II3230-KEAMANAN INFORMASI

Etika dan Hukum Penggunaan TOR

Faras Banas Lubis -18217046

SEKOLAH TINGGI ELEKTRO DAN INFORMATIKA (STEI)

INSTITUT TEKNOLOGI BANDUNG (ITB)

2020

Daftar Isi

Daftar Gambar

Ringkasan

TOR (The Onion Router) adalah server anonim yang bekerja dengan cara mengalihkan lalu lintas internet ke jaringan *overlay* sukarelawan yang gratis dan mendunia yang terdiri dari tujuh ribu lebih *relays*. Server ini berguna untuk menyembunyikan identitas penggunanya dari analisis lalu lintas dan penyadapan jaringan melalui *routing* lapisan bawang . Tujuan utama TOR adalah perlindungan untuk privasi para penggunanya.

Sejak terbentuknya TOR, ada beberapa pro dan kontra dalam penggunaannya. TOR sering digunakan oleh para pelapor perusahaan dan pemerintahan ketika perusahaan atau pemerintahan itu melakukan hal yang tidak etis. TOR membantu penyamaran identitas pelapor tersebut. Sebaliknya TOR juga sering digunakan untuk melakukan aktivitas ilegal seperti perdagangan narkoba dan senjata, penipuan, pemalsuan identitas diri serta pornografi anak-anak. Dikarenakan aktivitas ilegal tersebut, banyak pemerintahan mengeluarkan legislasi terhadap TOR, memblokirnya serta melakukan serangan terhadap jaringannya. Inilah kesulitan yang dihadapi TOR dalam tugasnya sebagai server yang menjamin anonimitas pada pengguna.

Di makalah ini akan dibahas pengaruh hukum negara dan internasional beserta etika dlama penggunaan TOR. Di bagian pertama akan dijelaskan bagaimana TOR bekerja dan pada bagian kedua akan menjelaskan konsekuensi penggunaan TOR pada privasi, hukum, dan kejahatan.

BAB I
PENDAHULUAN

Pada 1990-an, kurangnya keamanan di internet dan kemampuannya untuk digunakan dalam pelacakan dan pengawasan menjadi jelas, dan pada 1995, David Goldschlag, Mike Reed, dan Paul Syverson di US *Naval Research Lab* (NRL) mulai meneliti apakah ada cara untuk membuat koneksi internet yang tidak mengungkapkan siapa yang berbicara kepada siapa, bahkan kepada seseorang yang memonitor jaringan. Jawaban mereka adalah untuk membuat dan menggunakan desain penelitian pertama dan prototipe *Onion Routing*.

Tujuan dari *Onion Routing* adalah untuk memiliki cara menggunakan internet dengan privasi sebanyak mungkin, dan idenya adalah untuk merutekan lalu lintas melalui beberapa server dan mengenkripsi setiap langkahnya. Ini masih merupakan penjelasan sederhana untuk bagaimana TOR bekerja hari ini.

Pada awal 2000-an, Roger Dingledine, lulusan *Massachusetts Institute of Technology* (MIT), mulai bekerja pada proyek perutean bawang NRL dengan Paul Syverson. Untuk membedakan karya asli ini di NRL dari upaya *onion routing* lainnya yang mulai muncul di tempat lain, Roger menyebut proyek TOR, yang merupakan singkatan dari The Onion Routing. Nick Mathewson, rekan Roger di MIT, bergabung dengan proyek tersebut.

Sejak awal 1990-an, *onion routing* dirancang untuk bergantung pada jaringan yang terdesentralisasi. Jaringan perlu dioperasikan oleh entitas dengan beragam minat dan asumsi kepercayaan, dan perangkat lunak harus bebas dan terbuka untuk memaksimalkan transparansi dan pemisahan. Itu sebabnya pada Oktober 2002 ketika jaringan TOR pertama kali dikerahkan, kodenya dirilis di bawah lisensi perangkat lunak bebas dan terbuka. Pada akhir 2003, jaringan itu memiliki sekitar selusin *volunteer node*, sebagian besar di AS, ditambah satu di Jerman.

Menyadari manfaat TOR terhadap hak digital, *Electronic Frontier Foundation* (EFF) mulai mendanai karya Roger dan Nick di Tor pada 2004. Pada 2006, TOR Project, Inc., sebuah organisasi nirlaba 501 (c) 3, didirikan untuk mempertahankan Pengembangan TOR.

Pada tahun 2007, organisasi mulai mengembangkan jembatan ke jaringan TOR untuk mengatasi penyensoran, seperti kebutuhan untuk melalui *firewall* pemerintah, agar para penggunanya dapat mengakses web yang terbuka.

TOR mulai mendapatkan popularitas di kalangan aktivis dan pengguna yang tertarik pada privasi; tetapi masih sulit bagi orang yang kurang paham secara teknis untuk menggunakan, jadi mulai tahun 2005, pengembangan alat-alat selain *proxy TOR* dimulai. Pengembangan TOR Browser dimulai pada 2008.

Dengan TOR Browser telah membuat TOR lebih mudah diakses oleh pengguna internet biasa dan aktivis, TOR adalah alat yang penting selama *Arab Spring* yang dimulai pada akhir 2010. Ini tidak hanya melindungi identitas orang secara *online* tetapi juga memungkinkan mereka untuk mengakses sumber daya kritis, media sosial, dan situs web. yang diblokir.

Perlunya alat perlindungan terhadap pengawasan massa menjadi perhatian utama berkat wahyu Snowden pada 2013. TOR tidak hanya berperan penting bagi pengungkap fakta Snowden, tetapi isi dokumen juga menguatkan jaminan bahwa, pada waktu itu, TOR tidak bisa dipecahkan.

Kesadaran orang akan pelacakan, pengawasan, dan sensor mungkin telah meningkat, tetapi demikian juga prevalensi dari hambatan-hambatan ini terhadap kebebasan internet. Saat ini, jaringan ini memiliki ribuan relai yang dijalankan oleh sukarelawan dan jutaan pengguna di seluruh dunia. Dan keanekaragaman inilah yang membuat pengguna TOR aman.

BAB II
CARA KERJA TOR
A. Definisi TOR

Proyek Tor adalah organisasi nirlaba yang melakukan penelitian dan pengembangan dalam privasi dan anonimitas *online*. Ini dirancang untuk menghentikan orang - termasuk lembaga pemerintah dan perusahaan - mempelajari lokasi Anda atau melacak kebiasaan penelusuran Anda.

Berdasarkan penelitian itu, ia menawarkan teknologi yang memantulkan lalu lintas pengguna internet dan situs web melalui "*relay*" yang dijalankan oleh ribuan relawan di seluruh dunia, sehingga sangat sulit bagi siapa pun untuk mengidentifikasi sumber informasi atau lokasi pengguna .

Paket perangkat lunaknya - bundel peramban Tor - dapat diunduh dan digunakan untuk memanfaatkan teknologi itu, dengan versi terpisah yang tersedia untuk ponsel cerdas Android.

Ada beberapa *trade-off* yang harus dibuat: misalnya, menjelajah menggunakan Tor lebih lambat karena *relay* tersebut, dan memblokir beberapa plugin browser seperti Flash dan QuickTime.

Meskipun pengembang Tor awalnya membuat perangkat lunak untuk keperluan militer, itu telah berkembang menjadi alat yang dapat berguna bagi semua - terutama bagi mereka yang memiliki sesuatu untuk disembunyikan atau sebaliknya akan mendapat manfaat dari anonimitas *online*. Banyak jurnalis dan aktivis politik menggunakan Tor untuk menghindari penuntutan. Biasanya, orang-orang ini tinggal di negara-negara di mana pihak berwenang mungkin menghukum mereka karena pemikiran dan pandangan yang ingin mereka bagikan secara *online*.

Teknologi asli di belakang Tor dikembangkan oleh Angkatan Laut AS dan telah menerima sekitar 60% dari pendanaannya dari Departemen Luar Negeri dan Departemen Pertahanan, meskipun para pendukungnya yang lain termasuk pelobi hak digital, Electronic Frontier Foundation, jurnalisme dan badan komunitas Knight Foundation dan Badan Kerjasama Pembangunan Internasional Swedia.

Ketika diluncurkan pada tahun 2002, penekanan proyek Tor adalah melindungi privasi pengguna internet dari perusahaan daripada pemerintah.

Tim proyek Tor mengatakan penggunanya terbagi dalam empat kelompok utama: orang normal yang ingin menjaga aktivitas internet mereka tetap pribadi dari situs web dan pengiklan; mereka yang peduli tentang *cyberspying*; dan pengguna menghindari sensor di bagian dunia tertentu.

Tor mencatat bahwa teknologinya juga digunakan oleh para profesional militer - angkatan laut AS masih merupakan pengguna utama - serta aktivis dan jurnalis di negara-negara dengan sensor ketat terhadap media dan internet. Badan kampanye Reporters Without Borders menyarankan wartawan untuk menggunakan Tor, misalnya.

Tor juga mengutip blogger, eksekutif bisnis, profesional TI dan petugas penegak hukum sebagai pengguna utama, dengan yang terakhir termasuk polisi perlu menutupi alamat IP mereka ketika bekerja secara online, atau menyelidiki "situs web dan layanan yang dipertanyakan".

Menurut Wall Street Journal, pada 2012 sekitar 14% dari lalu lintas Tor terhubung dari Amerika Serikat, dengan orang-orang di "negara yang menyensor internet" sebagai basis pengguna terbesar kedua. Tor semakin sering digunakan oleh para korban kekerasan dalam rumah tangga dan pekerja sosial serta agen-agen yang membantu mereka, walaupun pekerja perlindungan mungkin atau mungkin tidak memiliki pelatihan profesional tentang masalah keamanan siber. Namun, penyebaran yang tepat tidak menghalangi penguntit digital, yang meningkat karena prevalensi media digital dalam kehidupan *online* kontemporer. Bersama dengan SecureDrop, Tor digunakan oleh organisasi berita seperti The Guardian, The New Yorker, ProPublica, dan The Intercept untuk melindungi privasi pelapor.

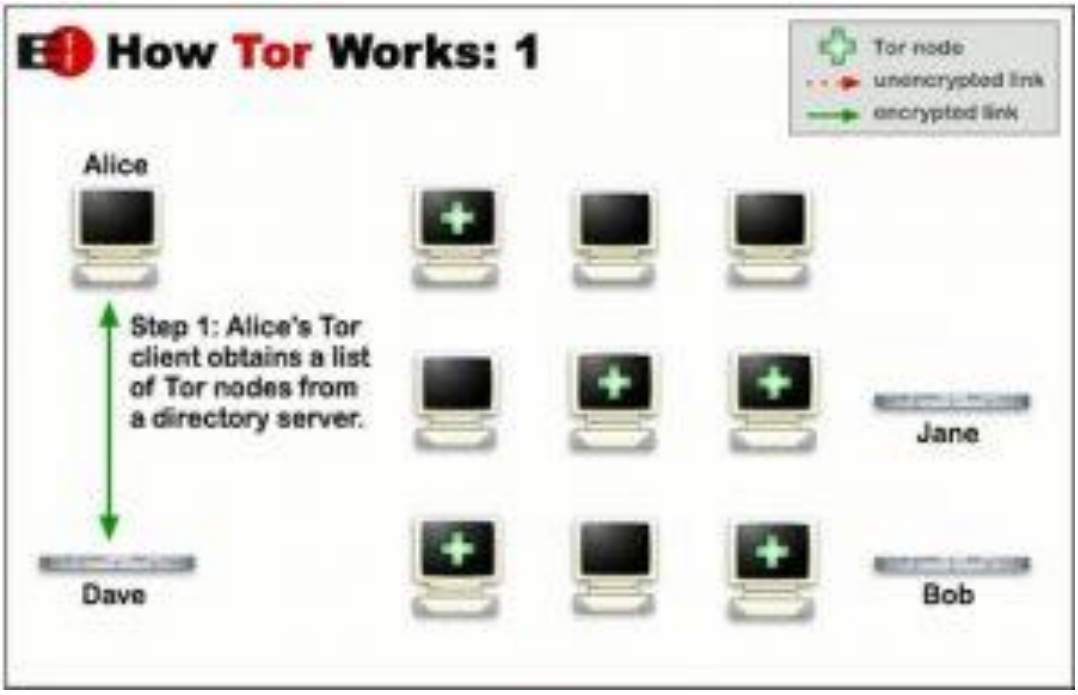
B. Fitur-Fitur TOR

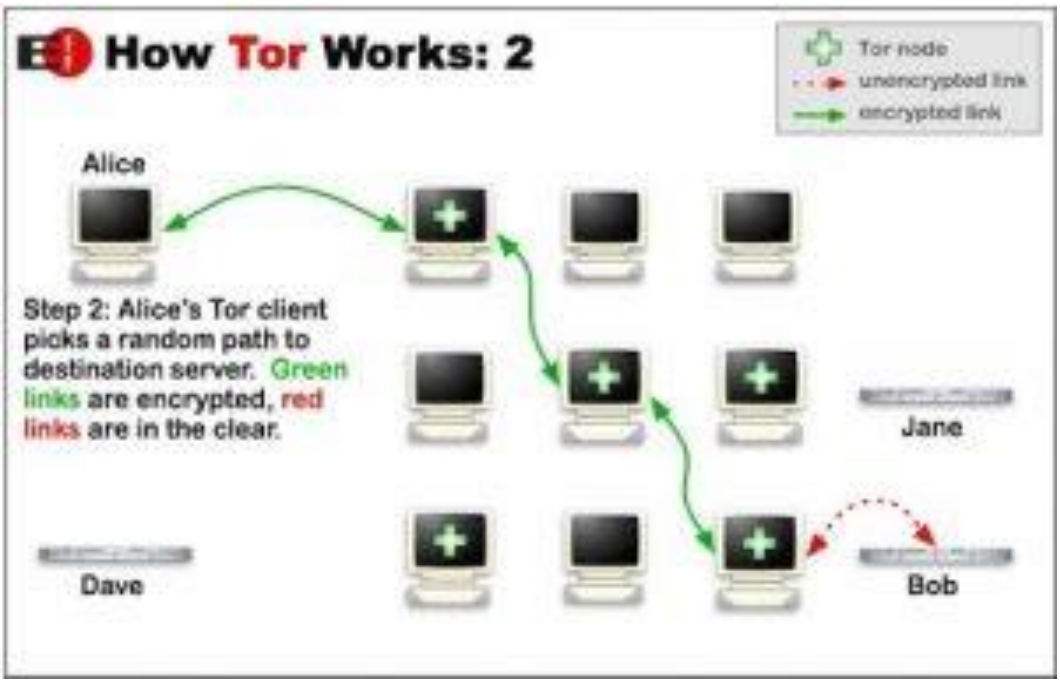
Fitur-fitur yang ada dalam TOR adalah sebagai berikut

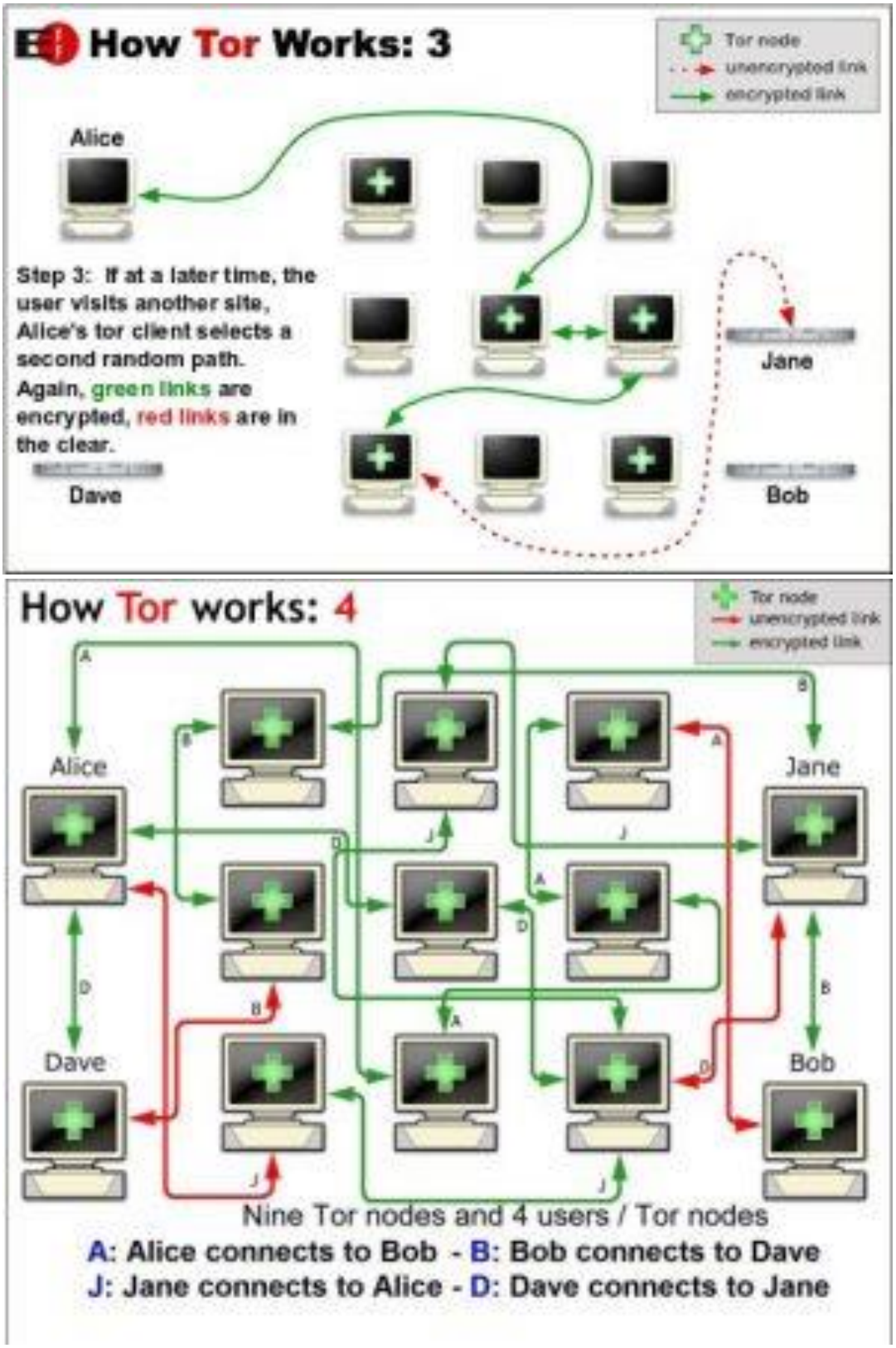
- Ketersediaan Cross-Platform. yaitu, aplikasi ini tersedia untuk Linux, Windows dan juga Mac.
- Enkripsi data yang kompleks sebelum dikirim melalui Internet.
- Dekripsi data otomatis di sisi klien.
- Ini adalah kombinasi dari Firefox Browser + Tor Project.
- Ini memberikan anonimitas ke server dan situs web.
- Itu memungkinkan untuk mengunjungi situs web yang dikunci.
- Melakukan tugas tanpa mengungkapkan IP Sumber.
- Mampu merutekan data ke / dari layanan dan aplikasi tersembunyi di balik *firewall*.

C. Cara Kerja TOR

Untuk memakai Tor, Anda harus mengunduh dan memasang Tor Browser yang akan Anda gunakan sebagai pengganti Chrome, Firefox atau peramban apa pun yang biasanya Anda pakai. Apa pun yang Anda kerjakan pada peramban ini akan terbebas dari mata-mata yang mengintai milik pemerintah, peretas, Iklan Google dan iklan lainnya. Data Anda dibundel ke dalam paket-paket enkripsi sebelum data memasuki jaringan Tor. Setelah itu, Tor mencomot bagian dari header paket yang mencakup informasi seperti sumber, ukuran, tujuan dan waktu, yang semuanya dapat dipakai untuk mengetahui hal-hal tentang pengirimnya. Berikutnya, Tor mengenkripsi sisa dari informasi yang bisa dikerjakan oleh koneksi internet biasa. Akhirnya, data terenkripsi dikirimkan secara acak melalui banyak server (disebut relai), masing-masingnya didekripsi dan kemudian mengenkripsi ulang data sekadar cukup untuk mengetahui dari mana asalnya dan ke mana tujuan berikutnya. Lapisan alamat terenkripsi dipakai untuk anonimitas paket data yang dikirimkan melalui jaringan Tor seperti *onion*, demikian juga yang lainnya


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

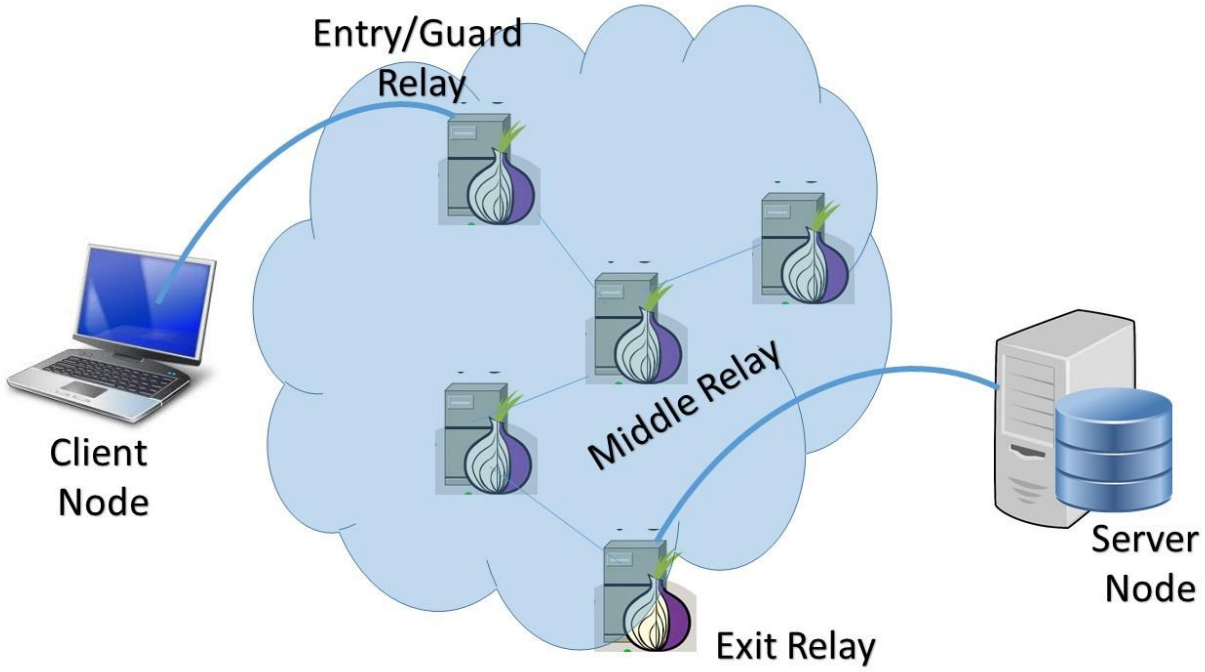


Gambar 1. Cara Kerja TOR [1]

a. Relay

Pada level yang sangat tinggi, Tor bekerja dengan memantulkan koneksi dari komputer Anda ke tujuan (seperti google.com) melalui serangkaian komputer perantara, atau *relay*.

Saat ini, ada sekitar 6000 *relay* perutean lalu lintas melalui jaringan Tor. *Relay* ini berlokasi di seluruh dunia dan dijalankan sepenuhnya oleh sukarelawan yang bersedia memberikan *bandwidth* untuk tujuan tersebut. Penting untuk dicatat bahwa sebagian besar *relay* tidak memiliki perangkat keras atau perangkat lunak khusus untuk dijalankan. Mereka hanya memiliki perangkat lunak Tor yang dikonfigurasi untuk bertindak sebagai *relay*.



Gambar 2. Relay TOR [2]

Secara umum, Tor memantulkan koneksi melalui 3 *relay*. Masing-masing memiliki peran khusus untuk dimainkan:

- **Entry / Guard Rela**y - Ini adalah titik masuk ke jaringan Tor. *Relay* dipilih untuk berfungsi sebagai penjaga relai setelah beberapa saat, serta telah terbukti stabil dan memiliki bandwidth tinggi.

- **Relay Tengah** - *Relay* tengah persis seperti itu - simpul tengah digunakan untuk mengangkut lalu lintas dari *relay* penjaga ke *relay* keluar. Ini mencegah penjaga dan *relay* keluar saling mengenal.

- **Exit Relay** - *Relay* ini adalah titik keluar di tepi jaringan Tor. *Relay* ini mengirimkan lalu lintas ke tujuan akhir yang dimaksudkan oleh klien.

Secara umum, aman untuk menjalankan penjaga atau relai tengah pada VPS atau server bersama (seperti DigitalOcean atau EC2), karena semua operator server akan melihat bahwa lalu lintas terenkripsi tidak berbahaya.

b.Bridge

Ketika klien Tor memulai, diperlukan cara untuk mengambil daftar semua entri, tengah, dan keluar *relay* yang tersedia. Daftar semua *relay* ini bukan rahasia. Meskipun membuat daftar ini bersifat publik diperlukan, ini juga menghadirkan masalah. Pemerintah atau ISP dapat:

- Blokir pengguna yang keluar dari Tor

- Blokir pengguna masuk ke Tor

Jembatan (*Bridge*) adalah solusi cerdas untuk masalah ini. Pada intinya, jembatan hanyalah entri masuk yang tidak diterbitkan. Pengguna yang berada di belakang jaringan yang disensor dapat menggunakan jembatan sebagai cara untuk mengakses jaringan Tor.

Jadi, jika jembatan tidak dipublikasikan, bagaimana pengguna tahu di mana mereka? Apakah daftar utama tidak perlu dipublikasikan di suatu tempat? Kami akan berbicara lebih banyak tentang daftar utama relai dan jembatan ini di pos berikutnya, tetapi untuk sekarang jawabannya adalah ya - ada daftar jembatan yang dikelola oleh proyek Tor.

Daftar ini tidak dipublikasikan.

Sebagai gantinya, proyek Tor telah menciptakan cara bagi pengguna untuk menerima sejumlah kecil jembatan sehingga mereka dapat terhubung ke seluruh jaringan Tor. Proyek ini, yang disebut BridgeDB memberi pengguna informasi tentang beberapa jembatan sekaligus. Ini masuk akal, karena hanya beberapa jembatan harus menjadi semua kebutuhan pengguna.

BAB III
ETIKA DAN HUKUM PENGGUNAAN TOR

Dari perspektif hukum, Tor adalah fenomena yang sangat menarik. Baik itu Tor atau jaringan lain, anonimitas akan menjadi bagian dari dunia maya selama Internet tetap 'global dan terbuka'. Namun, anonimitas dapat menjadi anugerah dan bencana, dan Tor juga menimbulkan banyak pertanyaan hukum. Akan dijelaskan beberapa masalah, yaitu kegiatan pemerintah sehubungan dengan Tor, aspek hak asasi manusia dari penggunaan Tor, tanggung jawab konten atas *exit node operators, and exit node monitoring.*.

A. TOR dan Pemerintah Negara

Penggunaan Tor telah mendapat reaksi beragam dari pemerintah. Hubungan antara Tor dan pemerintah sangat kompleks karena fakta bahwa Tor digunakan tidak hanya oleh warga negara yang mencari privasi, tetapi juga oleh entitas lain, mulai dari negara bagian hingga kelompok kejahatan terorganisir.[3] [4]

Adalah fakta yang terkenal bahwa organisasi nirlaba Proyek Tor didukung oleh beberapa entitas swasta dan publik serta oleh pemerintah. Faktanya, Tor pada awalnya dirancang, diimplementasikan, dan digunakan sebagai proyek perutean bawang generasi ketiga dari Laboratorium Penelitian Angkatan Laut. Awalnya dikembangkan dengan mempertimbangkan Angkatan Laut AS dengan tujuan utama melindungi komunikasi pemerintah, dan bahkan saat ini digunakan oleh berbagai entitas negara seperti militer dan penegak hukum. Bahkan hari ini ada saran bahwa pejabat pemerintah membantu mengembangkan jaringan dengan memberi tahu Tor tentang kemungkinan bug atau aspek lain di Tor yang perlu diperbaiki.

Dukungan pemerintah juga jelas dalam hal pendanaan Tor. Sponsor aktif pada 2013 termasuk Departemen Luar Negeri A.S. dan Departemen Pertahanan A.S., dengan penghargaan federal sebesar $ 1,8 juta. Sementara pada tahun 2012 bagian dari pendapatan yang berbasis Pemerintah AS berjumlah 60%, proyek Tor secara terbuka menyerukan kontribusi tambahan untuk mendiversifikasi sumber sponsor dan bersikeras tidak memiliki pintu belakang ke Tor.

Pada saat yang sama ada contoh negara yang secara terbuka menekan Tor. Misalnya, Cina telah melarang penggunaan Tor dan telah memblokir akses ke simpul masuk Tor, dan Arab Saudi dan Uni Emirat Arab sama-sama memblokir situs web Tor, seperti juga Irak.

Negara-negara lain melangkah lebih jauh dari itu. Meskipun tidak secara resmi dikonfirmasi, NSA telah dilaporkan telah melakukan upaya berulang untuk mengembangkan serangan terhadap individu yang menggunakan Tor. Pada 2013, disarankan bahwa sementara dokumen yang bocor mengkonfirmasi bahwa NSA memang mengoperasikan dan mengumpulkan lalu lintas dari beberapa *node* di jaringan Tor, tidak ada informasi lebih lanjut mengenai berapa banyak *node* yang sedang dikendalikan, dan apakah teknik de-anonimisasi yang diusulkan pernah diterapkan. Beberapa sumber mengklaim bahwa ‘NSA melacak pengguna yang diyakini tinggal di luar AS dan yang meminta informasi jembatan Tor melalui email atau yang mencari atau mengunduh Tor atau sistem operasi langsung TAILS '. Beberapa dokumen yang bocor berpendapat bahwa hal itu akan menjadi 'kontraproduktif' untuk 'menakuti' target yang menggunakan Tor dan menjauh dari Tor. Komentator lain percaya bahwa upaya AS untuk menargetkan atau merusak Tor akan meningkatkan kekhawatiran hukum bagi badan intelijen nasional, terutama mengenai apakah NSA telah bertindak, sengaja atau tidak, terhadap pengguna internet di AS ketika menyerang Tor ’.

Negara-negara lain juga telah mengusulkan langkah-langkah untuk menantang anonimitas yang dimungkinkan oleh Tor. Contohnya adalah Rusia yang, dengan tujuan 'untuk memastikan pertahanan dan keamanan negara', telah secara terbuka menawarkan hadiah $ 110.000 kepada siapa pun yang dapat memecahkan identitas pengguna jaringan Tor.

Dalam perkembangan baru-baru ini, EUROPOL mengumumkan pada tahun 2014 penghapusan 'lebih dari 410 layanan tersembunyi', angka-angka tersebut kemudian diperbaiki ke 27 situs web. Ada sedikit informasi bagaimana penegak hukum berhasil 'melanggar Tor' dan mengidentifikasi pengguna di balik layanan tersembunyi ini, selain itu metode itu tidak diungkapkan karena mereka 'sensitif' dan server yang berlokasi di negara asing diakses dan 'dicitrakan' . Proyek Tor berspekulasi bahwa jumlah pencopotan dan penyitaan *relay* Tor dapat berarti bahwa jaringan Tor diserang dengan tujuan untuk mengungkapkan lokasi layanan tersembunyi tersebut, seperti yang telah dicoba sebelumnya ketika sekelompok relai Tor 'aktif mencoba untuk memutus anonimitas pengguna dengan membuat perubahan pada *header* protokol Tor yang terkait dengan lalu lintas mereka melalui jaringan '. Sementara beberapa server yang dihilangkan jelas terkait dengan aktivitas ilegal seperti menjual obat-obatan, mereka diduga juga menyertakan beberapa yang bertindak sebagai infrastruktur untuk jaringan anonim Tor. Pertanyaan yang belum terjawab tentang bagaimana layanan ini ditempatkan diharapkan akan dijawab di pengadilan ketika menuntut para tersangka yang ditangkap. Tak perlu dikatakan, bukti yang diperoleh secara ilegal tidak dapat diterima di pengadilan.[5]

B. TOR dan Open-Source

Meskipun tidak mengangkat masalah hukum khusus terkait Tor, ada beberapa argumen menarik yang telah diajukan. Yang paling penting dari mereka terkait dengan Konvensi Eropa tentang Kejahatan Dunia Maya. Pasal 32 (a) Konvensi mengatur akses lintas batas ke data komputer yang tersimpan di mana ‘tersedia untuk umum (sumber terbuka) menyimpan data komputer, terlepas dari di mana data tersebut berada secara geografis '. Kecuali jika hukum domestik menyatakan sebaliknya, penegakan hukum dapat mengakses data yang sama yang umumnya dapat diakses oleh publik dan, jika diperlukan untuk tujuan ini, berlangganan atau mendaftar untuk layanan yang tersedia untuk publik. Menurut beberapa komentator, akses ke materi *open source* untuk keperluan investigasi kriminal telah menjadi praktik yang diterima secara umum. Karena Tor adalah layanan yang tersedia secara bebas untuk umum, ketentuan ini juga harus berlaku untuk kegiatan penegakan hukum yang melibatkan mempekerjakan Tor untuk mengumpulkan bukti.

Namun, ada pandangan minoritas yang berpendapat bahwa fakta belaka bahwa informasi tertentu tersedia untuk umum tidak menyiratkan tidak adanya batasan untuk memproses data tersebut. Pembatasan tersebut dapat berasal dari sarana dan volume data yang dikumpulkan. Bert-Jaap Koops menegaskan bahwa kekuatan investigasi saat ini yang berfokus pada investigasi ruang fisik mungkin perlu direvisi agar sesuai dengan kekhasan investigasi *open-source*, terutama yang menawarkan kemampuan pencarian skala besar otomatis yang luas seperti pengakuan entitas, konversi gambar-ke-teks dan terjemahan otomatis. Ini didasarkan pada asumsi bahwa investigasi *open-source* otomatis dapat memengaruhi hak privasi dan dengan demikian memerlukan pangkalan yang dikodifikasi secara hukum untuk memberi tahu warga tentang kemungkinan seperti itu. Jika alat pemrosesan data otomatis seperti itu digunakan melalui Tor atau menargetkan, misalnya, layanan tersembunyi Tor, regulasi hukum dari kemampuan pencarian skala besar semacam itu mungkin perlu dipertimbangkan oleh legislatif.[6]

C. TOR dan Data Pribadi

Seperti dapat dilihat dari bukti pencabutan layanan tersembunyi baru-baru ini, pengguna Tor tidak dapat diberikan anonimitas 100%, sehingga mengakibatkan kemungkinan situasi penegakan hukum yang memproses data pribadi yang tidak diperlukan untuk ruang lingkup asli penyelidikan. Mungkin juga Tor digunakan untuk mengakses data pribadi yang disimpan di, misalnya, beberapa layanan tersembunyi Tor. Inilah sebabnya mengapa penggunaan Tor oleh penegak hukum untuk investigasi kriminal mungkin memerlukan pemrosesan data pribadi, dan karenanya dapat dibatasi oleh undang-undang perlindungan data.

Kekhawatiran tentang kemungkinan pemrosesan data pribadi selama investigasi tentu tidak spesifik untuk Tor. Namun, reformasi perlindungan data Uni Eropa akan memiliki efek signifikan pada pekerjaan penegakan hukum, termasuk kemungkinan kegiatan investigasi yang dilakukan melalui Tor ketika data yang akan diproses adalah data pribadi. Ini berarti bahwa bahkan jika penegakan hukum menggunakan Tor untuk secara anonim mengakses situs web atau layanan tertentu, persyaratan dan solusi hukum yang berasal dari peraturan perlindungan data akan tetap berlaku.

Meskipun aspek prosedur pidana secara tradisional tidak tunduk pada peraturan UE yang terperinci, pendekatan UE berubah. Perjanjian Lisbon mengedepankan prinsip yang menurutnya perlindungan data berlaku untuk polisi dan kerja sama peradilan dalam masalah pidana. Proposal untuk mereformasi lanskap perlindungan data Uni Eropa (Peraturan Perlindungan Data Umum) dilengkapi dengan proposal untuk Arahan tentang perlindungan individu sehubungan dengan pemrosesan data pribadi oleh otoritas yang kompeten untuk tujuan pencegahan, penyelidikan, deteksi atau penuntutan pelanggaran pidana atau eksekusi hukuman pidana, dan pergerakan bebas data tersebut. Proposal ini bertujuan untuk menyelaraskan aturan yang berkaitan dengan pemrosesan data pribadi oleh otoritas yang kompeten seperti penegakan hukum, berlaku juga untuk pemrosesan dalam negeri. Proposal ini membahas tantangan yang diajukan oleh Kerangka Kerja Keputusan 2008/977 / JHA, yang mencirikan yang terakhir sebagai instrumen 'ruang lingkup terbatas dan berbagai kesenjangan lainnya, sering mengarah pada ketidakpastian hukum bagi individu dan otoritas penegak hukum, serta kesulitan praktis implementasi ' Setelah diadopsi, Arahan (sekarang draft) akan menjadi instrumen utama yang mengatur pemrosesan data pribadi oleh penegak hukum.

Reformasi ini sangat penting mengingat definisi luas 'data pribadi' di UE. Menurut Arahan Perlindungan Data 95/46 / EC, data pribadi dapat berupa informasi 'yang berkaitan dengan orang alami yang diidentifikasi atau dapat diidentifikasi', dan orang yang dapat diidentifikasi 'adalah orang yang dapat diidentifikasi, langsung atau tidak langsung, khususnya dengan merujuk pada nomor identifikasi atau satu faktor atau lebih yang spesifik untuk identitas fisik, fisiologis, mental, ekonomi, budaya atau sosialnya '. Sedangkan sampai sekarang, kegiatan penegakan hukum telah dikecualikan dari aturan perlindungan data Uni Eropa, penerapan Arahan yang diusulkan akan menimbulkan pertanyaan interpretatif mengenai jenis data tertentu yang perlu diproses, seperti alamat IP.

Ada juga masalah lain yang mungkin muncul selama implementasi Arahan yang diusulkan dan penggunaan Tor. Sementara masih dalam versi konsep, dan dengan demikian dapat berubah lebih lanjut, proposal menyatakan, antara lain, bahwa data pribadi harus 'dikumpulkan untuk tujuan yang ditentukan, eksplisit dan sah dan tidak diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut' (Pasal 4). (2)), dan 'disimpan dalam bentuk yang memungkinkan identifikasi subyek data tidak lebih dari yang diperlukan untuk keperluan di mana data pribadi

diproses' (Pasal 4 (e)). Proposal juga menyerukan perlunya 'pembedaan antara berbagai kategori subjek data' (Pasal 5) sehingga Negara-negara Anggota harus memastikan, sejauh mungkin, bahwa pengontrol membuat perbedaan yang jelas antara data pribadi dari berbagai kategori subyek data. Tidak ada indikasi bahwa penegak hukum akan dilarang menggunakan perangkat lunak anonim selama penyelidikan, tetapi pengumpulan data saat menggunakan Tor atau layanan tersembunyi harus diaktifkan mengikuti aturan-aturan ini dalam Petunjuk. Implementasi praktis dari aturan-aturan ini ketika mengumpulkan bukti melalui atau di dalam Tor dapat menjadi tantangan bagi penegakan hukum nasional. Misalnya, mungkin tidak selalu mungkin untuk menentukan secara penuh bagian mana dari data yang akan diproses yang memerlukan data pribadi (terutama dengan data yang lebih bersifat teknis seperti alamat IP), dan oleh karena itu apakah peraturan data pribadi berlaku untuk pemrosesan data tersebut, dan jika demikian, sampai sejauh mana. Tidak jelas apa yang memberikan ‘perbedaan yang jelas antara data pribadi dari berbagai kategori subjek data 'akan terlihat dalam praktik ketika diterapkan pada, misalnya, kumpulan data besar yang diterbitkan oleh layanan tersembunyi Tor.[7]

D. TOR dan HAM

Tor adalah salah satu alat paling terkenal untuk menyediakan anonimitas *online* dan dapat digunakan untuk tujuan legal dan ilegal. Dalam subbagian sebelumnya, kami mengeksplorasi kegiatan pemerintah yang mencoba untuk memerangi kejahatan yang dimungkinkan atau difasilitasi oleh penggunaan Tor. Dalam subbagian ini, kami beralih untuk memperkenalkan penggunaan hukum Tor: penggunaan Tor yang memungkinkan pengguna untuk melindungi dan menggunakan hak asasi mereka.[8]

a. Hak Mengekspresikan Diri

Hak atas kebebasan berekspresi diatur dalam Pasal 19 ayat 2 Kovenan Internasional tentang Hak Sipil dan Politik (ICCPR). Namun, beberapa pemerintah tidak menghormati hak ini, dan mereka mengatur sensor *online* yang tersebar luas. Tor adalah cara untuk memotong sensor tersebut dengan salah informasi *firewall* tentang sumber dan sifat lalu lintas tertentu. Tiongkok, misalnya, menghambat semua lalu lintas Internet melalui sistem yang dikontrol pemerintah dan menjadikannya inspeksi dan penyaringan menyeluruh. Di sini, meningkatkan infrastruktur Tor dengan memutakhirkan protokol kebingungan dan meningkatkan jumlah jembatan dengan transportasi *pluggable* memungkinkan pengguna Tor untuk melewati *'Great Firewall'*. Hak atas kebebasan berekspresi terbatas.

Dalam praktiknya, alasan yang diterima secara umum mencakup, tetapi tidak terbatas pada, pencemaran nama baik, ucapan kebencian, pornografi ilegal, pelanggaran hak cipta, atau membantu atau bersekongkol dengan kejahatan. Sejauh negara-negara tertentu terlibat dalam sensor *online* yang berlebihan, mereka menafsirkan pembatasan ini terlalu luas oleh standar internasional. Melarang atau menindas Tor tanpa pandang bulu berarti campur tangan dengan hak atas kebebasan berekspresi yang sulit untuk membayangkan pembenaran yang tepat.

b. Hak untuk Privasi

Bahkan negara-negara yang dianggap menjunjung tinggi kebebasan berekspresi telah terlibat dalam kegiatan yang sangat mengganggu privasi orang. Ada beberapa contoh terbaru tentang dugaan kegiatan pengawasan yang dilakukan oleh entitas Negara yang berbeda. Misalnya, pada Oktober 2013, setelah Kanselir Jerman 'dengan marah mengutuk perilaku "tidak dapat diterima" Amerika setelah "kecurigaan tegas" muncul bahwa badan-badan intelijen Amerika Serikat telah memantau telepon seluler pribadinya selama hampir empat tahun, muncul pertanyaan tentang penerimaan di mana-mana. pengawasan digital. Pada saat yang sama, Der Spiegel melaporkan pada Agustus 2014 bahwa collection agen pengumpulan intelijen asing Jerman memata-matai Turki. Laporan itu juga melaporkan, berdasarkan sumber-sumber anonim, bahwa panggilan yang dilakukan oleh Sekretaris Negara John Kerry dan mantan Menteri Luar Negeri Hillary Clinton secara tidak sengaja direkam. 'Gangguan yang melanggar hukum dengan privasi juga telah digarisbawahi oleh Komisaris Tinggi PBB untuk Hak Asasi Manusia yang dicatat dalam laporannya tanggal 30 Juni 2014 bahwa praktik di banyak negara telah [...] mengungkapkan kurangnya legislasi dan / atau penegakan hukum nasional yang memadai, pengamanan prosedural yang lemah, dan pengawasan yang tidak efektif, yang semuanya berkontribusi pada kurangnya pertanggungjawaban atas campur tangan yang sewenang-wenang atau melanggar hukum dalam hak privasi. 'Dalam lingkungan seperti itu, adalah wajar bahwa baik individu maupun entitas publik akan lebih memperhatikan perlindungan privasi mereka, bahkan jika mereka merasa bahwa kebebasan berekspresi mereka tidak terancam.

Namun, meskipun ICCPR tidak mengandung batasan eksplisit tentang hak privasi, jelas bahwa hak ini bukan tanpa batas. Konvensi Eropa tentang Hak Asasi Manusia, yang mendefinisikan hak dengan kata-kata yang sama, memberikan daftar pengecualian. Misalnya, langkah-langkah tertentu selama investigasi kriminal dapat secara hukum mengganggu hak privasi. Namun demikian, dugaan keberadaan pengawasan massal di mana-mana menimbulkan kekhawatiran tentang proporsionalitas antara hasil pengawasan tersebut dan gangguan terhadap privasi orang.

E. TOR dan Kriminal

Sebuah studi Desember 2014 oleh Gareth Owen dari University of Portsmouth menemukan bahwa jenis konten yang paling umum di-*hosting* di Tor adalah pornografi anak, diikuti oleh pasar gelap, sementara masing-masing situs dengan lalu lintas tertinggi didedikasikan untuk operasi *botnet* . Banyak situs *whistleblowing* tetap hadir] serta forum diskusi politik. Situs yang terkait dengan Bitcoin, layanan terkait penipuan, dan layanan pemesanan melalui surat adalah beberapa yang paling produktif.

Pada Juli 2017, Roger Dingledine, salah satu dari tiga pendiri Proyek Tor, mengatakan bahwa Facebook adalah layanan tersembunyi terbesar. *The Dark Web* hanya terdiri dari 3% dari lalu lintas di jaringan Tor.

Sebuah studi Februari 2016 dari para peneliti di King's College London memberikan rincian konten berikut ini dengan serangkaian kategori alternatif, menyoroti penggunaan ilegal layanan *onion*.[9]

a. Pasar Darknet

Pasar *darknet* komersial, yang memediasi transaksi untuk obat-obatan terlarang dan barang-barang lainnya, menarik liputan media yang signifikan, dimulai dengan popularitas Silk Road dan Diabolus Market dan penyitaan selanjutnya oleh otoritas hukum. Pasar lain menjual eksploitasi perangkat lunak dan senjata. Pemeriksaan perbedaan harga di pasar web Gelap versus harga di kehidupan nyata atau di World Wide Web telah dicoba serta studi dalam kualitas barang yang diterima melalui web Gelap. Salah satu penelitian tersebut dilakukan di Evolution, salah satu pasar *crypto* paling populer yang aktif dari Januari 2013 hingga Maret 2015. Meskipun menemukan informasi digital, seperti metode penyembunyian dan negara pengiriman, "tampaknya akurat", penelitian ini menemukan masalah dengan kualitas obat-obatan terlarang yang dijual di Evolution, yang menyatakan bahwa, "... kemurnian obat-obatan terlarang ditemukan berbeda dari informasi yang tertera pada daftar masing-masing." Kurang diketahui tentang motivasi konsumen untuk mengakses pasar-pasar ini dan faktor-faktor yang terkait dengan penggunaannya.

b.Peretasan

Banyak peretas menjual layanan mereka baik secara individu atau sebagai bagian dari grup. Kelompok-kelompok tersebut termasuk xDedic, hackforum, Trojanforge, Mazafaka, dark0de dan pasar *darknet* TheRealDeal. Beberapa telah diketahui melacak dan memeras pedofil. Kejahatan dunia maya dan layanan peretasan untuk lembaga keuangan dan bank juga telah ditawarkan melalui web Gelap. Upaya untuk memantau kegiatan ini telah dilakukan melalui berbagai organisasi pemerintah dan swasta, dan pemeriksaan alat yang digunakan dapat ditemukan dalam jurnal Procedia Computer Science. Penggunaan serangan Penyangkalan Layanan Terdistribusi DNS (DRDoS) skala Internet juga dilakukan dengan memanfaatkan Web Gelap. Ada banyak situs penipuan. Juga hadir yang akhirnya memberikan alat untuk mengunduh yang terinfeksi kuda trojan atau backdoors.

c.Terorisme

Setidaknya ada beberapa situs web nyata dan penipuan yang mengklaim digunakan oleh ISIL (ISIS), termasuk situs palsu yang disita dalam *Operation Onymous*. Dengan meningkatnya teknologi, itu memungkinkan teroris cyber untuk berkembang dengan menyerang kelemahan teknologi. Segera setelah serangan Paris pada November 2015, sebuah situs yang sebenarnya diretas oleh kelompok peretas yang berafiliasi Anonim, GhostSec, dan diganti dengan iklan Prozac. Kelompok Islam Rawti Shax ditemukan beroperasi di web gelap pada satu waktu.

d.Penipuan

Ada banyak forum carding, situs web perdagangan PayPal dan Bitcoin serta layanan penipuan dan pemalsuan. Banyak situs semacam itu adalah penipuan itu sendiri.[10]

Penutup

Di makalah ini dibahas bagian hukum yang menyajikan tantangan hukum terpilih terkait dengan penggunaan Tor. Kami pertama kali membahas hubungan antara pemerintah dan Tor, dan fokus pada penggunaan Tor oleh penegak hukum. Kami mengidentifikasi sejumlah masalah hukum yang harus dianalisis lebih lanjut, seperti penggunaan Tor untuk mengumpulkan bukti. Misalnya, intelijen sumber terbuka sumber daya Tor dianggap tidak kontroversial, tetapi ini dapat berubah seiring dengan kemajuan kemampuan teknis.

Kami kemudian beralih untuk membahas hak asasi manusia dan Tor. Kami menegaskan kembali bahwa anonimitas adalah bagian integral dari hak asasi manusia yang sudah mapan, dan oleh karena itu pelarangan total Tor atau pengawasannya yang tidak pandang bulu akan merupakan gangguan yang tidak semestinya terhadap hak-hak ini. Untuk alasan yang sama, intersepsi hukum apa pun yang melibatkan jaringan Tor tunduk pada persyaratan yang sama dengan intersepsi lalu lintas Internet lainnya.

Referensi

[1] P. Winter, “Securing web browsing: protecting the Tor network,” *The Conversation*, May, 2016. Retrieved from: https://theconversation.com/securing-web-browsing-protecting-the-tor-network-56840

[2] P. Paganini, “MIT researchers identify Tor hidden services with 88 percent accuracy,” *Massachusets Institute of Technology*, August, 2015. Retrieved from: https://securityaffairs.co/wordpress/39022/hacking/tor-hidden-services-hacking.html

[3] K. Hadjimatheou, “Ethical and Legal Issues with LEA operations on the Dark Web,” *University of Warwick*, November, 2017.

[4] E. H. Fiallo, "The lack of ethics in cyber space: a case for cyber ethics," *Proceedings. Eleventh International Conference on Computer Communications and Networks*, 2002, pp. 310-.

[5] M. Chertoff and T. Simon, “The Impact of the Dark Web on Internet Governance and Cyber Security”, *Centre for International Governance Innovation and the Royal Institute for International Affairs*, no. 6 — February, 2015.

[6] M. Chertoff (2017) “A public policy perspective of the Dark Web”, *Routledge Taylor & Francis Group*, 2017. Pp. 26-38

[7] A. T. Zulkarnine, R. Frank, B. Monk, J. Mitchell and G. Davies, "Surfacing collaborated networks in dark web to find illicit and criminal content," *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, 2016, pp. 109-114.

[8] E.Jardine, “The Dark Web Dilemma: Tor, Anonymity and Online Policing”. *Global Commission on Internet Governance Paper Series.* 2015, 24. 10.2139/ssrn.2667711.

[9] M. Schäfer, M. Fuchs, M. Strohmeier, M. Engel, M. Liechti and V. Lenders, "BlackWidow: Monitoring the Dark Web for Cyber Security Information," *2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2019, pp. 1-21.

[10] R. Upadhyaya and A. Jain, "Cyber ethics and cyber crime: A deep delved study into legality, ransomware, underground web and bitcoin wallet," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, 2016, pp. 143-148.