CfDS
CENTER FOR DIGITAL SOCIETY

WSIS PRIZES 2015 CHAMPION

CASE STUDY SERIES #21

MENGENAL LEBIH JAUH DARK WEB

Penulis
M. Diaz Praditya
Editor
Dirgayuza Setiawan, M.Sc
Viyasa Rahyaputra
Nabeel Khawarizmy Muna
Desain dan Tata Letak
Fadlilah Zahra Murti

Ringkasan

Tren peningkatan pengawasan pemerintah dan swasta telah menimbulkan kekhawatiran bagi sebagian pengguna Internet mengenai pengalaman privasi daring mereka. Keinginan untuk memiliki pengalaman internet yang lebih pribadi telah menyebabkan munculnya *Dark Web*, bagian Internet yang lebih rahasia yang membutuhkan cara khusus untuk mengaksesnya dan lebih efektif melindungi identitas pengguna. Tetapi, kualitas ini telah disalahgunakan oleh pelaku kriminal untuk melakukan kegiatan terlarang di Internet. Kajian ini memeriksa kasus-kasus mengenai dua industri kriminal yang paling subur di dark web, yaitu pasar gelap (kasus *Silk Road* dan *AlphaBay*) dan pornografi anak-anak (kasus Playpen). Kajian ini juga akan mangkaji pihak-pihak seperti pemerintah, penegak hukum dan masyarakat umum dalam menanggapi fenomena *Dark Web*. Dari kasus ini, kajian ini bertujuan untuk mendalami pemahaman umum tentang sifat *Dark Web* serta bagaimana hal tersebut mencerminkan sikap mengenai privasi di Internet.

Pendahuluan dan Metodologi

Pada zaman ini, sangat sedikit dari kita masih awam dengan gagasan bahwa keamanan itu mahal. Dalam dunia pasca 9/11 penyadapan, kegiatan spionase, dan *Patriot Act*, sebagian besar dari kita telah akrab dengan gagasan keamanan yang saat ini berisiko mengurangi kebebasan rakyat sipil. Terlepas dari itu, pertanyaan masih tersisa – apakah demi memiliki keamanan layak mengorbankan kebebasan pribadi? Libertarian akan berpendapat bahwa peningkatan pengawasan pemerintah demi keamanan sama dengan menganiaya warga sipil yang tidak bersalah atas kejahatan yang mungkin mereka lakukan atau tidak dilakukan di masa depan. Di sisi lain, lainnya berpendapat bahwa kebebasan individu adalah harga yang kecil untuk memperoleh kehidupan yang lebih aman; bahwa pada akhirnya, lebih baik mementingkan keamanan daripada kenyamanan.

Meningkatnya peran Internet dalam masyarakat kita hanya memperburuk pertanyaan-pertanyaan ini. Bagaimana pemerintah dengan benar dapat menegakkan hukum dan mengatur penggunaan Internet tanpa melanggar hak-hak pengguna; secara khusus, hak untuk bebas berbagi informasi dan hak privasi? Hak privasi, misalnya, dijamin dalam dalam Universal Deklarasi Hak Asasi Manusia Pasal 12 serta Pasal 8 Konvensi Eropa tentang Hak Asasi Manusia. Di Indonesia, hak kebebasan dijamin oleh keputusan Mahkamah Konstitusi dalam Putusan No. 5/PUU-VII/2010, sesuai dengan UUD 1945 Pasal 28G yang menyatakan bahwa,

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."[2]

Ada batas yang sulit dilihat, batas yang memutuskan apakah pengguna internet adalah anggota komunitas daring yang memiliki aturan dan kode etik untuk ditaati, atau pengguna produk dengan hak untuk memutuskan bagaimana menggunakan produk tersebut menurut kebijakan mereka sendiri. Sementara perdebatan memanas, pemerintah diseluruh dunia telah menerapkan kabijakan pengawasan mereka sendiri sehubungan dengan internet. Program paling terkenal, mungkin, adalah PRISM yang dilakukan oleh NSA dalam mengekstrak data konsumen dari sembilan perusahaan internet ternama, termasuk Microsoft, Yahoo, Google, Facebook, Palta, Aod, Skype, Youtube,and Apple.[3]

Namun, apakah kebijakan pengawasan membuat Internet lebih aman? Sebagian besar dari kita setidaknya pernah mendengar *Dark Web*. Sebagian bahkan mungkin pernah mengaksesnya. Akhir-akhir ini, *Dark Web* telah dimonologikan tentang cerita-cerita menakutkan yang terjadi di dalamnya. Kajian ini berpendapat bahwa keberadaan *Dark Web* terkait erat dengan meningkatnya keterkaitan internet dan keinginan dalam memiliki privasi yang lebih tinggi sebagai reaksi terhadapnya. Kemudian, hal ini menggaris bawahi beberapa kasus aktivitas kriminal, contoh, tanggapan pemerintah dan kebijakan penegak hukum terhadap kegiatan ini, dan juga keberhasilan dan kegagalan mereka. Bagaimana kedua lembaga yang sejauh ini telah beradaptasi dengan keberadaan *Dark Web* akan digunakan sebagai referensi dalam memproyeksikan bagaimana *Dark Web* telah mengubah internet dan persepsi kita tentangnya serta apakah keberadaan *Dark Web* akan dibenarkan.

Apa Itu Dark Web?

Pertama, harus dibedakan antara Dark Web dan kata yang lebih sering diguakan *"Deep Web"*. Deep Web didefinisikan sebagai konten web yang tidak dapat ditemukan di mesin pencarian.[4] Definisi ini awalnya akan terlihat misterius dan seram. Ada sejumlah hal yang biasa menjadi alasan mengapa halaman web tidak dapat diakses melalui mesin

pencari. Jurnal akademis yang disembunyikan oleh paywall, dokumen perusahaan yang memerlukan proses masuk untuk mengakses, atau bahkan halaman pengaturan profil sosial media Anda - dengan definisi ini – merupakan contoh isi deep web.

Konten yang kebanyakan orang sebut sebagai *Deep Web* sebenarnya adalah *Dark Web*. *Dark Web* adalah bagian dari *Deep Web*, tetapi *Dark Web* sering berisi konten yang sengaja disembunyikan dari akses publik, biasanya karena sifatnya yang ilegal.[5] Konten ini tersembunyi di balik lapisan server proxy dan membutuhkan metode khusus, perangkat lunak, konfigurasi atau izin untuk mengakses. Salah satu perangkat lunak pengakses tersebut adalah Tor peramban, yang saat ini merupakan salah satu cara paling populer untuk mengakses Dark Web.

Browser, atau lebih tepatnya jaringan Tor yang digunakan untuk mengakses Internet, diluncurkan oleh Tor Project pada tahun 2002 sebagai cara bagi pengguna internet untuk daring secara anonim. Jaringan ini bekerja dengan memantulkan lalulintas pengguna internet dan situs web melalui "relays" yang dijalankan oleh ribuan sukarelawan di seluruh dunia. Ini membuatnya sangat sulit untuk melacak lokasi asli pengguna dan penerima informasi yang dikirim. Jaringan ini terdiri dari sekitar 6.000 relay yang ditempatkan di server pada 89 negara di seluruh dunia.[6] Jaringan anonim seperti Tor semakin populer; perkiraan penempatan jaringan Tor berbasis harian bisa sampai antara 2,5 hingga empat juta.[7]

Rasionalitas di Balik Dark Web

Manusia menginginkan privasi untuk berbagai alasan. James Rachels, misalnya, berpendapat bahwa hal itu merupakan sifat manusia akan merasa takut jika informasi tentang diri kita tersebar tanpa persetujuan kita. Privasi adalah intrinsik bagi interaksi manusia, dan kita menjalin hubungan dengan orang lain

dengan cara melepas atau menahan informasi yang kita anggap perlu. Secara detail, dia mengatakan bahwa,

> "Jika kita tidak dapat mengontrol siapa yang memiliki akses terhadap kita, kadang-kadang termasuk dan terkadang mengecualikan berbagai orang, maka kita tidak dapat mengontrol pola perilaku yang perlu kita adopsi (ini adalah satu alasan mengapa privasi merupakan aspek kebebasan) atau jenis hubungan dengan orang lain yang akan kita jalin."[8]

Bagi kebanyakan orang, menjelajah Internet adalah pengalaman pribadi. Memang, bagi banyak orang, history pencarian data di Internet mereka adalah sebagian dari harta rahasia mereka yang paling krusial. Data ini dapat digunakan untuk mengumpulkan sebagian besar dari identitas seseorang; hobi mereka, situasi keuangan mereka, tempat keluar yang mereka sukai, relasi, bahkan preferensi seksual mereka. Informasi ini dapat sangat memengaruhi pandangan orang lain terhadap kita, dan dalam kasus history Internet, data terus-menerus dicatat dan dihitung oleh pemerintah, pengiklan, dan penyedia layanan internet tanpa persetujuan aktif kita. Mereka yang merasa bahwa jejak digital mereka tidak memiliki apa pun untuk disembunyikan akan merasa sedikit khawatir, tetapi apakah begitu mengejutkan bahwa orang lain lebih suka menyembunyikannya?

Jadi dalam kasus *Dark Web*, apa yang dilakukan penggunanya dengan privasi mereka? Satu hal yang harus ditekankan adalah bahwa tidak semua konten Dark Web yang terdapat dalam Jaringan Tor tidak dapat diterima. Banyak situs yang tampaknya tidak berbahaya, meskipun agak anti-mainstream. Contohnya termasuk klub buku sederhana dan forum yang mendukung literatur kontroversial, seperti "*Jotunbane's Reading Club"* atau "*Imperial Library of Trantor."* Lainnya, seperti *Sci-Hub,* menyediakan platform publikasi untuk makalah penelitian dan jurnal yang tidak didanai. Dr. Ian Walden, seorang Profesor Hukum Informasi dan Komunikasi di Universitas Queen Mary London, berkomentar bahwa, "Rasa kebersamaan sering kali yang mengikat subkultur ini, dalam dunia digital yang semakin berbeda dan tanpa tubuh."[9] Ironisnya, memakai topeng figuratif mendorong pengguna untuk mengekspresikan diri mereka dengan cara yang lebih terbuka dan jujur, tanpa harus khawatir tentang citra atau jejak kaki digital mereka .

Namun, cerita horor memang memiliki kebenaran pada kenyataannya. Anonimitas yang disediakan di *Dark Web* tampaknya mendorong banyak individu dengan selera yang buruk atau tidak menyenangkan. *The Dark Web* adalah platform komunikasi yang populer bagi para ahli teori konspirasi, pembangkang politik, dan hobi yang legalitasnya diragukan seperti pengambilan kunci dan penghancuran. Lebih gelap

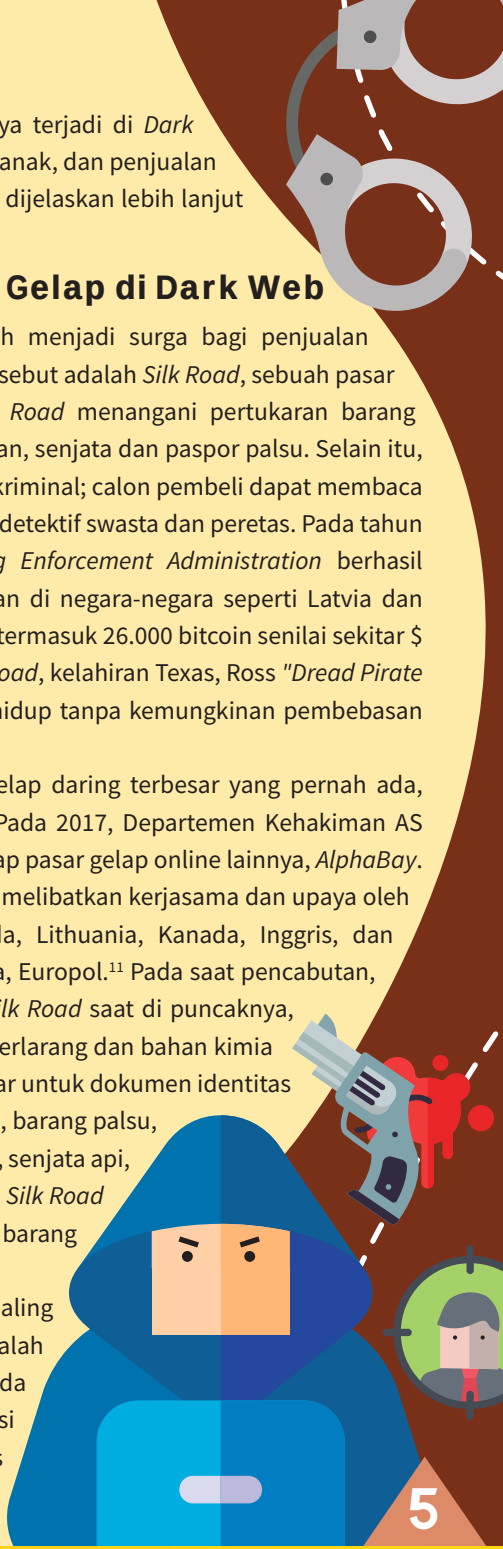
lagi adalah tindakan kriminal yang sebenarnya terjadi di *Dark Web*, seperti perdagangan narkoba, pornografi anak, dan penjualan layanan kriminal - beberapa contoh yang akan dijelaskan lebih lanjut di bagian bawah.

Contoh Kasus dari Aktivitas Gelap di Dark Web

Internet, khususnya *Dark Web*, telah menjadi surga bagi penjualan barang dan jasa ilegal. Salah satu situs web tersebut adalah *Silk Road*, sebuah pasar gelap online yang didirikan pada 2011. *Silk Road* menangani pertukaran barang termasuk tetapi tidak terbatas pada obat-obatan, senjata dan paspor palsu. Selain itu, situs ini juga memfasilitasi penjualan layanan kriminal; calon pembeli dapat membaca dengan teliti layanan dari pembunuh bayaran, detektif swasta dan peretas. Pada tahun 2014, operasi gabungan oleh FBI dan *Drug Enforcement Administration* berhasil menyusup ke server situs yang disembunyikan di negara-negara seperti Latvia dan Rumania, menutup situs dan menyita asetnya termasuk 26.000 bitcoin senilai sekitar $ 4 juta.[10] Pendiri dan administrator utama *Silk Road*, kelahiran Texas, Ross *"Dread Pirate Roberts"* Ulbricht, dijatuhi hukuman seumur hidup tanpa kemungkinan pembebasan bersyarat.

Silk Road adalah salah satu pasar gelap daring terbesar yang pernah ada, tetapi ini bukan yang terakhir dari jenisnya. Pada 2017, Departemen Kehakiman AS berhasil menyelesaikan operasi serupa terhadap pasar gelap online lainnya, *AlphaBay*. Operasi itu dipimpin oleh Amerika Serikat dan melibatkan kerjasama dan upaya oleh badan penegak hukum di Thailand, Belanda, Lithuania, Kanada, Inggris, dan Perancis, serta lembaga penegak hukum Eropa, Europol.[11] Pada saat pencabutan, pasar *AlphaBay* berkali-kali lebih besar dari *Silk Road* saat di puncaknya, dengan lebih dari 250.000 daftar obat-obatan terlarang dan bahan kimia beracun. Selain itu, ada lebih dari 100.000 daftar untuk dokumen identitas dan perangkat akses yang dicuri dan penipuan, barang palsu, malware, dan alat peretasan komputer lainnya, senjata api, dan layanan penipuan. Sebagai perbandingan, *Silk Road* tercatat sebagai hosting sekitar 14.000 daftar barang dan jasa ilegal pada saat itu diturunkan.

Mungkin contoh konten yang paling mengerikan yang tersedia di *Dark Web* adalah pornografi ilegal, terutama pornografi anak. Pada bulan Januari 2016, FBI mengatur operasi peretasan besar-besaran terhadap situs

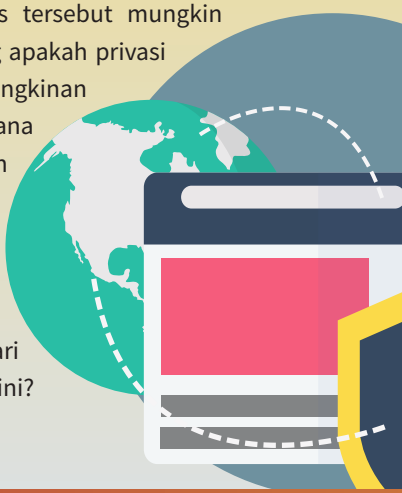


berbagi pornografi anak-anak di **Dark Web** yang dikenal sebagai *"Playpen"*. Pada puncaknya, situs ini menampung hampir 215.000 pengguna, dengan 11.000 pengunjung setiap hari.[12] Pada Februari 2015, FBI menyita server yang memfasilitasi situs tersebut di Lenoir, Carolina Selatan, tetapi alih-alih langsung membongkarnya, mereka mempertahankannya selama 13 hari untuk digunakan sebagai semacam "umpan" untuk menarik konsumen dan distributor pornografi anak. Kemudian, dengan menggunakan kode eksploitasi yang ada di browser Tor, mereka berhasil melacak alamat IP individu yang mengunjungi situs menggunakan browser. Sekitar 1.000 alamat IP berasal dari dalam Amerika Serikat; yang lain datang dari banyak negara lain termasuk Australia, Austria, Chili, Kolombia, Denmark, dan Yunani. Secara keseluruhan, mereka berhasil memperoleh hingga 8.000 alamat IP dari 120 negara.[13] Berdasarkan data ini, operasi tersebut adalah kampanye peretasan penegakan hukum terbesar hingga saat ini.

Situs tersebut adalah salah satu situs pornografi anak paling populer di *Dark Web,* tetapi bukan satu-satunya. Pada tahun 2009, penyelidik PBB Najat M'jid Maalla melaporkan lebih dari 4 juta situs web berpartisipasi dalam distribusi pornografi anak.[14] Perkiraan PBB menempatkan industri ini bernilai antara $3 miliar hingga $20 miliar.[15] Ini adalah industri tersibuk di *Dark Web*, yang mencakup sekitar 80% kunjungan *Dark Web.* Dengan statistik di atas, dapat ditentukan bahwa situs *Dark Web* menampung ratusan ribu atau jutaan predator seksual yang relatif aman di anonimitas.

Bagaimana Kita Beradaptasi dengan Dark Web?

Kasus-kasus yang disajikan di atas menyuguhkan sedikit informasi terkait hak asasi manusia. Skala di mana penjahat online beroperasi berdasarkan kasus-kasus ini mungkin tampak seperti aksi demoralisasi. Kasus-kasus tersebut mungkin menimbulkan beberapa implikasi yang merugikan tentang apakah privasi yang disediakan oleh *Dark Web* benar-benar memiliki kemungkinan munculnya tindakan kriminal. Dengan langkah cepat di mana Internet dan *Dark Web* berkembang, ada banyak pertanyaan tentang bagaimana kita dan institusi pemerintah dapat beradaptasi. Seringkali, kita merasa aman berdasarkan otoritas penegak hukum kita dan kesuksesan mereka. Berdasarkan kejahatan yang sebenarnya, pemerintah melakukan yang terbaik untuk melindungi warganya dari kejahatan siber. Namun, bagaimana mereka mencapai hal ini?



Sebagaimana dinyatakan di atas, ada beberapa keberhasilan oleh penegak hukum di seluruh dunia seperti dalam kasus *Playpen, AlphaBay,* dan *Silk Road.* Tetapi banyak perusahaan kriminal lainnya masih tetap ada, dan banyak lembaga penegak hukum masih bekerja untuk melawannya. Interpol, misalnya, telah memulai program untuk mendidik petugas polisi dalam mengidentifikasi metode dan teknik baru yang digunakan oleh sistem kejahatan terorganisir untuk menyembunyikan identitas, serta memahami infrastruktur teknis *Dark Web.*[16] Inggris, sementara itu, juga telah mengatur gugus tugas yang terdiri dari pejabat dari *Government Communication Headquarters* (GCHQ), dan badan penegak hukumnya, *National Crime Agency* (NCA) untuk menangani kejahatan online di Dark Web.[17]

Lembaga penegak hukum seperti FBI saat ini bekerja dengan banyak perusahaan keamanan siber yang mengkhususkan diri dalam menangani dark web untuk mendapatkan informasi terkait dengan memerangi unsur-unsur kriminal di dalamnya. Perusahaan seperti Terbium Labs, Owl Cybersecurity, dan InfoArmor Inc. bekerja di bidang seperti penyuratan otomatis dan analisis data mengenai konten *Dark Web.* Selain penegak hukum, mereka juga secara teratur bermitra dengan bank, pengecer dan entitas lain yang peduli dengan keamanan data mereka.[18] Para pemangku kepentingan lainnya di sektor swasta yang berurusan dengan *Dark Web* termasuk Aliansi Warga Digital, sebuah koalisi konsumen yang berbasis di Washington, bisnis internet dan para ahli yang menyediakan intelijen penting seperti data kuantitatif mengenai jumlah obat yang dijual di dark web.[19]

Di sektor sipil, banyak yang mencoba mengangkat dark web keluar dari reputasi buruknya. Pada 2015, sekelompok seniman "cybertwee" mengorganisir penggalangan dana yang menjual *cookie* di situs web di jaringan Tor. Hasil kegiatan ini disumbangkan ke organisasi bio-medis independen GynePunks, yang bekerja untuk membuat teknologi ginekologi tersedia secara bebas untuk wanita. Namun, sebagai tambahannya, salah satu penggalangan dana ini bertujuan utama juga untuk mendidik lebih orang-orang tentang dark web secara umum. Salah satu pendiri penggalangan dana, Gabriella Hileman, menyatakan bahwa,

> "Kami tidak begitu akrab dengan deep web, jadi insentif kami untuk ini adalah untuk mendidik diri kita sendiri, dan dalam melakukan itu mendidik orang lain dan menjadikannya usaha kelompok. Kami ingin membuat hal-hal seperti ini dapat diakses oleh lebih banyak orang sehingga kita semua dapat memanfaatkan alat seperti enkripsi. "[20]

Tapi penegak hukum tidak bisa ada di mana-mana, baik di dunia nyata atau dunia digital. Mereka dapat memblokir situs web, tetapi hanya membutuhkan beberapa klik untuk melewati dinding tersebut. Mereka dapat mencoba melacak

Kedua, Jaringan Tor sangat bermanfaat bagi para penegak hukum seperti halnya bagi para penjahat yang mereka lacak. Selain memanfaatkan jaringan dengan cara yang sama dengan *Playpen*, sebagai "jaring" untuk melacak pelaku yang dicurigai, pejabat pemerintah juga menggunakan anonimitas jaringan untuk kepentingan mereka sendiri. Proyek Tor mengakui bahwa jaringan Tor sebagian dibuat untuk memfasilitasi penegakan hukum online, dengan menyediakan cara untuk menyelubungi keberadaan online para penyidik penegak hukum.[21] Institusi pemerintah seperti Angkatan Laut Amerika Serikat telah menggunakan Tor untuk melakukan pengumpulan intelijen. Tanpa mengekspos Alamat IP pemerintahan dan institusi mereka, para penyidik penegak hukum bebas untuk melakukan operasi penyerangan dan menggunakan jaringan Tor dengan anonimitas yang sama diberikan kepada pengguna Tor.

Meskipun kasus-kasus di atas adalah contoh-contoh utama tentang bagaimana kita beradaptasi dengan *Dark Web*, dunia digital akan terus berkembang selama pengguna internet memiliki pilihan untuk menjaga aktivitas online mereka tetap terjaga kerahasiaannya. Pengguna internet mencari tahu cara-cara untuk menjaga privasi mereka melalui teknologi seperti browser Tor dan VPN, dengan risiko menyediakan sarana bagi penjahat online prospektif untuk bersembunyi dari hukum. Bitcoin telah mempermudah penjahat untuk berdagang tanpa berurusan dengan risiko menggunakan mata uang pemerintah. Instrumen yang ada dibuat untuk membuat komunitas online lebih aman dan lebih bebas juga memberikan manfaat yang sama dengan kejahatan terorganisir online. Pengawasan online adalah konsekuensi dari aktivitas kriminal daring, dan aktivitas kriminal online adalah konsekuensi dari kebebasan pengguna dalam penggunaan internet.

Kesimpulan

Dark Web adalah contoh utama tentang bagaimana Internet telah berevolusi - atau beberapa mungkin mengatakan, bermutasi - jauh melampaui ruang lingkup aslinya. Ketika World Wide Web mengambil langkah pertamanya dua puluh delapan tahun yang lalu di CERN, pengguna pertamanya mungkin sulit membayangkan bahwa suatu saat akan digunakan untuk menjual obat-obatan dan senjata. Tragedi yang sama juga terjadi pada banyak penemuan mutakhir lainnya. Alfred Nobel menciptakan dinamit sebagai cara baru menghancurkan batu untuk penambangan; Nobel Prize lahir dari kesalahannya setelah penemuannya membuka jalan bagi peledak dalam perang.[22] Einstein sangat menyesalkan temuannya berperan dalam menciptakan bom atom pertama. [23]

Namun, *Dark Web* juga dapat dikatakan sebagai konsekuensi dari pertumbuhan Internet. Ketika Internet menjadi lebih besar dan jaringan di dalamnya mencakup lebih banyak aspek dalam kehidupan kita, informasi pribadi kita semakin banyak diserahkan ke dalamnya - tidak selalu tanpa persetujuan kita. Iklan dibuat berdasarkan kebiasaan browsing kita. Informasi media sosial kita bebas diakses oleh individu-individu yang tidak pantas dari masa lalu kita. Situasi ini mungkin tidak ideal bagi yang lebih introvert atau skeptis di antara kita yang berhati-hati tentang bagaimana jejak digital mereka sedang diperiksa oleh pemerintah atau bisnis. Pilihan untuk menyembunyikan aktivitas Internet di jaringan mereka sendiri bukanlah konsekuensi yang tidak mungkin.

Hak mereka untuk membuat pilihan semacam itu, dan sah saja untuk bersosialisasi dalam jaringan mereka sendiri selama mereka tidak bertindak kriminal atau berkonspirasi untuk melakukan tindakan kriminal. Tragedi terjadi saat banyak pihak menggunakan hak itu bukan untuk melindungi diri mereka sendiri, tetapi untuk menyakiti orang lain. Lebih menyedihkan saat sebagian besar kejahatan yang terjadi, sampai pada titik pornografi anak online dan perdagangan narkoba yang menjadi industri sebagai hak mereka sendiri. Internet adalah kumpulan informasi terbesar dalam sejarah manusia. Ini adalah teknologi yang telah mengubah arah peradaban secara ireversibel - ia dapat dan seharusnya digunakan untuk kemajuan umat manusia. Prinsip privasi, kebebasan dan kemandirian yang memunculkan Dark Web sangat penting untuk pemenuhan tujuan itu. Kita tidak boleh membiarkannya terusak.

Prinsip-prinsip itu menjadi alasan mengapa nama *'Dark Web'* dapat dikatakan terlalu seram untuk mendeskripsikan objek yang dimaksud.

Dark Web tidak 'gelap' atau jahat, dan prinsip-prinsip yang menciptakannya sepenuhnya masuk akal. Studi kasus ini tidak bertujuan untuk menyebarkan ketakutan; bahkan dengan itu risiko bahayanya, *Dark Web* jauh dari menjadi sumber mimpi buruk yang akan menarik para penjahat ke depan pintu Anda dalam beberapa menit setelah Anda masuk ke jaringan Tor. Jawaban atas tindakan kriminal yang terjadi di dalamnya tidak seharusnya ditutup seluruhnya. Kita harus mendorong kemampuan beradaptasi, tidak hanya di kalangan penegak hukum tetapi juga dalam diri kita dan organisasi lain. Jika kita terus melakukannya secara reaktif dengan rasa takut dan enggan seperti pada umumnya, maka kesadaran mengenai hal itu tidak dapat menyebar dan unsur-unsur kriminalnya akan terus berkembang. Kesadaran adalah langkah pertama. Mungkin kemudian kita dapat mengurangi dampak negatif dari fenomena *Dark Web* yang, suka atau tidak, tampaknya *Dark Web* tetap akan ada di waktu-waktu ke depan.

Referensi

[1] Brown, I. and Kor_, D. (2009). Terrorism and the Proportionality of Internet Surveillance. European Journal of Criminology, 6(2), hal.120.

[2] Institute for Policy Research and Advocacy (ELSAM) (2016). The Right to Privacy in Indonesia. [ebook] Privacy International, hal.3. Tersedia di laman: https://privacyinternational.org/sites/default/-files/UPR27_indonesia_0.pdf [Diakses pada 14 Nov. 2017].

[3] Gellman, B. and Poitras, L. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. [daring] Washington Post. Terdapat di laman: https://www.washington-post.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [Diakses pada 14 Nov. 2017].

[4] BrightPlanet. (2014). Clearing Up Confusion - Deep Web vs. Dark Web - BrightPlanet. [daring] Tersedia di laman: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/ [Diakses pada 14 Nov. 2017].

[5] Ibid.

[6] Kelion, L. (2014). Struggle to keep Tor in the shadows. [daring] BBC News. Tersedia di laman: http://www.bbc.com/news/technology-28886465 [Diakses pada 14 Nov. 2017].

[7] Dredge, S. (2013). What is Tor? A beginner's guide to the privacy tool. [daring] the Guardian. Tersedia di laman: https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser [Diakses pada 14 Nov. 2017].

[8] Rachels, J. (1975). 'Why Privacy is Important.' Philosophy & Public A_airs, Vol. 4, No.4, hal. 331. Tersedia di laman: https://www.jstor.org/stable/pdf/2265077.pdf [Diakses pada18 Des. 2017]

[9] Yeung, P. (2014). A Tour of the Best, Entirely Legal Hangouts on the Deep Web. [daring] Motherboard. Tersedia di laman: https://motherboard.vice.com/en_us/article/vvbbd-b/the-legal-side-of-the-deep-web-is-wonderfully-bizarre [Diakses pada 14 Nov. 2017].

[10] Leger, D. (2013). How FBI brought down cyber-underworld site Silk Road. [daring] USA TODAY. Tersedia di laman: http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/ [Diakses pada14 Nov. 2017].

[11] Justice.gov. (2017). AlphaBay, the Largest Online 'Dark Market,' Shut Down. [daring] Tersedia di laman: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down [Diakses pada 27 Nov. 2017].

[12] Russon, M. (2016). FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web. [daring] International Business Times UK. Tersedia di laman: http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417 [Diakses pada 14 Nov. 2017].

[13] Cox, J. (2016). The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant. [daring] Vice. Tersedia di laman: http://www.vice.com/en_id/read/the-fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant-en-id [Diakses pada 14 Nov. 2017].

[14] msnbc.com. (n.d.). UN expert: child porn on Internet increases. [daring] Tersedia di laman: http://www.nbcnews.com/id/32880508/ns/technology_and_-science-security/t/un-expert-child-porn-internet-increases/ [Diakses pada14 Nov. 2017].

[15] Greenberg, A. (2014). Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study-Finds. [daring] WIRED. Tersedia di laman: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ [Diakses pada14 Nov. 2017].

[16] Richard (2015). Interpol Dark Web Training Course. [daring] Dark Web News. Tersedia di laman: https://darkwebnews.com/news/interpol-dark-web-training-course/ [Diakses pada 27 Nov. 2017].

[17] Cox, J. (2015). The UK Will Police the Dark Web with a New Task Force. [daring] Motherboard. Tersedia di laman: https://motherboard.vice.com/en_us/article/wnxeyn/the-uk-will-police-the-dark-web-with-a-new-task-force [Diakses pada 27 Nov. 2017].

[18] Johnson, T. (2017). Shocked by gruesome crime, cyber execs help FBI on dark web.[daring] Idaho Statesman. Tersedia di laman: http://www.idahostatesman.com/news/nation-world/national/article164797842.html [Diakses pada 27 Nov. 2017].

[19] Digital Citizens Alliance. (2014). Darknet Marketplace Watch. [daring] Tersedia di laman: http://www.digitalcitizensalliance.org/get-informed/dark-net-marketplace-watch/ [Diakses pada 27 Nov. 2017].

[20] Paul, K. (2015). Coming Soon to the Deep Web: Adorable Baked Goods. [daring] Motherboard. Tersedia di laman: https://motherboard.vice.com/en_us/article/jp5w3k/coming-soon-to-the-deep-web-adorable-baked-goods[Diakses pada 27Nov.2017].

[21] Levine, Y. (2014). Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government. [daring] Pando. Tersedia di laman: https://pando.com/2014/07/16/tor-spooks/ [Diakses pada14 Nov. 2017].

[22] Popova, M. (2013). How the Nobel Prize Was Born: A Surprising Story of Bad Journalism,Existential Guilt, and Dynamite. [daring] Brain Pickings. Tersedia di laman: https://www.brainpickings.org/2013/09/17/molly-oldfield-secret-museum-alfred-nobel-will/ [Diakses pada14 Nov.2017].

[23] Rosen, R. (2011). 'I've Created a Monster!' On the Regrets of Inventors. [daring] The Atlantic. Tersedia di laman: https://www.theatlantic.com/technology/archive/2011/11/ive-created-a-monster-on-the-regrets-of-inventors/249044/ [Diakses pada 14 Nov. 2017].

Center for Digital Society

Faculty of Social and Political Sciences
Universitas Gadjah Mada
Room BC 201-202, BC Building 2nd Floor,
Jalan Socio Yustisia 1
Bulaksumur, Yogyakarta, 55281, Indonesia

Phone : (0274) 563362, Ext. 116
Email : cfds.fisipol@ugm.ac.id
Website : cfds.fisipol.ugm.ac.id

facebook.com/cfdsugm
cfds.fisipol.ugm.ac.id
cfds_ugm
@cfds_ugm
@cfds_ugm
CfDS UGM