Analisis Pola Penyebaran Informasi Insiden Kebocoran Data Melalui Pendekatan *Social Network Analysis (SNA)*

Muhammad Novrizal Ghiffari[1)], Atika Nurliana[2)], Girinoto[3)]
(1) Badan Siber dan Sandi Negara, novrizal.ghiffari@bssn.go.id
(2) Badan Siber dan Sandi Negara, atika.nurliana@bssn.go.id
(3) Politeknik Siber dan Sandi Negara, girinoto@poltekssn.ac.id

Abstrak

Pada dekade terakhir ini, data menjadi salah satu aspek vital terutama pada data yang berklasifikasi terbatas maupun informasi sensitif. Insiden kebocoran data yang masif diberitakan media online dan media sosial dapat menjadi sentimen negatif bagi pemerintah dan perusahaan yang menjadi korban. Untuk itu perlu adanya usaha pengendalian terhadap penyebaran informasi tentang kebocoran data.. Pada penelitian ini berusaha melakukan analisis pola penyebaran informasi kebocoran data di Indonesia dengan menggunakan metode Social Network Analysis (SNA) dan Analisis Aktor. Dimana data yang digunakan adalah data twitter tentang kebocoran data pada periode satu tahun terakhir. Hasil SNA ditemukan tiga kelompok peredaran isu kebocoran data, karakteristik yang mendominasi peredaran informasi tentang kebocoran data tersebar dengan pola paling dominan adalah mentions dan retweet. Analisis aktor dapat ditunjukkan bahwa akun yang menjadi pusat peredaran isu adalah @PartaiSocmed dengan degree sejumlah 177. Dari nilai tersebut menunjukkan banyaknya kontribusi akun tersebut.

Kata kunci: Kebocoran Data, *Social Network Analysis (SNA)*, Twitter

Abstract

In the last decade, data has become one of the vital aspects, especially for classified and sensitive information. Massive data leaks incidents have been reported by online and social media, which can create negative sentiments for the affected government and companies. Therefore, efforts are needed to control the dissemination of information about data leaks. This study aims to analyze the pattern of data leak information dissemination in Indonesia using Social Network Analysis (SNA) and Actor Analysis methods. The data used in this study were tweets that spread information about data leaks in the last year. The SNA results found three groups of data leak circulation, and the dominant characteristic of data leak information circulation was through mentions and retweets. Actor analysis showed that the account @PartaiSocmed with a degree of 177 was the central hub of data leak issue circulation. This value indicates the significant contribution of this account.

Keywords: Data Breach, Social Network Analysis (SNA), Twitter

1. PENDAHULUAN

Data menjadi salah satu aspek vital selaras dengan kemajuan teknologi saat ini. Data dapat menjadi sumber daya yang lebih besar dalam memberikan pengaruh. Data juga mampu menjadi dasar dalam pengambilan keputusan dan melakukan prediksi. Hal tersebut bisa terjadi karena di dalam data terdapat informasi-informasi tertentu baik informasi umum maupun informasi sensitif. Mengutip dari Joko Widodo pada Puncak Peringatan Hari Pers Nasional 2023, menyatakan bahwa data memiliki harga yang tidak terhingga, karena data mampu mengendalikan preferensi masyarakat menggunakan algoritma tertentu [1]. Hal tersebut juga disampaikan Joko Widodo pada pidato kenegaraan[2]. Dapat dibayangkan bagaimana jika data-data tersebut dimanfaatkan oleh pihak-pihak tertentu bahkan data yang mengandung informasi sensitif.

Berdasarkan penelitian [3] salah satu dampak terburuk dari data breach adalah kerugian terhadap pihak yang memiliki sistem tersebut, diantaranya kerugian finansial dan kerugian reputasi. Selain itu bagi pengguna yang datanya telah bocor harus menanggung resiko terjadinya kejahatan siber, diantaranya scam dan phishing. Serangan tersebut rata-rata berdampak kepada kerugian finansial.

Pada 14 Maret 2023, kembali terjadi kebocoran data BPJS Ketenagakerjaan yang dilakukan oleh peretas Bjorka [4]. Kebocoran data yang sama telah terjadi sebelumnya di tahun 2021 [5]. Bjorka mengklaim bahwa kali ini telah meretas sebanyak 19 juta data. Akibat dari kebocoran data yang telah terjadi yakni menyebarnya data-data pribadi milik pengguna BPJS Ketenagakerjaan, serta turunnya kepercayaan masyarakat atas layanan dan keamanan yang diberikan oleh BPJS Ketenagakerjaan. Informasi terkait kasus ini menyebar melalui media publikasi maupun media *online*. Pada media *online*, informasi tersebut disebarkan oleh akun-akun pengguna dengan cepat. Untuk mengetahui pola penyebarannya, dilakukan analisis penyebaran informasi pada media sosial twitter dengan metode *social network analysis* (SNA). SNA merupakan metode yang digunakan untuk mengetahui pola dan persebaran informasi serta jaringan interaksi pada media sosial [6]. Dengan

menggunakan metode SNA, diharapkan dapat diketahui pola penyebaran informasi kebocoran data serta interaksi antar pengguna yang berkaitan dengan penyebaran tersebut.

2. LANDASAN TEORI

Pada bagian ini akan disampaikan beberapa landasan teori yang menjadi acuan dalam penelitian ini, mulai dari *Social-Cyber Security, Social Network Analysis* (SNA), Kebocoran Data, *Library* Snscrape, dan Twitter.

2.1. *Social-Cyber Security*

Social-cyber security merupakan pendekatan yang menggunakan ilmu sosial secara komputasional untuk melakukan identifikasi, mengantisipasi, menghitung serta menilai dampak dari sebuah komunikasi[6]. Pendekatan *social-cyber security* digunakan untuk beberapa bidang, yakni komunikasi, jurnalisme, riset pemasaran, intelijen dan forensik digital. Metode-metode yang digunakan dalam pendekatan *social-cyber security* ini diantaranya *machine learning, artificial intelligence, data science* dan *natural language processing* (NLP). Metode tersebut digunakan untuk memberikan bukti terkait aktor yang memanipulasi media sosial dan internet, metode yang digunakan, serta bagaimana mengatasinya.

Social-cyber security berfokus pada aktivitas yang ditujukan untuk mempengaruhi atau memanipulasi targetnya yang diantaranya adalah individu, kelompok, atau komunitas. Aktivitas yang dimaksudkan khususnya aktivitas yang memiliki konsekuensi besar bagi kelompok sosial, organisasi, dan negara [6]. Dengan mempengaruhi target-target tersebut, bertujuan untuk menyebarkan dan memberikan dampak yang luas atas pengaruh yang diberikan. Adapun terdapat beberapa ruang lingkup *social-cyber security*, diantaranya terdiri dari:

a. *Social Cyber Forensic* (WHO)
   Sosial cyber-forensik berkaitan dengan mengidentifikasi siapa yang melakukan serangan keamanan siber sosial. Berfokus pada pencarian tipe aktor, daripada aktor spesifik;
b. *Information Maneuvers* (WHAT)
   Melakukan deteksi, dan identifikasi rangkaian 'manuver' informasi dan menyediakan early warning;
c. *Motive Identification* (WHY)
   Memahami motif pelaku dalam melakukan serangan keamanan siber sosial atau operasi pengaruh informasi, misalnya kepentingan pemasaran, membuat kekacauan, polarisasi, propaganda atau hanya untuk motif pribadi;
d. *Diffusion* (WHERE)
   Melacak dan menelusuri penyerang, termasuk memprediksi potensi penyebaran kampanye atau operasi pengaruh informasi;
e. *Impact Measurement*
   Mengukur efektivitas serangan keamanan siber sosial, termasuk dampak jangka pendek dan dampak jangka panjangnya
f. *Mitigation* (HOW)
   Memahami bagaimana serangan sosial *cybersecurity* dilawan atau dimitigasi, serta memahami bagaimana masyarakat dapat menjadi lebih *resilience* terhadap serangan.

2.2. *Social Network Analysis* (SNA)

Social Network Analysis (SNA) adalah analisis yang dilakukan untuk mengetahui interaksi antar seseorang [6]. Interaksi ini dapat membentuk suatu jaringan-jaringan komunikasi dari skala kecil hingga besar. Jaringan komunikasi ini dapat digunakan untuk melacak dan mengidentifikasi kelompok dan aktor-aktor dalam penerapan intelijen. Dengan media sosial, teknik-teknik tersebut telah memungkinkan menjadi solusi terukur untuk data yang sangat besar yang memperhitungkan berbagai jenis hubungan di antara para aktor serta hubungan antara *resource*, ide, motif dan sebagainya.

SNA dapat menjadi salah satu alat untuk memetakan hubungan antar individu, dengan pendekatan yang digunakan untuk memetakan arus informasi secara horizontal maupun vertikal [7]. SNA dapat digunakan untuk mengidentifikasikan sumber dan tujuan dari penyebaran narasi, dapat membantu pemahaman terhadap posisi para aktor yang mempengaruhi akses terhadap sumber daya yang ada informasinya. Dengan identifikasi arus informasi, dapat membantu merencanakan strategi untuk berbagi informasi dibandingkan menciptakan strategi yang baru [8]. SNA mempelajari struktur hubungan yang mengaitkan individu atau unit sosial lain serta ketergantungan dalam perilaku atau sikap yang berhubungan dengan susunan hubungan sosial. SNA digunakan untuk menganalisis hubungan antar node atau aktor yang terdapat dalam *social network* dengan memanfaatkan teori graf [9], [10].

Dalam teori graf dan network analysis, terdapat empat cara untuk mengukur *centrality*, yaitu dengan cara menghitung *degree centrality*, *betweeness centrality*, *closeness centrality* dan *eigenvector centrality* [11]. *Betweenness centrality* adalah salah satu cara untuk mengukur centrality dalam suatu jaringan sosial. Perhitungan *Betweenness centrality* akan dijelaskan pada formula berikut:

$$C_B(vi) = \sum_{v_s \neq v_i \neq v_t \in V, s<t} \frac{\sigma_{st}(vi)}{\sigma_{st}}$$

σst = jumlah jalur terpendek melalui s menuju t
σst(vi) = jumlah jalur terpendek melalui s menuju t yang melewati simpul v.

Closeness centrality adalah salah satu cara untuk mengukur *centrality* dalam suatu jaringan sosial yang fokus terhadap seberapa dekat suatu aktor dengan semua aktor lainnya. Perhitungan *Closeness centrality*

akan dijelaskan melalui formula berikut:

$$C_c(vi) = \frac{n-1}{\sum_{j\neq i}^{n} g(vi, vj)}$$

g(vi, vj) = jarak *node* vi dengan vj
n = jumlah *node* yang berada dalam jaringan

2.2. Kebocoran Data

Peraturan perundang-undangan yang mengatur terkait kebocoran data di Indonesia adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Dalam UU ITE perbuatan yang dilarang yang menyangkut kebocoran data pribadi tercantum di dalam Pasal 27 ayat (1) yang mengatakan bahwa, "Setiap Orang dengan sengaja dan tanpa hak mendistribuksikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan."[12]. Sedangkan dalam UU PDP, tercantum di dalam pasal Pasal 65 ayat (1) yang mengatakan bahwa, "Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi."[13].

Kebocoran data merupakan pelanggaran keamanan dimana data sensitif, terlindungi atau data rahasia disalin, ditransmisikan, dilihat, dicuri, atau digunakan oleh individu yang tidak berwenang yang tidak berwenang untuk melakukannya [14]. Data tersebut bisa memicu adanya ancaman keamanan siber karena data tersebut bisa disalahgunakan kembali oleh pihak yang tidak bertanggung jawab. Jika data pribadi ini jatuh ke pihak yang tidak bertanggung jawab, maka data pribadi tersebut menjadi resiko terhadap terjadinya pencurian identitas atau mungkin tindak kejahatan lainnya seperti penipuan, impersonasi, pemerasan dan lainnya. Meski tidak semua data pribadi yang terbuka dapat mengakibatkan pencurian identitias, namun informasi yang terbuka dapat menimbulkan dampak yang cukup besar. Akibatnya dapat menimbulkan kejahatan siber yang bisa merugikan baik secara pribadi ke pemilik data maupun kerugian dalam bentuk materiil. [12]

Dari kebocoran data yang terjadi, terdapat 4 jenis cara kebocoran data bisa terjadi, yakni pencurian atau hilangnya perangkat penyimpanan, akses ilegal terhadap sistem atau informasi, keterlibatan orang dalam, serta kelalaian[15]. Dari penyebab kebocoran data tersebut, dapat diantisipasi dengan cara membuat tim tanggap insiden pelanggaran data, melakukan audit infrastruktur, memperbarui system pencadangan dan pemulihan secara teratur, serta membuat metode mitigasi sistem[16]–[18].

2.3. *Libary Snscrape*

Snscrape merupakan salah satu *library* dalam bahasa pemrograman python yang digunakan untuk proses pengambilan data dari media sosial Twitter dilakukan menggunakan teknik *crawling* [19], [20]. Proses pengambilan data *tweet* dilakukan dengan memanfaatkan sebuah *library* sehingga memudahkan untuk mengambil data *tweet* dengan jumlah yang besar dan rentang waktu yang lebih fleksibel. *Library* snscrape digunakan karena mudah digunakan dan tidak perlu mengakses langsung Twitter API dengan *access key* atau token, sehingga tidak diperlukan akun *Developer Twitter*. Selain itu pula, saat ini Twitter memberlakukan konsep berbayar dalam penggunaan Twitter API dalam bentuk Premium API.

Untuk menggunakan *Library* snscrape, pertama-tama melakukan instalasi dan *import* modul dari *library* snscrape yang berfungsi untuk mengambil data *tweet* dan *library* pandas untuk menampilkan serta menyimpan data dalam format .csv. Kemudian, tentukan jumlah data *tweet*, kata kunci dalam bentuk *query*, dan rentang waktu tertentu sesuai kebutuhan. *Library* snscrape dapat menjalankan *query* berupa pendefinisian start-date (*since*) dan end-date (*until*), serta filtering links (menghilangkan tweet yang mengandung URL) dan *filtering replies* (menghilangkan *tweet* yang mengandung *reply*/*mention*). *Tweet* yang telah didapatkan selanjutnya diproses dan ditulis ke dalam *file* .csv sehingga terdapat dua kolom yaitu *raw tweet* (kolom 'tweet') dan *processed tweet* (kolom 'processed').

2.4. Twitter

Twitter merupakan aplikasi media sosial yang dikembangkan oleh Twitter Inc dan berbasis di San Francisco. Twitter Inc didirikan pada bulan Maret 2006 oleh Jack Dorsey. Media sosial twitter berfungsi sebagai media sosial microblogging dengan jumlah karakter komentar (*tweet*) dibatasi maksimal 280 karakter [19]. Sebagai aplikasi media sosial *microblogging* twitter memiliki banyak pengguna aktif.

Terdapat beberapa terminologi dalam penggunaan media sosial twitter [19], [20], antara lain sebagai berikut:

a. *Tweet*, adalah tulisan yang di-posting seseorang di twitter. Jumlah tweet yang diperbolehkan tidak melebihi 280 karakter dalam sekali posting. Tweet biasanya berisi informasi, obrolan, ungkapan hati, motivasi dan lain sebagainya;
b. *Retweet*, adalah tweet orang lain yang di-posting kembali sebagai *tweet* pengguna lain. Fitur *retweet* memungkinkan untuk posting ulang *tweet* pengguna lain yang dianggap menarik dengan tetap mencantumkan sumber asli yang pertama kali membuat *tweet*;
c. *Mention*, adalah istilah ketika *tweet* yang dibuat akan ditujukan ke pengguna tertentu atau menandai pengguna tertentu agar pengguna yang ditandai tersebut mendapatkan notifikasi *tweet*

tersebut. *Mention* dapat dilakukan dengan menambahkan *username* pemilik akun twitter yang akan di-*mention* ke dalam tulisan *tweet*;

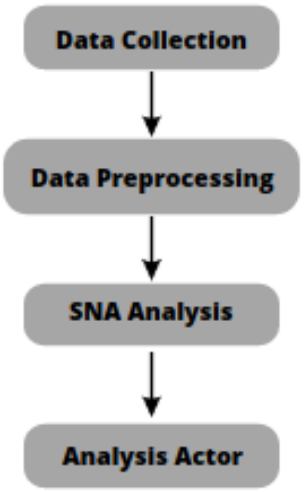
d. *Hashtag*, ditandai tanda pagar atau tagar (#) adalah istilah yang digunakan apabila pengguna menambahkan kata kunci berkaitan dengan *tweet* supaya dapat ditemukan oleh pengguna lain berdasarkan kata kunci tersebut;
e. *Followers*, adalah istilah untuk pengikut akun pengguna twitter. Seorang *follower* dapat melihat tweet pengguna twitter yang diikuti;
f. *Following*, adalah istilah untuk akun pengguna twitter yang diikuti. Dengan mengikuti akun twitter pengguna lain maka dapat melihat aktivitas pada *tweet*.

Saat ini, Twitter juga dilengkapi dengan berbagai fitur tambahan [20], antara lain:

a. *Fleets*, yaitu fitur yang mirip seperti Instagram Story atau Snapchat;
b. *Periscope*, yaitu fitur yang memungkinkan pengguna untuk melakukan *live streaming*;
c. *Thread*, yaitu fitur untuk membuat suatu rangkaian *tweet* yang bersambung.

3. METODOLOGI PENELITIAN

Metodologi yang digunakan pada penelitian ini secara general mengadopsi proses dalam penggunaan *machine learning* framework seperti pada Gambar 1.



Gambar 1 *Tahapan Penelitian*

Metode tersebut menggunakan metode dari penelitian [11], dengan beberapa penyesuaian. Pada tahap Data collection dilakukan proses *crawling data* menggunakan *library snscrape* dengan jumlah limitasi data mencapai 5000 data terkait dengan keyword *"Data Breach" OR "Kebocoran Data" OR "Data Bocor" OR "Bjorka"* pada rentang waktu satu tahun yaitu mulai tanggal 28 Maret 2022 hingga tanggal 28 Maret 2023. Pada data twitter, dilakukan *cleaning data* agar dapat diproses pada SNA, diantaranya dengan proses *regular expression, feature selection*, dan pengambilan image pada atribut *user*.

Dari data yang sudah dibersihkan, selanjutnya dilakukan analisis pada hubungan antar entitas twitter dengan isu kebocoran data. Pada analisis aktor akan terlihat entitas yang menjadi titik pusat dengan jumlah interaksi dan kedekatan antar entitas.

4. HASIL DAN PEMBAHASAN

Data yang diambil pada twitter menggunakan limitasi 5000 data pada rentang waktu satu tahun, dengan isu kebocoran data. Pada Gambar 2 menunjukan 5000 baris data dengan nama fitur diantaranya *DateTime, TweetId, Text, Username, Language, mentionedUsers, inReplyToUser, Hashtags, Url, ReplyCount, RetweetCount, LikeCount, QuoteCount, Media*.

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 5000 entries, 0 to 4999
Data columns (total 14 columns):
 #   Column          Non-Null Count  Dtype
---  ------          --------------  -----
 0   DateTime        5000 non-null   datetime64[ns, UTC]
 1   TweetId         5000 non-null   int64
 2   Text            5000 non-null   object
 3   Username        5000 non-null   object
 4   Language        5000 non-null   object
 5   mentionedUsers  1961 non-null   object
 6   inReplyToUser   1965 non-null   object
 7   Hashtags        1097 non-null   object
 8   Url             5000 non-null   object
 9   ReplyCount      5000 non-null   int64
 10  RetweetCount    5000 non-null   int64
 11  LikeCount       5000 non-null   int64
 12  QuoteCount      5000 non-null   int64
 13  Media           1128 non-null   object
dtypes: datetime64[ns, UTC](1), int64(5), object(8)
memory usage: 547.0+ KB
```

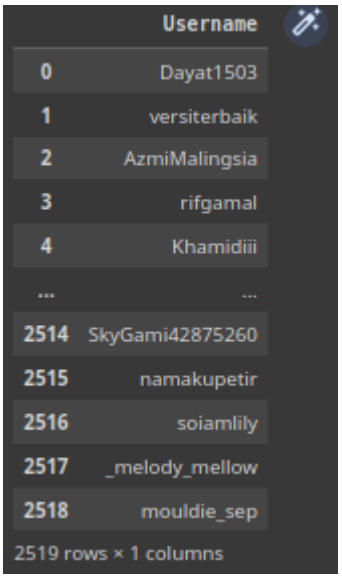
Gambar 2 *Kolom hasil pengambilan data tweet*

Proses pemetaan relational aktor dilakukan melalui fitur inReplyToUser dan mentionedUsers yang berhubungan dengan *Username*. Selanjutnya dilakukan *regular expression* untuk mengambil username pada kolom *inReplyToUser* dan *mentionedUsers.* Dari hasil pemetaan tersebut dibentuk satu fitur yang berisi hubungan antara user yaitu diantaranya *Reply, Mention,* dan *Tweet*.

Dari Ekstraksi fitur From, To dan Relationship menghasilkan data sejumlah 2982 data sebagaimana ditunjukan pada Gambar 3. Selanjutnya dilakukan ekstraksi atribut entitas atau user twitter seperti image profile, label, type, dan id. Pada gambar 4 adalah hasil ekstraksi user pada atribut entitas didapatkan 2519 unique user twitter yang terkait dengan isu kebocoran data.

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 2982 entries, 0 to 2981
Data columns (total 3 columns):
 #   Column        Non-Null Count  Dtype
---  ------        --------------  -----
 0   From          2982 non-null   object
 1   To            2982 non-null   object
 2   Relationship  2982 non-null   object
dtypes: object(3)
memory usage: 70.0+ KB
```

Gambar 3 *Kolom pemetaan akun dan hubungannya*



	Username
0	Dayat1503
1	versiterbaik
2	AzmiMalingsia
3	rifgamal
4	Khamidiii
...	...
2514	SkyGami42875260
2515	namakupetir
2516	soiamlily
2517	_melody_mellow
2518	mouldie_sep

2519 rows × 1 columns

Gambar 4 *Daftar user twitter terkait dengan isu kebocoran data*

4.1 *Social Network Analysis*

Pada Hasil SNA yang merujuk pada Gambar 5, menunjukkan bahwa pola peredaran isu kebocoran data terbagi menjadi tiga kelompok besar. Masing-masing kelompok tersebut memiliki pola dengan karakteristik yang berbeda dalam penyebaran informasi terkait isu insiden kebocoran data.

Gambar 5 *Visualisasi SNA*

Pola penyebaran isu kebocoran data pada kelompok pertama cenderung beredar isu dengan pola *reply*, dapat diketahui isu kebocoran data tersebut dibahas oleh beberapa entitas pada sosial media twitter kemudian entitas tersebut secara intens melakukan *reply tweet* sesama entitas. Pada kelompok kedua, peredaran isu kebocoran data memiliki dua tipe pola penyebaran yaitu dengan *reply tweet* dan *mentions*, pola tersebut dapat dilihat dari *edge* yang terbentuk. Pada kelompok ketiga isu kebocoran data beredar paling dominan adalah *mentions* atau *retweet*, sesuai pada hasil SNA *graph* terlihat kelompok ketiga memiliki *graph* yang cukup luas peredarannya. Selain itu pada kelompok ketiga terdapat beberapa entitas yang hanya melakukan *self tweet.*

Dari keseluruhan analisis SNA, dapat diketahui bahwa pola paling dominan adalah dengan *mentions* dan *retweet.* Hal tersebut berdampak kepada kecepatan peredaran informasi tentang isu kebocoran data yang tergolong cepat karena banyak entitas pada twitter yang membagikan isu tersebut.

4.2 Analisis Aktor

Dari hasil analisis SNA dapat diketahui bahwa beberapa akun yang menjadi pusat dari isu kebocoran data yang beredar pada sosial media diantaranya 3 dengan *degree* tertinggi, @PartaiSocmed @PaimonMontok dan @MandiriRusman. Akun dengan username @PartaiSocmed memiliki hubungan terbanyak yaitu dengan 177 *degree* pada analisis SNA, artinya bahwa akun tersebut sangat intens membahas dengan akun lainnya di twitter tentang isu kebocoran data dan menyebarkan isu tentang kebocoran data pada media twitter baik itu dengan *reply* atau *mentions*. Dilakukan analisis secara langsung pada akun dengan *degree* tertinggi, ditemukan akun tersebut dominan membahas tentang sentimen pemerintah, dimana kebocoran data di indonesia lebih dominan terjadi pada instansi pemerintahan.

Tabel 1. Perhitungan *Degre*, *Betweenness*, dan *Closeness*

Account	*Degree*	*Betweenness*	*Closeness*
PartaiSocmed	177	127330	0.28
PaimoMontok	165	5	0.80
MandiriRusman	141	2	0.66
p4c3n0g3	131	46100	0.21
RendyWi67527372	67	7348	0.15
detikcom	64	55274	0.25
worksfess	56	1430	0.98
BlekokUhuy	49	0	0.44
_SEKNAS_RI	46	0	0.50
bjorkanism_real	40	25643	0.12

Pada tingkat *betweenness* akun @PartaiSocmed memiliki nilai *betweenness* tertinggi sebesar 127330, karena *node* @PartaiSocmed sering dilewati pada peredaran isu kebocoran data, seperti dengan melakukan *mentions, retweet* atau *reply*. Akun twitter @worksfess memiliki nilai *closeness* sebesar 0.98, artinya entitas tersebut memiliki kedekatan yang paling tinggi dengan entitas lainnya jika dibandingkan dengan entitas *centrality* lainnya.

Terdapat beberapa faktor yang membuat sebaran informasi mengenai kebocoran data, diantaranya karena pengaruh sentralitas akun @PartaiSocmed yang cuitannya didominasi oleh isu terkait pemerintahan, yang diketahui kebocoran data

dominan terjadi pada instansi pemerintahan. Melalui pantauan secara manual isu dominan yaitu terkait kritik terhadap pemerintah yang memicu *netizen* untuk melakukan *mentions* kepada akun sosial media pejabat dan instansi pemerintahan terkait. Banyaknya akun *robot* dan akun kontra pemerintah seperti @PaimoMontok, @MandiriRusman, @RendyWi67527372, dan @BlekokUhuy mendukung penyebaran informasi kebocoran data yang cepat melalui *retweet.*

5. KESIMPULAN

Pada penelitian ini menunjukkan bagaimana pola peredaran isu atau informasi tentang kebocoran data beredar pada sosial media twitter dengan metode SNA. Melalui hasil analisis SNA ditemukan tiga kelompok peredaran isu kebocoran data, karakteristik yang mendominasi peredaran informasi tentang kebocoran data tersebar dengan pola paling dominan adalah *mentions* dan *retweet*. Hal tersebut berdampak kepada kecepatan peredaran informasi tentang isu kebocoran data yang tergolong cepat.

Selanjutnya, melalui analisis aktor dapat ditunjukkan bahwa akun yang menjadi pusat peredaran isu adalah @PartaiSocmed dengan *degree* sejumlah 177. Dari nilai tersebut menunjukkan banyaknya kontribusi akun tersebut. Pada interaksi sosial media di twitter akun tersebut dominan membahas sentimen terkait pemerintah, diketahui juga kebocoran data lebih dominan terjadi pada instansi pemerintahan.

REFERENSI

[1] Achmad Dwi Afriyadi, "Jokowi Bicara Pentingnya Data: Harganya Tak Terhingga!," *Detik.com*, Feb. 09, 2023.

[2] Kompas, "Pidato Kenegaraan Presiden Jokowi 2019," *Kompas.com*, Jakarta, Aug. 16, 2019.

[3] A. Singh Bhadouria, "Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches," *International Journal of Scientific and Research Publications*, 2022, doi: 10.29322/IJSRP.X.2022.p091095.

[4] Diva Lufiana Putri, "Bjorka Muncul Kembali, Diduga Bocorkan 19 Juta Data BPJS Ketenagakerjaan," *Kompas TV*, Mar. 14, 2023.

[5] "BPJS Kesehatan: Data ratusan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat', kata pakar," *BBC News Indonesia*, May 21, 2021.

[6] K. M. Carley, "Social cybersecurity: an emerging science," *Comput Math Organ Theory*, vol. 26, no. 4, pp. 365–381, Dec. 2020, doi: 10.1007/s10588-020-09322-9.

[7] I. Himelboim, "Social Network Analysis (Social Media)," in *The International Encyclopedia of Communication Research Methods*, Wiley, 2017, pp. 1–15. doi: 10.1002/9781118901731.iecrm0236.

[8] O. Serrat, "Social Network Analysis," 2009. [Online]. Available: www.adb.org

[9] J. Scott, "Social network analysis: developments, advances, and prospects," *Soc Netw Anal Min*, vol. 1, no. 1, pp. 21–26, Jan. 2011, doi: 10.1007/s13278-010-0012-6.

[10] R. A. Hanneman and M. Riddle, "Introduction to Social Network Methods: Table of Contents," 2009. [Online]. Available: http://www.faculty.ucr.edu/~hanneman/nettext/[8/

[11] B. Susanto and A. R. C, "Penerapan Social Network Analysis dalam Penentuan Centrality Studi Kasus Social Network Twitter." [Online]. Available: http://techcrunch.com/2011/12/22/googlesplus/?utm_source=feedburner&utm_medium=feed&u

[12] Indonesia, *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*.

[13] Indonesia, *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI*.

[14] HHS, "Administration for Children and Families U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES Administration for Children and Families."

[15] Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) BSSN, "Panduan Menghadapi Data Breach," 2019.

[16] Government of Philipines, "Data Breach Prevention," 2023.

[17] Australian Government, "Data breach preparation and response," 2019.

[18] Goverment of South Australia, "Personal information data breaches guideline," 2023.

[19] J. Eka Sembodo, E. Budi Setiawan, and Z. Abdurahman Baizal, "Data Crawling Otomatis pada Twitter," School of Computing, Telkom University, Sep. 2016, pp. 11–16. doi: 10.21108/indosc.2016.111.

[20] S. Naya Aprisadianti, "Analisis Sentimen Twitter terhadap Content Creator Sisca Kohl Menggunakan Regular Expression."