ANCAMAN PRIVASI DAN DATA MINING DI ERA DIGITAL: ANALISIS META-SINTESIS PADA *SOCIAL NETWORKING SITES* (SNS)

THREAT ON PRIVACY AND DATA MINING IN DIGITAL ERA: A META-SYNTHESIS ANALYSIS ON SOCIAL NETWORKING SITES (SNS)

Vannyora Okditazeini[1], Irwansyah[2]
[1]Program Pascasarjana Ilmu Komunikasi, Departemen Ilmu Komunikasi Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Indonesia, Kampus Salemba, Jakarta Pusat, Indonesia
[2] Departemen Ilmu Komunikasi, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Indonesia, Kampus Salemba, Jakarta Pusat, Indonesia
[1]vannyora2013@gmail.com; [2]irwansyah@ui.ac.id

Diterima tgl. 09/03/2018; Direvisi tgl. 04/10/2018; Disetujui tgl. 17/10/2018

ABSTRACT

This paper will elaborate how the threats to privacy and data mining on SNS (Social Networking Sites / Online Social Networking). By first exposing the concept of privacy and data mining itself in the big data industry nowaday, the authors offer a meta-synthesis analysis to conduct the research. Various references and literature studies were conducted to find data relevant to the issue of privacy threats and data mining on the SNS. The conceptual elaboration results found that the threat of privacy and data mining on SNS can be categorized into three things: threats of multimedia content, traditional threats, and social threats. Each category is clustered into several types of threats. The authors identify in addition to utilizing the privacy features that have been provided by the SNS site, the user must also as early as possible literated theirself to distinguish information and secrets. Users should be aware in selecting what content should be disseminated in the SNS and which are not.
Keywords: *Privacy*, *Data Mining*, SNS, *Big Data*

ABSTRAK

Tulisan ini akan mengelaborasi bagaimana ancaman terhadap privasi dan *data mining* di SNS (*Social Networking Sites*/Jejaring Sosial Online). Dengan lebih dahulu memaparkan konsep atas privasi dan *data mining* itu sendiri dalam industri *big data* saat ini, penulis menawarkan analisis meta-sintesis. Berbagai referensi dan studi literatur dilakukan untuk mencari data yang relevan dengan isu ancaman privasi dan *data mining* pada SNS. Hasil elaborasi konseptual peneliti menemukan bahwa ancaman privasi dan *data mining* pada SNS dapat dikategorikan dalam tiga hal: ancaman konten multimedia, ancaman tradisional, dan ancaman sosial. Setiap kategori diklasterisasikan ke dalam beberapa tipe ancaman. Penulis mengidentifikasi selain dengan memanfaatkan fitur privasi yang telah disediakan oleh situs SNS, pengguna sendiri juga harus sedini mungkin meliterasi dirinya untuk membedakan informasi dan rahasia. Pengguna harus sadar dalam menyeleksi konten apa yang harus disebarkan di SNS dan mana yang tidak.

Kata Kunci: Privasi, *Data Mining*, SNS, *Big Data*

1. PENDAHULUAN

Jejaring sosial online (*Social Networking Sites*/SNS) menjadi hal yang tak dapat dipisahkan dari kehidupan sosial masyarakat saat ini. Tentunya hal ini tidak terlepas dari kemajuan teknologi yang menginvasi corak dan pola interaksi masyarakat. Ditambah dengan teknologi baru yang semakin gencar mengembangkan inovasi-inovasi sehingga masyarakat secara tidak langsung harus mengikutinya. SNS menjadi sarana untuk mengatasi sebagian besar permasalahan di berbagai bidang, baik itu komunikasi, birokrasi, hiburan, pendidikan, dan lain-lain. Dengan bawaan sifatnya yang cepat, mudah, dan dengan biaya yang murah, media sosial menjadi alternatif untuk tetap berhubungan dengan orang lain.

SNS ini menjadi populer karena memfasilitasi pengguna untuk tetap bisa terhubung (*log in*) secara terus menerus sehingga para pengguna tersebut tetap dapat menerima pesan dari kolega dan

kerabat setiap harinya. Para pengguna bisa berhubungan dengan komunitas-komunitas virtual lainnya, baik itu dengan keluarga, teman, rekan kerja, dan bahkan dengan orang yang sama sekali tidak mereka kenal. Menurut Henson et.al, dalam beberapa dekade terakhir SNS telah berevolusi dari dunia baru yang menghibur menjadi industri global bernilai miliaran dolar, dengan pengguna dari berbagai kalangan (Henson, Reyns, & Fisher, 2011, p. 253). Sehingga, hal ini memunculkan industri baru dalam SNS.

Penggunaan SNS mendorong seseorang untuk mengungkapkan informasi pribadinya (misalnya usia, orientasi seksual atau politik, tanggal lahir, pembelian suatu barang, dan lain-lain) (Milham & Atkin, 2018, p. 55). Tentunya pengungkapan informasi pribadi ini penuh dengan resiko. Seperti penelitian yang dilakukan Clemens et.al (2015) (dalam Milham & Atkin, 2018, p. 57), bahwa pengungkapan informasi ini dicurigai dapat mengakibatkan pencurian identitas ataupun sanksi di sekolah atau tempat kerja karena mengangkat suatu isu yang sensitif. Dalam penelitiannya, Henson et. al menunjukkan hasil bahwa sekitar 42% pengguna mahasiswa SNS mengalami beberapa bentuk ancaman privasi selama hidup mereka, ini menjadi masalah penting yang membutuhkan perhatian lebih lanjut (Henson, Reyns, & Fisher, 2011, p. 267).

Social Networking Sites (SNS) merupakan jenis jasa web untuk membangun jaringan virtual diantara orang yang memiliki kesamaan minat, latar belakang dan aktivitas (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 43). SNS dapat sangat bermanfaat bagi penggunanya karena menghilangkan batas ekonomi dan geografi, dan juga dapat berguna dalam mencapai tujuan yang berkaitan dengan pencarian kerja, hiburan dan pendidikan. Namun, Rathore et.al (2017) mengidentifikasi kepopuleran SNS tersebut juga menciptakan resiko yang tinggi bagi penggunanya. Ketika sejumlah data pribadi dibagikan dalam SNS menjadikan pengguna target yang menggoda untuk diserang, seperti spam, malware, socialbots dan pencurian identitas. Bahkan penyerang dapat juga menemukan data signifikan lain, seperti informasi akun bank, yang kemudian digunakan untuk kejahatan seperti penipuan, kemudian identitas pribadi dan lokasi (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 44).

Tulisan ini akan mengelaborasi bagaimana ancaman terhadap privasi dan *data mining* di SNS. Dengan lebih dahulu memaparkan konsep atas privasi dan *data mining* itu sendiri dalam industri *big data* saat ini, penulis menawarkan paparan konseptual. Berbagai referensi dan studi literatur dilakukan untuk mencari data yang relevan dengan isu ancaman privasi dan *data mining* pada SNS. Berdasarkan latar belakang yang sudah dipaparkan, penulis membatasi permasalahan pada hal-hal berikut:

1) Bagaimana ancaman privasi dan *data mining* di jejaring sosial online (SNS); dan
2) Bagaimana konseptualisasi ancaman terhadap privasi dan *data mining* di industri digital?

2. METODE PENELITIAN

Tulisan ini merupakan tulisan konseptual yang mengadaptasi pedoman meta-sintesis dari Francis dan Baldesari dengan pendekatan meta-agregasi kualitatif. Pendekatan kualitatif dalam meta-sintesis digunakan untuk mensintesis (merangkum) hasil-hasil penelitian yang bersifat deskriptif kualitatif. Metode mensintesis (merangkum) hasil-hasil penelitian kualitatif ini disebut dengan "meta-sintesis". Secara definisi, meta-sintesis adalah teknik melakukan integrasi data untuk mendapatkan teori maupun konsep baru atau tingkat pemahaman yang lebih mendalam dan menyeluruh (Perry & Hammond, 2002, p. 34).

Dalam melakukan meta-sintesis (sintesis data kualitatif) terdapat 2 (dua) pendekatan, yakni meta-agregasi (*meta-aggregation*) dan meta-etnografi (*meta-ethnography*) (Lewin, 2008, p. 189). Pada meta-agregasi, sintesis bertujuan untuk menjawab pertanyaan penelitian (*review question*) dengan cara merangkum berbagai hasil penelitian (*summarizing*). Sementara, meta-etnografi,

sintesis bertujuan untuk mengembangkan teori baru (*new theory*) dalam rangka melengkapi teori yang sudah ada.

Pada meta-agregasi topik penelitian dielaborasi menjadi tema-tema tertentu untuk menghasilkan kerangka analisis (*conceptual framework*). Kemudian, dalam tema-tema tertentu tersebut dilakukan pencarian artikel hasil penelitian yang relevan dan dibandingkan dan dirangkum antar yang satu dengan yang lainnya. Pada pendekatan meta-agregasi, hasil sintesis merupakan "agregat" dari berbagai hasil penelitian sesuai dengan tema yang relevan.

Francis dan Baldesari mengidentifikasi langkah-langkah dalam melakukan meta-sintesis (Francis & Baldesari, 2006, p. 92):

1) Memformulasikan pertanyaan penelitian (*formulating the review question*)
   Fokus dari kajian ini adalah untuk mengetahui bagaimana ancaman privasi dan *data mining* pada *Social Networking Sites* (SNS). Untuk itu dirancang beberapa pertanyaan yang ingin diperoleh jawabannya dari hasil kajian literatur ini.
   Pertanyaan 1 (Q1) : Di forum publikasi apa pembahasan mengenai privasi dan *data mining* diterbitkan?
   Pertanyaan 2 (Q2) : Apa saja permasalahan/isu yang ditemukan dalam penelitian yang ada?
   Pertanyaan 3 (Q3) : Bagaimana kontribusi masing-masing konsep pada pengintegrasian SNS?
2) Melakukan pencairan literatur (*conducting a systematic literature search*)
   Pada kajian literatur ini sumber data yang akan digunakan adalah makalah yang tersedia pada halaman website SAGE (https://www.journals.sagepub.com). Semakin banyak sumber data yang digunakan maka kemungkinan untuk menemukan literatur yang sesuai juga semakin besar. Strategi dalam melakukan pencarian dibangun melalui penentuan kata kunci dan sinonim dari fokus kajian.
3) Melakukan *screening* dan seleksi artikel penelitian yang cocok (*screening and selecting appropiate research articles*)
   Penerapan pencarian tersebut berkemungkinan menghasilkan jumlah makalah yang cukup banyak. Oleh karena itu, identifikasi lebih lanjut diperlukan untuk memperoleh makalah yang dapat dijadikan studi primer. Identifikasi dapat dilakukan dengan menerapkan kriteria inklusi dan eksklusi. Penerapan kriteria inklusi dan eksklusi ini akan menjamin bahwa makalah yang digunakan adalah makalah yang benar-benar sesuai dengan konteks kajian.
   a) Kriteria Inklusi
      - Makalah yang menjelaskan konsep, manfaat, teknik, metode, strategi, dan segala sesuatu dalam penerapan privasi dan *data mining* pada SNS secara bersamaan
      - Makalah yang disajikan dalam Bahasa Inggris.

   b) Kriteria Eksklusi
      - Makalah yang hanya fokus pada pembahasan privasi di SNS saja
      - Makalah yang hanya fokus pada pembahasan *data mining* di SNS saja
      - Makalah yang fokus pada pembahasan privasi di SNS dengan disiplin konsep selain *data mining*
      - Makalah yang fokus pada pembahasan *data mining* di SNS dengan disiplin konsep selain privasi
4) Melakukan analisis dan sintesis temuan-temuan kualitatif (*analyzing and synthesizing qualitative findings*)
   Prosedur pemilihan makalah dilakukan dengan teknik membaca cepat seluruh kandidat studi primer. Membaca cepat yaitu membaca bagian abstraksi dari makalah yang tersedia. Selanjutnya berdasarkan kriteria inklusi dan eksklusi yang dibuat maka dapat ditentukan apakah makalah tersebut dapat dijadikan studi primer.
5) Memberlakukan kendali mutu (*maintaining quality control*)

Berdasarkan perencanaan review yang telah disusun, langkah selanjutnya adalah mengeksekusi rencana tersebut. Eksekusi pencarian pada halaman website yang dijadikan sumber data menghasilkan 151 makalah yang merupakan kandidat studi primer.

6) Menyusun laporan akhir (*presenting findings*)
Selanjutnya diterapkan kriteria inklusi dan eksklusi dengan cara membaca bagian abstraksi dari seluruh kandidat studi primer. Penerapan kriteria inklusi dan eksklusi menghasilkan sebanyak 13 makalah studi primer yang sesuai dengan kriteria yang dimaksud sebagaimana 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, B., & 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., & Popescu, M Kayes, I., & Iamnitchi, 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., & Atkin, D.

3. HASIL DAN PEMBAHASAN

3.1. Kerangka Konseptual

3.1.1 Definisi Operasional

a) Privasi

Sissela Bok mendefinisikan privasi sebagai ranah dimana masalah pribadi dan kebebasan tidak dirusak (Brennen & Primeaux, 1997, p. 23). Dari sudut pandang hukum, pengadilan telah memutuskan bahwa hak atas privasi adalah aspek mendasar dari budaya Barat. Di Amerika Serikat, Samuel Warren dan Louis D. Brandeis pertama-tama mengonsep privasi sebagai perumusan hukum dalam esainya tahun 1899: 'The Right to Privacy'. Dengan demikian, hukum privasi fokus pada 'pelarangan terhadap gangguan yang mendalam pada martabat manusia oleh mereka yang memiliki kekuatan ekonomi atau pemerintahan' (Brennen & Primeaux, 1997, p. 24).

Wolak et al. (2008) meneliti hubungan antara interaksi online / kegiatan dan inisiasi yang merugikan privasi seseorang di Internet (Henson, Reyns, & Fisher, 2011, p. 255). Mereka menyimpulkan bahwa memposting informasi pribadi atau menggunakan SNS tidak dengan sendirinya berisiko perilaku, tetapi berinteraksi dengan orang yang tidak dikenal dan memiliki orang yang tidak dikenal di daftar teman membuat remaja rentan terhadap ancaman privasi di SNS. Tampaknya dengan siapa pengguna berbagi informasi sensitif lebih penting dalam mencegah ancaman privasi online daripada mengatur profil seseorang ke akses pribadi, baik di kalangan pemuda dan mahasiswa.

Hasil penelitian yang dilakukan Milham dan Atkin (2018) mengkonfirmasi dan memperluas eksplorasi historis dari hubungan antara sikap privasi dan perilaku pengungkapan identitas pribadi, terutama di antara pengguna yang menempatkan perhatian lebih besar pada informasi pribadi mereka dan merasa protektif terhadapnya. Temuan Milham dan Atkin ini sejalan dengan penelitian sebelumnya yang dilakukan oleh Child et.al (2011) (dalam Milham & Atkin, 2018, p. 65) tentang pengungkapan informasi pribadi ke publik. Hasil penelitian Child et.al mengkonfirmasi bahwa pengguna yang menitikberatkan perhatian lebih besar untuk masalah privasi, cenderung tidak

banyak yang menjadi korban penyalahgunaan pada SNS. Desain situs web yang sangat interaktif saat ini mendorong *oversharing* informasi pribadi yang tidak disadari, salah satu yang dikhawatirkan oleh pengguna SNS.

Privasi adalah fenomena spesifik budaya (Liang, Shen, & Fu, 2017, p. 1475). Ketika platform SNS menjadi global, pertanyaan mengenai praktik privasi dalam konteks lintas budaya menjadi semakin penting. Sebuah penelitian dari Liang et.al (2017) menguji variasi budaya pengaturan profil dalam privasi dan keterbukaan diri melalui fasilitas geolokasi di Twitter (Liang, Shen, & Fu, 2017, p. 1476). Liang et.al secara acak memilih 3,3 juta akun Twitter dari lebih dari 100 kelompok demografi masyarakat. Hasil penelitiannya mengungkapkan perbedaan budaya dan masyarakat yang cukup besar dalam mempengaruhi perilaku pengguna SNS dalam menggunakan pengaturan privasi di akunnya. Pengaturan privasi dalam masyarakat yang kolektif lebih efektif dalam mendorong keterbukaan diri, dan tampaknya kurang penting bagi pengguna dalam masyarakat yang coraknya individualistis. Penetrasi internet juga merupakan faktor signifikan dalam memprediksi baik adopsi pengaturan privasi dan geolokasi keterbukaan diri.

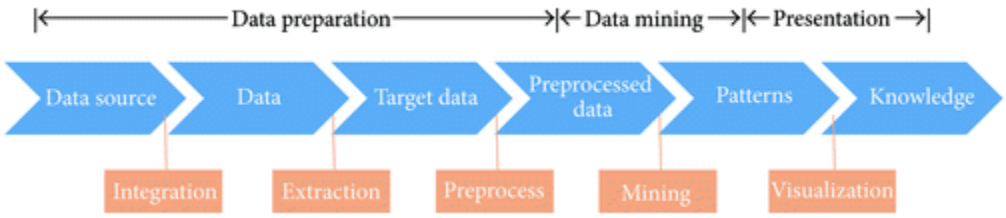
Dengan difusi teknologi internet, privasi online menjadi masalah utama yang dihadapi semua pengguna Internet. Kebocoran informasi pribadi yang tidak disengaja dapat menyebabkan serangkaian konsekuensi negatif seperti penyalahgunaan akun, email yang tidak diminta atau panggilan telepon, atau bahkan kerugian finansial. Banyak pengguna SNS menyatakan keprihatinan serius tentang kebocoran informasi pribadi secara online. Namun, menurut Rainie dan Madden (2015) (dalam Liang, Shen, & Fu, 2017, p. 1477), hanya 30% dari semua orang dewasa AS telah mengambil langkah ini untuk melindungi privasi mereka secara online, seperti mengubah pengaturan privasi mereka di SNS.

Perbedaan sikap untuk mengubah peraturan privasi pada sejumlah pengguna terjadi karena cara bagaimana SNS digunakan saat ini; artinya, *cyberspace* didominasi oleh platform SNS (Liang, Shen, & Fu, 2017, p. 1478). Menurut Boyd (2008), praktik-praktik privasi di platform SNS sering paradoks. Di satu sisi, pengguna internet sering termotivasi untuk mengungkapkan informasi pribadi untuk menghadirkan identitas unik yang membedakan diri dari orang lain dan mengakumulasi modal sosial dalam SNS. Di sisi lain, perusahaan SNS mempertahankan sejumlah besar informasi pribadi yang dikumpulkan dari para penggunanya, dan informasi tersebut dapat dengan mudah disalahgunakan (Liang, Shen, & Fu, 2017, p. 1479).

Untuk membantu mengatasi dilema ini, hampir semua platform SNS populer memungkinkan pengguna untuk menyesuaikan pengaturan privasinya. Pengguna dapat membuat aturan deterministik yang menetapkan bagian konten mana yang akan dibagikan, dan kepada siapa konten tersebut dapat diakses. Menurut Stutzman et.al (2011), ketika mengendalikan privasi mereka, individu cenderung mengungkapkan informasi lebih lanjut (Liang, Shen, & Fu, 2017, p. 1479). Telah banyak Studi dilakukan untuk memahami perilaku perlindungan privasi pada platform media sosial (diantaranya Boyd dan Marwick, 2011; Madden et al., 2013; Stutzman et al., 2011; Stutzman dan Kramer-Duffield, 2010) (dalam Liang, Shen, & Fu, 2017, p. 1480).

b) Data Mining

Menurut Chen et.al, *data mining* adalah proses menemukan pengetahuan yang menarik dari sejumlah besar data yang disimpan baik dalam database, gudang data, atau repositori informasi lainnya (Chen, Deng, Wan, Zhang, Vasilakos, & Rong, 2015, p. 2). Berdasarkan definisi penambangan data dan definisi fungsi *data mining*, proses *data mining* yang umum meliputi langkah-langkah berikut:



Gambar 1: *Overview Data Mining*
(Chen, Deng, Wan, Zhang, Vasilakos, & Rong, 2015, p. 2)

Proses *data mining* berdasarkan *overview* dari Chen et.al dapat dijelaskan sebagai berikut (Chen, Deng, Wan, Zhang, Vasilakos, & Rong, 2015, p. 3):

1. Persiapan data: mempersiapkan data untuk *mining*. Hal ini mencakup 3 langkah mengintegrasikan data dalam berbagai sumber data dan membersihkan suara dari data. ekstrak beberapa bagian data ke dalam sistem *data mining*, pre-proses data untuk memfasilitasi *data mining*
2. *Data mining*: menerapkan algoritma ke data untuk menemukan pola dan mengevaluasi pola pengetahuan yang ditemukan
3. Presentasi data: memvisualisasikan data dan mewakili pengetahuan yang di-*mining* kepada pengguna

Kennedy et.al (2017) mengidentifikasi ketika penggunaan global SNS tumbuh, demikian juga dengan *data mining* di SNS (Kennedy, Elgesem, & Miguel, 2017, p. 270). Data SNS dapat dipahami sebagai apa yang dikatakan dan dibagikan di SNS, yang mengatakan dan membagikannya, dimana mereka berada, kepada siapa mereka terhubung, seberapa berpengaruh dan aktifnya mereka dan seperti apa pola aktivitas mereka sebelumnya (Kennedy, Elgesem, & Miguel, 2017, p. 271). *Data mining* ini mencakup berbagai kegiatan yang dilakukan untuk menganalisis, mengatur, mengklasifikasikan dan memahami data tersebut, mulai dari menghitung *like* dan berbagi konten hingga mengukur jangkauan, sentimen dan pemberi pengaruh utama, menggunakan teknik seperti analisis jaringan sosial, analisis jaringan masalah dan pemrosesan bahasa alami, dan lain-lain (Kennedy, Elgesem, & Miguel, 2017, p. 275).

Kennedy et.al juga mengkonfirmasi bahwa kenaikan *data mining* SNS telah didorong oleh sejumlah faktor: meningkatnya ketersediaan data pada pengguna dan perilaku online mereka, karena lebih banyak kegiatan sosial dilakukan secara online; penurunan biaya pengumpulan data, penyimpanan dan pemrosesan data; dan perluasan platform SNS dari mana banyak data ini diambil (Kennedy, Elgesem, & Miguel, 2017, p. 275). Data SNS yang *mining* sering digabungkan dengan data dari sumber lain, seperti pengungkapan Edward Snowden tentang operasi *data mining* dari National Security Agency di Amerika Serikat dan Kantor Pusat Komunikasi Pemerintah di Inggris Raya. Dalam penelitiannya, Hill (2012) juga menemukan kasus atas *data mining*, misalnya, dalam iklan bertarget, seperti kasus yang tersebar luas dari wanita muda yang ayahnya menjadi sadar bahwa dia hamil ketika sebuah department store online menargetkan iklan untuk produk-produk terkait kehamilan kepadanya sebagai hasil dari pelacakan perilaku online-nya (Kennedy, Elgesem, & Miguel, 2017, p. 276). Kejadian sehari-hari ini layak dipelajari sebagai bentuk *data mining* yang harus lebih diperhatikan.

Hasil penelitian Kennedy et.al (2017) memperlihatkan bahwa pengguna SNS tersebut banyak yang merasakan ketidakadilan atas data personal mereka yang diambil dari mereka. Menurutnya, ketidaknyamanan dari beberapa informan dengan apa yang platform SNS lakukan dengan informasi dan data mereka menunjukkan bahwa ada perbedaan antara praktik platform dan harapan normatif pengguna (Kennedy, Elgesem, & Miguel, 2017, p. 279). Pertimbangan peserta tentang

bagaimana untuk memastikan transparansi yang lebih besar dalam kaitannya dengan praktik *data mining*, pada gilirannya, tampaknya menunjukkan minat di antara pengguna SNS dalam kemungkinan dunia SNS yang lebih adil.

c) Big Data

Istilah "big data" telah menjadi salah satu hal yang paling banyak diperbincangkan beberapa dekade belakangan ini (Baruh & Popescu, 2017, p. 579). Menurut situs Wikibon (2014), perkiraan nilai pasar *big data* sebesar US $ 50,1 miliar pada tahun 2015 (Baruh & Popescu, 2017, p. 580). Ekspansi yang cepat dari pasar *big data* memberikan efek khususnya pada munculnya model publikasi dengan pola yang baru beserta penggunaannya di berbagai bidang yang berbeda seperti *human digital* dan prediksi pemilihan pada suatu kampanye pemilihan pemimpin. Penerapan masalah big data yang sudah merambah ke berbagai area komersial menghasilkan perubahan besar dalam industri dengan dampak langsung atas kehidupan manusia, seperti asuransi, perawatan kesehatan, atau perbankan, dan lain-lain.

Big data adalah istilah luas yang digunakan untuk kumpulan data yang memiliki ukuran (misalnya, dimensi, volume, dan kecepatan) serta kompleksitas (misalnya keragaman, variabilitas) yang melebihi kemampuan alat yang digunakan secara tradisional untuk menangkap, memproses dan menganalisa data dalam kerangka waktu yang dapat ditolerir (Guo, 2016, p. 333). Dalam ilmu sosial, "*big data*" mengacu pada kumpulan data yang terlalu besar bagi manusia untuk mengkode sampel yang representatif dari keseluruhan dataset (Guo, 2016, p. 334)

Penelitian yang dilakukan oleh Kitchin dan McArdie (2016), mengidentifikasi 7 (tujuh) karakteristik *big data* (Kitchin & McArdie, 2016, p. 3):

1. Keluwesan (keseluruhan sistem data)
2. Berjaringan halus (mempunyai resolusi yang kecil) dan unik (antara satu data dan data lain berbeda, terutama ditandai dengan URL)
3. Relasionalitas (bisa digeneralisasikan dan memungkinkan untuk digabung dari dataset yang berbeda)
4. Ekstensionalitas (dapat menambah / mengubah bidang baru dengan mudah) dan skalabilitas (dapat meluas dalam ukuran dengan cepat)
5. Kebenaran (data bisa amburadul, *crowd* serta mengandung ketidakpastian dan kesalahan)
6. Nilai (banyak wawasan yang dapat diekstraksi dan data dialihkan)
7. Variabilitas (data yang artinya dapat secara konstan berubah dalam kaitannya dengan konteks di mana mereka dihasilkan)

Frith (2017) mengelaborasi penyebaran big data dalam melihat pertumbuhan kota pintar (*smart city*). Istilah kota pintar mengacu pada penggunaan teknologi digital untuk menghasilkan data yang dapat meningkatkan efisiensi kota, kelayakan hidup warga, dan meningkatkan keselamatan warga (Frith, 2017, p. 169). Dalam artikel ini Frith menggunakan frasa kota pintar untuk merujuk ke proyek perkotaan berbasis data di kota-kota. Contoh dari penerapan big data pada kota pintar adalah penggunaan moda trasnportasi yang sudah canggih, teknologi untuk mendeteksi dan mitigasi bencana, penggunaan uang elektronik, dan lain-lain.

d) Konseptualisasi Ancaman Privasi dan Data Mining

Ancaman terhadap privasi dan *data mining* dikonseptualisasikan secara komprehensif oleh Shailendra Rathore, Pradip Kumar Sharma, Vincenzo Loia, Yong-Sik Jeong, dan Jong Hyung Park pada tahun 2017 dalam tulisan mereka *Social Network Security: Challenges, Threats, and Solutions*. Menurut Rathore et.al, dalam kaitannya dengan ancaman privasi dan *data mining,* terdapat beberapa kategori ancaman, diantaranya (Rathore, Sharma, Loia, Jeong, & Park, 2017, pp. 53-54):

1. Ancaman Terhadap Konten Multimedia

   Tipe ancaman yang terjadi dalam kategori ini adalah:

   - Paparan konten multimedia.

- Kepemilikan bersama.
- Manipulasi konten.
- *Steganografi*. Adalah istilah yang digunakan untuk kegiatan yang menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui.
- Metadata.
- Link yang dibagi bersama.
- Transparansi data.
- *Tagging*.

2. Ancaman Tradisional
   - *Phishing*, yaitu tindakan memperoleh informasi pribadi seperti User ID, Password, dan data-data sensitif lainnya dengan menyamar sebagai orang atau organisasi yang berwenang melalui sebuah email.
   - *Malware (Malicious Software)*, yaitu suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer. Malware mencakup virus, *worm*, *trojan horse*, sebagian besar *rootkit*, *spyware*, *adware* yang tidak jujur, serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna PC.
   - Serangan *Sybil* dan profil palsu, yaitu kegiatan dengan menggunakan akun palsu untuk mengancam keamanan pengguna komputer.
   - *Spamming*, yaitu kegiatan mengirim email palsu dengan memanfaatkan server email yang memiliki "smtp *open relay*" atau pengiriman informasi atau iklan suatu produk yang tidak pada tempatnya dan hal ini sangat mengganggu bagi yang dikirim.
   - Serangan de-anonimisasi, yaitu strategi pada *data mining* dimana data yang tidak dikenal (anonim) dirujuk dengan sumber data lain untuk mengidentifikasi sumber data anonim.
   - Serangan kloning profil, yaitu istilah yang digunakan untuk pemalsuan suatu profil/identitas untuk mengecoh seseorang.
3. Ancaman Sosial
   - *Cyber-bullying*, yaitu segala bentuk kekerasan yang dialami anak atau remaja dan dilakukan oleh teman seusia mereka melalui internet.
   - *Cyber-stalking*, yaitu kejahatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan email, dan dilakukan berulang-ulang.

3.1. Analisis dan Diskusi

Berbagai penelitian tentang analisis *big data* mengidentifikasi sejumlah kasus yang berpotensi berbahaya bagi pengguna. Menurut penelitian yang dilakukan oleh Dixon dan Gellman (2014), ketersediaan basis data konsumen yang besar telah menghasilkan industri yang berkembang dari skor konsumen yang tidak diatur (Baruh & Popescu, 2017, p. 581). Pasquale (2015) mengidentifikasi bahwa logika penyebaran data pengguna ini berdasarkan pada logika algoritma yang bisa memprediksi segala data yang masuk dari basis data lintas-konteks yang semakin masif, menyortir individu ke dalam segmen di berbagai bidang yang beragam seperti pekerjaan, penyewaan, atau ritel (Baruh & Popescu, 2017, p. 582). Oleh karena itu, di luar aspek teknis pemrosesan data besar dan aplikasi praktisnya, menurut Andrejevic (2013), *big data* tampaknya menghasilkan organisasi sosial pengetahuan baru yang menormalkan iklim hilangnya privasi saat mereproduksi atau bahkan menonjolkan ketidaksetaraan yang ada (Baruh & Popescu, 2017, p. 583).

Gavinson (1980) memperkenalkan istilah otonomi individu, bahwa privasi seharusnya melindungi kekuatan individu atas bagaimana menentukan nasib sendiri dan, paling tidak,

kapasitas individu untuk definisi diri (Baruh & Popescu, 2017, p. 584). Dalam lingkungan pengumpulan data, diskusi privasi dipersulit oleh dugaan kesulitan mendefinisikan pelanggaran privasi pada individu. Menurut Solove (2013), berbagai upaya dalam beberapa tahun terakhir dilakukan untuk memperbarui perlindungan privasi atas dugaan pengumpulan data digital, sambil mempertahankan strategi literasi yang mengasumsikan pengguna yang sadar akan privasi (Baruh & Popescu, 2017, p. 584).

Dengan berkembangnya SNS saat ini, isu terkait bagaimana menjaga privasi dan keamanan dari pengguna juga mulai mencuat terutama ketika pengguna mengunggah konten multimedia seperti foto, video dan audio. Henson et.al juga mengidentifikasi bahwa dengan banyaknya pengguna *online* saat ini juga menumbuhkan ancaman *online* di situs SNS (Henson, Reyns, & Fisher, 2011, p. 254). Hal ini bisa diatasi individu dengan membuat 'perlindungan diri' dengan menggunakan fitur-fitur privasi dari SNS yang ada. Karena pada akhirnya, perlindungan tersebut untuk lapis pertama memang harus dilakukan oleh pengguna sendiri.

Menurut Harris (2014), keamanan jaringan adalah penyensoran terhadap jaringan/konten-konten yang dilarang di *online,* yang diproses secara terorganisir dan diimplementasikan melalui kontrol vertikal (Kayes & Iamnitchi, 2017, p. 5). SNS telah menjadi fenomena budaya *mainstream* bagi jutaan pengguna internet. Menggabungkan profil yang dibuat pengguna dengan mekanisme komunikasi yang memungkinkan pengguna menjadi berhubungan secara pseudo-permanen, SNS memanfaatkan hubungan sosial dunia nyata pengguna dan memadukan lebih banyak lagi kehidupan online dan offline pengguna. Pada 2017, Facebook memiliki 1,94 miliar pengguna aktif bulanan dan ini adalah situs ketiga yang paling banyak dikunjungi di Internet (Kayes & Iamnitchi, 2017, p. 7). Twitter, *platform micro-blogging* sosial, mengklaim lebih dari 313 juta pengguna aktif bulanan, yang mengirim *Tweets* dalam lebih dari 40 bahasa

Karena pengguna di SNS biasanya terhubung dengan teman, keluarga, dan kenalan, persepsi umum yang kemudian muncul adalah bahwa SNS menyediakan lingkungan yang diperantarai Internet yang lebih aman, pribadi, dan terpercaya untuk interaksi online. Namun dalam kenyataannya, SNS telah meningkatkan taruhan untuk perlindungan privasi karena ketersediaan jumlah data pengguna pribadi yang di luar ekspektasi, baik yang dipublikasikan ataupun tidak. Lebih penting lagi, SNS mengekspos informasi dari berbagai bidang sosial - misalnya, informasi pribadi di Facebook dan aktivitas profesional di LinkedIn - yang terkumpul dan mengarah ke profil yang lebih terperinci.

Pengungkapan informasi pengguna yang tidak diinginkan ini menyebabkan SNS jadi punya konsekuensi yang mengerikan. Media berita meliput beberapa di antaranya, seperti kasus seorang guru yang dituntut karena memposting foto senapan, atau karyawan yang dipecat karena berkomentar tentang gajinya dibandingkan dengan bosnya (keduanya adalah kasus di Facebook). Lebih dari itu, SNS itu sendiri, baik secara sengaja (mis. Kontroversi Facebook Beacon) atau secara tidak sengaja (misalnya, mempublikasikan data sosial anonim yang digunakan untuk men-deanonimisasi) berkontribusi terhadap pelanggaran privasi pengguna. Selain itu, tingginya volume data pribadi, baik yang diungkapkan oleh pengguna atau karena kegagalan SNS untuk menyediakan alat privasi yang canggih, telah menarik berbagai organisasi (misalnya, GNIP – GNIP Inc. adalah perusahaan agregasi API media sosial yang menyediakan data dari lusinan situs media sosial melalui satu API) untuk menggabungkan dan menjual jejaring sosial pengguna terhadap datanya. Selain itu, sifat hubungan SNS yang terpercaya telah menjadi mekanisme yang efektif untuk menyebarkan *spam*, *malware*, dan serangan *phishing*. Entitas jahat meluncurkan berbagai serangan dengan membuat profil palsu, menggunakan kedok akun SNS yang dicuri yang dijual secara ilegal atau menyebarkan isu melalui *bot* (Kayes & Iamnitchi, 2017, p. 3)

Internet Security Threat Report (ISTR) menyebutkan bahwa peningkatan penggunaan SNS oleh peretas tidak bisa diabaikan (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 40). Di tahun 2015 layanan semacam itu berubah menjadi sumber *spam* dan *malware*, dan digunakan sebagai

cara untuk membuat uang ilegal di web. Dan di tahun 2016, SNS menjadi target utama dalam kejahatan pencurian identitas dan *spear pishing* (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 45).

Penelitian yang dilakukan oleh Rathore et.al (2017) mengonfirmasi beberapa solusi untuk mencegah ancaman tersebut. Diantaranya yaitu *watermarking*, *steganalysis* dan *digital oblivion* untuk melindungi pengguna SNS melawan ancaman terkait data multimedia. Selain itu juga ada solusi seperti *spam detection* dan *phishing detection* yang ditawarkan untuk mengatasi ancaman tradisional (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 46). Dan bahkan solusi keamanan *built-in* seperti mekanisme otentikasi dan pengaturan privasi, serta solusi komersial seperti minor monitor dan aplikasi perlindungan sosial juga digunakan untuk pengamanan dari kedua tipe ancaman dalam SNS.

Penelitian Gao, et al. mengkategorikan isu keamanan utama dalam SNS ke dalam empat kategori (1) isu privasi, (2) pemasaran viral, (3) struktur jaringan berdasarkan serangan dan (4) serangan *malware* (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 48). Jin et al. mempelajari perilaku pengguna SNS dari empat sudut pandang (1) perilaku *malicious*, (2) perilaku *mobile social*, (3) *traffic activity* dan (4) koneksi dan interaksi (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 48). Fire et al. membagi ancaman keamanan terkini menjadi empat kategori (a) ancaman klasik, (b) ancaman modern, (c) ancaman kombinasi dan (d) ancaman yang mentargetkan anak-anak (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 48).

Dengan tingginya penggunaan SNS, reputasi pengguna online juga meningkat melalui web. Reputasi pengguna mempengaruhi status dan kredibilitas pengguna di kehidupan nyata. SNS dapat merusak reputasi bisnis dan organisasi besar, misalnya dengan adanya postingan negatif dari pegawainya dapat merusak reputasi organisasi dan pegawai.

SNS juga digunakan oleh beberapa perusahaan besar untuk membentuk profil lengkap individu dengan tujuan untuk menjual produk dan merekam perilaku individu. Namun semuanya itu biasanya dilakukan tanpa izin individu yang bersangkutan. Selain itu berdasarkan penelitian Smith, 38% perusahaan menghabiskan lebih dari 20% anggaran iklan mereka pada SNS di tahun 2015, dengan facebook dan twitter paling banyak memajang iklan (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 49).

Rathore et.al kemudian mengkategorikan ancaman keamanan menjadi tiga kategori utama, yaitu (1) ancaman konten multimedia, data *sharing* menjadi fitur penting dalam SNS dimana mereka dapat membagikan foto, video, aktivitas, dan minat (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 50). Bahkan dengan kemajuan dalam teknik pengambilan multimedia, seperti estimasi lokasi, pengenalan wajah, pencarian web dan *geotagging*, meningkatkan adanya penyalahgunaan secara ilegal. Ancaman konten multimedia ini meliputi paparan konten multimedia, berbagi kepemilikan, manipulasi konten multimedia, steganografi, metadata (konten multimedia dalam SNS merupakan metadata karena mengandung begitu banyak data penting seperti identitas dan lokasi, contoh GPS), berbagi link konten multimedia, link statis, *outsourcing* dan transparansi data *center*, *video conference*, kemampuan *tagging link* dari data multimedia yang dibagikan, dan pengungkapan data secara ilegal. Kategori (2) ancaman tradisional, meliputi *pishing*, *malware*, serangan sybil dan profil palsu, *spamming*, *clickjacking*, serangan *deanonymization*, serangan *inference*, dan *profile cloning* (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 51). Kategori (3) ancaman sosial, meliputi *cyberbullying* dan *cybergrooming*, spionase perusahaan, dan *cyberstalking* (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 51).

Beberapa solusi yang ditawarkan oleh Rathore et.al (2017) dalam mengatasi masalah keamanan SNS diantaranya yaitu *watermarking*, *co-ownership*, *steganalysis*, *digital oblivion*, *storage encryption*, *metadata removal* and *analysis*, *malware detection*, *sybil defense* dan deteksi profil palsu, deteksi *pishing*, deteksi *spammer*, solusi komersial, solusi keamanan SNS *built-in* dan deteksi profile *cloning* (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 53).

Masalah keamanan dan privasi ini terus diproses untuk mencapai titik mapan dan dapat menanggulangi serangan –serangan keamanan dan privasi tersebut di dunia SNS. Diakui pula bahwa tanpa adanya dukungan legislatif, isu negatif ini hanya dapat diminimalisir dampaknya saja tanpa ada solusi menyeluruh. Henson et al. juga menawarkan alternatif untuk tidak hanya mengandalkan fitur keamanan yang dibangun di situs web jaringan, melainkan menggunakan fitur keamanan dan privasi bersama dengan kriteria pemindaian selektif dalam memutuskan siapa yang akan mengizinkan akses ke situs web mereka terutama dengan informasi yang sensitif (Henson, Reyns, & Fisher, 2011, p. 268).

Pendiri Facebook, Mark Zuckerberg pernah menyatakan argumentasinya ketika privasi ramai dipertanyakan di SNS, yang dalam hal ini adalah Facebook yang dibuatnya. Mark Zuckerberg telah berulang kali menyatakan bahwa tujuannya adalah untuk membantu orang berbagi informasi dengan lebih efisien (Boyd, 2008, p. 18). Dengan mengumpulkan informasi sosial dan menyiarkannya, News Feeds mengambil apa yang dapat diakses oleh orang dan menempatkannya pada hal yang sangat menjadi perhatian mereka. Zuckerberg mengklaim bahwa tidak ada privasi yang dikompromikan dalam prosesnya (Boyd, 2008, p. 18). Namun, Boyd menekankan, privasi adalah tentang bagaimana orang mengalami hubungan mereka dengan orang lain dan dengan informasi. Privasi adalah rasa kontrol atas informasi, konteks dimana berbagi terjadi, dan audiens yang dapat memperoleh akses (Boyd, 2008, p. 19).

Untuk itu, jika melihat dari argumen Boyd, informasi tidak bersifat pribadi karena tidak ada yang tahu, karena individu lah yang membuat batas dan kontrol terhadap hal tersebut. Boyd juga menekankan bahwa ada area abu-abu yang sangat besar antara rahasia dan informasi yang dimaksudkan untuk disiarkan kepada publik. Pengguna tidak mungkin memposting rahasia, tetapi mereka sering memposting informasi yang hanya relevan dalam konteks tertentu (Boyd, 2008, p. 20). Asumsinya adalah jika mengunjungi halaman Facebook seseorang, kita dapat mengakses informasi dalam konteks. Dengan kata lain, pilar utama untuk membatasi ruang dan gerak privasi dalam konteks ancaman terhadap privasi dan *data mining* di SNS adalah *diri kita sendiri*.

Dalam akhir penelitiannya mengenai privasi di Facebook, Boyd juga mengargumentasikan bahwa privasi bukan hak mutlak - ia adalah hak istimewa yang harus dilindungi secara sosial dan struktural agar selalu menjadi perhatian utama (Boyd, 2008, p. 19). Hal yang kemudian dipertanyakan apakah privasi masih ada atau tidak adalah sesuatu yang konteksnya sangat tergantung pada masyarakat. Apakah masyarakat memilih untuk memperhatikan hal ini atau tidak.

Mengacu atas konseptualisasi ancaman privasi dan *data mining* yang sudah dipaparkan Rathore et.al, dalam Tabel 1 berikut disajikan beberapa rangkuman beserta dampak dan praktik yang dapat mengancam privasi dan *data mining* di era digital.

Tabel 1. Rangkuman Ancaman Privasi dan *Data Mining* di Era Digital

No	Kategori Ancaman	Tipe Ancaman	Praktik	Dampak
1	Ancaman terhadap Konten Multimedia	Paparan konten multimedia	Dalam hal ini, ancaman terhadap paparan konten berhubungan dengan informasi sensitif seseorang, seperti nomor telepon atau alamat rumah	pembeberan informasi, kehilangan reputasi, kebocoran lokasi, kekerasan *cyber*, kehilangan keamanan
		Kepemilikan bersama	Informasi yang dibagikan untuk dikonsumsi secara bersama cenderung berhubungan dengan beberapa orang saja, namun tidak semua orang mengatur apakah informasi tersebut akan dibagikan kepada orang lain juga atau hanya untuk dikonsumsi pribadi saja	kehilangan pemilik konten
		Manipulasi konten	Pengguna yang tidak	*blakcmailing*, kehilangan

			bertanggungjawab banyak menggunakan informasi yang didapatkan dari SNS, semisal foto seseorang, untuk mengolok-olok ataupun mengancam orang tersebut dengan memanipulasi kontennya.	reputasi
		Steganografi	Penyebaran *memes* yang tidak benar di SNS merupakan praktik steganografi yang dapat mengancam privasi seseorang	pembeberan informasi
		Metadata	Kemampuan SNS untuk menyerap informasi dengan sangat banyak memungkinkan ancaman dalam penemuan lokasi sekarang ataupun ID seseorang.	kebocoran lokasi, *profiling*
		Link yang dibagi bersama	SNS mempunyai fitur untuk bisa berbagi link. Jika link tersebut dibagikan kepada orang lain secara simultan, hal ini bisa menimbulkan ancaman link tersebut bisa kehilangan sumber utamanya, sehingga sangat rentan untuk menyebarkan informasi yang dimanipulasi.	kehilangan pemilik informasi, *hoax*
		Transparansi data	Oleh karena data yang disebarkan di SNS tidak dienkripsi, maka praktik penyebaran informasi tanpa adanya otoritas yang jelas menjadi isu tersendiri dalam ancaman privasi dan *data mining*.	kebocoran informasi rahasia
		Tagging	Kegiatan yang menyebutkan data seseorang bisa mengancam privasi orang tersebut, terlebih jika orang tersebut tidak menginginkan apapun data dari dirinya diinformasikan ke publik.	kebocoran informasi, kehilangan reputasi
2	Ancaman Tradisional	*Phishing*	pengguna akan diarahkan pada sebuah alamat URL palsu dan akhirnya bisa tertipu dengan akun tersebut	kebocoran informasi rahasia
		Malware	pengguna diarahkan untuk mengakses suatu situs tertentu, yang ternyata merupakan situs yang dapat menyerap informasi rahasia pengguna	kebocoran informasi rahasia
		Serangan *sybil* dan profil palsu	pembuatan akun/identitas palsu	mencuri informasi rahasia pengguna
		Spamming	mengirimkan pesan yang dapat mengganggu pengguna	kehilangan reputasi
		Serangan de-anonimisasi	pengguna dapat diidentifikasi dengan informasi *cookies*-nya dan memetakan aktivitas seseorang	kebocoran identitas
		Serangan kloning profil	melakukan kloning atas identitas seseorang dengan tujuan tertentu	kehilangan reputasi
3	Ancaman sosial	*Cyber-bullying*	banyak anak-anak yang dipermalukan oleh temannya sendiri dan menyebarkannya di SNS	kekerasan *cyber*

	Cyber-talking	mencari informasi seseorang secara intens dan berulang, kemudian menggunakan informasi tersebut untuk mengancam ataupun melakukan teror	kekerasan *cyber*, *blackmailing*

Sumber: Olahan

4. PENUTUP

Social Network Sites (SNS) merupakan jenis jasa web untuk membangun jaringan virtual diantara orang yang memiliki kesamaan minat, latar belakang dan aktivitas (Rathore, Sharma, Loia, Jeong, & Park, 2017, p. 43). SNS dapat sangat bermanfaat bagi penggunanya karena menghilangkan batas ekonomi dan geografi, dan juga dapat berguna dalam mencapai tujuan yang berkaitan dengan pencarian kerja, hiburan dan pendidikan. Penggunaan SNS mendorong seseorang untuk mengungkapkan informasi pribadinya (misalnya usia, orientasi seksual atau politik, tanggal lahir, pembelian suatu barang, dan lain-lain) (Milham & Atkin, 2018, p. 55).

Dengan berkembangnya SNS saat ini, isu terkait bagaimana menjaga privasi dan keamanan dari pengguna juga mulai mencuat terutama ketika pengguna mengunggah konten multimedia seperti foto, video dan audio. Henson et,al juga menawarkan alternatif untuk tidak hanya mengandalkan fitur keamanan yang dibangun di situs web jaringan, melainkan menggunakan fitur keamanan dan privasi bersama dengan kriteria pemindaian selektif dalam memutuskan siapa yang akan mengizinkan akses ke situs web mereka terutama dengan informasi yang sensitif (Henson, Reyns, & Fisher, 2011, p. 268).

Boyd mengatakan bahwa informasi tidak bersifat pribadi karena tidak ada yang tahu, karena individu lah yang membuat batas dan kontrol terhadap hal tersebut. Boyd juga menekankan bahwa ada area abu-abu yang sangat besar antara rahasia dan informasi yang dimaksudkan untuk disiarkan sebagai publik mungkin. Pengguna tidak mungkin memposting rahasia, tetapi mereka sering memposting informasi yang hanya relevan dalam konteks tertentu (Boyd, 2008, p. 20). Dengan kata lain, pilar utama untuk membatasi ruang dan gerak privasi dalam konteks ancaman terhadap privasi dan *data mining* di SNS adalah *diri kita sendiri*.

Maka dari itu, selain dengan memanfaatkan fitur privasi yang telah ditawarkan oleh berbagai SNS, kita perlu menyadari bahwa itu saja tidak cukup. Asumsinya adalah jika mengunjungi halaman Facebook seseorang, kita dapat mengakses informasi dalam konteks. Sehingga, untuk menghindari hal-hal semacam ini, perlu proteksi diri sendiri dan dalam hal ini adalah literasi untuk peka terhadap privasi di SNS.

Artikel ini diharapkan dapat berkontribusi dalam kajian lebih lanjut mengenai ancaman privasi dan *data mining* di era digital yang lebih kompleks. Dengan pemaparan kategori-kategori, tipe, praktik, dan dampak ancaman privasi dan *data mining* sesuai dengan elaborasi konseptual yang dilakukan peneliti diharapkan juga dapat menjadi acuan untuk penelitian komunikasi kedepannya. Keterbatasan dalam penelitian ini membuka ruang baru untuk penelitian lebih lanjut. Penelitian ini hanya memaparkan konseptual tentang bagaimana ancaman terhadap privasi dan *data mining* dalam SNS. Akan lebih kaya jika kedepannya mengangkat isu dalam konteks geolokal yang lebih spesifik. Isu ancaman ini juga sebenarnya dirasakan oleh masyarakat Indonesia dan tidak sedikit kasus yang membuktikan hal ini harus diperhatikan lebih lanjut. Terlebih dalam meliterasi masyarakat untuk sadar akan bahaya dan ancaman privasi yang muncul jika tidak disadari lebih dini.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam penelitian ini, dan kepada Redaksi Jurnal Studi Komunikasi dan Media (JSKM) Balai Pengembangan SDM dan Penelitian Kominfo Jakarta yang telah berkenan memberikan koreksi dan menerbitkan artikel ini.

DAFTAR PUSTAKA

Baruh, L., & Popescu, M. (2017). *Big Data Analytics and the Limits of Privacy Self-Management.* Retrieved April 3, 2018, from New Media & Society, Vol. 19(4) 579-596: http://www.doi.org/10.1177/1461444815614001

Boyd, D. (2008). *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence.* Retrieved April 3, 2018, from The Internasional Journal of Research into New Media Technologies. Volume: 14 issue: 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 of Things: Literature Review and Challenges.* Retrieved April 3, 2018, from International Journal of Distributed Sensor Network, Volume: 11 issue: 8: https://doi.org/10.1155/2015/431047

Francis, C., & Baldesari. (2006). *Systematic Reviews of Qualitative Literature.* Oxford: UK Cochrane Centre.

Frith, J. (2017). *Big Data, Technical Communication, and The Smart City.* Retrieved April 3, 2018, from Journal of Business and Technical Communication, 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 Dictionary Based-Text Analysis and Unsupervised Topic Modelling.* Retrieved April 3, 2018, from Journalism & Mass Communication Quarterly, Volume: 93 issue: 2, page(s): 332-359 : https://doi.org/10.1177/1077699016639231

Henson, B., Reyns, B., & Fisher, B. (2011). *Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization.* Retrieved April 2, 2018, 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, from Online Social Network and 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 Data Mining.* Retrieved April 3, 2018, from The International Journal of Research into New Media Technologies, Volume: 23 issue: 3, page(s): 270-288: https://doi.org/10.1177/1354856515592507

Kitchin, R., & McArdie, G. (2016). *What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets.* Retrieved April 3, 2018, from Big Data & Society, Volume: 3 issue: 1: https://doi.org/10.1177/2053951716631130

Lewin, S. (2008). *Methods to Synthesis Qualitative Evidence Alongside a Cochrane Intervention Review.* London: London School of Hygiene and Tropical Medicine.

Liang, H., Shen, F., & Fu, K.-w. (2017). *Privacy Protection and Self-Disclosure Across Societies: A Study of Global Twitter Users.* Retrieved April 2, 2018, from New Media & Society, Vol 19(9), 1476-1497: http://www.doi.org/10.1177/1461444816642210

Milham, M., & Atkin, D. (2018). *Managing the Virtual Boundaries: Online Social Networks, 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. *Psychology Learning and Teaching, 2(1)*, 32-35.

Rathore, S., Sharma, P., Loia, V., Jeong, Y.-S., & Park, J.-H. (2017). *Social Network Security: Issues, Challenges, Threats, and Solutions.* Retrieved April 3, 2018, from Information Sciences, 421 (2017), 43-69: https://doi.org/10.1016/j.ins.2017.08.063