang dilakukan pemain di dalam game merupakan tanggung jawab dari masing-masing pemain, perusahaan tidak akan ikut bertanggung jawab atas hal dan kerugian yang bisa saja terjadi akibat perbuatan pemain di dalam game. Perusahaan tidak bertanggung jawab apabila akun pemain mengalami kerusakan atau kerugian karena dicurangi, terkena *hack*, hilang password yang disebabkan oleh kesalahan pemain.

Perusahaan dapat menghapus akun yang telah didaftarkan tanpa adanya pemberitahuan apabila ditemukan adanya ketidaksesuaian data yang didaftarkan, tindakan mencurangi game, tindakan yang melanggar norma, dan tindakan yang mengubah paksa fitur-fitur yang ada di dalam game. Semua perusahaan secara tertulis mengakui bahwa mereka akan selalu melakukan pengawasan untuk mencegah dan memberantas hal-hal tersebut. Mengenai masalah transaksi yang dilakukan oleh pemain, semua perusahaan melarang transaksi yang dilakukan di luar layanan yang telah disediakan perusahaan dan tidak akan bertanggung jawab atas apa yang terjadi saat dan setelah transaksi di luar layanan tersebut terjadi.

Berdasarkan aturan tersebut, dapat disimpulkan bahwa perusahaan-perusahaan di Indonesia sudah cukup tanggap dan sadar dalam mengantisipasi potensi pencurian dan penyalahgunaan transaksi yang dilakukan di dalam game. Transaksi yang terdeteksi akan langsung ditindak dan dihapus datanya dari sistem game. Namun, hal itu hanya terbatas pada transaksi di luar layanan perusahaan yang prosesnya dilakukan di dalam game, melalui chat atau pesan pribadi di dalam game yang dapat dilacak oleh perusahaan. Perusahaan tidak dapat mendeteksi transaksi seperti RMT yang komunikasi dan pembayarannya dapat dilakukan di luar game yang dapat dilihat hanyalah proses tukar barang di dalam game tanpa adanya pembayaran di dalam game, yang diperbolehkan oleh aturan perusahaan, karena pertukaran barang antar pemain merupakan salah satu fitur game agar pemain dapat berinteraksi dengan pemain lain.

Di sisi lain, terdapat celah pada kebijakan mengenai penghapusan akun pemain yang bermasalah. Penghapusan akun berhenti setelah akun yang bermasalah dihapus dari sistem, tanpa adanya konsekuensi lebih lanjut kepada pemainnya di dunia nyata. Pemain dapat dengan mudah membuat email aktif yang baru. Pembuatan email dapat dilakukan secara cepat dan email dapat dibuat secara massal dengan berbagai macam identitas tanpa adanya kebutuhan untuk verifikasi keaslian data pada saat itu juga. Pemain kemudian dapat membuat akun baru untuk mendaftar ke dalam sistem dan kembali memainkan game, sehingga menciptakan anonimitas, celah, dan waktu yang cukup untuk dapat disusupi dan disalahgunakan untuk tindakan-tindakan curang, di mana salah satunya adalah *cyber laundering*.

Penulis juga telah melakukan penelitian ke lembaga pemerintah yang berwenang yang sesuai dengan tema *cyber laundering*, yaitu Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). Dalam diskusi yang penulis lakukan bersama dengan perwakilan PPATK, penulis menemukan fakta bahwa PPATK telah menyadari adanya potensi ancaman metode pencucian uang baru melalui media elektronik dan digital. PPATK pun telah melakukan riset terhadap potensi pencucian uang melalui *online games*. PPATK menyatakan bahwa telah terjadi fenomena peralihan sarana pencucian uang dari media

konvensional menuju ke media *cyber*, terutama pada negara-negara maju yang mengandalkan teknologi digital untuk transaksi ekonominya.

Menurut PPATK, mereka telah melakukan langkah-langkah antisipasi dalam menghadapi peralihan metode pencucian uang tersebut. Hanya saja, untuk isu potensi ancaman *cyber laundering* melalui *online game* di Indonesia, meskipun mereka sudah menyadari dan mulai mempelajarinya, masih belum terdapat regulasi yang secara jelas mengatur mengenai transaksi di dalam game. Mereka mengatakan, dengan perumpamaan, apabila suatu ketika terjadi kasus *cyber laundering* melalui *online games*, mereka hanya dapat melihat dan tidak dapat menindak karena tidak adanya regulasi atau aturan hukum untuk menjerat pelaku *cyber laundering*.

Sebagai tambahan, PPATK memberitahu penulis adanya kemungkinan bahwa kesadaran pemerintah mengenai potensi ancaman ini akan datang sedikit terlambat ke Indonesia karena masih kurangnya kesadaran aparat penegak hukum pemerintah terhadap perkembangan teknologi. Begitu pula dari sisi pelaku kejahatan, menurut keterangan PPATK, sejauh ini mereka lebih sering mengurus kasus pencucian uang yang dilakukan secara tradisional. Akan tetapi, PPATK menganggap hal ini bukan berarti potensi ancaman *cyber laundering* melalui *online games* tidak ada. Potensi ini tetap ada, hanya saja untuk sementara ini masih tersembunyi karena kurangnya kesadaran teknologi aparat penegak hukum. Ditambah dengan faktor di mana *game* masih dianggap hal yang remeh dan sekedar menjadi alternatif hiburan, tentu saja akan menarik calon pelaku pencucian uang untuk menyamarkan uang mereka ke dalam pasar *online games*.

Terkait dengan potensi ancaman *cyber laundering* melalui *online games*, penulis menganggap bahwa potensi tersebut perlu disekuritisasi. Dalam proses sekuritisasi mengenai ancaman tersebut, maka diperlukan untuk mengidentifikasi komponen-komponen yang dibutuhkan dalam proses sekuritisasi. Komponen pertama adalah aktor. Aktor yang berusaha untuk mensekuritisasikan hal ini adalah pihak pemerintah dari negara *online games* tersebut berada, dan atau dibuat. Tidak hanya pemerintah, pengembang dan perusahaan dari *online games* tersebut juga sebenarnya termasuk ke dalam kategori aktor karena mereka juga memiliki kekuatan untuk melakukan langkah-langkah penciptaan keamanan di dalam *online games* tersebut. Namun, aktor sekuritisasi adalah pihak yang berusaha untuk melakukan sekuritisasi. (Buzan, Waever dan Wilde, 1998) Aktor pada proses sekuritisasi memiliki kekuatan untuk menyimpulkan tindakan yang diperlukan terhadap suatu masalah dan juga kekuatan politik untuk melakukan pengamanan (*securitizing*) terhadap suatu isu. Dalam pembahasan ini, maka aktor yang memiliki kemampuan untuk mensekuritisasikan potensi ancaman *cyber laundering* melalui *online games* adalah pihak pemerintah. Dari hasil penelitian penulis, pihak pemerintah sama sekali belum melakukan komponen kedua, yaitu *speech act* untuk menunjukkan bahwa terdapat potensi ancaman *cyber laundering* melalui *online games*. *Speech act* adalah usaha penyampaian mengenai suatu ancaman atau isu yang perlu untuk segera diamankan kepada komponen ketiga yaitu *audience*.

Audience pada kasus ini menurut penulis ada tiga pihak, yaitu dari pihak pemerintah itu sendiri untuk melakukan *speech act* kepada dirinya sendiri, terutama aparat penegak hukum dan pejabat yang terkait dengan bidang ekonomi dan teknologi karena mereka belum menyadari potensi ancaman yang ada, pihak perusahaan baik pengembang dan distributor dari *online games* yang ada, serta seluruh pemain dari *online games* tersebut. Ketiga pihak ini harus diyakinkan agar semua terlibat dalam proses sekuritisasi dan tidak meninggalkan celah yang kemudian memicu potensi ancaman yang lebih besar dari *cyber laundering* melalui *online games*. Namun, karena kurangnya kesadaran dari aktor dan tidak adanya regulasi, belum ada sama sekali upaya *speech act* dari para aktor kepada *audience*.

Dengan ketiadaan *speech act* ini, maka dapat disimpulkan bahwa aktor tidak menganggap atau tidak menyadari potensi ancaman *cyber laundering* melalui *online games* sebagai sebuah potensi ancaman yang akan mengancam aktor kelak. Ketidadaan *speech act* dan anggapan ini kemudian justru semakin memperkuat potensi dari ancaman *cyber laundering* melalui *online games*. Dengan tidak adanya *speech act*, maka proses sekuritisasi tidak dapat berjalan dan membuat potensi ancaman ini bebas. Pemerintah tidak menyadari potensi ancaman ini karena kurangnya pemahaman aparat mengenai perkembangan teknologi. Hanya beberapa lembaga yang menyadari mengenai potensi ini. Namun, mereka tidak dapat berbuat lebih jauh karena pemerintah sendiri tidak memiliki regulasi yang memberi lembaga-lembaga tersebut akses untuk menindak potensi ancaman *cyber laundering* ini. Ditambah dengan transaksi yang berada di bawah parameter pengawasan dan perusahaan game yang pasarnya terus berkembang, membuat nominal transaksi terkait dengan *online games* yang terus meningkat merupakan hal yang wajar sehingga sulit untuk diawasi.

Di dalam *speech act* disampaikan mengenai komponen keempat, *existential threat*, yaitu ancaman yang akan disekuritisasi, yang mengancam komponen kelima yaitu *referent object*, objek yang terancam. (Buzan, Waever dan Wilde, 1998) Ancaman yang perlu disekuritisasikan adalah ancaman mengenai *cyber laundering* melalui *online games* itu sendiri yang dapat terjadi sebagai akibat adanya celah di dalam pengawasan transaksi melalui *online games*. Celah yang berpotensi mengancam perekonomian negara baik nasional maupun internasional karena aliran dana yang beredar secara illegal dapat membuat sistem ekonomi negara tidak stabil karena merugi. Celah ini disebabkan oleh kurangnya kesadaran dari masing-masing pihak yang telah dijelaskan sebelumnya dan juga karena isu ini masih dianggap sebagai sesuatu yang tidak mengancam bagi pemerintah.

Aliran dana yang lolos berpotensi untuk dipergunakan kembali dalam pendanaan tindak kejahatan transnasional yang sama atau berbeda, yang kemudian juga akan berdampak pada keamanan negara itu sendiri, merongrong sektor swasta yang sah, mengganggu integritas pasar keuangan, hilangnya pendapatan negara dari sumber pembayaran pajak, hilangnya kendali pemerintah terhadap kebijakan ekonomi, dan menimbulkan biaya sosial yang tinggi. Hal ini juga dapat mengganggu hubungan antar negara dan rasa percaya antar negara terhadap kredibilitas keamanan dan sistem keamanan ekonomi antara satu negara dengan negara lain. Negara-negara akan berpikir bahwa negara yang menjadi tempat praktek *cyber laundering* merupakan negara yang pengawasan atau regulasi ekonominya tidak baik dan keamanan nasionalnya tidak stabil, yang akan mempengaruhi hubungan dan juga kerjasama ekonomi diantara mereka.

Kesimpulan

Berdasarkan hasil penelitian yang peneliti lakukan, terdapat potensi ancaman *cyber laundering* melalui *online games* di Indonesia. Potensi tersebut bersifat nyata, dilihat dari rendahnya tingkat kesadaran pihak-pihak yang terkait terhadap isu yang penulis angkat, ketidadaan regulasi yang mampu untuk menanggulangi potensi tersebut, dan lingkungan pemain yang masih mendukung untuk melakukan transaksi di luar pengawasan perusahaan pemilik *online games*, anonimitas yang tercipta sebagai akibat dari keterbatasan kebijakan perusahaan, memberikan celah yang dapat disusupi oleh upaya-upaya pencucian uang sehingga membuat *cyber laundering* melalui *online games* ini cukup besar meskipun masih bersifat laten.

Layanan-layanan yang disediakan dan penggunaan aset dari *online games* yang telah di jelaskan memberikan keleluasaan modus bagi para pelaku pencucian uang. Hal ini semakin diperkuat dengan hasil penelitian penulis. Pihak-pihak yang terlibat di dalam lingkaran transaksi *online games*, masih belum menyadari adanya potensi ancaman *cyber*

laundering melalui *online games*. Belum terdapat regulasi yang mengikat dan jelas dari pemerintah terkait isu ini. Jika dilihat melalui konsep-konsep sekuritisasi, aktor di Indonesia, yaitu pemerintah, masih belum menyadari potensi ancaman *cyber laundering* melalui *online games* ini. Dengan aktor yang tidak menyadari ancaman, maka upaya sekuritisasi tidak dapat dilakukan meskipun terdapat potensi ancamannya karena tidak ada *speech act* yang meyakinkan *audience*.

Jika disimpulkan, potensi ancaman *cyber laundering* melalui *online games* bersifat nyata di Indonesia, namun, belum atau bahkan tidak adanya pengetahuan baik dari sisi pemerintah, perusahaan, maupun pemain membuat seakan – akan ancaman tersebut bersifat tidak nyata. Pihak-pihak yang terkait tersebut tidak merasa terancam meskipun potensi ancaman tersebut berada dekat dengan mereka. Hal ini semakin memperkuat potensi ancaman tersebut dan tentu saja bukan merupakan keadaan yang bagus bagi keamanan ekonomi Indonesia karena adanya potensi ancaman yang bebas.

Referensi

- Basitt. t.thn. *Kotakgame.com*. Diakses April 06, 2017.
http://www.kotakgame.com/feature/detail_feature/244/0/12-Tahun-Perkembangan-Game-Online-di-Indonesia.
- Buzan, Barry, Ole Waever, dan Jaap de Wilde. 1998. *Security: a New Framework for Analysis*. Colorado: Lynne Rienner.
- Filipkowski, Wojciech. 2008. "Cyber Laundering : An Analysis of Typology and Tecniques." *International Journal of Criminal Justice Sciences*. 15-27.
- Keegan, Brian, Dmitri Williams, Muhammad Aurangzeb Ahmed, dan Jaideep Srivasta. 2010. "Dark Gold : Statistical Properties of Clandestine Networks in Massively Multiplayer Online Games." *IEEE*.
- Levi, Michael, dan Peter Reuter. 2006. *Money Laundering*. Chicago: The University of Chicago.
- Marchand, Andre, dan Thorsten Hennig Thureau. 2013. "Value Creation in the Video Game Industry: Industry Economics, Consumer Benefits, and Research Opportunities." *Elsevier*.
- Newzoo. 2014. "Global Games Market Will Reach \$102.9 Billion in 2017." *Newzoo*. 12 May. Diakses March 14, 2016. <https://newzoo.com/insights/articles/global-games-market-will-reach-102-9-billion-2017-2/>.
- Newzoo. 2015. "Global Report: US And China Take Half Of \$113 Bn Games Market in 2018." *Newzoo*. 18 May. Diakses March 14, 2016. <https://newzoo.com/insights/articles/us-and-china-take-half-of-113bn-games-market-in-2018/>.
- Oh, Gyuhan, dan Taiyong Ryu. 2007. "Game Design on Item-selling Based Payment Model in Korean Online Games."
- Richet, Jean-Loup. 2013. "Laundering Money Online: A Review of Cybercriminals' Methods." *Tools and Resources for Anti-Corruption Knowledge*.
- Solicitor General Canada. 1998. "Electronic Money Laundering: An Environmental Scan."
- Steinkuehler, Constance A., and Dmitri Williams. 2006. "Where Everybody Knows Your (Screen) Name : Online Games as "Third Places"." *Journal of Computer-Mediated Communication*.
- Strauss, Killian. 2013. "How Can We Effectively Combat the Use of the Internet for Money Laundering?"
- Trend Micro. 2016. 10 Oktober. Diakses Juni 8, 2017.
<https://documents.trendmicro.com/assets/wp/wp-cybercrime-online-gaming-currency.pdf>.

Tropina, Tatiana. 2014. "Fighting Money Laundering in the Age of Online Banking, Virtual Currencies, and Internet Gambling." *Springer*.

Versace, Christopher. 2014. "The Time Is Here For Online Gaming." *Forbes.com*. 26 Februari. Diakses December 25, 2015.

<http://www.forbes.com/sites/chrisversace/2014/02/26/the-time-is-here-for-online-gaming/>.