Ancaman Data Pribadi di Era Digital Dalam Perspektif Islam

Agam Anantama
Institut Agama Islam Negeri (IAIN) Metro
Jl. Ki Hajar Dewantara 15 A MetroTimur Kota Metro Lampung
agamanantama@metrouniv.ac.id

Abstract

This paper discusses threats to personal data on social networks from the point of view of Islamic studies. By first explaining the concept of personal data in the big data industry at this time, various sources and literature were conducted to find data that was appropriate and relevant to the issue of threats to personal data on social media from an Islamic point of view through meta-analysis. The results of data and conceptual processing from the researchers found that threats to personal data on social media can be grouped into three things, namely threats to multimedia content, threats to society and threats to psychology. Each category is classified into several versions of the threat. The author identifies that in addition to utilizing the privacy features provided by social media sites, as early as possible users must also self-literate to be able to distinguish between secrets and information. Everyone must have awareness to be able to select content that is disseminated on social media and especially in Islam which strictly prohibits theft.

Keywords *: Personal Data, Online social networks, Big Data, Islamic Perspective*

A. Pendahuluan

Perkembangan tekhnologi diakui sangat membantu manusia dalam melakukan interaksi dan komunikasi antar sesama tanpa hambatan waktu dan jarak. Media online (Social Networking Sites) menjadi hal yang tidak terpisahkan dengan kehidupan sosial. Hal tersebut tidak dapat dipisahkan dari majunya tekhnologi yang terintegrasi dalam model interaksi masyarakat. Belum lagi perkembangan tekhnologi baru yang selalu berinovasi sehingga memaksa masyarakat untuk mengikuti perkembangannya. Media sosial merupakan sarana dalam mengatasi permasalahan di berbagai bidang, seperti pendidikan, sains, administrasi, birokrasi, investasi, komunikasi dan lainnya. Memiliki keunggulan dalam hal kecepatan, kemudahan akses serta murahnya biaya, jaringan sosial online menjadi alternatif dalam melakukan hubungan dengan sesama[1].

Media Online menginovasikan fiturnya dengan membuat pengguna tetap terhubung secara terus menerus (*Log in*) yang membuat pengguna dapat menerima pesan

[1] Baruh and Popescu, "Big Data Analytics and the Limits of Privacy Self-Management."

dari rekan sosial online dimanapun dan kapanpun. Pengguna juga dapat melakukan hubungan dengan komunitas secara virtual lainnya baik dengan teman, partner kerja, keluarga, bahkan dengan orang yang belum dikenal sekalipun.

Dalam beberapa masa terakhir ini, media sosial telah berevolusi menjadi dunia baru yang berkembang menjadi industri global dengan omset triliunan dolar dan pemakai lintas kalangan.[2]

Media online memaksa pengguna untuk mengungkap seluruh informasi pribadinya sebagai syarat mengakses sebuah platform (umur, tanggal lahir, orientasi seksual atau politik, rekam pembelian barang dan lainnya) [3]. Tentu saja informasi data pribadi yang diungkap sangat bresiko. Informasi data pribadi ini dicurigi dapat berdampak pada pencurian identitas atau penyalahgunaan informasi sebab mengangkat isu yang sensitif. Dalam penelitian yang dilakukan oleh Henson (2020) membuktikan terkait dengan hasil yang bahwasanya sekitar 42% pengguna media sosial adalah mahasiswa dengan mengallami berbagai bentuk ancaman terhadap privasi mereka selama hidup, hal ini merupakan masalah penting yang memerlukan perhatian yang cukup serius.[4]

Media online *(Social Networking Sites)* adalah salah satu jenis jasa web dlam membangun suatu hubungan virtual antar seseorang yang memiliki persamaan minat, bakat, hoby, latar belakang dan keseharia [5]. Media Online merupakan sarana komunikasi yang sangat diminati oleh pemakainya sebab dapat menghilangkan batas ekonomi, sosial budaya, geografi, serta dapat bermanfaat dalam mencapai tujuan yang memiliki kaitannya dengan mencari pekerjaan, ritual agama, hiburan maupun pendidikan.

Namun, Rathore (2017) mewaspadai kepopuleran media sosial tersebut menciptakan bahaya yang cukup besar bagi para penggunanya. Ketika data pribadi dibagikan di media sosial dapat menjadikan pemakai sebagai target yang empuk guna diancam yakni dengan cara *spam, socialbot, malware*, serta pecurian data pribadi. Bahkan pelaku dapat saja memperoleh data penting lainnya seperti informasi akun dari bank yang dapat dikenakan guna melakukan aksi penipuan serta mendapat informasi pribadi lainnya[6].

Peyalahgunaan informasi berupa data pribadi merupakan ancaman yang sangat nyata. Sebab pengguna tanpa sadar memberikn sejumlah informasi pribadinya dan dapat menjadi komoditas bagi

[2] Henson, Reyns, and Fisher, "Security in the 21st Century: Examining the Link between Online Social Network Activity, Privacy, and Interpersonal Victimization." H.21

[3] Millham and Atkin, "Managing the Virtual Boundaries."

[4] Henson, Reyns, and Fisher, "Security in the 21st Century: Examining the Link between Online Social Network Activity, Privacy, and Interpersonal Victimization."

[5] Rathore et al., "Social Network Security: Issues, Challenges, Threats, and Solutions."

[6] Rathore et al.

penyerang data yang mencuri data pribadi melalui jaringan internet.

Islam sangat mengecam bentuk pengambilan informasi atau segala sesuatu tanpa izin dari si pemilik yang dikategorikan sebagai tindakan pencurian. Setiap prilaku pencurian sangat dilarang keras dalam ajaran Islam. Seperti yang termuat dalam QS. Al Maidah Ayat 38 :

> "*Adapun orang laki-laki maupun perempuan yang mencuri potonglak kedua tangannya (sebagai) balasa atas perbuatan yang mereka lakukan sebagai siksaan dari Allah. Dan Allah Maha Perkasa, Maha Bijaksana*"

Mengambil sesuatu tanpa sepengetahuan pemiliknya merupakan Tindakan yang sangat tercela. Bahkan tindakan mencari keuntungan atas informasi orang lain tidak lepas dari kategori pencurian yang dikecam oleh Allah SWT. Sebagaimana dijelaskan dalam Q.S. al-Baqarah : 188

> *"Dan janganlah kamu makan harta di antara kamu dengan jalan yang batil, dan (janganlah) kamu menyuap dengan harta itu kepada para hakim, dengan maksud agar kamu dapat memakan sebagian harta orang lain itu dengan jalan dosa, padahal kamu mengetahui"*[7].

Tulisan ini akan mencoba mengupas bagaimana ancaman data pribadi pada Media online. Berdasarkann latar belakang tersebut, penulis membatasi permasalahan sebagai berikut:

1) Sejauh mana ancaman pencurian data pribadi di Media Online
2) Bagaimana konseptualisasi ancaman terhadap data pribadi di industri digital menurut perspektif Islam?

B. Metode Penelitian

Dalam mengurai permasalahan diatas, Tulisan ini mengadaptasi pedoman meta-sintetis dari Francis dan juga Baldesari dengan menggunakan pendekatan meta-agregasi kualitatif. Dimana pendekatan kualitatif dalam meta-sintetis ini digunakan dengan meringkas hasil penelitian secara kualitatif ini disebut dengan "meta-sintesis". Secara definisi, meta-sintesis merupakan teknik melakukan integrasi data untuk memperoleh konsep maupun teori baru atau singkat pemahaman yang lebih mendalam dan menyeluruh[8].

Ada dua pendekatan untuk melakukan sintesis visual (sintesis dan kualitatif), yaitu *meta-agregasi* (meta-agregasi) dan *meta-etnografi* (meta-etnografi). Dalam meta agregasi, sintesis bertujuan untuk menjawab beberapa pertanyaan penelitian (*review question*) dengan merangkum hasil penelitian (*summary*). Pada saat yang sama, meta etnografi sintetik mencoba mengembangkan teori-teori baru untuk melengkapi teori sebelumnya.

Dalam meta-agregasi, topik penelitian dikelompokkan kedalam bidang studi tertentu yang menghasilkan kerangka kerja analitis (kerangka konseptual). Artikel penelitian yang relevan dalam topik ini kemudian dicari, dibandingkan, dan dirangkum. Dalam pendekatan meta-agregasi,

[7] "Surah Al-Baqarah - سُورَة البقرة | Qur'an Kemenag."

[8] Schmidt and Hansson, "Doctoral Students' Well-Being."

hasil sintetis merupakan "agregat" dari banyak macam sumber hsil penelitian sesuai dengan topi yang relevan.

Francisco dan Baldesari mengidentifikasikan tahapan metasintesis sebagai berikut ini:

1. Perumusan pertanyaan penelitian (*formulation of a control question*). Fokus penelitian ini adalah untuk dapat mengetahui apa saja ancaman terhadap data pribadi di media online.

   Oleh karena itu, berdasarkan hasil kajian pustaka ini, direncanakan jawaban atas beberapa pertanyaan.

   Pertanyaan 1 (Q1) :

   Di forum publikasi mana diskusi tentang data pribadi akan dipublikasikan?

   Pertanyaan 2 (Q2) : Apa pertanyaan/masalah dalam penelitian ini? Pertanyaan 3 (Pertanyaan3) : Bagaimana setiap konsep berkontribusi pada integrasi komunitas online?

   a) Pelaksanaan pencarian literatur secara sistematis Pencarian literatur ini menggunakan sumber data di website SAGE (http://www.journals.sagepub.com). semakin banyak sumber data yang dibahas, semakin besar peluang untuk dapat enemukan literatur yang memiliki kesesuaian. Strategi pencarian dibangun dengan mendefinisikan kata kunci dan sinonim untuk fokus penelitian.

   b) Melakukan *screening* dan seleksi artikel penelitian yang sesuai (*Screening and selection of proper research article*)

   Menggunakan pencarian ini kemungkinan besar akan menghasilkan banyak artikel. Oleh karena itu, diperlukan identifikasi lebih lanjut untuk mendapatkan artikel yang digunakan sebagai studi primer. Dengan menerapkan kriteria inklusi dan eksklusi iidentifikasi penelitian dapat dilakukan. Penerapan kriteria inklusi dan eksklusi untuk memastikan bahwasanya artikel yang digunakan relevan dengan konteks penelitian.

   a) Kriteria Inklusi
      - makalah yang menjelaskan konsep, keunggulan, teknik, metode, strategi, dan segala sesuatu yang telibat dalam penerapan privasi serta penambangan data secara simultan di media online.

   b) Kriteria Pengecualian
      - Postingan yang berfokus hanya pada pembahasan privasi di media online.
      - Artikel secara eksklusif berfokus pada pemrosesan data pribadi di media online
      - Melakukan analisis dan sintesis temuan

kualitatif (Analisis dan Sintesis Temuan Kualitatif)

2. *Quality Control* (menjaga kualitas).
3. Membuat laporan akhir (mewakili pengamatan) Kriteria inklusi dan eksklusi kemudian diterapkan dengan membaca rangkuman dari seluruh siswa sekolah dasar. Sebagai hasil penerapan kriteria inklusi dan eksklusi, diperoleh total 13 artikel studi primer yang sesuai dengan kriteria masing-masing sesuai Tabel 1.

Tabel 1. Hasil Eksekusi Kriteria Inklusi dan Eksklusi

Tahun Publikasi	Jurnal
1997	Brennen, B., & Primeaux, D.
2008	Boyd, D
2011	Henson, B., Reyns., & Fisher, B.
2015	Chen, F., Deng, P ., Wan, J., Zhang, D., Vasilakos, A., &Rong, X.
2016	Guo, L Kitchin, R., & McArdie, G.
2017	Baruh, L., & Popecu, M Keyes, I, & Iamnichi, A. Rathore, S., Sharma, P., Loia, V., Jeong, Y.-S., & Park, J.-H. Liang, H., Shen, F., & Fu, K. Kennedy, H., Elgesem, D., & Miguel, C. Frith, J.
2018	Milham, M., dan & Atkin, D.

C. Pembahasan

Beberapa penelitian tentang analisis data besar telah melakukan identifikasi pada beberapa kasus yang sangat urgent bagi penggunanya. Menurut sebuah studi yang diterapkan oleh Dixon dan Gellman (2014), ketersediaan database pelanggan yang tergolong besar telah menyebabkan berkembangnya industri agen konsumen yang tidak diatur.[9]

Pasquale (2015) menemukan bahwasanya logika tersebarnya data bagi penggunna didasarkan pada logika algoritma yang mampu memberikan prediksi pada semua data yang masuk ke database lintas kontekstual yang terus berkembang dan mengelompokkan orang kedalam domain yang beragam seperti jenis pekerjaan dan persewaan.., atau penjualan eceran.[10]

Oleh karena itu, menurut Andrejevic (2013), selain aspek teknis data besar serta aplikasi praktisnya, data besar menciptakan organisasi sosial informasi baru yang menormalkan suasana kehilangan privasi sekaligus

[9] Baruh and Popescu, "Big Data Analytics and the Limits of Privacy Self-Management."

[10] Frith, "Big Data, Technical Communication, and the Smart City."

menciptakan bahkan meninjolkan ketidak setaraan yang ada.[11].

Gavinson (1980) mengenalkan gagasan otonomi individu, yang menurutnya privasi harus melindungi hak dan kekuasaan individu untuk menentukan nasibnya sendiri dan setidaknya kapasitas individu untuk menentukan nasib sendiri.[12].

dalam ruang lingkup pengumpulan data, diskusi tentang privasi diperumit oleh dugaan kesulitan dalam memberi definisi pada pelanggaran privasi idividu. menurut Solove (2013), upya telah dilakukan dalam beberapa tahun terkahir guna dapat melakukan pembaharuan pada perlindungan privasi dalam mengumpulkan data digital dilakukan dengan mempertahankan strategi lierasi yang membutuhkan penggna uang sadar dengan privasi [13] . Dengan berkembangnya media online saat ini, muncul juga isu terkait menjaga privasi serta keamanan konsumen, terutama saat pengguna mengupload konten di media seperti foto, video, dan suara.

Henson dkk, juga menemukan bahwasannya jumlah pengguna online yang besar juga dapat meningkatkan berbagai ancaman siber di jejaring sosial.[14].

Individu dapa tmengatasinya dengan menciptakan "perlindungan diri" terhadap penggunaan fitur privasi media online yang ada. Bagaimanapun, langkah perlindungan pertama harus diambil oleh pengguna itu sendiri.

Menurut Harris (2014), keamanan online merupakan suatu penyensoran pada jaringan atau konten yang tidak diperbolehkan di media sosial online, dikelola secara terorganisir dan dilaksanakan dengan kontrol vertikal. [15] . Media online telah menjadi budaya arus utama bagi jutaan orang yang menggunakan internet diseluruh dunia. dengan menggabungkan profile yang diaktifkan oleh pengguna, dengan menggunakan dmekanisme dalam komunikasi yang memberi kemungkinan pada pengguna untuk terhubung secara tetap atau permanen, media online memasuki hubungan sosial aktual pengguna serta lebih banyak lagi mengintregasikan kehidupan secara online maupun offline bagi pengguna media sosial.

Pada tahun 2017, 1,9 miliar pengguna aktif bulanan yang dimiliki oleh facebook dan merupakan situs web yang paling banyak dikunjungi ke tiga di web[16]. Twitter, platform micro bolgging sosial, melakukan klaim lebih dari 313 juta pengguna aktif bulanan yang membagikan tweet dalam lebih dari sekitar 40 bahasa dari berbagai negara.

---

[11] Baruh and Popescu, "Big Data Analytics and the Limits of Privacy Self-Management."

[12] Millham and Atkin, "Managing the Virtual Boundaries."

[13] Baruh and Popescu, "Big Data Analytics and the Limits of Privacy Self-Management."

[14] Henson, Reyns, and Fisher, "Security in the 21st Century: Examining the Link between Online Social Network Activity, Privacy, and Interpersonal Victimization."

[15] Kayes and Iamnitchi, "Privacy and Security in Online Social Networks."

[16] Kayes and Iamnitchi.

Pengguna media sosial biasanya terkoneksi dengan temannya, keluarganya, dan kenalan-kenalannya. Persepsi yang muncul umumnya ialah bahwasannya media sosial akan lebih aman, rahasia, dan dapat terpercaya guna berinteraksi secara daring (online). Namun secara realitas, media sosial telah meningkatkan resiko guna memberikan perlindungan terhadap privasi disebabkan dari ketersediaan terhadap jumlah data dari para pengguna milik pribadi yang ada di luar ekspektasi mereka, baik yang di publikasikan maupun tidak.

Terlebih, media sosial melakukan ekspos pada informasi dari banyak macam sektor sosial seperti informasi milik pribadi dalam Facebook maupun aktivitas profesional di LinkedIn yang telah terkumpul serta lebih mengarah pada profil yang lebih rinci.

Pengungkapan terhadap informasi bagi pengguna yang tidak diingikan ini dapat memberi akibat pada media sosial jadi memiliki konsekuensi menghawatirkan. fenomena seperti kasus pada seorang dokter yang dituntut sebab mengupload foto alat kontrasepsi, atau karyawan yang dipecat sebab berkomentar tentang gajinya yang melakukan perbandingan dengan gaji bosnya (keduanya kasus dari Facebook).

Selain itu, media sosial baik itu disengaja ataupun tidak (misalnya mempublishkan data sosial anonim yang dipergunakan bagi mendeanonimisasi) sebagaimana berkontribusi pada pelanggaran bagi privasi pengguna. Selain itu, volume data pribadi yang cukup tinggi, baik yang diungkap oleh pengguna atau yang disebabkan dari kegagalan media sosial guna menyediakan alat privasi yang lebih canggih, telah menarik berbagai pandangan organisasi seperti (GNIP–GNIPInc merupakan perusahaan agregasi API sosial media yang menyediakan berbagai data dari puluhan situs sosial media melalui satu API) dengan tujuan guna menjual sekaligus menggabungkan jaringan jejaring sosial pengguna terkait data tersebut. selain itu, sifat dari korelasi media sosial yang dapat dipercaya telah menjadi suatu mekanisme yang efektif guna melakukan penyebaran *spam, malware*, dan *phishing*.

Entitas jahat yang meluncurkan banak macam serangan dengan membuat profile palsu pada akun pengguna, memakai kedok akun media sosial yang di curi atau dijual secara illegal atau menyebarkan isu melalui*bot*[17]. *Internet Security Threat Report* (ISTR) menyebutkan bahwasanya peningkatan penggua media sosial oleh peretastidak dapat diabaikan[18].

Pada 2015, pemberian layanan seperti itu menjadi sumber *spam, malware*, dan digunakan untuk mendapatkan uang ilegal secara online. Dan pada tahun 2016, media online menjadi target utama pencurian identitas dan *spear-phishing*.[19].

Sebuah studi oleh Rathore. Dkk (2017) menegaskan beberapa solusi

[17] Richard West and Lynn H. Turner, *Introducing communication theory : analysis and application / Richard West, Lynn H. Turner*.

[18] Rathore et al., "Social Network Security: Issues, Challenges, Threats, and Solutions."

[19] Rathore et al.

untuk mencegah ancaman ini. Ini termasuk water marking, analisis brace dan pelupaan digital untuk melindungi pengguna media online dari ancaman yang terkait dengan data multimedia. Selain itu, solusi seperti deteksi spam serta deteksi phishing juga ditawarkan guna mengatasi ancaman tradisional[20].

Penelitian Gao, dkk. mengkategorikan permasalahan keamanan yang paling utama dalam Media social ke dalam empat golongan yaitu:

1. Isu privasi.
2. Pemasaran viral.
3. Struktur jaringan berdasarkan serangan.
4. Serangan *malware*.

Jin dkk. Mempelajari perilaku pengguna media online dari empat sudut pandang, yaitu:

1. Perilaku *malicious*.
2. Perilaku mobile social.
3. *Traffic activity*.
4. Koneksi dan interaksi.

Fire dll. Membuat pembagian ancaman keamanan yang kini menjadi empat kategori, yakni ancaman klasik, ancaman modern, ancaman kobinasi, serta ancaman dengan target anak-anak [21]. dengan penggunaan yang tinggi pada media online, reputasi pengguna online juga mendapat peningkatan melalui web.

Reputasi para pengguna dapat memberi pengaruh pada posisi serta kredibilitas para pengguna di dalam kehidupan nyata. Jejaring social online dapat menjatuhkan reputasi suatu perusahaan maupun organisasi besar, contohnya pesan negative dari karyawan dapat merusak reputasi organisasi dan karyawan perusahaan.

Media online juga kerap digunakan oleh beberapa perusahaan besar guna menyusun profil secara lengkap dari tiap individu yang bertujuan guna menjual produk serta merekam segala macam perilaku individu. Akan tetapi, semuanya itu kerap dilakukan tanpa adanya izin dari dindividu yang bersangkutan.

selain itu, berdasar pada penelitian dari Smith, dalam media online tahun 2015, menghabiskan lebih dari 20% banyaknya anggaran digunakan oleh 38% perusahaan untuk melakukan iklan. Yakni aplikasi Twitter dan Facebook yang paling banyak dipergunakan untuk memasang iklan.[22]

Rathore dkk, lalu mengelompokkan ancaman dari keamanan menjadi tiga bentuk yakni (1) ancaman konten dalam multimedia, data *sharing* yang sebagaimana menjadi karakter penting pada media online dimana mereka dapat membagikan foto, video, aktivitas, dan minat dengan mudah[23].

Meskipun telah ada

[20] Guo et al., "Big Social Data Analytics in Journalism and Mass Communication: Comparing Dictionary-Based Text Analysis and Unsupervised Topic Modeling."

[21] Rathore et al., "Social Network Security: Issues, Challenges, Threats, and Solutions."

[22] Rathore et al.

[23] Rathore et al.

peningkatan dalam teknik pengambilan terhadap multimedia seperti estimasi lokasi, mengenali wajah, mencari situs web, serta geo tagging, maupun mencari penyalahgunaan ilegal yang terus meningkat. Sebagaimana ancaman yang ada pada konten multimedia termasuk dalam paparan konten dari multimedia, berbagai macam properti, memanipulasi konten dari multimedia, metadata, steganografi, berbagi tautan ke konten yang ada pada multimedia, tautan statis, outsourcing, sekaligus transparansi terhadap pusat data, konferensi video, kemampuan penandaan tautan data dalam multimedia secara bersama, serta pengungkapan informasi ilegal. (2) ancaman secara tradisional, dimana meliputi phishing, malware, serangan sybil serta profil yang palsu, spam, clik bait, serangan anonimisasi, serangan inferensi, serta cloning profil. properti, manipulasi konten[24].

Kategori ke (3) yakni dancaman alam lingkup social, yang dimana terdiri atas *cyberbullying, cybergrooming, cyberstalking,* dan *spionase* terhadap perusahaan[25].

Beberapa solusi dan saran yang telah ditawarkan oleh Rathoreet dkk, (2017) yakni dalam menangani masalah terhadap keamanan di media online yakni seperti *co-ownership, watermaking, digitaloblivion, steganalysis, storage encryption, metada removal, analisys, malware detection, sybil defense,* deteksi profil yang palsu, deteksi *pishing,* deteksi *spammer,* solusi pada komersial, solusi terhadap keamanan media online *built-in,* serta mendeteksi *profile cloning*[26].

Permasalahan terhadap keamanan sekaligus ini akan terus di proses guna mencapai titik mapan serta dapat mengatasi serangan-serangan terhadap keamanan dan juga privasi dalam media sosial. Hal ini telah dibuktikan bahwasannya tanpa dengan adanya dukungan dari legislatif, yakni isu yang negatif hanya dapai di minimalisisr akan perubahan sekaligus dampak saja tanpa adanya solusi dan saran secara menyeluruh.

Pendiri Facebook, yakni Mark Zuckerberg sebelumnya beragumen bahwa ketika privasi tersebut ramai untuk dipertanyakan di media online, dalam hal ini ialah Facebook sebagai aplikasi yang telah diciptakannya. Mark Zuckerberg telah berkali-kali menegaskan akan tujuannya guna membantu para pihak dari berbagai informasi yang lebih efisien[27].

Dengan cara mengumpulkan informasi social sekaligus meyampaikannya melalui siaran, maka News Feeds memutuskan hal apa yang dapat diakses oleh tiap orang serta memposisikannya pada hal yang menjadi pusat perhatian mereka. Zuckerberg menegaskan bahwasannya tidak ada privasi yang direncanakan dalam prosesnya [28] .

[24]Rathore et al.

[25]Chen et al., "Data Mining for the Internet of Things: Literature Review and Challenges."

[26] Rathore et al., "Social Network Security: Issues, Challenges, Threats, and Solutions."

[27]Dana Boyd, "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence."

[28]Dana Boyd.

Namun, Boyd menekankan bahwasanya privasi merupakan tentang bagaimana seseorang mengalami korelasi yang menunjukkan mereka dengan orang lain dan dengan informasi. Privasi merupakan rasa *control* atas informasi yang didapat, konteks yang dimana berbagi telah terjadi, serta *audiens* yang dapat mendapatkan akses[29].

Dengan demikian, jika ditinjau dari pendapat Boyd, menyatakan bahwasannya informasi yang memiliki sifat pribadi dikarenakan tidak ada pihak yang mengetahuinya, dikarenakan juga individu tersebut yang menciptakan batas serta control terhadap hal-hal yang demikian. Boyd juga menyatakan bahwasannya ada wilayah abu-abu yang sangat dominan antara rahasia dengan informasi sebagaimana dijelaskan yakni guna disampaikan kepada khalayak umum.

Pengguna media online juga tidak akan mungkin memposting dan membagikan hal-hal yang memiliki sifat rahasia, akan tetapi mereka akan lebih sering untuk memposting sekaligus membagikan informasi yang sifatnya relevan dalam konteks yang disesuaikan[30].

Pikirnya, jika seseorang melakukan kunjungan pada halaman Faecebook milik orang lain, maka kita dapat mencari informasi yang sesuai dengan konteks yang kita butuhkan. Dengan maksud lain yaknipilar utama guna memberi batasan pada ruang dan gerak dari privasi dalam konteks yang berupa ancaman pada privasi serta data *mining* yang ada pada media online yakni diri sendiri.

Dalam akhir penelitian yang meliputi privasi di aplikasi Facebook, Boyd juga menyatakan bahwasannya privasi tidak hanya meliputi hak yang mutlak, namun merupakan hak yang istimewa sebagaimana hak yang harus dilindungi secara sosial serta structural agar dapat selalu menjadi perhatian yang utama bagi amsyarakat. Hal yang selanjutnya menjadi pertanyaan yakni apakah privasi seseorang masih ada ataupun tidak ialah suatu yang sebagaimana konteks tersebut sangatlah bergantung pada masyarakat, lalu apakah masyarakat memilih lebih memperhatikan hal ini atau sebaliknya.

Hal ini juga mengacu pada konseptualisasi terhadap ancaman yang melibatkan data pribadi sebagaimana hal yang telah dijelaskan oleh Rathore dkk, dalam Tabel 1 berikut beberapa ringkasan serta berbagai dampak dan praktik oknum yang dapat mengancam data pribadi pada era digital.

Tabel 1. Ringkasan Ancaman pada data pribadi di EraDigital

Ancaman data pribadi di era digital juga berdampak terhadap psikologis. Secara umum faktor yang mempengaruhi psikologis manusia secara situasional terbagi dalam beberapa factor sebagai berikut

[29]Carlos A. Cuevas and Callie Marie Rennison, *The Wiley Handbook on the Psychology of Violence*.

[30] Noyes, "Never Mind the Qualitative Feel the Depth! The Evolving Role of Qualitative Research in Cochrane Intervention Reviews."

1. Aspk-aspek objektif pada lingkungan
   Aspek-aspek objektif yang berasal dari lingkungan yakni terdiri atas :
   a) Faktor ekologis, faktor geografis serta faktor iklim dan meteorologis,
   b) Faktor desain dan arsitektural,
   c) Faktor temporal,
   d) Analisis terhadap suasana perilaku,
   e) Faktor teknologis,
   f) Faktor sosial
      1) Struktur organisasi,
      2) Sistem peranan,
      3) Struktur kelompok,
      4) Karakteristik populasi.
2. Lingkungan dalam psikoanalisis
   a) Iklim organisasi dan kelompok.
   b) Athos dan iklim institusional dan kultural.
   c) Stimulasi yang mendorong serta memperkuat perilaku pada orang lain.
   d) Situasi pendorong terhadap perilaku. [31]
3. Faktor ekologis
   Gaya hidup serta prilaku manusia dapat dipengaruhi oleh faktor lingkungannya. Misal, sikap seseorang yang tinggal di pantai yakni cenderung bernada tinggi dalam berbicara sebagaimana keseharian mereka yang tinggal dalam kondisi pantai dengan cuaca yang panas serta hembusan angin yang cukup kencang sehingga lebih emosional dalam berbicara. Hal ini berbeda dengan orang yang bermukim di pedalaman, misal pegunungan dimana mereka cenderung berbucara dengan nada yang rendah dan lembut karena mereka bermukim ditempat yang berhawa sejuk.
   Sebagian dari pandangan mereka yang telah diteliti, yakni efek temperatur pada perilaku kekerasan dan interpersonal.
4. Faktor rancangan serta arsitektural
   Saat ini para arsitektur telah berpengaruh pada lingkungan yang diciptakan oleh manusia dengan perilaku para penghuninya. Mereka menegaskan bahwasannya desain bangunan tertentu akan berpengaruh pada perilaku tiap penghuninya. Osmond (1957) dan Sommer (1969) memberi perbedaan antara desain bangunan yang cenderung mendorong orang guna dapat berinteraksi dengan lingkungan serta orang sekitard dan rancangan bangunan yang tidak dapat membuat orang guna bersosialiasasi dan berinteraksi[32].
   Contoh pengaruh arsitektural dan pengaruh rancangan terhadap tingkah laku manusia dapat dilihat pada bentuk rumah. Seseorang yang tinggal dengan rumah tanpa pagar ataupun pagar rendah akan lebih mencerminkan bahwasanya pemilik merupakan seseorang yang terbuka dan tidak dicurigai oleh lingkungan sekitarnya. Oleh sebab itu, seseorang yang tinggal dengan arsitektur rumah seperti ini dianggap lebih mau bersosial

[31] Taufik, *Etika Komunikasi Islam*.

[32] Ledolter and VanderVelde, *Analyzing Textual Information: From Words to Meanings through Numbers*.

dengan masyarakat sekitar dibandingkan seseorang dengan rumah berpagar tinggi, rapat, serta dengan arsitektural yang megah bagai istana.
5. Faktor temporal
6. Suasana perilaku (behavior settings)
7. Faktor teknologi
8. Faktor-faktor sosial
9. Lingkungan psikososial[33]

Islam Memandang Ancaman Data Pribadi

Tindakan ancaman data pribadi sebagaimana yang dijelaskan di atas merupakan perbuatan yang sangat dilarang dalam ajaran Islam. Tindakan tersebut termasuk kategori pencurian yang sangat tidak diridhoi Allah SWT. Sebagaimana yang diriwayatkan dalam hadits Rasulullah SAW " *Allah melaknat pencuri yang mencuri sebutir telur, lalu di lain waktu ia dipotong tangannya karena mencuri tali*." (HR. Bukhari. 6285).

Pada dasarnya, mengambil informasi tanpa sepengetahuan pemiliknya, seperti yang dilakukan oleh banyak perusahaan besar, adalah mengambil milik orang lain secara tidak jujur. Menurut hadits, harta seorang Muslim yang diperoleh secara tidak benar adalah haram. Sebagaimana sabda Rasulullah SAW "*sesungguhnya Allah telah mengharamkan atas sesama kalian darah kalian untuk ditumpahkan dan hartta kalian untuk dirampas dan kehormatan kalian untuk dirusak.*" (HR. Bukhari.1742)

Dalam hukum Islam terdapat asas – asas yang menyebabkan jatuhnya suatu putusan yang dikalsifikasikan menjadi tiga hal, yiatu :

1. Asas legalitas, yaitu tidak adanya pelanggaran dan sanksi sebelum adanya undang-undang atau peraturan yang mengaturnya. Asas ini termaktub dalam Al-Qur'an Surah Al-Isra' ayat 15 :
2. Asas material, asas ini ialah asas yang berkaitan dengan unsur material yang ada dalam hukum pidana Islam. Berdasar dengan asas material, menjelaskan bahwasannya hukuman yang ada dalam hukum pidana Islam dibagi menjadi tiga jenis, yakni *Qishas/Diyat, Hudud* dan *Takzir.* Jenis sanksi yang meliputi tindak pidana yakni: (a) ketentuan hukum yang ditetapkan oleh Al-Qur'an dan Hadits. (b) ketentuan hukum yang ditetapkan oleh hakim atau penguasa sebagaimana ditetapkan oleh putusan yang disebut juga sebagai hukuman takzir.
3. Asas moralitas, yakni asas yang berkesinambungan dengan moral hukum pidana Islam. Dimana asas dalam moral tersebut meliputi asas "*dam al-uzri, raf'u al-kalam, dan suquth al-'uqubath*" (gugurnya suatu hukuman).[34]

Tindak kejahatan pencurian terkait dengan data pribadi mempunyai definisi kejahatan yang dimana pelaku mengambil atau berusaha guna mendapatkan data-data dari target pengguna media social di jejaring social online.

[33] Meutia, "Built Urban Heritage Conservation in Islamic Societies."

[34] Taufik, *Etika Komunikasi Islam*.

Dalam Islam disyariatkan tentang pemidanaan tindak pidana yang dapat merugikan. Sebagaimana dengan adanya pemidanaan ini yakni memiliki tujuan guna melakukan perbaikan perilaku dari manusia serta menghindarkan manusia dalam melakukan perbuatan tersebut sehingga menurunkan tingkat kemaksiatan dan kesesatan.

Dalam Al-Qur'an dijelaskan mengenai bentuk tanggung jawab atas perbuatan manusia sbegai berikut :

QS Al-An'am ayat 164
QS Al Mudatsir ayat 38
QS An Najm Ayat 38-39

Mengenai dengan pelanggaran terhadap keamanan cyber tidaklah dijelaskan secara spesifik dalam Al-Qur'an dan juga Hadits. Jika ditinjau dalam sanksi Islam pelanggaran ini termasuk dalam penguhukuman *Hudud* dan *Qishas*, dikarenakan tidak adanya penjelasan yang tegas. Namun Islam sendiri telah melarang manusia untuk dmelakukan perbuatan yang dapat menimbulkan kerusakan maupun merugikan pada orang lain.

Takzir dapat ditetapkan bagi pelaku yang telah melakukan pelanggaran terhadap kasus pencurian terkhusus pencurian pada data pribadi, dikarenakan dalam Al-Qur'an tidak mengatur akan ketentuan yang jelas tentang *punishment* yang ditetapkan. Sanksi yang dapat dijatuhkan kepada pelaku yakni ditentukan oleh hakim atau penguasa yang mempunyai kewenangan dengan ukuran besar kecilnya sanksi yang diberikan berdasarkan tindakan yang telah diperbuat oleh pelaku dan kerugian yang dialami pengguna yang dicuri data pribadinya.

Hukuman diberikan berdasarkan tingkat kerugian dan fakta-fakta dalam pengadilan. Apkah hanya sebatas informasi umum (nama, alamat, jenis kelamin dll) atau bersifat khusus dan rahasia seperti nomor rekening, alamat email, nomor telepon dll. Sanksi tersebut dapat berupa sanksi pidana penjara, sanksi pidana denda, serta pengucilan dan juga sanksi social.

Unsur khusus yang menjadi pertimbangan dalam pencurian data pribadi byaitu :

1. Baligh
2. Berakal
3. Memiliki niatan merugikan pengguna
4. Melakukan tindak kejahatan dengan sengaja

Dan terdapat unsur umum yakni meliputi unsur formil (Nash atau Undang-undang), unsur moril (pelaku adalah mualaf), serta unsur materiil (sifat melawan hukum).

Maka dari penjelasan diatas mengenai pencurian data pribadi adalah dijatuhi hukuman takzir dikarenakan unsur tindak pidana pencurian tidak terpenuhi yakni tidak memenuhi syarat barang yang telah dicuri. Maka sanksi yang sesuai yakni sanksi kurungan atau denda kepada pelaku.

D. Simpulan

Jejaring social online adalah jenis layanan online yang menciptakan jaringan virtual untuk orang-orang dengan minat, latar belakang, dan aktivitas yang sama. Jejaring social online akan sangat berguna bagi penggunanya dikarenakan dapat menghilangkan Batasan finansial

dan geografis serta memiliki manfaat yakni guna mencapai suatu tujuan yang hendak dicapai. Sehubungan dengan akses mencari pekerjaan, informasi tentang hiburan dan juga pendidikan. Bagi penggunaan jejaring social online mendorong pengungkapan informasi pribadi (usia, orientasi seksual ataupun politik, tanggal lahir, dan pembelian barang).

Dengan berkembangnya jejaring social online saat ini, muncul juga masalah terkait menjaga data yang bersifat privasi serta menjaga keamanan para pengguna jejaring sosial, terutama Ketika seseorang hendak mengunggah atau membagikan konten dalam konteks multimedia seperti halnya membagikan foto, video, dan juga suara. Henson dkk, juga memberikan penawaran akan kemampuan guna tidak hanya dengan menggunakan fitur security serta privasi dan kriteria pemindaian yang selektif yakni guna memutuskan siapa saja yang dapat memiliki akses untuk melihat ke situs website yang dimiliki, paling utamanya diperuntukan bagi informasi yang memiliki sifat sensitif.

Boyd menjelaskan bahwasannya informasi tersebut tidak memiliki sifat pribadi dikarenakan tidak ada pihak yang mengetahuinya sebab individulah yang menentukan Batasan sekaligus mengontrolnya. Boyd juga menegaskan bahwasannya ada wilayah abu-abu yang sangat berpeluang diantara rahasia serta informasi yang harus dibagikan secara terbuka.

Dengan maksud lain yakni, pilar utama guna memberi batasan antara privasi dan mobilitas terkait dengan ancaman data pribadi dikomunitas online ialah diri sendiri, oleh karena itu selain menggunakan fitur privasi yang telah ditawarkan oleh berbagai oknum di jejaring social online, kita harus memahami bahwasannya ini saja tidak cukup. Pikir mereka yakni ketika kita hendak mengunjungi halaman Facebook milik seseorang, kita bisa mendapatkan informasi yang kontekstual. Maka guna menghindari adanya hal tersebut diperlukan perlindungan diri sekaligus dalam hal ini suatu keterampilan pada literasi memiliki tujuan agar mereka dapat peka terhadap hal-hal privasi di jejaring social online yang mereka miliki.

DAFTARPUSTAKA

Baruh, L., & Popescu, M. (2017). *Big Data Analytics and the Limits of Privacy Self-Management.* RetrievedApril3,2018,fromNewMedia&Society,Vol.19(4)579-596:

Boyd, D. (2008). *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence.* RetrievedApril 3, 2018, from The Internasional Journal of Research into New Media Technologies. Volume: 14issue:1, page(s):13-20:https://doi.org/10.1177/1354856507084416

Brennen, B., & Primeaux, D. (1997). *Public or Private? E-mail and he Ethics of Privacy.* Retrieved April 3,2018, from THe International Journal of REaserach into New Meda Technologies. Volume: 3 issue: 3,page(s):22-26:https://doi.org/10.1177/135485659700300304

Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A., & Rong, X. (2015). *Data Mining for the Internet ofThings: Literature Review and Challenges.*Retrieved April 3, 2018, from International Journal ofDistributedSensorNetwork,Volume:11 issue:8:https://doi.org/10.1155/2015/431047

Francis,C.,&Baldesari.(2006).*SystematicReviewsofQualitativeLiterature.* Oxford:UKCochraneCentre.

Frith, J. (2017). *Big Data, Technical Communication, and The Smart City.* Retrieved April 3, 2018, fromJournalofBusinessandTechnicalCommunication,Vol.3(2)168-187:http:www.doi.org/10.1177/1050651916682285

Guo, L. (2016). *Big Social Data Analytics in Journalism and Mass Communication: Comparing DictionaryBased-Text Analysis and Unsupervised Topic Modelling.* Retrieved April 3, 2018, from Journalism &MassCommunicationQuarterly,Volume:93issue:2,page(s):332-359:https://doi.org/10.1177/1077699016639231

Henson,B.,Reyns,B.,&Fisher,B.(2011).*Securityinthe21stCentury:ExaminingtheLinkBetweenOnline Social Network Activity, Privacy, and Interpersonal Victimization.* Retrieved April 2, 2018, fromCriticalJusticeReview,Volume36(3),253-268:8, from Critical Justice Review, Volume 36 (3), 253-268: http://www.doi.org/10.1177/0734016811399421

Kayes, I., & Iamnitchi, A. (2017). *Privacy and Security in Online Social Network.* Retrieved April 3, 2018,fromOnlineSocialNetworkand Media,3(4),1-21:https://doi.org/10.1016/j.osnem.2017.09.001

Kennedy, H., Elgesem, D., & Miguel, C. (2017). *On Fairness: User Perspectives on Social Media DataMining*.RetrievedApril3,2018,fromTheInternationalJournalofResearchintoNewMediaTechnologies,Volume:23issue:3,page(s):270-288:https://doi.org/10.1177/1354856515592507

Kitchin,R.,&McArdie,G.(2016).*WhatmakesBigData,BigData?Exploringtheontologicalcharacteristics of 26 datasets.* Retrieved April 3, 2018, from Big Data & Society, Volume: 3 issue: 1:https://doi.org/10.1177/2053951716631130

Lewin,S.(2008).*MethodstoSynthesisQualitativeEvidenceAlongside aCochraneInterventionReview.* London: LondonSchoolofHygiene andTropicalMedicine.

Liang, H., Shen, F., & Fu, K.-w. (2017). *Privacy Protection and Self-Disclosure Across Societies: A Study ofGlobal Twitter Users.* Retrieved April 2, 2018, from New Media & Society, Vol 19(9), http://www.doi.org/10.1177/1461444816642210

Milham,M.,&Atkin,D.(2018).*ManagingtheVirtualBoundaries:OnlineSocialNetworks, Disclosure,and Privacy Behaviours.* Retrieved April 2, 2018, from New Media & Society, Volume 20(1), 50-67:http://www.doi.org/10.1177/146144816654465

Perry, A., & Hammond, N. (2002). Systematic Review: The Experience of a PhD Student. *PsychologyLearning andTeaching, 2(1)*, 32-35.

Rathore, S., Sharma, P., Loia, V., Jeong, Y.-S., & Park, J.-H. (2017). *Social Network Security: Issues,Challenges,Threats,andSolutions.*RetrievedApril3,2018,fromInformatio nSciences,421(2017), 43-69:43-69: https://doi.org/10.1016/j.ins.2017.08.063