PRIVACY AND ONLINE SOCIAL NETWORK: a model for analysis of collecting personal data

Privacidade e Rede Social Online: um modelo para análise de coleta de dados pessoais

Fernando de Assis Rodrigues (1), Ricardo Cesar Gonçalves Sant'Ana (2)

(1) Federal University of Pará (UFPA), Brazil, deassis@ufpa.br

(2) São Paulo State University (UNESP-Tupã), Brazil, ricardo.santana@unesp.br

Abstract

The popularization of Information and Communication Technologies allowed new forms of interaction, including Online Social Network (OSN) services. These services could share personal data with third-party organizations through Application Programming Interfaces (API), making it a complex task to observe the data flow. This research proposes a model to identify levels and elements available in the flow of personal data via API between organizations holding OSN services and external agents. It converged the recurrent mechanisms into providing data sets from the OSN services to external agents from a systematized reading of the technical documentation to establish a database model to fetch unitedly the possibility of storing information about the levels in which API provided personal data to external agents, applying the Entity-Relationship Model. Subsequently, it presents a Data Mart as a proof of concept for the proposed database model, intending to compare the ways of accessing the personal data attributes stored and, following, shared by the OSN services to external agents. It showed that the model could clarify the elements inherent in the data flow, allowing a more structured analysis, including the possibility of monitoring changes in the API by organizations over time.

Keywords: Data models; Database models; Privacy; Social networking

Resumo

A popularização das Tecnologias de Informação e Comunicação permitiu novas formas de interação, incluindo os serviços de Rede Social Online (RSO). Esses serviços podem compartilhar dados pessoais com organizações terceirizadas por meio de Interfaces de Programação de Aplicativos (API), tornando uma tarefa complexa observar o fluxo de dados. Esta pesquisa propõe um modelo para identificar níveis e elementos disponíveis no fluxo de dados pessoais via API entre organizações detentoras de serviços RSO e agentes externos. Convergiu os mecanismos recorrentes em fornecer conjuntos de dados dos serviços RSO para agentes externos, a partir de uma leitura sistematizada da documentação técnica para estabelecer um modelo de banco de dados para buscar de forma conjunta a possibilidade de armazenar informações sobre os níveis em que as API forneceram dados pessoais a agentes externos, aplicando o Modelo Entidade-

Rodrigues, Fernando de Assis, and Sant'Ana, Ricardo Cesar Gonçalves. Privacy and Online Social Network: a model for analysis of collecting personal data. *Brazilian Journal of Information Science: research trends*, vol. 17, publicação contínua, 2023, e0230005. DOI: 10.36311/1981-1640.2023.v17.e0230005

Relacionamento. Posteriormente, apresenta um *Data Mart* como prova de conceito para o modelo de banco de dados proposto, pretendendo comparar as formas de acesso aos atributos de dados pessoais armazenados e, em seguida, compartilhados pelos serviços RSO para agentes externos. Demonstrou que o modelo pode esclarecer os elementos inerentes ao fluxo de dados, permitindo uma análise mais estruturada, incluindo a possibilidade de monitoramento de mudanças na API pelas organizações ao longo do tempo.

Palavras-chave: Modelos de Dados; Modelos de Banco de Dados; Privacidade; Redes Sociais

Resumen

La popularización de las Tecnologías de la Información y la Comunicación permitió nuevas formas de interacción, incluidos los servicios de Redes Sociales en Línea (RSO). Estos servicios pueden compartir datos personales con organizaciones de terceros a través de interfaces de programación de aplicaciones (API), lo que hace que sea una tarea compleja observar el flujo de datos. Esta investigación propone un modelo para identificar niveles y elementos disponibles en el flujo de datos personales vía API entre organizaciones que poseen servicios de RSO y agentes externos. Convergieron los mecanismos recurrentes en la prestación de conjuntos de datos de servicios de RSO a agentes externos, a partir de una lectura sistemática de la documentación técnica para establecer un modelo de base de datos para buscar en conjunto la posibilidad de almacenar información sobre los niveles en los que las APIs proporcionaron datos personales a agentes externos, aplicando el Modelo Entidad-Relación. Posteriormente, presenta un Data Mart como prueba de concepto para el modelo de base de datos propuesto, con la intención de comparar las formas de acceder a los atributos de los datos personales almacenados y luego compartidos por los servicios de RSO a agentes externos. Demostró que el modelo puede aclarar los elementos inherentes al flujo de datos, lo que permite un análisis más estructurado, incluida la posibilidad de monitorear los cambios en la API por parte de las organizaciones a lo largo del tiempo.

Palabras clave: Modelos de datos; Modelos de bases de datos; Privacidad; Redes sociales

1 Introduction

The popularization of Information and Communication Technologies allowed new interaction forms between individuals, communities, and public and private organizations, such as those mediated by Online Social Network (OSN) services. These complex services are an integral part of reflections on the new characteristics of society and the functioning of the social fabric, with new possibilities of interaction and relationship between different types of entities, mediated by applications, computers, and networks, as verified in the concepts of Cyberculture (Lévy 2001) and Network Society (Castells 2009).

The OSN services are available globally (with few exceptions) as an integral part of a new business model for organizations that usually offer these services free of charge to users but with multiple considerations to enable profitability. Therein lies the duality and the antagonism of this environment: the OSN services are free, accessible, with great potential to reduce geographic

barriers to interrelationships between individuals (Lengyel et al. 2015), but they are developed and maintained as products that depend on profitability to ensure the viability of the business model of the organizations who support them (Zhang et al. 2016).

The OSN organizations compete for public attention, bringing constant innovation to the services offered, resulting from a highly competitive and profitable global market. A total of 4.2 billion people accessed an OSN service at least once in January 2021, representing 53.6% of the population (Statista 2021), an increase of 490 million users between January 2020 and January 2021 (We Are Social 2021). It is also important to emphasize that the largest OSN holding organizations are listed in the NASDAQ Top 100 Stock Index, except for some of the Chinese organizations (NASDAQ 2021), in addition to being part of the most accessed applications and websites (Alexa 2021).

Based on the news broadcast by the media, part of society understands that one of the forms of profitability of organizations holding OSN services is related to the sale of advertising space for their services (Wall Street Journal 2021). However, one of the main success factors that set OSN services apart from other advertising spaces resides in the fact that they may be more assertive to delimit the target audience expected by the advertiser since individuals exchange information about their personal and professional activities in the OSN services, including natural and artificial attributes, entertainment options, cultural options, among other details. In synthesis, individuals tend to share personal data with the services (Rodrigues and Sant'Ana 2016).

These personal data are collected and stored in the Database Management Systems of the organizations holding the OSN services. The collected data are strictly systematized, applying data structure models and transforming them into data sets that, among other activities, allow a systematic, continuous, uniform, and customizable recovery process for each type of informational demand required (Rodrigues et al. 2018). Also, it is important to foreground the existence of channels to data access for partners, called external agents (Rodrigues et al. 2018; Rodrigues 2017), representing a vital part of the revenue to OSN services (Lanier 2018). The OSN services extend access to personal data to a set of organizations where the OSN service offers a dataset supply channel (OSN service → External Agent) and determines which datasets will be available to external agents without the requirement for human interaction in the process. The organizations provide data through interfaces specifically for those exchange operations, widely adopting a

concept from Computer Science, developed in the 1960s, the Application Programming Interface (API) (Manikas 2016). The APIs have become an integral component of the software that manages OSN services and part of the model for building large software integrator solutions (Manikas 2016).

The OSN services became a complex research domain since the 1990s, analyzed from the most varied perspectives and bringing new opportunities and challenges to researchers (Baatarjav and Dantu 2011; Boyd and Ellison 2007). In this context, it is essential to build analysis' structures that make it possible to clarify the elements of the data flow between OSN services and external agents and to reduce the user's lack of awareness about shared personal data among these entities. The motivating problem of this research is the difficulty in perceiving the levels at which the OSN services deal with access to the personal data of their users and, consequently, support the diagnoses of possible actions that potentiate breaches of the users' privacy from personal data that is collected, stored and shared with external agents.

Therefore, this research proposes a model to identify levels and elements available in the flow of personal data via API between organizations holding OSN services and external agents.

2 Literature Review

One of the leading research fields about OSN services use is related to the context of potential data access actions that impact personal data privacy. The discussions on the subject of personal data privacy are plural and addressed from different perspectives, such as the absence of privacy guarantees in the data transferred between two nodes of the network, as in the sharing of characteristics of the use of OSN services by men and women (Fogel and Nehmad 2009; Schneider et al. 2009), by teenagers (Barnes 2006; Boyd 2013) and students (Acquisti and Gross 2006; Ellison et al. 2007; Tufekci 2007); the lack (or the limited) of knowledge about how it works the OSN services and its relationship with the privacy of personal data (Krasnova et al. 2009); self-disclosure and publicity of personal or professional activities in OSN services (Trepte and Reinecke 2011; Young and Quan-Haase 2009); the classification of activities with potential harm to personal data's privacy in OSN services (Rodrigues and Sant'Ana 2016); the ethical use of personal data from OSN services in scientific research (Zimmer 2010); the exposure and the

invasion of personal data stored in OSN services (Boyd 2008); and the leakage of personal data (Krishnamurthy and Wills 2009).

However, the context for this research is related to scientific studies involving proposals of analysis models that identify transmitted data on the network, besides the relationships between content and actors, including service users, OSN services maintainers, and external agents. The dynamics between content and actors integrated into the digital social fabric present complexity for analysis of what happens to personal data, essentially in virtue of data and functionalities constantly changing (Watts 2004). Stand out the research as the proposals for the analysis of Uniform Resource Identifiers (URIs) used for the formation of the digital social fabric (users and groups/communities) and the relationships between entities and contents transferred in the OSN services (Mislove et al. 2007); the nucleation model to clustering users with common interests through personal data (Zhang et al. 2017); the privacy aspects of personal data when shared with OSN service partner platforms via third-party servers (Krishnamurthy and Wills 2008); the analysis of user behavior and different uses of OSN services (Penni 2017); the data accessibility model to elucidate the privacy and security risks and concerns in using OSN services (Creese et al. 2012; Lankton et al. 2020); the content structuring in OSN services via the semantic web (Mika 2007; Rodrigues et al. 2018); and the detachment of OSN services spaces into user, social and technological domains (Caviglione et al. 2014).

Hence, the leading global OSN services form the OSN supernetworks (Donath 2007), overcoming the geographic barriers (Lengyel et al. 2015), bringing new marketing and community-building possibilities (Zhang et al. 2016; Weber 2007), implying new ways of obtaining social capital (Ellison et al. 2007), enabling new sentiment analysis techniques based on the conveyed content (Khan et al. 2016; Pozzi et al. 2017), and personal data mining for behavior analysis (Singla and Richardson 2008). Besides, OSN supernetworks bring new concerns, such as security aspects of the information stored in these services (Altshuler 2013) and the development of defense systems against web crawling in OSN interfaces (Mondal et al. 2011).

3 Material and Methods

The method adopted consists of an exploratory analysis of OSN services, by direct and non-participant observation, of a quantitative and qualitative nature, with the use of combined and convergent methods (Sandelowski 2000; Brannen 2005), from the exploration of the technical characteristics of its APIs and the reading of document collections available. It was divided into three perspectives, starting from a study of the steps available on OSN documentation (called levels in this research) required to provide personal data from the OSN services to external agents, followed by detailing the characteristics of personal attributes at the moment of data collection by external agents, and a proposal of a database modeling to support query processes.

This research studied APIs from OSN services: Facebook, Twitter, and LinkedIn, respectively, the Graph API (Meta, Inc. 2021), the Twitter API (Twitter, Inc. 2021), and the LinkedIn API (Microsoft, Inc. 2021). Three factors established the eligibility criteria: the availability of technical material in English, services free of charge to API users, and no access limitation. Besides, those OSN services have the highest monthly access (Alexa 2021; Statista 2021). Were discarded to analyze other OSN services offered by the same organization, opting to select only the service with the highest number of monthly users (*e.g.*, Meta Inc. owns more than one service).

It adopted a systematized reading of the technical documentation about the operation of APIs made by OSN services and available to software developers. Afterward, it converged the recurrent mechanisms to provide data sets from the OSN services to external agents. These two steps are interrelated and described in the fourth section of this article. In the third stage, was established a database model to fetch unitedly the possibility of storing information about the levels at which APIs provided personal data to external agents, using the specialization → generalization process and applying the Entity-Relationship Model (Silberschatz et al. 2011). Subsequently, it presents a proof of concept for the proposed database model, intending to compare the ways of accessing the personal data attributes stored and, following, shared by the OSN services to external agents.

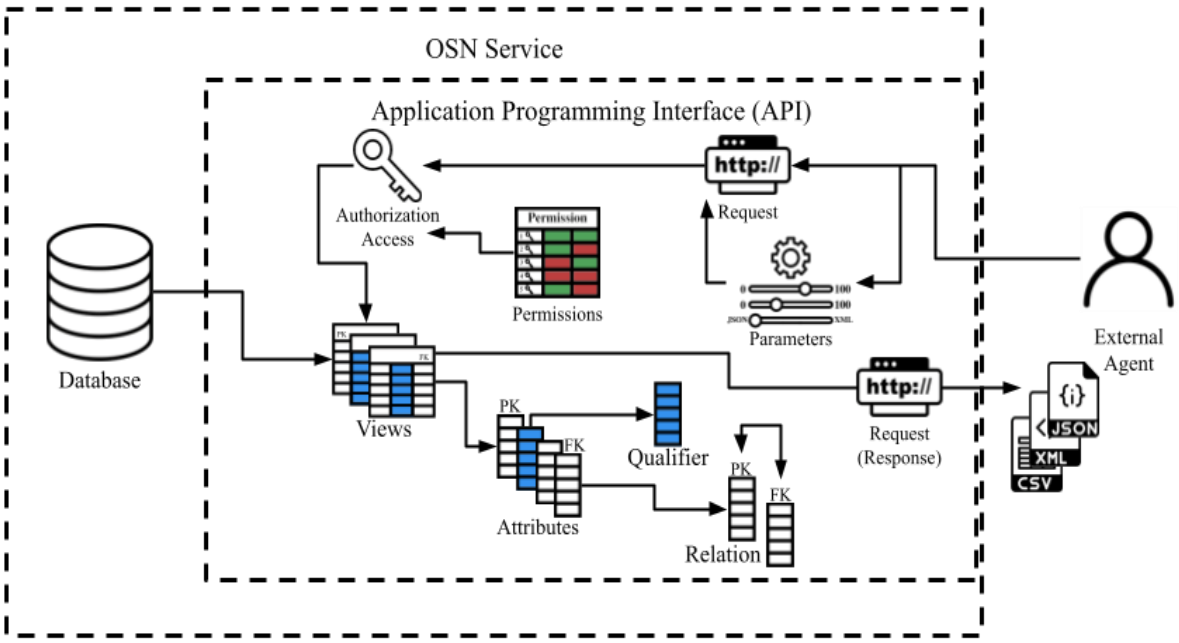
About the material, was used i) electronic spreadsheets to systematize the readings of technical documents, including the collection of information about the components that are part of

the personal data collection process, in addition to the attributes of available personal data, ii) Database Workbench tool for database modeling and script generation in Structured Query Language (SQL) format, and, iii) MariaDB Database Management System to apply the script, to enable the proof of concept of the model proposed in this research.

4 Provision of Data by OSN Services

The Facebook, LinkedIn, and Twitter APIs are similar in providing data to external agents, except for the authorizing access process to the data for external agents. It is possible to assert that Facebook subtly differs from the others by the degree of complexity, with more significant numbers concerning the documentation available about features, object and attribute data, and in the information about what could be done with the stored personal data on the terms of use. Nevertheless, the issues discussed in this section are not based on the extension of the available elements or the amount of existing content on these services, but on the levels of what is required for the external agent to begin a process of collecting data in the OSN services.

Figure 1 – Flow diagram for OSN services data collection, via API, by external agents



Source: Authors.

As aforementioned, the API data collection process is subtly different in some technical details. Facebook's Graph API differs from the others by adopting a two-level access authorization system, while the other services analyzed use a one-level authorization system. However, for all services analyzed, it is possible to synthesize the data collection process in 9 (nine) levels, detailed in sequence in this section: API, Access Authorizations, Permissions, Requests, Parameters, Qualifiers, Views, Attributes, and Relationships - all the levels are summarized in Figure 1. This model for analysis of collecting data from these services discarded elements related to the terms of use of the OSN services, which are part of the contract established between the organizations holding the OSN services, external agents, and users.

The first level for collecting data is connecting an external application to the OSN service via API. An interface as the API extends beyond a set of rules for data interoperability. The API offers the possibility of connecting one or more information systems with the data source, with platform independence, the feasibility of access control, and using standards and languages to

control the request and response of data sets, including documentation in the form of operationalization.

Unlike other data collection methods, adopting an API allows greater independence for the external agent to understand the possibility of implementing a continuous process of data inter-operation between two information systems. This method does not require direct contact between the external agent and the OSN service development teams to understand how requests could be implemented on algorithms or how data will be retrieved when collecting. The OSN services may have one or more APIs according to their size and market need. For example, Facebook designed an API for advertising actions and business management.

The API functionalities are under constant development. It is common for OSN services to use version control in implemented APIs. The OSN service designates an API version number when adding or removing features. It is also relevant to highlight the use of existing technologies, such as the Transmission Control Protocol/Internet Protocol (TCP/IP) for data transmission between the origin and destination points, the HyperText Transfer Protocol Secure (HTTPS) as the protocol to structure requests made by external agents, and the eXtensible Markup Language (XML) or the JavaScript Object Notation (JSON) as markup languages applied to the data structure transfer process. In some cases, it is also possible to identify datasets structured in Comma-Separated Values (CSV).

The OSN services use Access Authorizations and Permissions to guarantee the feasibility of different types of access to data sets in the same API. These services implement the Access Authorizations in the form of tokens distributed by the organization holding the ONS service to external agents, granting them access to a predetermined set of requests. Therefore, Access Authorizations allow or deny requests for access to part of the data sets stored by OSN service, which may include personal data. The tokens are the credentials that external agents must keep, guard and use for the initial verification of credentials when requesting data to collect.

In the case of OSN service implementing authorization at one level, the Access Authorization contains a static set of Permissions, defining possible executable requests by an external agent. Yet, when an OSN service API applies a hierarchical access system, Access Permissions may grant access to different Permissions. In other words, each Access Authorization

and Permission binomial could authorize a different number of requests, where OSN service users must consent to access their data. For example, when a user accepts to share personal data with an application external to the OSN service, the information system shows a dialog for users with which sets of personal data will be susceptible to the external application to collect. In this approach, the external agent will only be able to gather the personal data previously allowed by the user.

Consequently, the Access Authorizations and Permissions grant multiple points of entry to an API, each containing a set of Requests available for the external agent. The Requests are the data collection entry points in the OSN services, with their individualized characteristics detailed in technical documents made available by the OSN, aimed at the external agent's software developers and, therefore, with a language-oriented towards this sort of professionals. Each Request triggers a data access request from an expression in HyperText Transfer Protocol (HTTP) REQUEST syntax via HTTPS. The Requisition response is transmitted to the external agent via HTTPS and structured in XML and JSON markup languages or, to a lesser extent, in CSV format.

The Requests have a predefined set of Parameters to allow the external agent to customize the data to be collected (*e.g.*, filters and sort order). The technical documents of the Requests detailed the Parameters, made available by the OSN, intended for software developers from the external agent. The Parameters may also customize the Request response structure (*e.g.*, change the markup language from the Request's Response).

The Parameters could have Qualifiers, which are flags that identify the status of the Parameter. The investigation identified a total of 3 (three) Qualifiers in the analyzed APIs: core (the Parameter is part of the API’s core), default (the Parameter is a standard for API), and deprecated (the Parameter discontinued in the version of the API).

The available data sets in each Request do not directly originate from the OSN service database. The APIs implementation by these services uses information security's best practices and, consequently, reduces the risk of allowing external agents to perform direct access to tables from the OSN database that contains personal data. The API grant access to a View, a previously selected set of attributes about an object stored in the database. For example, a User's Personal

Data Request does not allow access to the password attribute. As a result, each Request gives access to a View containing a predetermined set of Attributes by the OSN.

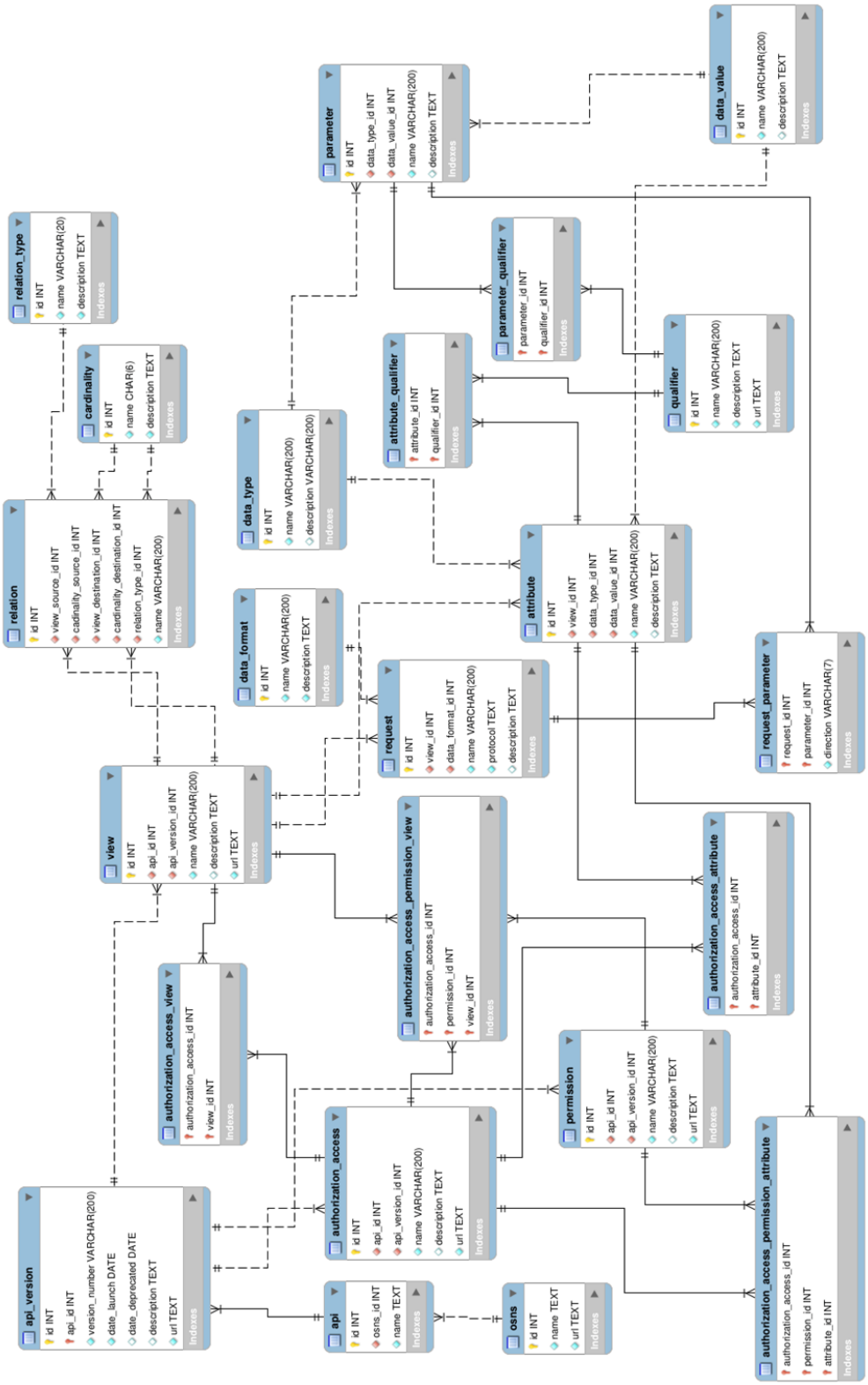
Hence, each Request will supply access to a structured set of data from a View containing a predetermined set of Attributes. It is possible to locate in the OSN services technical documents the Attribute's data type (*e.g.*, a number, a date, a string of characters, among others). Similar to the Parameters, Attributes could also have Qualifiers: core (is part of the core of the API), default (standard for API), and deprecated (deprecated in the API version).

Part of the View's Attributes has the function of linking to other Views available inside the API. This function enriches the process, allowing the triggering of a Request to be the beginning of a path to access and collect data sets from other Views, in which the external agent could access data linked to the initial Request. This link between two Views through an Attribute is called a Relation, an equivalent of Attributes marked with Integrity constraints (Primary Key - PK and Foreign Key - FK) proposed in Entity-Relationship Model (Silberschatz et al. 2011). For example, it is possible to access a user's data through a Relationship, collect data about their followers (available in an Attribute on the first Request) and, next, collect data about each follower (a second Request). The availability of Relationships is a crucial characteristic of analysis techniques such as data drilling (The Apache Software Foundation 2020).

5 Model for Analysis of Collecting Personal Data

It has created a structure to store the information about the components and the levels of data collection in OSN services, using the Entity-Relationship Model as a basis (Codd 1990; Silberschatz et al. 2011). As data management, the MariaDB Database Management System – open source – and the MySQL Workbench – compatible with MariaDB – were adopted to assist in the model construction.

Figure 2 – The Entity-Relationship Diagram about levels to provide personal data in OSN services



Source: Authors.

The model uses a total of 23 tables to represent this structure, interrelated (Figure 2), as follows: eleven (11) main tables, representing nine (9) basic entities of the data collecting levels in OSN services via API; two (2) tables to store information about OSN and their API versions; five (5) auxiliary tables, for storing data that complement the minimum semantics of the system, and; seven (7) tables to allow Many-to-Many (M:M) cardinality relationships.

Table 1 (in Appendix A) summarizes the model information about data tables and their attributes, presenting the Data Dictionary containing the name and description of the informational content of each table and its attributes, as well as the domain, size, and integrity constraints of each table attribute. The model's main tables are osns, api, api_version, authorization_access, permission, view, attribute, relation, request, parameter, and qualifier, systematized to store data referring to the levels of the data collecting process in OSN services (Silberschatz et al. 2011). The model's auxiliary tables are cardinality, data_format, data_type, data_value, and relation_type. The authorization_access_attribute, authorization_access_permission_attribute, authorization_access_permission_view, authorization_access_view, attribute_qualifier, parameter_qualifier, and request_parameter are the associative entity tables, which are a set of tables that assist the join of two or more entities in one-to-many and many-to-many modes (Silberschatz et al. 2011). All tables adopted artificial primary keys composed of auto-incremental integer numbers.

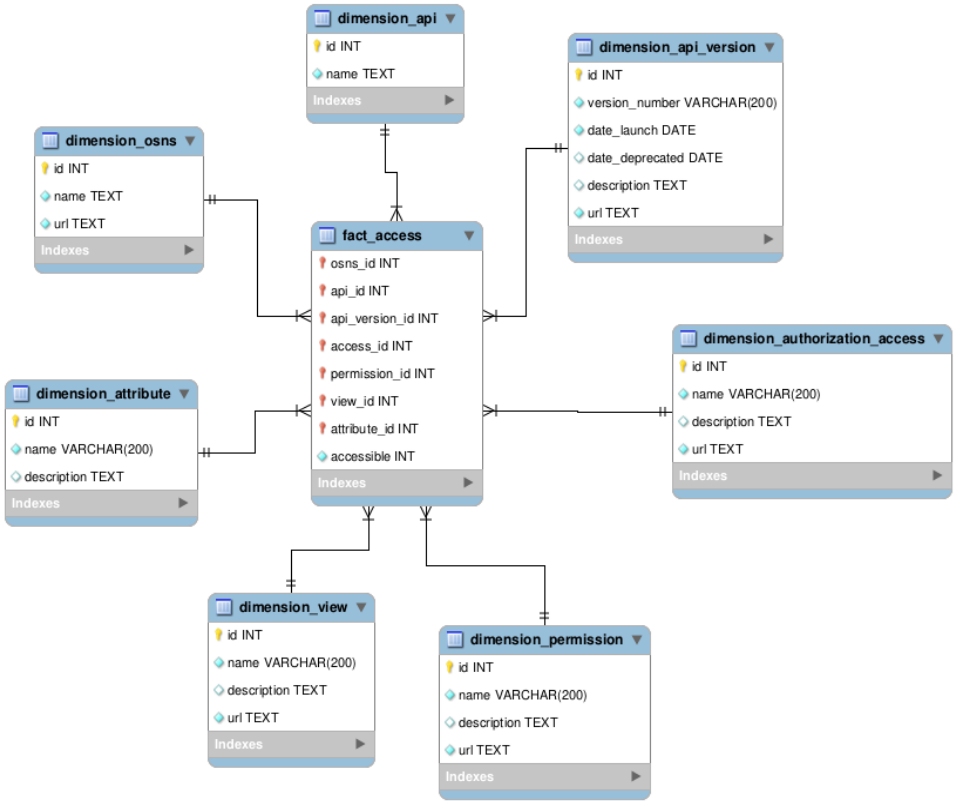
In function of the access to personal data by external agents through the OSN service, part of the challenges in establishing an analysis perspective on aspects related to privacy endures in the complexity of creating mechanisms that allow measuring information about the data set accessible by APIs. The structure model to store the information proposed in this research establishes this type of subsidy to analyze through different prisms. In other words, depending on the objective or hypothesis raised, the researcher could build their search strategies to suffice their demand (in the form of instructions in SQL Query format). When the data collected on the OSN services are normalized and stored in a single structure, it allows a researcher to compare what is recurrent or differs between the OSN services.

The benefit of structuring data in a model concomitant to the Entity-Relationship Model is the possibility of creating other structures based on the original proposal. In this sense, it is possible to reorganize the design of the initial structure to fit a specific demand. As a proof of concept, the

model was reorganized to a multidimensional form of a Data Mart with a star schema topology (Kimball and Ross 2011; Inmon 2005; Silberschatz et al. 2011). The goal is to centralize the perspective of the analysis to answer the required permission for access to each attribute.

As the aforementioned is a proof of concept, it decided to develop the new structure in the MariaDB Database Management System, despite a specific tool for this type of analysis being recommended (Thomsen 2002). However, the purpose is to simplify the analysis by researchers outside areas related to the theory of multidimensional analysis. In this sense, the MariaDB Database Management System offers essential support for the proposed activities.

Figure 3 – The Entity-Relationship Diagram of Data Mart structure with focus on data access permission in OSN services



Source: Authors.

The Data Mart (Figure 3) has seven dimensions, each one representing an access point for data query, all of which have the dimension_ prefix, as follows: osns, containing data about the OSN services; api, containing data from each API; api_version, containing data for each API

version; authorization_access, including data about Access Authorizations; permission, with data about the Permissions; view, having data about the Views, and; attribute, containing data about the Attributes.

It is worth considering the discard of some structural dependencies, such as the relationship between View and Attribute (view and attribute dimensions, respectively). It has chosen the star schema instead of the snowflake schema to avoid complexity in the construct of SQL queries, following the principle of de-normalization (Silberschatz et al. 2011).

The data of each dimension had origin in the first structure (Figure 2) processed from an Extract, Transform, Load (ETL) task, an operation used to transform transactional datasets into analytic and multidimensional datasets (Kimball and Ross 2011; Inmon 2005; Silberschatz et al. 2011). A dedicated Data Dictionary was dismissed for this model, as the reorganization into a multidimensional form did not change the value of the data collected (Appendix A).

It was created a fact table in addition to the dimensions, called fact_access. The fact_access table contains a set of foreign keys to relate to the dimensions and an attribute (labeled accessible) to receive a Boolean value representing whether a given combination of dimension parameters grants or denies access to OSN services data, via API, for external agents. A dataset from the fact_access table is retrieved when someone triggers a query into one of the dimensions. The data from the attribute accessible flagged with the boolean value TRUE will indicate which OSN services data will be available for collection by external agents. Oppositely, the data flagged with the boolean value FALSE will indicate which OSN services data will not be available for collection by external agents, opening the possibility of developing eventual tautologies and contradictions.

For example, a researcher could perform a query A to retrieve if in a given OSN service (S_x), in an available API (A_x), in an API version (AV_x), with an Access Authorization (AA_x) and with a Permission (P_x), in a View (V_x), if an Attribute ($Attr_x$) is available for access by an external agent, represented by the Expression 1.

$$A = S_x, A_x, AV_x, AA_x, P_x, V_x, Attr_x \qquad (1)$$

If a researcher requires to compare another Permission (Py) that has a different result from query A, a new query B could be performed, represented by the Expression 2.

$$B = S_x, A_x, AV_x, AA_x, P_y, V_x, Attr_x \quad (2)$$

Assuming that values retrieved from attribute accessible from queries A and B is unknown and considering the TRUE value as synonymous with access granted (represented by the number 1) and FALSE value as synonymous with access denied (represented by the number 0). It is possible to build a Truth Table (*e.g.*, Table 2) to summarize all feasible queries, increasing the potential for more complex expressions, for example, to treat queries as functions, part of the logic proposed in Boolean Algebra.

Table 2 – Truth Table for queries A and B, including conjunction and disjunction operations

A	**B**	**A ^ B (AND)**	**A v B (OR)**
0	0	0	0
1	0	0	1
0	1	0	1
1	1	1	1

0 = False; 1 = True.

Source: Authors.

This logic behavior allows a researcher to use queries in SQL language tailored for each type of analysis, for example, to use elements of Logic and Mathematics to quantify and qualify the data access from these services by external agents.

5.1 Model Limitations

The proposed model has Minimum Viable Product (MVP) characteristics that require adjustments to enable the comparison of data access via API with other techniques, such as scraping data available in human-interaction interfaces, *i.e.*, web scrapping User Interfaces (UI) in HyperText Markup Language (HTML). It is common sense that there are non-expected ways of collecting data in the UI through algorithms and adaptive libraries such as Python and Selenium, respectively.

In addition, a relevant by-product of the model is the perception of datasets accessible to external agents concerning information on OSN's Terms of Use. It was not practicable to confirm whether this relationship could be operated directly in the proposed database model. There would

be a requirement to transform unstructured data into structured data since the Terms of Use documents do not currently have versions in machine-readable formats.

Another factor still under analysis is the possibility of inserting new semantic elements in the model, allowing an improvement in understanding the impact on users on the data access to a particular set of attributes for an external agent means. Besides, adding more semantics to the model could identify elements of the model that, despite homonymous nomenclatures, have different meanings (Rodrigues et al. 2018). Inserting a higher-level semantic layer could increase the syntropy of the proposed model.

6 Conclusion and Future Work

The context of analysis of data collected from OSN services is already a research reality in several areas of knowledge, such as Information Science, Sociology, and Computer Science. However, the context proposed in this research will still require more studies on the adaptation of existing tools and greater detail on the possibility of using measurable elements and, therefore, qualifiable to support hypotheses about data collection by external agents and to justify diagnoses of possible actions that could potentially harm the privacy of personal data.

The model aims to systematize and contribute with reference structures to assist analysis of the sharing of personal data collected by OSN services with third-party organizations. One of the results of this research – the model for analyzing the data collected from OSN services – could contribute to clarifying elements that allow a more structured perception, including the possibility of monitoring changes in the API by organizations over time. It is relevant to explain that, in analogy to the object-oriented, this model is closer to the definition of classes than to instantiated data. In this sense, its application is suitable for structural analysis but not for the data obtained in each profile in each OSN service.

Despite the relevance of the proposed model, the assignment of analyzing the structures of networks (especially social networks) still lacks new components that, from demands generated by public scrutiny, will emerge over the next few years (including possible consequences elucidated in this research).

Notes

(1) This work was supported in part by a grant from Brazilian Coordination for the Improvement of Higher Education Personnel – CAPES Foundation.

References

Acquisti, Alessandro, and Ralph Gross. “Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.” *Privacy Enhancing Technologies*, edited by George Danezis and Philippe Golle, vol. 4258, Springer Berlin Heidelberg, 2006, pp. 36–58. *CrossRef*, https://doi.org/10.1007/11957454_3.

Alexa. “The Top 500 Sites on the Web.” *The Top 500 Sites on the Web*, 2021, https://www.alexa.com/topsites.

Altshuler, Yaniv, editor. *Security and Privacy in Social Networks*. Springer, 2013.

Baatarjav, Enkh-Amgalan, and Ram Dantu. “Current and Future Trends in Social Media.” *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, 2011, pp. 1384–85. *IEEE Xplore*, https://doi.org/10.1109/PASSAT/SocialCom.2011.125.

Barnes, Susan B. “A Privacy Paradox: Social Networking in the United States.” *First Monday*, vol. 11, no. 9, Sept. 2006. *CrossRef*, https://doi.org/10.5210/fm.v11i9.1394.

Boyd, Danah. “Facebook’s Privacy Trainwreck: Exposure, Invasion, and Social Convergence.” *Convergence: The International Journal of Research into New Media Technologies*, vol. 14, no. 1, Feb. 2008, pp. 13–20. *CrossRef*, https://doi.org/10.1177/1354856507084416.

Boyd, Danah. *Making Sense of Teen Life: Strategies for Capturing Ethnographic Data in a Networked Era*. 2013.

Boyd, Danah, and Nicole Ellison. “Social Network Sites: Definition, History, and Scholarship.” *Journal of Computer-Mediated Communication*, vol. 13, no. 1, Oct. 2007, pp. 210–30. *CrossRef*, https://doi.org/10.1111/j.1083-6101.2007.00393.x.

Brannen, Julia. “Mixing Methods: The Entry of Qualitative and Quantitative Approaches into the Research Process.” *International Journal of Social Research Methodology*, vol. 8, no. 3, July 2005, pp. 173–84. *DOI.org (Crossref)*, https://doi.org/10.1080/13645570500154642.

Castells, Manuel. *The Rise of the Network Society*. 2nd ed., Wiley-Blackwell, 2009.

Caviglione, L., et al. “A Taxonomy-Based Model of Security and Privacy in Online Social Networks.” *International Journal of Computational Science and Engineering*, vol. 9, no. 4, Jan. 2014, pp. 325–38. *inderscienceonline.com (Atypon)*, https://doi.org/10.1504/IJCSE.2014.060717.

Codd, E. F. *The Relational Model for Database Management: Version 2*. Addison-Wesley, 1990.

Creese, S., et al. “A Data-Reachability Model for Elucidating Privacy and Security Risks Related to the Use of Online Social Networks.” *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, 2012, pp. 1124–31. *IEEE Xplore*, https://doi.org/10.1109/TrustCom.2012.22.

Donath, Judith. “Signals in Social Supernets.” *Journal of Computer-Mediated Communication*, vol. 13, no. 1, Oct. 2007, pp. 231–51. *CrossRef*, https://doi.org/10.1111/j.1083-6101.2007.00394.x.

Ellison, Nicole B., et al. “The Benefits of Facebook ‘Friends:’ Social Capital and College Students’ Use of Online Social Network Sites.” *Journal of Computer-Mediated Communication*, vol. 12, no. 4, July 2007, pp. 1143–68. *Silverchair*, https://doi.org/10.1111/j.1083-6101.2007.00367.x.

Fogel, Joshua, and Elham Nehmad. “Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns.” *Computers in Human Behavior*, vol. 25, no. 1, Jan. 2009, pp. 153–60. *CrossRef*, https://doi.org/10.1016/j.chb.2008.08.006.

Inmon, William H. *Building the Data Warehouse*. 4th ed., Wiley, 2005.

Khan, Jawad, et al. “Sentiment Analysis at Sentence Level for Heterogeneous Datasets.” *Proceedings of the Sixth International Conference on Emerging Databases: Technologies, Applications, and Theory*, Association for Computing Machinery, 2016, pp. 159–63. *ACM Digital Library*, https://doi.org/10.1145/3007818.3007848.

Kimball, Ralph, and Margy Ross. *The Data Warehouse Toolkit The Complete Guide to Dimensional Modeling*. John Wiley & Sons, 2011. *Open WorldCat*, http://nbn-resolving.de/urn:nbn:de:101:1-2014122311140.

Krasnova, Hanna, et al. “Privacy Concerns and Identity in Online Social Networks.” *Identity in the Information Society*, vol. 2, no. 1, Dec. 2009, pp. 39–63. *link.springer.com*, https://doi.org/10.1007/s12394-009-0019-1.

Krishnamurthy, Balachander, and Craig E. Wills. “Characterizing Privacy in Online Social Networks.” *WOSN ’08: Proceedings of the First Workshop on Online Social Networks*, Association for Computing Machinery, 2008, pp. 37–42. *ACM Digital Library*, https://doi.org/10.1145/1397735.1397744.

Krishnamurthy, Balachander, and Craig E. Wills. “On the Leakage of Personally Identifiable Information via Online Social Networks.” *Proceedings of the 2nd ACM Workshop on Online Social Networks*,

Association for Computing Machinery, 2009, pp. 7–12. *ACM Digital Library*, https://doi.org/10.1145/1592665.1592668.

Lanier, Jaron. *Ten Arguments for Deleting Your Social Media Accounts Right Now*. 1st ed., Henry Holt and Company, 2018.

Lankton, N. K., et al. "Understanding the Antecedents and Outcomes of Facebook Privacy Behaviors: An Integrated Model." *IEEE Transactions on Engineering Management*, vol. 67, no. 3, Aug. 2020, pp. 697–711. *IEEE Xplore*, https://doi.org/10.1109/TEM.2019.2893541.

Lengyel, Balázs, et al. "Geographies of an Online Social Network." *PLOS ONE*, edited by Wei-Xing Zhou, vol. 10, no. 9, Sept. 2015, p. e0137248. *DOI.org (Crossref)*, https://doi.org/10.1371/journal.pone.0137248.

Lévy, Pierre. *Cyberculture*. University of Minnesota Press, 2001.

Manikas, Konstantinos. "Revisiting Software Ecosystems Research: A Longitudinal Literature Study." *Journal of Systems and Software*, vol. 117, July 2016, pp. 84–103. *ScienceDirect*, https://doi.org/10.1016/j.jss.2016.02.003.

Meta, Inc. "Graph API." *API Documentation*, 2021, https://developers.facebook.com/docs/graph-api/.

Microsoft, Inc. *LinkedIn API*. 2021, https://docs.microsoft.com/en-us/linkedin/.

Mika, Peter. *Social Networks and the Semantic Web*. 1st ed., Springer, 2007.

Mislove, Alan, et al. "Measurement and Analysis of Online Social Networks." *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, ACM Press, 2007, pp. 29–42. *CrossRef*, https://doi.org/10.1145/1298306.1298311.

Mondal, Mainack, et al. "Limiting Large-Scale Crawls of Social Networking Sites." *Proceedings of the ACM SIGCOMM 2011 Conference*, Association for Computing Machinery, 2011, pp. 398–99. *ACM Digital Library*, https://doi.org/10.1145/2018436.2018487.

NASDAQ. "Quotes For NASDAQ-100 Index." *NASDAQ*, 10 Mar. 2021, https://www.nasdaq.com/market-activity/quotes/nasdaq-ndx-index.

Penni, Janice. "The Future of Online Social Networks (OSN): A Measurement Analysis Using Social Media Tools and Application." *Telematics and Informatics*, vol. 34, no. 5, Aug. 2017, pp. 498–517. *ScienceDirect*, https://doi.org/10.1016/j.tele.2016.10.009.

Pozzi, Federico Alberto, et al., editors. *Sentiment Analysis in Social Networks*. 1st ed., Elsevier Inc., 2017.

Rodrigues, Fernando de Assis. *Coleta de dados em redes sociais: privacidade de dados pessoais no acesso via Application Programming Interface*. Universidade Estadual Paulista, 3 Mar. 2017, https://repositorio.unesp.br/handle/11449/149768.

Rodrigues, Fernando de Assis, et al. “Identifying Semantic Characteristics of User Interaction Datasets through Application of a Data Analysis.” *Advances in Knowledge Organization*, edited by International Society for Knowledge Organization (ISKO) et al., 1st ed., vol. 16, Ergon Verlag, 2018, pp. 581–87.

Rodrigues, Fernando de Assis, and Ricardo César Gonçalves Sant’Ana. “Use of Taxonomy of Privacy to Identify Activities Found in Social Network’s Terms of Use.” *Knowledge Organization*, vol. 43, no. 4, 2016, pp. 285–95.

Sandelowski, Margarete. “Combining Qualitative and Quantitative Sampling, Data Collection, and Analysis Techniques in Mixed-Method Studies.” *Research in Nursing & Health*, vol. 23, no. 3, June 2000, pp. 246–55. *CrossRef*, https://doi.org/10.1002/1098-240X(200006)23:3<246::AID-NUR9>3.0.CO;2-H.

Schneider, Fabian, et al. “Understanding Online Social Network Usage from a Network Perspective.” *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement*, Association for Computing Machinery, 2009, pp. 35–48. *ACM Digital Library*, https://doi.org/10.1145/1644893.1644899.

Silberschatz, Abraham, et al. *Database System Concepts*. 6th edition, McGraw-Hill, 2011.

Singla, Parag, and Matthew Richardson. “Yes, There Is a Correlation - From Social Networks to Personal Behavior on the Web.” *WWW 2008*, WWW2008 Organizing Committee, 2008, pp. 655–64.

Statista. “Global Social Network Penetration Rate as of January 2021, by Region.” *Statista*, Jan. 2021, https://www.statista.com/statistics/269615/social-network-penetration-by-region/.

The Apache Software Foundation. *Analyzing Social Media - Apache Drill*. 2020, https://drill.apache.org/docs/analyzing-social-media/.

Thomsen, Erik. *OLAP Solutions: Building Multidimensional Information Systems*. 2nd ed., Wiley Computer Pub, 2002.

Trepte, Sabine, and Leonard Reinecke, editors. *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer-Verlag, 2011.

Tufekci, Zeynep. “Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites.” *Bulletin of Science, Technology & Society*, vol. 28, no. 1, Dec. 2007, pp. 20–36. *CrossRef*, https://doi.org/10.1177/0270467607311484.

Twitter, Inc. *Twitter API Documentation*. 2021, https://developer.twitter.com/en/docs/twitter-api.

Wall Street Journal. “How to Fix Social Media.” *Wall Street Journal*, 29 Oct. 2021. *www.wsj.com*, https://www.wsj.com/articles/how-to-fix-social-media-11635526928.

Watts, Duncan J. *Six Degrees: The Science of a Connected Age*. W. W. Norton & Company, 2004.

We Are Social. “Digital 2021: The Latest Insights into the ‘State of Digital.’” *We Are Social*, 27 Jan. 2021, https://wearesocial.com/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital.

Weber, Larry. *Marketing to the Social Web: How Digital Customer Communities Build Your Business*. John Wiley & Sons, 2007.

Young, Alyson L., and Anabel Quan-Haase. “Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook.” *Proceedings of the Fourth International Conference on Communities and Technologies*, ACM Press, 2009, pp. 265–74. *CrossRef*, https://doi.org/10.1145/1556460.1556499.

Zhang, Fan, et al. “When Engagement Meets Similarity: Efficient (k,r)-Core Computation on Social Networks.” *Proceedings of the VLDB Endowment*, vol. 10, no. 10, June 2017, pp. 998–1009. *CrossRef*, https://doi.org/10.14778/3115404.3115406.

Zhang, Huiyuan, et al. “Profit Maximization for Multiple Products in Online Social Networks.” *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, IEEE, 2016, pp. 1–9. *IEEE Xplore*, https://doi.org/10.1109/INFOCOM.2016.7524470.

Zimmer, Michael. “‘But the Data Is Already Public’: On the Ethics of Research in Facebook.” *Ethics and Information Technology*, vol. 12, no. 4, Dec. 2010, pp. 313–25. *CrossRef*, https://doi.org/10.1007/s10676-010-9227-5.

Research Data

You can find all data used in the research in the Tables and Figures of this document. Additional information may be made available upon request by email.

Appendix A

Table 1 – The Data Dictionary for the Entity-Relationship Model about levels to provide personal data in OSN services.

Table Name	Table Description	Attribute Name	Domain (Size)	Description	Integrity constraints
osns	Represents the OSN services to which the APIs are bound.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key
					Not Null
		name	Text(65,535)	The name of Online Social Network service.	Not Null
					Unique
		url	Text(65,535)	The main Uniform Resource Location of the Online Social Network Service.	Not Null
					Unique
api	Contains information about each API.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key
					Not Null

Table Name	Table Description	Attribute Name	Domain (Size)	Description	Integrity constraints
		osns_id	Integer(4)	The foreign key of the relationship between osns and api tables.	Foreign Key Not Null
		name	Text(65,535)	The name of Application Programming Interface.	Not Null Unique
api_version	Contains information about versions of each API.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		api_id	Integer(4)	The foreign key of the relationship between api and api_version tables.	Foreign Key Not Null
		version_number	Varchar(200)	The API version number.	Not Null Unique
		date_launch	Date(10)	The API version working start date.	Not Null
		date_deprecated	Date(10)	The API version deprecated date.	
		description	Text(65,535)	When available, the original description of the API version, without interpretation from the data collector.	
		url	Text(65,535)	The main Uniform Resource Location to access the reference document of the API version.	Not Null
authorization_access	Stores information about Access Authorizations.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		api_id	Integer(4)	The foreign key of the relationship between api and authorization_access tables.	Foreign Key Not Null
		api_version_id	Integer(4)	The foreign key of the relationship between api_version and authorization_access tables.	Foreign Key Not Null
		name	Varchar(200)	The given name of the Access Authorization.	Not Null Unique
		description	Text(65,535)	When available, the original description of the authorization access, without interpretation from the data collector.	
		url	Text(65,535)	The main address to access the document about the authorization access, in Uniform Resource Locator (URL) format.	Not Null
permission	Stores information about Permissions.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		api_id	Integer(4)	The foreign key of the relationship between api and permission tables.	Foreign Key Not Null
		api_version_id	Integer(4)	The foreign key of the relationship between api_version and permission tables.	Foreign Key Not Null
		name	Varchar(200)	The given name of the permission.	Not Null Unique
		description	Text(65,535)	When available, the original description of the permission, without interpretation from the data collector.	
		url	Text(65,535)	The main address to access the document about the permission, in Uniform Resource Locator (URL) format.	Not Null
view	Stores information about Views.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		api_id	Integer(4)	The foreign key of the relationship between api and view tables.	Foreign Key Not Null
		api_version_id	Integer(4)	The foreign key of the relationship between api_version and view tables.	Foreign Key Not Null
		name	Varchar(200)	The original name of the View as described in the reference documentation.	Not Null Unique

Table Name	Table Description	Attribute Name	Domain (Size)	Description	Integrity constraints
		description	Text(65,535)	When available, the original description of the view, without interpretation from the data collector.	
		url	Text(65,535)	The main address to access the document about the view, in Uniform Resource Locator (URL) format.	Not Null
attribute	Contains information about the Attributes available in each of the Views.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		view_id	Integer(4)	The foreign key of the relationship between view and attribute tables.	Foreign Key Not Null
		data_type_id	Integer(4)	The foreign key of the relationship between attribute and data_type tables.	Foreign Key Not Null
		data_value_id	Integer(4)	The foreign key of the relationship between attribute and data_value tables.	Foreign Key Not Null
		name	Varchar(200)	The original name of the attribute as described in the reference documentation.	Not Null Unique
		description	Text(65,535)	When available, the original description of the attribute, without interpretation from the data collector.	
relation	Stores information about relationships between Views.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		view_source_id	Integer(4)	The foreign key of the relationship between relation and view (source) tables.	Foreign Key Not Null
		cardinality_source_id	Integer(4)	The foreign key of the relationship cardinality of the view (source).	Foreign Key Not Null
		view_destination_id	Integer(4)	The foreign key of the relationship between relation and view (destination) tables.	Foreign Key Not Null
		cardinality_destination_id	Integer(4)	The foreign key of the relationship cardinality of the view (destination).	Foreign Key Not Null
		name	Varchar(200)	The name of the relationship.	Not Null Unique
request	Stores information about the Requests.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		view_id	Integer(4)	The foreign key of the relationship between view and request tables.	Foreign Key Not Null
		data_format_id	Integer(4)	The foreign key of the relationship between request and data_format tables.	Foreign Key Not Null
		name	Varchar(200)	The name of the request.	Not Null Unique
		protocol	Text(65,535)	Name of the protocol used to make the request and collect the data.	Not Null
		description	Text(65,535)	When available, the original description of the request, without interpretation from the data collector.	
parameter	Stores information about the Parameters available in Requests.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		data_type_id	Integer(4)	The foreign key of the relationship between parameter and data_type tables.	Foreign Key Not Null
		data_value_id	Integer(4)	The foreign key of the relationship between parameter and data_value tables.	Foreign Key Not Null
		name	Varchar(200)	The given name of the parameter.	Not Null
		description	Text(65,535)	When available, the original description of the parameter, without interpretation from the data collector.	

Table Name	Table Description	Attribute Name	Domain (Size)	Description	Integrity constraints
qualifier	Stores information about Attribute and Parameter Qualifiers.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		name	Varchar(200)	The original qualifier name, as described in the reference documentation.	Not Null
		description	Text(65,535)	When available, the original description of the qualifier, without interpretation from the data collector.	Not Null
		url	Text(65,535)	The main address to access the document about the qualifier, in Uniform Resource Locator (URL) format.	Not Null
cardinality	Auxiliary table to describe the cardinalities between the relationships of Views.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		name	Char(6)	The cardinality name, which can be One-to-one, One-to-Many, and Many-to-Many.	Not Null Unique
		description	Text(65,535)	The description of cardinality.	Not Null
data_format	Auxiliary table for describing the Data Formats available at the time of data collection for the Requests.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		name	Varchar(200)	The format name in which data can be collected.	Not Null Unique
		description	Text(65,535)	The data format description.	Not Null
data_type	Auxiliary table for describing the Data Types linked to Attribute or Parameter.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		name	Varchar(200)	The name of the data type.	Not Null Unique
		description	Text(65,535)	The description of the characteristics of the data type.	Not Null
data_value	Auxiliary table to describe the Types of Data Values used in each Attribute or Parameter.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		name	Varchar(200)	The name of the Data Value.	
		description	Text(65,535)	The description of the characteristics of the expected value type for each data.	Not Null
relation_type	Auxiliary table to describe the Type of Relationship between Views.	id	Integer(4)	The artificial ID to the table, automatically generated (auto-increment).	Primary Key Not Null
		name	Varchar(20)	The name of the type of relationship between views.	Not Null Unique
		description	Text(65,535)	A description of the characteristics of the type of relationship between views.	Not Null
authorization_access_attribute	Associative Entity Table to join authorization_access and attribute tables.	authorization_access_id	Integer(4)	The foreign key represents the relationship between the authorization_access and the attribute tables with id value from the authorization_access table.	Primary Key Not Null
		attribute_id	Integer(4)	The foreign key represents the relationship between the authorization_access and the attribute tables with id value from the attribute table.	Primary Key Not Null
authorization_access_permission_attribute	Associative Entity Table to join authorization_access, permission, and attribute tables.	authorization_access_id	Integer(4)	The foreign key represents the relationship between the authorization_access, permission, and attribute tables with id value from the authorization_access table.	Primary Key Not Null
		permission_id	Integer(4)	The foreign key represents the relationship between the authorization_access, permission, and attribute tables with id value from the permission table.	Primary Key Not Null
		attribute_id	Integer(4)	The foreign key represents the relationship between the authorization_access, permission, and attribute tables with id value from the attribute table.	Primary Key Not Null

Table Name	Table Description	Attribute Name	Domain (Size)	Description	Integrity constraints
authorization_access_permission_view	Associative Entity Table to join authorization_access, permission, and view tables.	authorization_access_id	Integer(4)	The foreign key represents the relationship between the authorization_access, permission, and view tables with id value from the authorization_access table.	Primary Key Not Null
		permission_id	Integer(4)	The foreign key represents the relationship between the authorization_access, permission, and view tables with id value from the permission table.	Primary Key Not Null
		view_id	Integer(4)	The foreign key represents the relationship between the authorization_access, permission, and view tables with id value from the view table.	Primary Key Not Null
authorization_access_view	Associative Entity Table to join authorization_access and view tables.	authorization_access_id	Integer(4)	The foreign key represents the relationship between the authorization_access and view tables with id value from the authorization_access table.	Primary Key Not Null
		view_id	Integer(4)	The foreign key represents the relationship between the authorization_access and view tables with id value from the view table.	Primary Key Not Null
attribute_qualifier	Associative Entity Table to join the attribute and qualifier tables.	attribute_id	Integer(4)	The foreign key represents the relationship between the attribute and qualifier tables with id value from the attribute table.	Primary Key Not Null
		qualifier_id	Integer(4)	The foreign key represents the relationship between the attribute and qualifier tables with id value from the qualifier table.	Primary Key Not Null
parameter_qualifier	Associative Entity Table to join the parameter and qualifier tables.	parameter_id	Integer(4)	The foreign key represents the relationship between the parameter and qualifier tables with id value from the parameter table.	Primary Key Not Null
		qualifier_id	Integer(4)	The foreign key represents the relationship between the parameter and qualifier tables with id value from the qualifier table.	Primary Key Not Null
request_parameter	Associative Entity Table to join the request and parameter tables.	request_id	Integer(4)	The foreign key represents the relationship between the request and parameter tables with id value from the request table.	Primary Key Not Null
		parameter_id	Integer(4)	The foreign key represents the relationship between the request and parameter tables with id value from the parameter table.	Primary Key Not Null
		direction	Varchar(7)	The parameter direction at the time of the request. It can be a) input, b) output and c) input and output.	Not Null

Source: Authors.

Received: 11/11/2022 Accepted: 10/01/2023