ANKARA YILDIRIM BEYAZIT UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE

GDPR COMPLIANCE OF CRAs: LOOKING THROUGH THE LENS OF TWITTER

M.Sc. Thesis by
Kübra AYDİN

Department of Computer Engineering

April, 2021

ANKARA

GDPR COMPLIANCE OF CRAs: LOOKING THROUGH THE LENS OF TWITTER

A Thesis Submitted to

The Graduate School of Natural and Applied Sciences of

Ankara Yıldırım Beyazıt University

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering, Department of Computer Engineering

by

Kübra AYDİN

April, 2021

ANKARA

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **“GDPR COMPLIANCE OF CRAs: LOOKING THROUGH THE LENS OF TWITTER”** completed by **KÜBRA AYDİN** under supervision of **ASSIST. PROF. MUHAMMED ABDULLAH BÜLBÜL** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. Muhammed Abdullah BÜLBÜL

Supervisor

Asst. Prof. Mücahid KUTLU

Jury Member

Asst Prof. Fahreddin Şükrü TORUN

Jury Member

Prof. Dr. Ergün ERASLAN

Director

Graduate School of Natural and Applied Sciences

ETHICAL DECLARATION

I hereby declare that, in this thesis which has been prepared in accordance with the Thesis Writing Manual of Graduate School of Natural and Applied Sciences,

- All data, information and documents are obtained in the framework of academic and ethical rules,
- All information, documents and assessments are presented in accordance with scientific ethics and morals,
- All the materials that have been utilized are fully cited and referenced,
- No change has been made on the utilized materials,
- All the works presented are original,

and in any contrary case of above statements, I accept to renounce all my legal rights.

Date: **Signature: …………………………………………..**

Name & Surname: Kübra AYDİN

ACKNOWLEDGMENTS

First of all, I would like to thank Rahime Belen SAĞLAM, who was my first supervisor and who did not spare her support and her guidance until I finished my thesis even though she left the university and went abroad.

Secondly, I would like to thank Assist. Prof. Dr. M. Abdullah BÜLBÜL for accepting to be my second supervisor and for all his support and guidance to continue my thesis.

Finally, I would like to thank my mother, father and brother for their endless support. I could not be successful without their support.

2021, 29 January **Kübra AYDİN**

GDPR COMPLIANCE OF CRAs:
LOOKING THROUGH THE LENS OF TWITTER

ABSTRACT

Collecting information about consumers and businesses from various sources, Credit reference agencies (CRAs) help many organizations. CRAs' business model depends on processing a high volume of personal data including highly sensitive ones, which must be processed within the relevant legal frameworks in different countries they operate their business, e.g., the European Union's new GDPR (General Data Protection Regulation). This thesis is about a data-driven analysis of CRA- and GDPR-related discussions on Twitter. Our analysis covers the three largest multi-national CRAs: Equifax, Experian and TransUnion and we also looked at the UK's data protection authority, ICO, and two UK-based privacy-advocating NGOs, Privacy International and Open Rights Group (ORG). We have analyzed public tweets of their official Twitter accounts and other public tweets talking about them. We performed a two-stage analysis in our study. The first phase is a descriptive analysis where we manually labelled tweets and identified main themes in the discussions. Our analysis revealed a very surprising lack of awareness of CRA- and GDPR-related data privacy issues within the general public and an surprising lack of active communications of CRAs to the general public on relevant GDPR-related privacy issues: out of 39,549 collected tweets we identified only 153 relevant tweets. This small number of tweets are dominated by mentions of security issues, especially data breaches affecting CRAs, not data subject rights or privacy issues directly. At the second stage, we applied an automatic text classification by using the pretrained model BERT and neural network algorithms. By dividing the whole set into three main labels GDPR/CRA_Related, GDPR/CRA_Unrelated and NONGDPR we train our machine and apply the model on the raw 39,549 data to find if there are data missed while manual labelling. Both the automatic and manual results give consistent results. It is observed in both manual and automatic results that most of the tweets are posted by individuals. Our study reveals that CRAs don't prefer to be salient about data privacy discussions from GDPR's point of view.

Keywords : Credit reference agencies, general data protection regulation, GDPR, online social networks, social media, twitter, data protection, law, privacy

CRA’lerin GDPR UYUMLULUĞU: TWITTER’ın MERCEĞİNDEN BAKARAK

ÖZ

Çeşitli kaynaklardan tüketiciler ve işletmeler hakkında bilgi toplayan Kredi referans ajansları (CRA'lar), birçok kuruluşun, başvuru sahiplerinin ve hizmetlerinin müşterilerinin kredi itibarını değerlendirmesine yardımcı olur. CRA’ların iş modeli, Avrupa Birliği’nin yeni GDPR (Genel Veri Koruma Yönetmeliği) gibi işlerini yürüttükleri farklı ülkelerde ilgili yasal çerçeveler dahilinde işlenmesi gereken son derece hassas olanlar da dahil olmak üzere yüksek hacimli kişisel verilerin işlenmesine dayanır. Bu belge, Twitter'daki CRA ve GDPR ile ilgili tartışmaların veriye dayalı bir analizini bildirmektedir. Analizimiz, en büyük üç çok uluslu CRA'yı kapsamaktadır: Equifax, Experian ve TransUnion ve ayrıca Birleşik Krallık'ın veri koruma otoritesi ICO ve iki Birleşik Krallık merkezli gizlilik savunucu STK, Privacy International ve Open Rights Group (ORG) 'ye de baktık. Resmi Twitter hesaplarının herkese açık tweet'lerini ve onlar hakkında konuşan diğer herkese açık tweet'leri analiz ettik. Analizimiz, genel kamuoyunda CRA ve GDPR ile ilgili veri gizliliği sorunlarına ilişkin çok şaşırtıcı bir farkındalık eksikliğini ve ilgili GDPR ile ilgili gizlilik konularında genel kamuoyuna CRA'ların aktif iletişiminin şaşırtıcı bir eksikliğini ortaya çıkardı: toplanan 39.549 tweetten sadece 153 alakalı tweet belirledi. Bu az sayıdaki tweet'e, veri sahibi haklarını veya gizlilik sorunlarını doğrudan değil, özellikle CRA'ları etkileyen veri ihlalleri başta olmak üzere güvenlik sorunlarından bahsedilmektedir. İkinci aşamada, önceden eğitilmiş model BERT ve sinir ağı algoritmalarını kullanarak otomatik bir metin sınıflandırması uyguladık. Tüm seti GDPR / CRA_Related, GDPR/CRA_Unrelated ve NONGDPR olmak üzere üç ana etikete bölerek makinemizi eğittik ve manuel etiketleme sırasında eksik veri olup olmadığını bulmak için modeli ham 39.549 veriye uyguladık. Hem otomatik hem de manuel sonuçlar tutarlı sonuçlar verdi. Hem manuel hem de otomatik sonuçlarda tweetlerin çoğunun bireyler tarafından atıldığı görülmektedir. Çalışmamız, CRA'ların GDPR açısından veri gizliliği tartışmaları konusunda öne çıkmayı tercih etmediğini ortaya koyuyor.

Anahtar Sözcükler : Kredi referans ajansları, genel veri koruma yönetmeliği, GDPR, çevrimiçi sosyal ağlar, sosyal medya, twitter, veri koruma, hukuk, gizlilik

CONTENTS

NOMENCLATURE

Acronyms

LR Logistic Regression

NB Naïve Bayes Classification

RF Random Forest Classification

SVM Support Vector Machines

TF-IDF Term Frequency-Inverse Document Frequency

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Credit scoring is a technology used as a decision-making tool to measure the creditworthiness of applicants (e.g., opening a bank account, applying for a loan from a lender, or trying to rent a property). In order to measure the credit score of an individual, a range of information is taken into account including information provided directly by the individual whose credit is being evaluated. It is often the case that all or part of such information is provided to the service provider by an intermediate agency called a credit reference agency (CRA).

CRAs are informational brokers that collect information that includes name, address, record on the electoral roll, information about credit accounts and payment history, links financially, public record information like bankruptcies and county court judgements from various sources such as banks, credit card providers, loan firms, mortgage lenders and utility companies. They provide credit-related information on individual and corporate consumers to other organizations to facilitate contract establishments and transactions between them. Different terms are used to refer to CRAs in different countries and sectors, e.g., “credit bureau”, “consumer credit (reporting) agency” and “consumer credit information supplier”. We use the term CRA throughout the thesis as it is used by the Association of Consumer Credit Information Suppliers (ACCIS) [1], an industrial association of CRAs in Europe, and in the UK Consumer Credit Act 1974.

The sensitive nature of personal data CRAs collect from many sources and store for serving their customers has profound privacy implications. CRAs do proactively disclose what data they collect and how they process the data. For instance, the three main CRAs in the UK (Equifax, Experian and TransUnion) disclose the details of their data processing via their joint Credit Reference Agency Information Notice (CRAIN) [1], which is a document that explains how the CRAs obtain, process and share personal data about individual and corporate consumers. However, many data protection issues are not widely known by the general public. For instance, CRAs do not depend on data subjects' explicit consents to collect and process personal data, but other "lawful bases" allowed by data protection laws including the latest European Union (EU)'s General Data Protection Regulation (GDPR) [3], especially the so-called "legitimate interests" (see Chapter 3 of [1] and also the guideline on CRAs from the ICO, UK's data protection authority [2]). In addition to data protection laws, CRAs are normally registered with financial regulators and their activities regulated by consumer credit legislation (e.g., Consumer Credit Act 1974 in the UK [3]).

Considering the legal grounds of CRAs' data collection and processing practices, privacy concerns on CRAs and the strengthened data subject rights introduced in the GDPR in 2018 led some privacy advocating non-governmental organizations (NGOs) to challenge the legal grounds of CRAs. One of those campaigns which is Privacy International [5], a London-based NGO, called people to request their data deleted by seven of those data brokers including also the two large CRAs (Equifax and Experian) and files official complaints to the ICO requesting an assessment notice on those data brokers' compliance with the EU GDPR and the UK Data Protection Act 2018 [4] [5] [6]. They have started another campaign 5 months after GDPR came into effect and highlighted rights of individuals with regard to the protection of their data strengthened by the GDPR [7].

Even though the campaigns run by those organizations, there is a lack of research on how the general public perceive the privacy debate around CRAs. To fill this research gap, we conducted a data-driven analysis of CRA- and GDPR-related discussions on Twitter, which is the easiest platform to follow the current events and last-minute developments in the world. We focused on the GDPR as a representative data protection law because it covers many countries and has triggered a lot of discussions on data subject rights in other application areas including blockchains [8], IoT systems [9] or AI based applications [10].

After making a preliminary study on Twitter and make some researches on CRAs and organizations (detailed information is available in chapter 4), we decided to do our analysis based on tweets of official accounts of six organizations; the three largest multi-national CRAs operating in the UK and many other countries, Experian, Equifax and TransUnion, the UK data protection authority ICO [4], and two privacy-advocating NGOs, Privacy International and Open Rights Group (ORG). We collected tweets from official accounts of the six organizations and also public tweets mentioning their names or their official Twitter accounts and analyzed their contents.

We performed a two-stage analysis in our study the first phase is a descriptive analysis and the second an automated analysis. Our descriptive analysis revealed a very surprising lack of awareness of CRA related data privacy issues within the general public and an astonishing lack of active communications of CRAs to the general public on relevant privacy issues: out of 39,549 collected tweets we identified only 153 tweets (0.387%) mentioning both CRAs and the GDPR. Most tweets in this small set are discussions on security issues (%73.2), especially data breaches affecting CRAs, not on data subject rights or privacy issues. The remaining tweets are mostly about complaints regarding inaccurate data in credit files and questions about how to exercise right to rectification, just two of many data subject rights defined in the GDPR.

In the automatic stage we tried to train our machine with RNN, LSTM and GRU by using the pre-trained model BERT. According to the literature GRU trains and performs better then LSTM when training with small dataset. Our data set consists of 1371 train and test data so we tried to find if GRU trains better than LSTM. Our research results showed that GRU has a bigger accuracy %62.10 and LSTM has a accuracy of %59.70, RNN %42.70. We also saw that the training accuracy of GRU reaches %100 by using 100 epochs.

After we decided to use GRU as training model and apply this model on the raw data (~ 40000) to find if any data was missed while manual filtering. As result we find that our automatic text classification model labeled 2091 data as GDPR/CRA_Related, 26319 data as GDPR/CRA_Unrelated and 11700 as NONGDPR. While manual labeling results were 153 GDPR/CRA_Related, 10608 data as GDPR/CRA_Unrelated and 29349 as NONGDPR.

The rest of the thesis is organized as follows. In the next chapter, we give an overview of both CRAs and the GDPR as useful background. Chapter 3 introduces related work concerning both CRAs and GDPR. After that we introduce data we used for our study in Chapter 4 and the results of our data analysis in Chapter 5. The final chapter concludes the thesis.

CHAPTER 2

BACKGROUND

2.1 CRAs

CRAs as a sector have tried to make their data collection and processing practices transparent to the general public, and they have published a number of reports [1] [11] [12]. Other organizations especially the national data protection authorities (DPAs) and consumer organizations also have interests in how CRAs operate and have published their own guidance documents and reports [13]. In this section, we give a brief overview of CRAs' data collection and processing practices given in the above public reports and guidance documents.

Several organisations from different sectors provide data to CRAs such as (public, private or postal and cooperative banks and credit unions), rental companies, credit card providers, mortgage suppliers, retail loan providers, the insurers, debt collectors, 'executive departments' (courts, tax authorities and the police), governmental departments, telecommunication operators, internet service providers, television suppliers, utility (electricity, gas and other fuel) suppliers and brokers. Information collected by CRAs can be categorizes into a number of classes;

- General consumer data used to identify the individual such as 'name', 'address', 'date of birth', 'gender ', 'identification number' or 'tax number' or any other identification number.
- Information on the credit applications such as enquiries from lenders, information for identification of cheques, information about the presence of consumers in a rejected checklist, credit stoppage, customer inquiries for their own credit reports, negative data of other bureaus and business phone file for identification checks
- Legal information about 'court decisions' and 'bankruptcy'
- Information on family
- Income
- Assets

- Loan Data such as ‘home purchases/mortgages’, ’credit and store cards’, ‘overdrafts’, ‘retail credit’, ‘telecoms’, ‘mail orders’ and ‘utilities’. Details on credit contracts such as original loan amount, the duration, the outstanding amount, information about repayment periods, and interest rate ‘other’ data regarding the payment type and account relationship
- Payment Data collected from the client or public sources

Given the value of the information collected by CRAs and the need to make decisions based on accurate and up-to-date information, source organizations update CRAs regularly about any changes of such information, and often electronically in real time. CRAs normally employ independent inspection and internal controls such as periodical checks as data quality strategies. In addition to those internal checks, CRAs also respond directly to consumer complaints and data protection/regulator requests from organizations and the authorities. Individuals also have the right to make a complaint to the national data protection authority, if there is an obvious inaccuracy and neither the CRA and nor actual data source is willing to correct [14].

CRAs have to comply with various laws and regulations both at the regional (e.g., EU) and the national level. For instance, the EU GDPR and the UK Consumer Credit Act 1974 [3] give individuals the right to request changes to inaccurate data held by the CRAs, although this may have to be done by contacting the relevant information source organizations. They have to align with national laws on personal data and consumer protection and banking laws on private credit reporting [12] .

Principal national regulator differs from country to country where it could be data protection authorities, the Ministry of Finance, Parliament or National Bank [12]. With the rich information collected, CRAs can serve other organizations in both the private and public sectors, who can request access to relevant information relating to an applicant of their service and decide if the application should be accepted. Such information consuming organizations normally establish their legal ground to access such information by obtaining the data subject’s consent. It is important to note that an information receiving organization can access the information from CRAs only when it has allowable reason which is specified in the law. It is available on request to

CRA clients for credit risk assessment, credit scoring or other purposes, such as employment fees or renting an apartment within a legal framework [15].

There are several possible ways of gathering data subject's consent: explicit informed consent, unambiguous informed consent as part of general terms and conditions, and through a specific agreement signed by the data subject [16]. However, some reports revealed that some negative data about individuals could be collected without any form of consent.

Some reports also cover privacy concerns raised by consumers. Such concerns are mostly about the collection and sharing of credit data in general. Other privacy concerns include difficulties for data subjects to access their own data for rectification and the lack of transparency regarding third party access to their credit data.

In this study, we covered three CRAs which operate in several countries including UK and US; Experian, Equifax and TransUnion. Experian was founded in 1996 and is working in 44 countries with more than 235 million individual consumers and 25 million businesses . Equifax is working since 1899 and is active in 44 different countries. This credit reporting agency has more than 800 million individual consumers and 88 million businesses [17]. Transunion started to work in 1968 and is available in more than 30 countries with more than 1 billion individual consumers [17].

2.2 GDPR

The GDPR, which became applicable across the EU in May 2018, is the European Commission's latest attempt to protect the privacy of data subjects in the EU (not just EU citizens) regardless of the location of their data, and personal data of any data subjects (not necessarily present in the EU) that are collected or processed in the EU. In order to achieve its set goals, the GDPR defines a set of principles and the lawful basis for data controllers and data processors to process personal information. It also provides several rights for data subjects, individuals whose data are collected and processed. Data controllers are defined in Article 4 as natural or legal persons, public authorities, agencies or other bodies who determines how and why data will be used by the organization, and data processors process any data that a data controller gives them [16]. Given these definitions, a CRA could be considered both as data processor and a data controller.

In this section, we present some of the most pertinent elements of the GDPR, to facilitate the later discussions on our work and results. In Article 5, the GDPR defines various data protection principles an organisation must comply with when processing personal data. The first set of principles requires data controllers to process personal data lawfully, fairly and in a transparent way. The data minimization requires controllers to ensure that personal data processed is adequate, relevant and limited in relation to the purposes for which they are processed. Another principle, storage limitation, requires that personal data be kept in a way that does not allow the identification of data owners for longer than is necessary for the purposes for which it is processed. The accountability principle requires data controllers/processors to take responsibility for what they do with personal data and how they comply with the other principles. Those bodies are also expected to have appropriate measures and records in place to be able to demonstrate their compliance. The accuracy principle requires the data collector to take all the responsibility on the data correctness that they hold. The knowledge of the purpose of collect the data is another principle named purpose limitation. The data collector must be clear about the aim of collecting the data and use the data only for their main purpose or for a new purpose if this purpose is relevant with your main purpose and if the collector get permission for using the data. Another responsibility of data controller is given in Article 34(1) which requires data controllers to notify identified individuals impacted by the breach in the event of a security breach. Organizations are supposed to report data breaches within 72 hours.

In addition to those principles, GDPR also outlines lawful basis for processing personal information which includes obtaining explicit consent and legitimate interest. If a data controller/processor has legitimate interest and can show that the processing is necessary to achieve it, they do not need to obtain consent.

Finally, the GDPR provides several rights to individuals. The right to be informed lets individuals know what is being done with their information, and right to access allows data subjects to ask for a copy of their personal data, the purposes of processing their data, the categories of the data being processed, and the third parties or categories of third parties that will receive their data. Under the GDPR, data subjects have also a right to rectify or erase inaccurate or out of date information which is known as right to rectification. The GDPR also introduces a right for individuals to have personal data erased if there is no longer a lawful basis for processing or if the data subject withdraws consent.

2.3 Technical Background

Confusion Matrix: A confusion matrix show the success and failure of the classification method. Each row shows the predicted target and each column shows the actual target. So, a matrix is generated as seen simply in figure 4.2. By using the values given in the confusion matrix many statistic calculations can be done in order to measure the performance of the classifier.

Table 2.1 Confusion matrix

	Actual Class Positive	Actual Class Negative
Predicted Class Positive	TP	FP
Predicted Class Negative	FN	TN

- TP: True Positive, the predicted and the actual value both are “Positive”.
- TN: True Negative, the predicted and the actual value both are “Negative”.
- FP: False Positive, the predicted value is “Positive”, but the actual value is “Negative”.
- FN: False Negative, the predicted value is “Negative”, but the actual value is “Positive”.

Accuracy: Accuracy is a measurement metric which shows what the success of the prediction of our classification method is. The calculation is dividing the “Number of correct predictions” into “Total number of predictions”.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{2.1}$$

Precision: How many of the positive predictions were actually positive? The number of actual “Positive” values predicted as “Positive” divided by the total number of predicted “Positive” values.

$$Precision = \frac{TP}{TP + FP} \tag{2.2}$$

Recall: How many of the actual positive values were correctly predicted? The number of actual “Positive” values predicted as “Positive” divided by the total number of actual “Positive” values.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{2.3}$$

F1 Score: This statistical calculation can measure by both precision and recall using. This scoring method is more sensitive according to accuracy.

$$\text{F1-Score}=2 * \frac{\text{precision * recall}}{\text{precision + recall}} \tag{2.4}$$

The rest of this part give deeper information about the algorithms used in the study.

Our dataset consists of 2 columns. The first column are the tweets which are the input values. The second column are the labels, the output values.

2.3.1 Embeddings

Embedding (like word embedding and sentence embedding) is a vector representation or numeric representation of textual document, sentences. The main aim is making a human readable and understandable sentence also understandable to a machine. The words with the same meaning are represented in the same way so that in natural language processing (NLP) problems and algorithms the system can learn and behave the same for the synonyms. In short embedding is representing words and sentences as vectors or numbers. From the past until today there were many embedding models are offered.

The oldest methods are methods which are developed by the frequency of a word containing in the document. Examples about these methods can be given as “TF-IDF”, “LSA” or “PMI”. These kinds of method leave their places to methods which were trained by neural networks. The trained or pre-trained methods can be divided into two main categories. Contextual and non-contextual.

Non-contextual pre-trained embedding methods can be gives as “word2vec”, “glove” or “FastText”.

Contextual pre-trained embedding methods can be gives as “Flair”, “Elmo” or “Bert”. The difference between contextual and non-contextual embeddings is that in contextual embeddings the model care on the sequence of the word in the sentence. The word before and after the actual word is important. So, this model can also learn the different meanings of the polysemous.

2.3.1.1 TFD-IDF

The TF-IDF correspond to Term frequency – Inverse Document Frequency. This means that the TF-IDF word embedding technique calculates the importance of a word in the whole document. The frequency of the term in the document and how long the document itself is.

2.3.1.2 LSA (Latent semantic analysis)

Latent semantic analysis (LSA) is a statistical embedding model. Topic modelling, text classification or text summarization systems can use this embedding model. Like in cosine similarity, latent semantic analysis uses also a matrix of unique word containing in the document as rows and the documents as columns. The matrix input is the number of occurrences of each word in each document. The main purpose of LSA is that the word which’s meaning are near to each other occurs more frequently together. For better results the numbers situated in a LSA matrix can be replaced with tf-idf scores.

2.3.1.3 PMI(Pointwise mutual information)

Pointwise mutual information is also a statistical embedding model very similar to TF-TDF and LSA. The aim is to find a connection between the words in your document and the category of a classification problem. As in TF-IDF and LSA also in PMI the model finds the importance of a word in the document. If the word can guide the model to find the right category.

2.3.1.4 WORD2VEC

Word2vec is a model which coverts words to vectors in a vector space. It is an unsupervised learning and predicting based method. This model is discovered by researchers from google in 2013. The model has 2 sub models used while converting. The first one is "CBOW (Continuous Bag of Words)" and "Skip-Gram".

2.3.1.5 GLOVE

Glove is another word to vector model. This model is very similar to word2vec. Like the word2vec model Glove model also evaluate each word individually and look at the whole corpus how many times a word occurs. The main difference is word2vec optimize the vector when the individual word is found but in glove the optimization is done at the end of the process. So, this means that glove trains the model faster than word2vec.

2.3.1.6 FASTTEXT

Fasttext is one more model which is not much different from word2vec and glove. The main differences and maybe the advantage is that word2vec and glove train the model only according to the words in the corpus. But Fasttext train the model according to the words in the corpus and bag of sub words.

Bag of sub words is a solution to train the model also with the words not containing in the corpus. The subword-bag of characters parse the word occurring in the corpus in to sub words or characters. So, this provide the model to train with different words as well. By the way also word miswritten in the corpus can be used in their correct writing and meaning.

One more advantage of Fasttext is that the model supports 157 different languages.

2.3.1.7 FLAIR

Flair is an embedding model which is based on contextual string embeddings. In this type of embedding model, the characters are sent one by one to the "contextual string embedding" and after that the forward and backward LSTM is used.

2.3.1.8 ELMO

Elmo is also an pre-trained contextual embedding model. Elmo is also trained with neural network LSTM.

2.3.1.9 BERT

Bert is a pre-trained contextual embedding model which is formed to train bidirectional. The pre-trained models that were introduced before are designed to train the model unidirectional. But the authors say that this cause knowing the context relation with only the word before. But it can also be important to know the meaning of the word in fully context.

Bert (Bidirectional Encoder Representations from Transformers) contains two models while training. The first one is "masked language model" (MLM) and the second is "next sentence prediction"

2.3.1.9.1 Masked Language Model

The masked language model masks several words in the input sentence. The model has the aim of predicting these words according to the places in the sentence. This is a process like filling in the blanks. Masked language model helps Bert to understand a bi-directional context within the sentence.

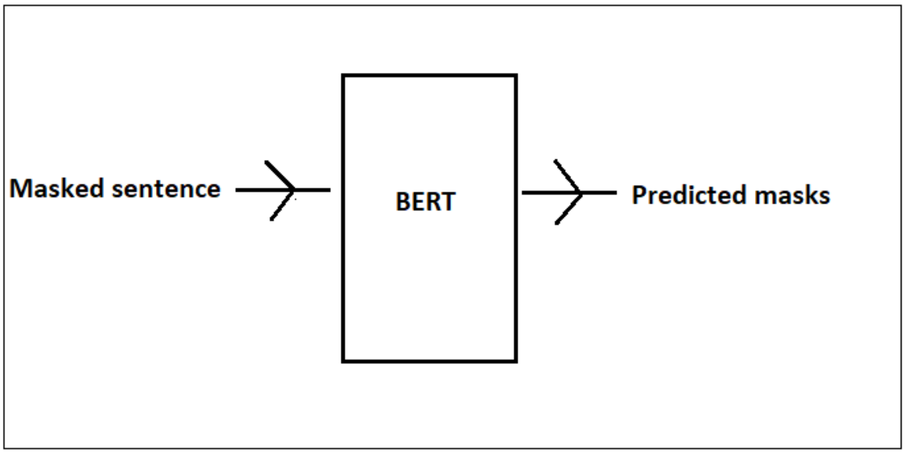


Figure 2.1 Bert stage-1

2.3.1.9.2 Next Sentence Prediction

The next sentence prediction part is prepared to establish relationship between sentences that follow each other. Bert takes into two sentences identify if the second sentence follows the first sentence. This part of the process the next sentence prediction provides Bert to understand the context between different sentence

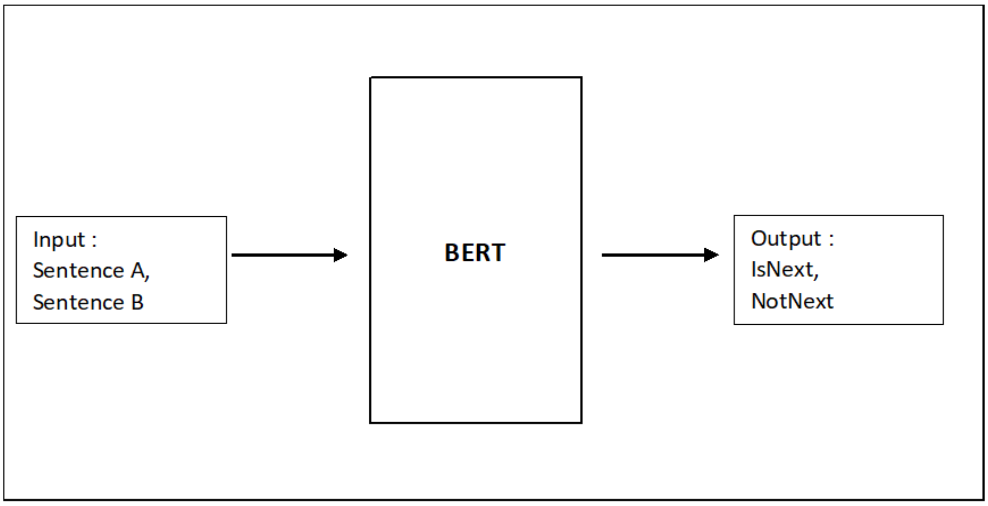


Figure 2.2 Bert stage-2

Using this both steps together Bert gets a good understanding of language.

2.3.2 Neural Network

Neural network is a machine learning model which inspire from human brain and neural system. Neural networks consist of 3 main layers. The first one is the input layer the third one is the output layer and the second or middle one is the hidden layer. The hidden layer does not have to occur of one layer. Hidden layers can occur of more than one layer. The layers contain a number of neurons and the neurons are connected to each other via synapses. Each synapse has a weight which are different from each other.

The values of each neuron are calculated by multiplying the input value and the weight of the synapse. After the value is calculated an activation function will be executed an if the value after the result of the activation function is bigger than the threshold the neuron will be fired or with in other words the neuron will be activated. This means the activated neurons transmits data to the neurons of the next layer through the synapse (channels). This process is called forward propagation.

2.3.2.1 Convolutional Neural Network (CNN)

Convolutional neural network is a deep learning algorithm that is frequently used in image processing or image recognition. With many different operations the convolutional neural network catches the features from the pictures. These algorithms contain many different layers like convolutional layer, pooling and fully connected. All these layers have different issues they must do.

2.3.2.2 Recurrent Neural Network (RNN)

The recurrent neural networks are suitable for sequence data processing like NLP or voice recognition. Because the recurrent neural networks contain a reminder. So, while training the recurrent neural networks (RNN) calculate or predict the next step by reminding and using the step before. There is a problem occurring named in the literature as “Vanishing Gradient Problem” To solve this problem two solutions have been found LSTM “Long-Short Term Memory” and GRU “Gated Recurrent Units”

2.3.2.2.1 Backpropagation

Neural network algorithms need to be train. At the beginning of the algorithm we give some weight values to the edges so that the input will be multiplied with the determined weight and the result will be given to the activation function and according to the comparison of the result and the threshold defined for the activation function the node will be fired or not. But right on the first time it is very difficult to find the correct outputs. Therefore, a backpropagation algorithm is executed. This algorithm find the distance as value between the output of the neural network and the real output and generate a loss value. By using this loss value, the algorithm train the weights of the neural network and by using the gradient value it find new weights. After some enough iterations the values of the weights will be more accurate, and our prediction results and actual results will be very close to each other. In the backpropagation process the model learn actually if the algorithm should increase or decrease the weights by calculating the gradient value. By looking at the minimum error. For example, at the beginning of the process the algorithm decides to increase the value of the weight but after this process it find out that the error is bigger than the error before. At this time the algorithm learn that it should decrease the value. Until it can find the minimum error value.

2.3.2.2.2 Vanishing Gradient Problem

In the backpropagation process some errors may occur. The gradient value is the value that determine the new weights and the bias values. But at neural networks that are long and connected to each other it is possible that while calculating the gradient value it will be decrease and disappear at some point. And this will make it more difficult to find the correct results. Because all the layers and the nodes are connected to each other by multiplying, after taking the derivatives of these multiplied values can cause destroy the value. There are some solutions to this problem.

1. Giving the best weight values at the beginning of the neural network process.
2. Using ReLU as activation function instead of sigmoid or tanh.
3. Using some methods that are designed to solve this problem like LSTM or GRU.

2.3.2.3 Gated Recurrent Network

When reading a review about a film or maybe a book we do not remember all the words in the text. A human brain will only remember the important points of the article or review. If the film was good or bad was it romantic or science fiction. A gated recurrent network works also like this. If any information from the step before is important for the step after the gated recurrent networks will remember them via the gates. There are two gated recurrent networks LSTM (long – short term memory) and GRU (gated recurrent unit).

2.3.2.4 Long-Short Term Memory (LSTM)

LSTM is a gated recurrent network. A recurrent network that contains gates. These gates help to decide which information should be remembered or forgotten. So, if the income data is not important it will be forgotten and if it is important it will be remembered. The LSTM consists of 3 gates. Each gate has an activation function sigmoid or tanh.

1. Forget Gate : The forget gate decide which information will be forgotten and which will be remembered. The information income from the previous hidden layer and the current input enter the sigmoid activation function. If the result of the sigmoid function near to zero it will be forgotten if it is near to one it will be remembered.
2. Input Gate: This gate updates or create the candidate cell state. The information income from the previous hidden layer and the current input enter firstly a sigmoid function and after that they enter a tanh function. The output of this gate is calculated by multiplying the results of these two functions.
3. Output Gate: This gate decide the value that will be transferred to the next layer. Firstly the information income from the previous hidden layer and the current input enter a sigmoid function again which we can call the A step. Secondly the state cell value transferred from the previous layer will multiplied with the result value of the forget gate and after that it will be added up with the result value of the Input gate. And lastly the updated state cell will enter a tanh function and will multiplied with A step. So the state cell will be updated.

2.3.2.5 Gated Recurrent Units (GRU)

The GRUs are very similar to the LSTMs the main difference is that the GRU has only two gates and the GRUs have no state cell which the LSTM used for information transfer. Instead GRU uses the hidden state for information transfer. GRU have two gates.

1. Update Gate: The update gate acts as the forget gate and the input gate of LSTM. Deciding which information will be forgotten and which one will be remembered and also which one will be new added.
2. Reset Gate: The reset gate decide how much past information will be forgotten.

CHAPTER 3

RELATED WORK

3.1 CRAs' Responses to GDPR

Association of Consumer Credit Information Suppliers (ACCIS) is an international association without profit. The main purpose of ACCIS is protecting the common benefits of its members [11]. ACCIS published an article in February 2020 [18] to summarize their contributions on informing the European Commission for the latter's 2020 evaluation report on the application of the GDPR. In its article, ACCIS claimed that its members (CRAs in Europe) had taken GDPR readiness very seriously. Updating data protection statements in order to comply with the extended transparency obligations under the GDPR is given as one of the actions taken by CRAs. The ACCIS article states that such statements have been made visible via CRAs' websites, and links to those statements have been covered in all email communications. In addition, online portals were set up for this purpose. Launching industry-wide public information notices is given as another strategy to prove transparency about the type of information CRAs hold and the legality of handling personal data.

The ACCIS article also talks about statistics of GDPR related data subject requests and how CRAs work with national data protection authorities to ensure the GDPR compliance. It explains how the GDPR could cause challenges on applications of new technologies and on data breach notifications. Communicating with several CRAs, ACCIS reported that there was an overall increase in the number of data subject requests including full subject access requests and rectification requests after the GDPR [11]. Data erasure requests and data portability requests were much rare.

ACCIS also stated that complaints and court action usually relate to the right of access, the right to erasure and the right to object. It underlines the importance of ongoing dialogue with DPAs for possible situations of non-compliance [11]. On the other hand, inconsistencies among DPAs is also highlighted and it is added that when there is a legal uncertainty, CRAs would turn to their local DPAs for guidance. The report explicitly states that GDPR has made it not easier to enable new technologies and methods.

Regarding the developments of new technologies such as artificial intelligence, CRAs are reported to have different opinions where some CRAs think that current safeguards are sufficient to grant fair and trustworthy data processing whereas others think that additional rules or guidance are needed to clarify how the data protection principles should be applied in practice. Regarding the data breaches, ACCIS highlighted the risk that controllers might overreact when it comes to notifying a data breach due to unbearable fines [11]. It argues that this may lead companies notify in circumstances where notification was not essential thereby putting unnecessary strain on DPAs.

While the ACCIS article [18] highlighted CRAs' efforts to be GDPR ready and compliant, the Credit Reference Information Notice (CRAIN) Version 1.1 [1], jointly compiled by three large CRAs in the UK (Equifax, Experian and TransUnion), has no a single mention of the GDPR, even though it was revised in March 2020, nearly two years after the GDPR became effective. This phenomenon also appeared in our results of analysis on tweets from the three CRAs' official accounts (see Section 5 for more details), reflecting a lack of active communication by CRAs to the general public on GDPR issues.

3.2 Twitter for Text-Mining

Social media platforms are used generally by people to express their opinion about any topic on the web. Twitter is one of the most popular social media platforms where users can share their thoughts [19]. User-generated information is a great way to analyze and understand the public's general judgment and perspective on an issue. Twitter has 330 million monthly and daily 145 million active users as of 2020 [20]. The ages of 63 percent of the users on Twitter are between 35- 65 [20]. Every day approximately 500 million tweets are posted [20].

A big amount of studies about text mining, user opinion analyses sentiment analyses and also some other applications use Twitter data [21]. Twitter data is used in many studies for different purposes Karami et al. made a study about the topics of studies related to twitter and they listed 40 topics as result of this study [22].

One of this topic is politics researchers made studies about elections. In the study of Tumasjan et al. As a result of examining tweets that generally mention politics or refer to a political party, the researchers concluded that Twitter is a platform for discussing political views [23]. Also, studies were done about the elections like the opinions and participations of twitter users [24]. According to the study of Karami et al. [22] the topic sentiment analysis and topic modeling are two of the most popular topics. Studies under this topic do research on whether tweets are positive, negative or neutral. Are twitter users' opinions about any given subject positive, negative or neutral? And which topics are discussed about the given subject [25] [26]?

Spatial analyses are used also usually. Under this topic the studies use the geolocation data of tweets [27] [28]. Also, disease surveillance is a popular topic which monitor diseases such as Chikungunya outbreak [29], Zika virus [30] and the outbreak experienced today corona virus [31]. The topics public relations with media organizations [32] or global organizations [33] and citizen-government interactions like monitoring the food policy of South Korea [34] are also listed in the list of 40 popular topics [22].

3.3 Text Categorization

A big amount of studies about text mining, user opinion analyses sentiment analyses and also some other applications use Twitter data as well [20]. It does not matter which topic will be analyzed. Like in one of the past studies Saura, Reyes-Menedez and Alvarez-Alonso tries to understand the user opinions in Twitter about world environment day. The aim this study is to identify the environmental, cultural, social and economic factors related to environment and public health. They collect tweets containing the hashtag #WorldEnvironmentDay. The conclusion reached at the end of the study is that most of the users who share their opinion about this hashtag on twitter are worried about extreme weather, deforestation, acid rain, climate risks and water pollution [25]. Saura et al. made one more study similar to the study about world environment day which was a descriptive analyze to find opinions if Black Friday deals worth it. The aim of this study is understanding the consumer behavior by analyzing user-generated content (UGC) by using Twitter. Three research questions were answered in the study. The first one is finding the main topics in interactions between users and companies that have campaign in Black Friday via Twitter. They try to find the feelings about the topics obtained by the first research question as the second research question and lastly as the third research question the making a textual analyze to identify insights. The researchers collect the data containing the hashtag #BlackFriday. As result to the first research question they found out 7 important topics in which the first three were about “offers and discounts” where the tweets were published by companies, “exclusive promotions” and “fraud”. They listed the results of the sentiment analysis grouping by the companies and they make a text analysis to find out which of the topics are discussed positively which one negatively and neutrally [26]. Nowadays the whole world is fighting an epidemic COVID-19. Lopez et al. generate a dataset from twitter to mine and understand the perception of COVID-19 policies. Starting from the starting of the disease, people have expressed their opinions via social media platforms like Twitter. They create a dataset containing multilanguage tweets about COVID-19 which started to be created on January 22 until 13 March 2020 according to the paper. They share a dataset which is available on Github and the recent date is 12 November 2020 with 1.137.174.200 tweets. They used the keywords virus, coronavirus, ncov19, ncov2019 and covid while collecting the tweets. The 63.4 percent of the dataset consists of English tweets and Spanish, and Portuguese are the languages following English. The researchers continuously collecting and updating the dataset and as feature work they will identify common popular topics related with the pandemic and show the differ across the time [31].

3.4 GDPR-Related Discussions on Social Media

Considering the massive amount of studies that analyze the impact of the GDPR in several contexts such as cloud computing, Internet of Things [9] and blockchain technologies [8], there has been surprisingly less research looking at social media discussions regarding the challenges raised by the GDPR. In one of those studies, Yang et al. investigated the discussions on Twitter around the right to be forgotten (RtbF) through social network analysis [35] .

Researchers examined the various topics discussed in relation to RtbF and the role of influencers in this debate. Their dataset firstly includes the tweets containing the keyword “right to be forgotten” and the hashtag #rtbf. After collecting some data, they realize that the hashtags #2beforgotten and #righttobeforgotten were used in most of the collected tweets and they include these keywords as well.

Researchers reported that Google’s role in RtbF and Russia (discussions in Russia regarding how public figures could abuse the law by removing compromising reports to enhance their online reputation) are the dominating topics around this right. They explain the domination of Google in three reasons.

The first reason is that people often use the word google in "to google", which they use to mean searching the web. The first reason is that people often use the word “google” in "to google", which they use to mean searching on web. Secondly, in Europe as a search engine Google is the number one. Lastly the right to be forgotten rule may threaten the free speech on internet depending on deny access to information and this does not fit Google’s code of ethics.

On the other hand, companies that are affected by the RtbF decision directly, experts including privacy researchers and lawyers, and news portals have been identified to be the key players in the network for this discussion [35].

In a similar study, Grudz et al. studied the discussion about the GDPR in a broad sense with the aim of examining public opinions and organizational public relations strategies about the GDPR [36]. Researchers collected tweets with the hashtag #gdpr for 6 months and applied social network analysis to find opinion leaders. They used Netlytic which is a collecting and analyzing tool for social media.

It is reported that there are three common types of opinion leaders; “Most Active Posters”, “Most Engagement Account”, “Most Mentioned Account”. To determine the “Most Active Posters” they sort their whole dataset according to the number of tweets published by each user. For the topics “Most Engagement Account” and “Most Mentioned Account” they used some metrics that belong to social network analysis such as out-degree and in-degree centralities. With these measurements, they identify the accounts that are most mentioned by other accounts and whose tweets are retweeted and replied most by other accounts as “Most Mentioned Account”. The accounts which mention other accounts the most and retweet or reply those accounts tweets were determined as “Most Engagement Account”.

After identifying the accounts two independent validators analyze the bio information on each identified twitter account profile to understand who these influencers are. Their results indicate that the GDPR is being actively discussed by a variety of stakeholders, but especially by cyber-security and IT-related firms and consultants. One of the most interesting finding has been reported as that some of the stakeholders like companies that store or process personal data, government and regulatory agencies, mainstream media, and academics were expected to have a more active role were less related. [36].

Social media analysis on data privacy is not limited to discussions around the GDPR. There are also studies conducted to understand what people think and how they are affected from data breaches. After the discovery that Facebook gave unauthorized access to personally identifiable information (PII) of more than 50 million Facebook users to the data firm Cambridge Analytica [37], Gonzalez et al. conducted a study to understand how data privacy concerns vary across the world. They conducted a cross-language study of online conversations to compare how people speaking different languages (English vs Spanish) react to data privacy breaches on Twitter. They used Python and the real time streaming API named Tweepy to collect the tweets.

Their ultimate goal was to collect tweets about the Cambridge Analytica and Facebook data breach. Consequently, they used keywords like “#CambrideAnalytica”, “#DeleteFacebook”, “Zuckerberg” and “Facebook Privacy” to access related discussions. Revealing the cultural differences in data privacy perspectives, their results show that the tweets written in English, in which Americans were the most active group of users, blame companies about these data breach. American Twitter users published tweets which blame big companies like Facebook and Google, whereas Spanish users are more likely to blame users because of their irresponsibility about reading the terms of service of Facebook and ignoring protection of their personal data [38].

In a similar study, Vemprala and Dietrich tried to cover all the discussions regarding data breaches and collected tweets that contain predefined keywords related to data breaches [39]. They used word embedding to find similar words in context, so they represented the words as vectors and measured the similarity of words in content with this method. They mainly focused on information diffusion and tried to identify what characteristics of a breach message makes the information diffuse. The impact of the existence of evidence in the form of media files, URLs and videos, drive information diffusion. In addition, the social media users who exchange wide amounts of breach messages have been investigated.

By examining the messages both linguistically and visually through social networks, the researchers found that messages containing technical features, threat and severity related security characteristics were spreading rapidly [39]. The messages are spread widely by technology groups and around groups which are doing studies about security instead of conventional news channels [39].

While there have been several studies on social media discussions regarding data privacy issues, there has been very little research on discussions about CRAs. In one of those studies, Novak and Vilceanu [40] analyzed crisis communications via Twitter after the 2017 Equifax data breach. The data breach experienced in 2017 was not the first one for Equifax [40]. In 2015, the credit referencing agency experienced one more [40]. Nevertheless, the breach experienced in 2017 was more effective because of the impact of the breach. According to the predictions, approximately 144,5 million people over 18 years old were affected from this data breach. After the explanation of the CEO of Equifax, Equifax was trend topic on Twitter for 3 days [40]. Like during or after many other crises also after the data breach citizens turn to Twitter to obtain and share information about the event.

Novak and Vilceanu aimed to analyze the general thoughts about the crisis collecting the related tweets published on Twitter. They sought answers to the three research questions; Finding the reactions of users to the Equifax data breach, find out how twitter simplify the communications across communities and finally who were blamed by the users as guilty of the data breach. They collected tweets with some predefined hashtags (#Equifax, #Equifail, #WheresMyData, #Equifaxbreach, etc.) during the 3 weeks after the breach was disclosed by Equifax. Through a qualitative analysis, they identified discourses that represented user disappointment and reactions to the incident. Breaking news, anger and outrage, and blame attribution were reported as major discursive patterns [40].

The aim of this thesis is to explore CRA related privacy concerns observing the interactions between CRAs and their customers. Concerns raised by different groups such as national authorities in charge of data protection issues are also covered to enrich our findings.

CHAPTER 4

METHODOLOGY AND DATA USED

In this chapter the methodology and data used in the study is explained, including how the raw data is collected and how we conducted pre-processing and manual selection of tweets for further analysis.

4.1 Organizations and Social Media Accounts Studied

The three major CRAs existing in the US and also serving in many other countries (Experian, Equifax, and TransUnion) [17] were selected as representative CRAs for our study. All the CRAs we mentioned that we used in the study hold credit records of billions of individuals and businesses. In addition to the three CRAs, we also looked at the UK's data protection authority, ICO, and two UK-based privacy-advocating NGOs, Privacy International and Open Rights Group (ORG). In the choice of social media platforms, we decided to focus on Twitter because as of 2020 there are 340 million active users at twitter and approximately 98 thousand tweets are sent in one minute. People are discussing and expressing their opinions and feelings on this platform about a topic discussed.

Twitter has become the easiest platform to follow the current events and last-minute developments in the world. Many past studies on social media analysis used data on Twitter because Twitter is a more lexical platform than other social media platforms. The other ones are more visual. Some organizations have multiple Twitter accounts, they have accounts with country names in which they serve like @Experian_US, @Experian_TR, @TransUnionUK, @TransUnionSA, and we decided to limit our study to the main official account (@Experian, @Equifax, @TransUnion, @ICOnews, @privacyint, @OpenRightsGroup), assuming that one has a broader coverage on issues such as the GDPR and faces all visitors of the organization. The actual Twitter accounts used can be found in Table 4.1. The description of the table is as following;

- A = tweets collected from each target organization's official Twitter account(s),
- B = public tweets mentioning each target organization's official Twitter account(s),

- C = public tweets mentioning each target organization’s official Twitter account(s)

Table 4.1 Twitter accounts and number of tweets

Organization(Account)	#(A)	#(B)	#(C)
Experian (@Experian)	3.400	540	13.629
Equifax (@Equifax)	3.598	210	2.574
TransUnion (@TransUnion)	3.330	120	1.878
ICO (@ICOnews)	3.292	233	-
Privacy International (@privacyint)	3.268	128	-
ORG (@OpenRightsGroup)	3.244	105	-

4.2 Raw Twitter Data

Tweets used in the study were collected via a Python library called Tweepy. Tweepy allow the user easily to access to different Twitter APIs but before using Tweepy the user should ask for API keys from twitter. These access keys let the user use the API. With the methods which the API contains the user can access to some information of the tweet the API returns a JSON set. The JSON returned includes tweet and user information.

A tweet has a creation date, an unique id, the tweet (text) itself and sometime a location information that are described as following.

- created_at:
- id_str
- text:

- place

A user has a unique id also, users name, screen name and most of the users have account bio.

- user:
    - id
    - name
    - screen_name
    - location
    - url
    - description

The enitities object includes the hashtags, urls and user mentioned in the tweet.

- entities
    - hashtags
    - urls
        - unwound
            - url
            - title
    - user_mentions

Firstly, we used Twitter's Search API to collect public tweets that cover the names of CRAs. The search API takes 10 parameters API.search(q [,geocode] [,lang] [,locale] [,result_type] [,count][,until][,since_id][,max_id][,include_entities])

- q: This parameter is the query parameter. The user can search for any query up to 500 characters.
- geocode: This parameter contains a string of latitude, longitude and radius (the radius should be described it is either mi(miles) or km(kilometers)) '37.781157, -122.398720,1mi'. The API searches for the users containing the latitude and longitude within the specified radius.

- Lang: This is the language parameter. For searching a specific language by using the ISO 639-1 code.
- Locale: The language of the query the user sends.
- Result_type: The user can choose 3 options for this parameter. “mixed”, “recent”, “popular”. The default option is “mixed” which returns both recent and popular tweets. “recent” returns only recent tweets, “popular” returns only popular tweets.
- Count: The number of tweets to return from each page.
- Until: This is a date format parameter. The user can define until what date the crawling has to be done. But it is important to note that the search API crawls only 7 days before the current date. So, determining a date older than 7 days will not return you any tweets.
- Since_id: The user can identify a tweet id. This parameter returns tweets with bigger id than the identified id.
- Max_id: With the max_id the user can reach tweets with smaller id than the identified max_id.
- Include_entities: This parameter gets Boolean value “true” or “false” when choosing false the entities will not include in the return set. The default is true.

In our study we used only the q (query) parameter which was q= (‘Experian OR Equifax OR TransUnion’). My main aim was collecting tweets containing the names of the CRAs in anywhere of the tweet. The q parameter is case sensitive. We started collecting the data in November 2019 and kept crawling for 3 months to obtain representative samples. Tweets containing the name “Experian” were totally 13.629, “Experian” had the number of 2.574 and the number of tweets containing “TransUnion” were 1.878. The details can be seen in table 4.1.

Secondly, we collected tweets in which official twitter accounts of the six target organizations were mentioned using ScrapeHero Cloud. ScrapeHero is a crawling tool which is web based. It has premade (ready) crawlers and also APIs the client can be used. With this tool or the API the user can scrape data from web sites like Amazon, Instagram, Google, Twitter etc. In this study the premade tool has been used. During the crawling you can control the crawl status if it is finished and how many pages are crawled until that time and after the crawling process you can obtain the total pages crawled in the current crawling. The data that is scraped can be downloaded in many types like CSV, JSON and XML. You can also transfer the results to your dropbox. The user can also set a program so that the crawler can start whenever you set it and can crawl the up to dated data from the websites. ScrapeHero Cloud is a paid app only the first 25 pages to crawl is free and after that the tool has packages you have to pay for.

The tool allowed us to retrieve tweets published since January 2018 until February 2020 in which the data collection process was completed. Choosing the beginning date as January 2018 was because of the announcement of the GDPR. The GDPR was announced in May 2018. So, start from the beginning of the year was a good idea. We ended our whole data collection process in February 2020. To use the ScrapeHero a url needs to be created from twitters advanced search.

Twitter Advanced Search is a twitter interface to find some specific tweets easier by creating a query. On this web interface you can define many parameters like; words, accounts, interactions and dates. The "words" parameter can determine the following five properties. All the words stated (anywhere in the tweet), exactly the words stated (in the written order), anyone of the words stated (anywhere in the tweet), tweets without all the words stated (anywhere in the tweet) and hashtags. The "accounts" parameter can determine the following three properties. Tweets published by the stated accounts, tweets that were answered to the stated accounts and tweets which mention the stated accounts. The interaction parameter contains the minimum numbers of replies, minimum numbers of likes and the minimum numbers of retweets. And lastly the date parameter returns the tweets published after the stated starting date and before the stated finishing date.

Lastly, we collected the most recent tweets published by official Twitter accounts of the six target organizations using the User_Timeline API. The User_Timeline API returns the most recent tweets published by a specified user of the authenticated user.This method takes five parameters. API.user_timeline([id/user_id/screen_name][, since_id][,max_id][,count][,page])

- id/user_id/screen_name: This parameter is the unique id, user id or the screen name of the user of which the recent tweets will be collected.
- Since_id: The user can identify a tweet id. This parameter returns tweets with bigger id than the identified id.
- Max_id: With the max_id the user can reach tweets with smaller id than the identified max_id.
- Count: The count of tweets to retrieve.
- Page: The page to retrieve.

All these parameters are optional. If the method is used by no parameter, it returns the most recent tweets of the authenticated user as default. In this study only the screen_name parameter is used for all the target organisations (ICOnews, Experian, TransUnion, Equifax, privacyint, OpenRightsGroup). The user_timeline returns the most recent 3200 tweets. We tried to get these tweets within a loop so that we can get the last published tweets also. Because the total number of tweets published by each account are different from each other the oldest dated tweet of each 3200 tweet of each account are also different. In other words, the number of tweets of the accounts used determines how historical the tweets collected are.

In this perspective tweets of Experian were since October 2019 and of Equifax were since May 2019. The number of tweets posted by TransUnion was relatively low, so we retrieved tweets of this CRA since March 2017. It was a similar case for the ORG where we could access to tweets posted since April 2017. We could access to tweets of the ICO since February 2019 and tweets of the Privacy International since May 2018. At the end, we collected 39,549 tweets in total. The number of tweets crawled for each group can be seen in Table 4.1.

4.3 Data Pre-Processing and Cleaning

Our data collection protocol includes the following three main steps.

1. CRA-related filtering: The data collection process as described in the previous part was contains 3 main collection types which was collecting the tweets in which the names of the CRAs (Experian, Equifax, TransUnion) contain as the first type. The second one was collecting the tweets which mention the six target organizations (Experian, Equifax, TransUnion, ICO, Privacy International, Open Rights Group) by the tool ScrapeHero Cloud and lastly the most recent tweets published by the six target organisations official accounts. This allowed us to narrow down our focus to the CRA context.
2. GDPR-related filtering: As we obtained the tweets of the 6 target organizations (Experian, Equifax, TransUnion, ICO, Privacy International, Open Rights Group), in order to eliminate irrelevant tweets, we identified a list of keywords considering related elements of the GDPR in the CRA context. We extracted 85 keywords manually from the GDPR document itself and the ICO's guideline to the GDPR (see Table 4.2) as well as we make a analyse on the tweets we collected until that date. Words existing in the tweets frequently related about the main subject GDPR and CRA. We kept out dataset in database tables. So, we construct a SQL query to find the tweets relevant with the 85 keywords. We limited our analysis to tweets that cover at least one of the identified keywords. We ended up with more than 12,000 tweets after this filtering step.
3. Manual Filtering: A majority of the tweets obtained in the second step are generic tweets published to inform people about data privacy or the GDPR. Since the aim of the study is to observe meaningful discussions around both CRA- and GDPR-related discussions, we included tweets that have direct and implicit mentions of the GDPR or any element of it. We also eliminated informative tweets manually that give very general information about the GDPR. After applying this step, we surprisingly found that only a very small set of 153 tweets remained as relevant, which were used for our further analysis.

Table 4.2 Table of keywords

Access	Accountability	Accuracy	Adequate	Automated
Certification	Codes of conduct	Confidential	Consent	Contract
Controller	Correct	Criminal	Cyber	Cyberattack
Data integrity	Data leak	Data safety	Delete	Decision
Encryption	Erase	Erasure	Fair	Fairness
Forget	Forgotten	Format	GDPR	Hold
Impact	Inform	Law	Lawful	Legal
Legitimate	Limit	Limitation	Long	Machine Readable
Minimization	Minimum	Needed	Object	Obligation
Offence	Outside	PECR	Period	Personal
Probability	Principle	Processing	Processor	Profiling
Protection	Public Task	Purpose	Rectification	Relevant
Remove	Request	Restrict	Retain	Retention
Revoke	Right	Secure	Security	Sell
Sensitive	Sold	Special Category	Storage	Third Party
Third Parties	Transfer	Transmit	Transparency	Transparent
Update	Vital Interest	Confidentiality	Withdraw	Years

4.4 Descriptive Analysis

We used thematic analysis to analyse our data. Thematic analysis is used generally for qualitative studies. Fundamentally thematic analysis is used to find an answer to the question of the researcher. These questions are usually about people's views, knowledge, opinions or experience about any subject, a device, a software used widely, in short about anything the researcher is curious about. Data can be collected from various platforms like interviews, social media platforms, blogs where discussions made etc. There are many approaches to processing thematic analysis but the widely used contains 6 steps [41].

- Familiarization: Firstly, it is important that the researcher know the data. The researcher should be familiar about the data collected.
- Coding: In this phase the data should be highlighted according to the sentences, words, phrases that are related with the research question. The highlighted sentences are coded by the feeling or idea of it.
- Generating themes: After coding each highlighted phrase. The researcher combines the codes related with each other and generates new themes.
- Reviewing themes: When the generating themes phase ended a general review should be done to find out if the themes generated are consistent with the research question. Do the themes generated occur really in the dataset or is something missing can new themes added, or should anything has changed?
- Defining and naming themes: Finally, the theme list the researcher has must be named, labelled according its meaning. The names given to the themes should be succinct and easy to understand.
- Reporting: Lastly the researcher should report the results.

The count of the themes varies. A theme defines something important in the dataset related to the research question. So, the important thing is not the count of themes but does the theme adequately describe the importance of the data set for the research question is more important [42].

We manually labelled the 153 tweets to uncover CRA-related data privacy issues discussed on Twitter. While labelling, we took the definitions given in the GDPR about individual rights, lawful basis for processing and key principles into consideration and performed the labelling accordingly. Individual rights consist of eight titles.

- Right to be informed: The data owner has the right to be informed about the usage of his/her data and the information of the personal data that the data processor hold.
- Right to access: The data owner has the right to access his/her information and take a copy of them.
- Right to rectification: The data owner has the right to correct incorrect data and complete if there is any missing data.
- Right to erasure: The right to erasure also named as the right to be forgotten give the data owner the right to request to delete the personal data hold by the data processor.
- Right to restrict processing: The data owner has the right to request hiding or restricting his/her data.
- Right to data portability: The data subject has the right to request the reuse of his/her data or request to transfer his/her personal data to another location for another use.
- Right to object: The individuals have the right to protest the processing of his/her personal data in some situations.

Law basis for processing contains eight titles. Lawful basis are the rights of the data controllers while processing data. If a data controller want process someone's personal data, the controller must have a valid law basis. None of the law basis is more important than the other. The importance changes according to the aim of processing and the relationship with the data subject.

- Consent: Consent means offering individuals real choice and control. The data subject give permission to the data controller for processing personal data.
- Contract: A contract is a document based on the processing of personal data. Used if you offer a contract service.
- Legal Obligation: If the data controller needs to process the personal data because of a general law or a legal obligation this lawful basis is the one he/she can rely on.

- Vital interests: If the data controller process the personal data to protect someone's life then the vital interest lawful basis is sensible but if there is any other solution without processing personal data then this lawful basis is not useful.
- Public task: The data controller can rely on this lawful basis if it is to be processed for official use.
- Legitimate interests
- Special category data: Special category data are sensitive data like ethnic origin, political opinions, religious etc. To rely on this lawful basis the data controller should comply one of the situations defined in Article 9 in the GDPR.
- Criminal offence data: If the data controller has official authority, he/she can process personal data related to criminal provisions and crimes with an official capacity.

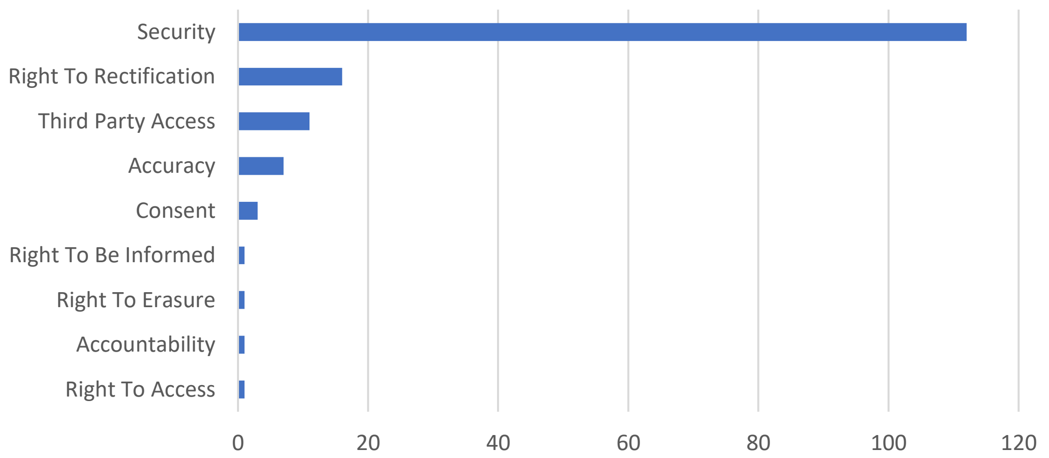
And lastly key principles contain 7 titles

- Lawfulness, fairness and transparency:
- Purpose limitation: The data holder should determine his/her exact aim at the beginning.
- Data minimisation: The data holder must be sure that the data he/she hold is necessary for his/her purpose. The data processor should not contain more data than is redundant for its purpose.
- Accuracy: The data holder is responsible about the correctness of the data he/she hold. Hosting incorrect data is the data holder's fault and to correct, update the data is also its responsibility.
- Storage Limitation: The data processor has not the right to hold the personal data longer than needed.
- Integrity and confidentiality(security): The data subject must have suitable security precautions about data holding.
- Accountability principle: The data holder should take responsibility on what he/she do with the personal data held.

We follow the six steps explained as thematic analysis steps. We coded our data set and we generate themes according to the results that were obtained after coding. After reviewing the themes by reviewing the whole data set, we gave names to the themes that we extracted based on the definitions given in the GDPR about individual rights, lawful basis for processing and key principles into consideration.

The labels were checked by two independent researchers. The identified labels and their distributions are given in Figure 4.1.

Table 4.3 Distributions of tweets per GDPR-related topic



	Right To Access	Accountability	Right To Erasure	Right To Be Informed	Consent	Accuracy	Third Party Access	Right To Rectification	Security
	1	1	1	1	3	7	11	16	112

4.5 Automated Analysis

After labelling the 153 tweets manually we tried to make analysis by automatize with machine learning algorithms. Machine learning algorithms are basically divided into two; supervised learning and unsupervised learning. Supervised learning has some input variables and output variables. It is called supervised because a set of labelled inputs are given in the system so the algorithm learns from this set. This set is named as training set it is a kind of teacher therefore it is called supervised learning the training set looks like a teacher or a supervisor. Support Vector Machines, Linear Regression, Logistic Regression, Naïve Bayes, Decision Trees and Neural networks can be given as examples for supervised learning. Unsupervised learning algorithms have only input variables. There are no output variables, there isn't a set for training. The algorithms are based on clustering. The inputs which are similar to each other will be contain in the same cluster. As example K-means clustering, K-NN (k-nearest neighbours) can be given.

In the automatic part of the thesis we make an automatic labelling across the whole dataset. The data set at the beginning of the descriptive analysis was around 40.000 tweets. We prepared a dataset that contains three different labels.

1- GDPR/CRA_Related
2- GDPR/CRA_Unrelated
3- Non_GDPR

In the pre-processing and cleaning part of data we mentioned 3 stages of filtering;

1- CRA-related Filtering
2- GDPR-related Filtering
3- Manual Filtering

In the first stage we had data collected from twitter based on some accounts (). This stage contained around 40.000 tweets. In this corpus there were many irrelevant data with both GDPR and CRAs. So, we applied a second stage which was GDPR related filtering. This stage was applied by using a keyword list of 85 keywords. After that we get around 12.000 tweets which are relevant with GDPR and there were still tweets irrelevant with CRA. Therefore, we made lastly a manual filtering where we labelled the 12.000 dataset as IN and OUT. After this stage we get only 153 tweets.

The first label which is GDPR/CRA_Related contains the 153 tweets that were labelled manually in the descriptive analysis part.

The second label GDPR/CRA_Unrelated are the labels that are relevant with GDPR but irrelevant with CRA.

The last label NONGDPR are the tweets irrelevant both with GDPR and CRA.

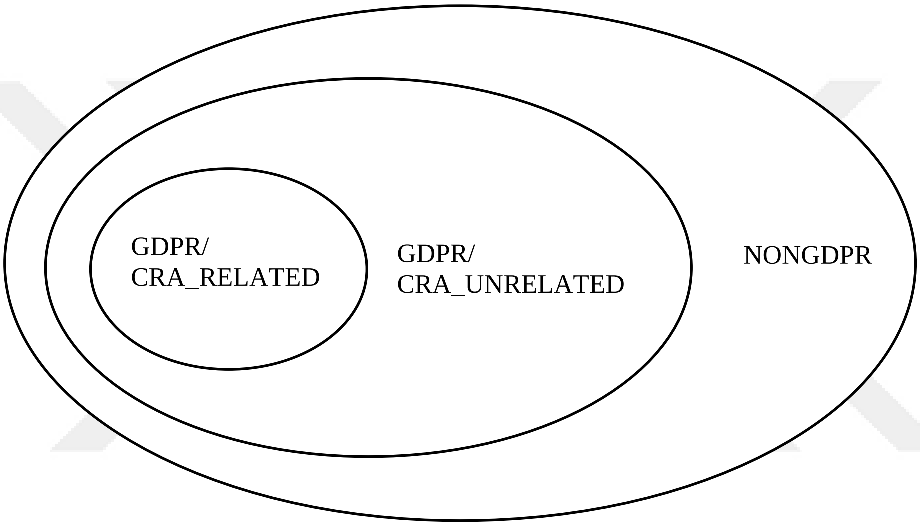


Figure 4.1 Data description

We prepared a dataset of 1377 tweets and divide this dataset into %70 train and %30 test. Because we had only 153 tweets of GDPR/CRA_Related label we made a data_multiplexing by including one tweet of the 153 tweets 3 times in the dataset. After that we choose randomly 459 tweets from each of the rest of the labels. So, a balanced dataset was prepared.

We used Bert embedding as embedding model and some different neural network algorithms to train our machine. At the end of the training we found the “confusion matrix”, “accuracy”, “loss values” for each epoch and train and validation sets separately.

After training and creating the model we test the whole dataset on the saved model. So that we can see if there are tweets overlooked, missed while labelling manually.

We used pytorch for all the process. Pytorch is a library that uses the power of GPU and is used for deep learning research. It provides maximum flexibility and speed in such algorithms. This library is very similar to Numpy library but pytorch use the advantages of the GPU and is very useful while creating deep neural networks. This library can create neural network models without problem.

We used Bert (bidirectional encoder representation from transformers) language model in this thesis. Bert was published in 2018 by some Google employees. Bert developed for English-language has two models. Bert_base which has total 110M parameters and Bert_large which has total 340M parameters. In this thesis Bert_base is used as tokenizer.

A definition is needed for labels and text fields. This definition defines the type of the data and explanations for converting the data to Tensor. The field class takes many parameters which define the type of the data of the tensor like;

- Use_vocab: This parameter is a Boolean parameter and the default value is true. This parameter indicates if the field should be converted to numerical vocab. If the value is false, the field should already be numerical. In this thesis it is used as false.
- Tokenize: This parameter defines the function that will tokenize the field. In this thesis Bert language model is used as tokenizer.
- Preprocessing: The preprocessing parameter convert the tokens after the tokenize method into the indexes.

The labelfield class identify the type of the label data and in this thesis it is used as int64.

After the fields should be defined. In this thesis there are 2 columns in the dataset so there are 2 fields named text and label. The next step after defining the fields is to read the csv files from the training file. The TabularDataset class create a dataset in table format from the given “csv”,”tsv” or “json” file path.

A batch size is a size parameter which is needed for big training sets. While training a model in neural network backpropagation takes lots of time and with lots of data training at the same time it can be take lots of hours maybe days. Therefor a batch size is defined for this kind of problems. This parameter determines the number of data that should be taken into each iteration. The best batch size can be found by trying many but if the size of the data is smaller than 2000 than it is possible to use the length of the whole data set as batch size.

While building the model firstly we should load the pre-trained model and this model should be the same as the model given as tokenizer. The pre-trained model is used as embedding. In this thesis three different neural network methods are used. RNN , GRU and LSTM. To see if there are differences while training and validating.

In the training phase an optimizer and a criterion a “loss function” is defined. Optimization functions are functions used in neural networks to find the optimum result for the problem. There are some optimization functions which calculate the optimal learning rate by itself. In this thesis Adam optimization function is decided to use after making a research on different text classification studies using neural network. Most of the studies used Adam as optimization function.

Criterion or loss functions are function to calculate the differences between the predicted result and the actual result. According to the loss function result the weights of the neural network will be updated. Optimization functions and loss function are working together.

As loss function this study used crossentropyloss. This loss function is used by many different studies and it works well for mutli class problems.

CHAPTER 5

RESULTS

5.1 Descriptive Analysis Results

Reviewing the 153 relevant tweets, it is clear that data privacy discussion on Twitter were dominated by data breach incidents. Other popular topics were sharing personal data with third parties, some generic security issues and accuracy of the data processed by CRAs. Although not very common, we can still see tweets about some data subject rights like the right to be informed, the right to erasure and the right to rectification. We also observed that discussions were dominated by individuals. 109 tweets of our dataset which contains 153 tweets were published by individuals. While CRAs posted data privacy tweets just to inform their followers about their security measures or to answer their customers' questions about incorrect data in their credit files. Surprisingly, we could not find any tweets published by the ICO, Privacy International or Open Rights Group, which explicitly mentioned both CRA- and GDPR-related topics.

In order to identify cultural differences in reactions to CRAs, we have also tried to access country information of the individuals. Among the 86 unique accounts who involved in the discussions, we could have accessed country information of 56 accounts. The country information is searched manually. All the bio information of each account containing in the 86 unique account was examined and the country information of the accounts which stated were collected. A majority of the individuals which were 44 accounts are from the US (51.2%) and there are only 5 accounts from the UK (5.8%). The other countries were the Netherlands, South Africa, and Algeria. Detailed data is given in figure 5.1.

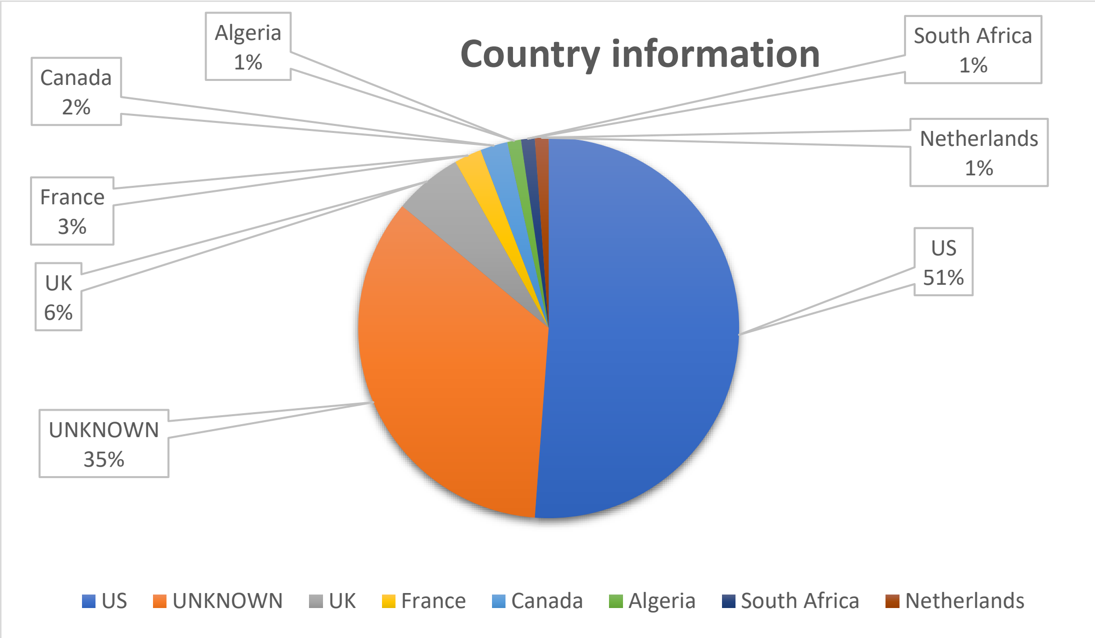


Figure 5.1 Country distributions of tweets in the dataset

5.1.1 Security

It can be seen clearly that security issues are dominated in the discussions on GDPR related discussions in CRA context. The discussed security issues can be divided into two main subjects; one discussed by individuals and the one by CRAs. Majority of the tweets published by individuals are about data breach incidents whereas CRAs' security discussions are limited to information they provide regarding their security measures. So, we divided the security topic into two topics as data breach incidents and general security issues.

5.1.1.1 Data Breach Incidents

Among the 153 tweets, 72 of them have been identified to be related to data breaches incidents. According to the GDPR the data controller has rules to do after a data breach. Firstly, the notification of the data breach to the supervisory authority. A supervisory authority is an authority which will supervise the regulation in this case GDPR. For example, UKs supervisory authority is Information Commissioner's Office (ICO). If a personal data breach happened the data controller should notify the supervisory authority about the data breach without any unnecessary delay, the optimal time is not later than 72 hours after aware of the data breach. If the data controller notifies the data breach later than 72 hours the data controller must notify the breach with a valid reason [16].

The notification should include at least four important explanation;

1. The data controller should describe the content of data subject of the data breached. The kind of categories of the data subject and approximate number estimated.
2. For more information the contact information of the data protection officer or someone who can give detailed information if necessary.
3. The data controller should explain the possible outcomes, results, of the data breach.
4. The notification should include an explanation about the measures taken or suggested.

If all the information requested cannot reported at the same time, the information should be reported progressively without any unnecessary delay. Secondly the data controller should notify the data breach to the data subject. If the results of the data breach will create or created a big risk to the rights or the freedoms of the individuals the data breach must be reported to the data subjects without any unnecessary delay. The notification that will be done should contain the items 2, 3 and 4 explained at the supervisory authority notification part. The notification to the data subject is not required if one of the following occurs [16].

1. After the data breach if the data controller took every precaution or if previously taken measures such as encryption and if sure that any 3. party who is not authorised could not access any data information. The notification to the data subject is not required.
2. If the data controller took precautions against any risk to the rights or freedoms of all data subjects.

According to the information above as data subjects the key role players in those discussions are individuals, the CRAs as data controllers are not as active as expected where Equifax published 3 and Experian published 2 tweets. The tweets published by

Equifax are informative tweets given as a reply to individuals about 2017 data breach. An example can be given as;

"@D… Thank you for contacting Equifax. If you have a question about the 2017 data breach settlement, please visit: https://t.co/EVlbzHwHQo. -George R."

Two tweets published by Experian provide links to podcast published on the company's website about Experian data breach resolution. We have observed several tweets that reminds the deadline for claims for cash payment and free services for the ones who are a part of this breach. There also complaints about this application such as:

"What's the security of my private data worth? Apparently, less than $9. Thanks, @Experian!"

It is possible to add that tweets under this category are the ones that cover anger or blame attribution the most.

This tweet also points to the rule given in the GDPR. According to the tweet a late notification is the subject. The data controller has to notify the data subject without any unnecessary delay if there are risks to the rights or freedoms of individuals.

5.1.1.2 General Security Issues

Credit reference agency information notice (CRAIN) which is the document jointly published by the three main CRAs that we cover in our study, Experian, Equifax and TransUnion explains how these CRA obtain, process and share the personal data they hold. Because the CRAs are based in UK they hold their data in databases located in the UK. Before sharing the data with any third party they make sure that the third party is a real and legal business. Even if they are sure that the third party is a real and legal organisation, they record details of each search and they named it "search footprint". If any of the credit reference agency sends the personal data to any other country except UK and countries in the European Economic Area, they ensure that appropriate security measures are taken according UK and European data protection requirements like GDPR. The tweets about the general security issues discussion were dominated by the CRAs. Under this topic the CRAs introduce their security measures. A tweet published by TransUnion in 2018 November can be given as a representative example to this category:

"We're proud of the credit and identity protection tools that we provide to consumers. Read our Corporate Responsibility Report at: ..."

or another one published by Equifax in August 2018

"We've been working diligently to improve cybersecurity efforts. Learn more about how our Workforce Solutions team is transforming security: ..".

CRAs also use Twitter to suggest their customers to freeze their credit to avoid potential identity theft. Examples can be seen as follows;

"The idea behind a freeze is that you are blocking access to your report from a potential identity thief credit freeze may seem like an extreme move, but it can be powerful way to protect against identity theft."

which was published by Experian in December 2019 and which was published by TransUnion in August 2019 respectively.

"You protect your smartphone, so you should protect your credit too. Freeze your credit and keep identity thieves out - for free!."

Here it may worth to note that a credit freeze means taking control on financial information given in your credit report. This prevents identity theft and block access of potential creditors to credit reports. After freezing a credit, only current creditor and government agencies can access the credit report in some emergence cases [43]. Setting up an fraud alert to warn the creditor in case of identity theft or any other fraud is another approach suggested by CRAs.

Very few tweets published by individuals are complaints regarding data confidentiality where an interesting example can be given as:

"@Equifax @AskEquifax my account currently showing other people's financial information. Insane level of privacy breach. Your reset password page also does not work. Any UK phone contacts?".

It is possible to report privacy concerns of the individuals as a consequence of existing or potential data breaches.

"Chinese Hacking Is Alarming. So Are Data Brokers. Companies like Equifax threaten our personal privacy and our national security".

5.1.2 Right to Access

Right of access is one of the most important right which contains in the GDPR. This right this right paves the way for some other rights like Right to Rectification and Right to Erasure. With the right of access, the information the data subject can get access are such as following [16];

- Processing purposes.
- The categories of personal data processed.
- The recipients.
- The planned period of storage.
- Information about the rights of the data has.
- Instructions on the right to lodge a complaint with the authorities.
- Information about the origin of the data, if these were not collected from the data subject himself.
- Any existence of an automated decision-taking process.

Our data set covers only one tweet about Right to access which introduce credit and identity protection tools to consumers via TransUnion.

"We're proud of the credit and identity protection tools that we provide to consumers. Read our Corporate Responsibility Report"

5.1.1 Right to Rectification

We have identified 16 tweets regarding right to rectification and 11 of them were published by CRAs to engage with their customers due to an inaccurate information in credit files. The date subject has the right to request a rectification on his/her personal information. As the data controller the CRAs are obliged to meet this request without undue delay. As well as data correction under this rule the data owner has the right to complete his/her incomplete personal data. According to the tweets identified as right to rectification we can see that people are aware about their rectification right and they take steps related to it. It is surprising to see that CRAs reply to complaints via Twitter and ask their customer details via direct messages to response their enquiries. Following tweet of TransUnion can be given as a representative example:

"@S… Hi Shalom! I'm sorry to hear you are now seeing this inaccuracy. We can assist with correcting this information on your TransUnion credit file...!"

which was sent as a reply to a tweet of a customer:

"Please explain to me @Experian & @TransUnion how can I have a 30 day late payment reported to my credit report for an account that was paid in full over a month ago? …"

A reply from Equifax to a similar user tweet can be given as:

"@E… We apologize for the trouble this has caused, please send us a DM with your personal information, so we can properly assist you."

5.1.3 Accuracy

According to GDPR Article 5 accuracy is defined as a principle which is related to processing personal data. In Article 5 it is mentioned that personal data shall be accurate and if it is necessary it to keep the data up to date. The data controller has the responsibility to delete or correct the personal data according to their usages without delay. Under this category, we have limited our focus to tweets that only disclose/mention data inaccuracies without asking for correction. Following this approach, we have identified 7 tweets 6 of which were published by individuals. The most interesting tweet can be given as follows:

"@Equifax has been hit with a class action lawsuit from a consumer who claims she is a victim of inaccurate credit reporting..."

"GDPR on the credit agencies? They hold inaccurate info on you. They must correct it"

5.1.4 Third Party

GDPR defines "third party" in Article 4 as a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data. We have identified 11 tweets under this category all of which were published by individuals to display their frustrations and reactions to third party data access. Some examples can be seen below;

"@Experian Stop selling customer information to companies. Since making an account with you all 5 days, I ´ ..ve been receiving at least 8 spam emails a day."

"@TransUnion This was just after your employees stole their IDs and sold them online and to your business partners aka collection companies!."

"So turns out @Experian sold my contact info to credit card companies without my consent ... Pretty underhanded. Time for some subject access requests I think. #GDPR"

5.1.5 Right to be Informed

Even though right to be informed has stated to be one of the rights that challenges CRAs the most [18]. Data subjects have the right to be informed about the collections and the usage of their personal data. According to the GDPR the information to be provided changes according to where the personal data collected from. The law changes if personal data are collected from the data subject itself and if it obtained not from the data subject. In the case when the data provider is the data subject, the data owner has the right to be informed about the identity and contact details of the data controller, the purpose, reason of collecting personal data and the legal basis for processing, if there are third parties to share information about them and in addition to these cases the time of how long these data will be stored, the data subject has the right to be informed about his/her rights on the data like rectification, erasure or access to personal data etc, the data owner also have the right to know about withdraw consent at any time and also the right of making a complaint to a supervisory authority.

If giving personal data is a contractual or legal requirement and is it a must for the data subject to provide his/her personal data, the data subject must be informed about any automated decision-making and lastly if the personal data collected before for another purpose will now or in the future be used with an different purpose the data subject must be informed about the new purpose. In the second case where the data provider is not the data subject information to be provided are the same as in the first case excluding one item which is about if giving personal data is a contractual or legal requirement and is it a must for the data subject to provide his/her personal data instead of this rule the data subject must be informed from which source the personal data originate. In addition to all the rules when the data provider is not the data subject the data controller has some restrictions in time like after collecting data at latest within one month the data subject had to be informed.

If the personal data is collected to contact with the data owner the notification must have been given before the first contact with the data subject and if the data is to be shared with someone else the information must have been given before share. There are some exceptional circumstances there is no necessity to inform [16]. According to this information containing in the GDPR we have identified very few tweets related to this right, which can be given as follows;

"..Equifax are sending a data processor to your system that gathers personal data and returns an automated decision. Do you inform users of this? How does GDPR apply for cases like this?".

5.1.6 Right to Erasure (Right to be Forgotten)

According to article 16 in the GDPR if the purpose for gathering the personal data has ended the data owner has the right to request for an erasure or also when the data owner withdraw his/her consent and if the data have been unlawfully processed. The data controller has to meet the requested request and also if the data controller shared the personal data with any third party, he/she has the responsibility to inform these third parties that the data subject request an erasure [16].

We could have identified only one tweet regarding right to be forgotten which points to the impossibility of exercising this right.

"@wbm312 At least Transunion is candid about selling your information. Even it you're unable to get the info deleted, a little more power over non-transaction use of your data is huge."

5.1.7 Accountability

Principles mentioned in the GDPR are "Lawfulness, fairness and transparency" , "Purpose limitation", "Data minimisation", "Accuracy", "Storage limitation" and "Integrity and confidentiality (security)" the data controller has to be responsible for all these principles and show that it works in accordance with these principles our dataset covers just one tweet about accountability which has been published by an individual to share his/her reaction regarding the responsibility of the CRAs.

"@Equifax you need to be accountable to each persons data stolen every person that this affects remove all inquiries and increase scores by 50points PERIOD this pisses me off https://t.co/KRzgQzVfht"

5.1.8 Consent

If a processing is based on consent the data controller should be sure that the consent of the data owner is taken and can prove it. A data owner has the right to give consent as well as withdraw consent. When a data subject withdraws his/her consent the data controller should meet this request. Withdrawing a consent should be as easy as giving a consent.

Given the fact that the CRAs do not need to collect consent from their users, we were expecting to see some data privacy discussions around this issue. However, we have observed only 3 tweets mentioning consent.

"You can opt out of the sale of your data (as well as request access and deletion) at @TransUnion..."

One of those tweets was about the right to withdraw consent regarding emailing service of Experian.

" @Experian stop emailing me. I've unsubscribed #GDPR"

5.2 Automated Analysis Results

After labelling the 153 tweets manually we tried to make analysis by automatize with machine learning algorithms. A neural network structure is prepared. We tried 3 different neural network variations RNN, LSTM and GRU. LSTM and GRU are two variations of RNN.

Our data set consists of 3 main labels. GDPR/CRA_Related, GDPR/CRA_Unrelated, NONGDPR. There are 459 samples for each label. Totally the data set contains 1377 data. This data set is divided into %70 train set and %30 test set.

After training our models with these three neural network variations an automatic labelling phase was done. The automatic labelling phase is done on the 40.000 raw data set where no filtering has been done on it yet and we compared the results of the three variations.

Table 5.1 Hyperparameters used

Epoch	100
Hidden dimension	300
Bi-directional	False
Output dimension	3
Activation Function	Sigmoid

5.2.1 RNN (Recurrent Neural Network)

According to the past studies of text classification and neural network "adam" is used as optimization and "sigmoid function" as activation function.

After training the model with RNN the accuracy is %42.55. The confusion matrix is as following. The precision value of GDPR/CRA_Related is %28.26 and the recall is %31.70.

Table 5.2 RNN confusion matrix

	PREDICTED VALUES			
		GDPR/ CRA RELATED	GDPR/ CRA UNRELATED	NONGDPR
ACTUAL VALUES	GDPR/ CRA_RELATED	**13**	**1**	**32**
	GDPR/ CRA_UNRELATED	**15**	**16**	**106**
	NONGDPR	**13**	**18**	**108**

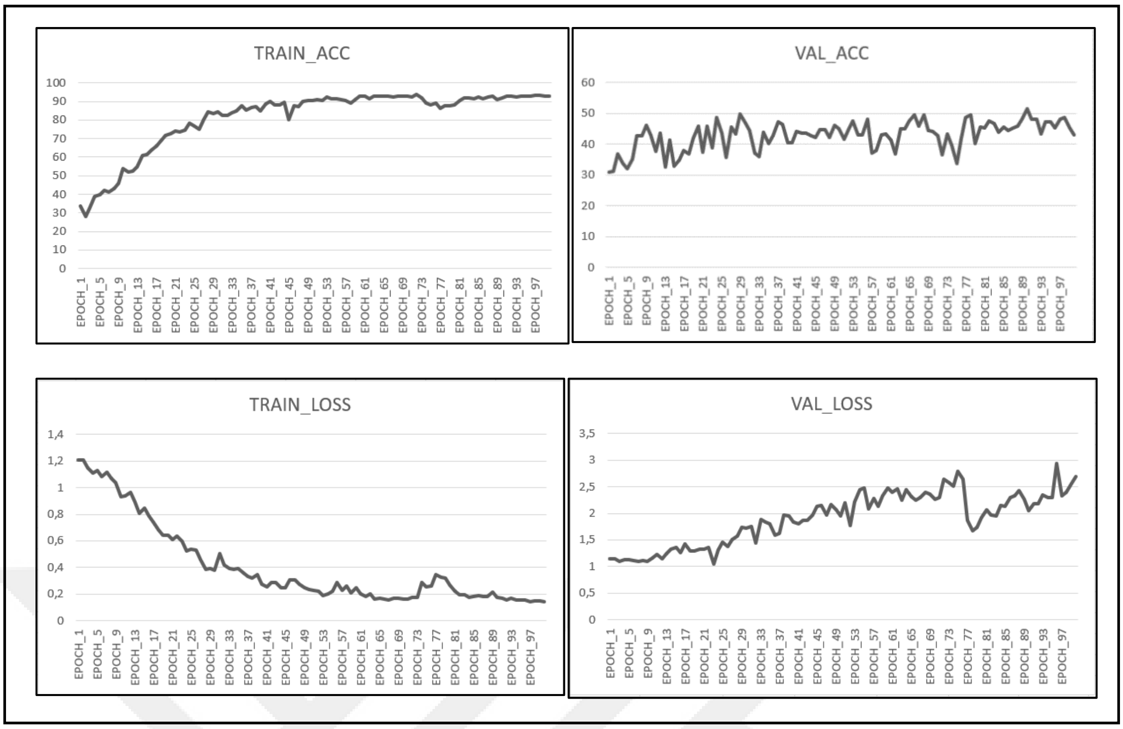


Figure 5.2 RNN accuracy and loss results for 100 epoch

5.2.2 LSTM (Long-Short Term Memory)

According to the past studies of text classification and neural network “adam” is used as optimization and “sigmoid function” as activation function.

After training the model with LSTM the accuracy is %59. The confusion matrix is as following. The precision value of GDPR/CRA_Related is %65.21 and the recall is %46.15.

Table 5.3 LSTM confusion matrix

		PREDICTED VALUES		
		GDPR/ CRA RELATED	GDPR/ CRA UNRELATED	NONGDPR
ACTUAL VALUES	GDPR/ CRA_RELATED	**30**	**10**	**6**
	GDPR/ CRA_UNRELATED	**11**	**99**	**27**
	NONGDPR	**24**	**54**	**61**

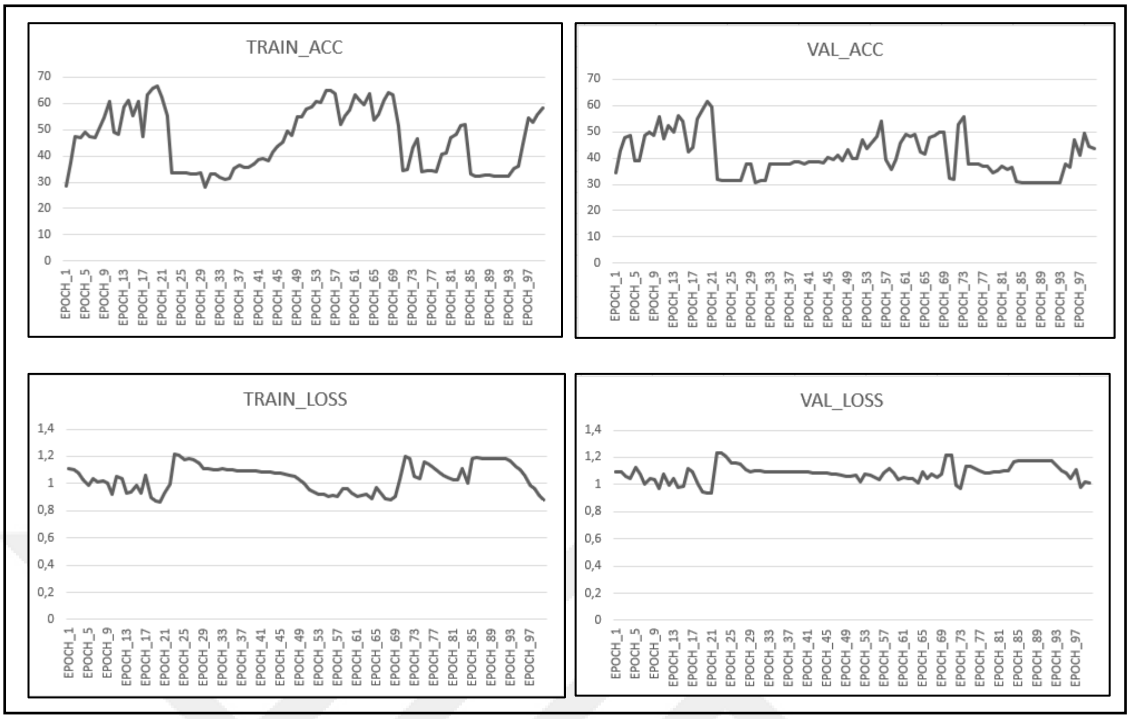


Figure 5.3 LSTM accuracy and loss results for 100 epoch

According to the past studies of text classification and neural network “adam” is used as optimization and “sigmoid function” as activation function.

After training the model with GRU the accuracy is %59.31. The confusion matrix is as following. The precision value of GDPR/CRA_Related is %80.43 and the recall is %38.95.

Table 5.4 GRU confusion matrix

	PREDICTED VALUES			
ACTUAL VALUES		GDPR/ CRA RELATED	GDPR/ CRA UNRELATED	NONGDPR
	GDPR/ CRA_RELATED	**37**	**1**	**8**
	GDPR/ CRA_UNRELATED	**25**	**68**	**44**
	NONGDPR	**33**	**20**	**86**

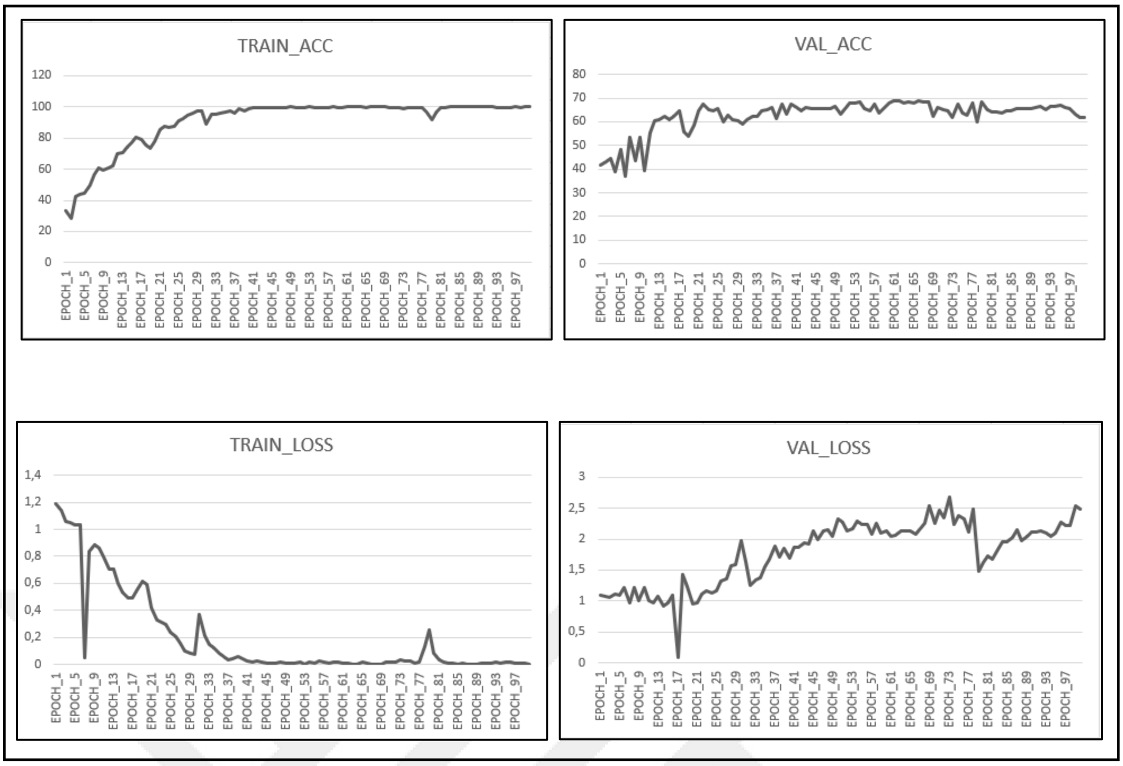


Figure 5.4 GRU accuracy and loss results for 100 epoch

big different in results. There is an experimental result that GRU trains faster and performs better when the dataset is small. By using larger datasets LSTM will give better results. GRU and LTSM are both solutions for vanishing gradient problem and because of the reminder structure both works well with language modeling. The results of this thesis also shows that GRU works better when using small dataset.

After the training part a automatic text classification was perform on the raw dataset of 40.000 data by using the model which gave the best accuracy (GRU).

The result are given as in the tables. There were 1868 data labeled as GDPR/CRA_Related and manually we labeled only 153 of the whole dataset.

Table 5.5 Manual and automatic label counts

	MANUAL LABELLED VALUES	AUTOMATIC LABELLED VALUES
GDPR/CRA_Related	153	1868
GDPR/_CRA_Unrelated	10608	25439
NONGDPR	29349	11835

Some of the examples of data which is missed can be seen as follows.

"@ … ' m mostly worried that places like transunion have a trove of data on me"

"@ … @ experian https : / / t . co / xquf9vn0zf"

"@ experian a2 cards being declined , collectors calling you , bank notifications for weird transactions , # creditchat credit drop"

It can be seen that after training the tweets containing the names of the CRAs are also labeled as GDPR/CRA_Related. The first one and the third one can be labeled as GDPR/CRA_Related. But the second one does not contain any information about GDPR but because the tweet contains the name of one of the CRAs it is labeled as GDPR/CRA_Related.

Some samples which are predicted as GDPR/CRA_Unrelated are given as following.

"@ … you would need to file a new dispute if it has been 3 years since you last disputed this information ."

Because this tweet is a reply from one of the CRAs. The tweet looks like only a general tweet about GDPR but not about CRAs. But because it is a reply this tweets was labelled manually as GDPR/CRA_Related.

“xiaomi partners with experian to offer free credit score update in the mi credit app . https : / / t . co /”

“@ … @ …. @ experian @ … wait , what ? ! ? the dmv sells my data ? oh that better be covered under this new law !”

“and experian will take no rsponsibilty for its validity , accuracy or loss . they will just monitise it . https : / / t . co / wnywdutarb”

There are also tweets labelled as NONGDPR.

“@ … hi , the reason why the scores you notice are different is due to the two accounts using separate scoring models . chase is using the vantage scoring model and bank of america uses the fico scoring model . thanks”

“@ … i already contacted them to ask them to sort that out they said it will take about 10 days to update but even now it still appears as a areas @ transunion please help”

The history of this tweet is also about a wrong information in the credit files published by Transunion. Therefore it was labelled as GDPR/CRA_Related Manually.

CHAPTER 6

CONCLUSION AND FUTURE WORK

We have conducted a study based on a large database of the public communications on Twitter made by CRAs, their followers (or others who mention them in their tweets) and organizations that organise campaigns against CRAs. Even though it is widely known that CRAs collect sensitive personal information from several sources and process it, to the best of our knowledge, this is the first study that investigates the privacy discussions regarding this processing. Both the automatic and manual analysis both gave consistent results with each other. Our study reveals that CRAs don't prefer to be salient about data privacy discussions from GDPR's point of view. Perhaps most interestingly, organisations that organise data privacy campaigns or even ICO were not involved in the privacy discussions on Twitter either. The automatic results also support this idea because the vast majority of the 2091 were published by individuals and CRAs. Both in manual labeling and automatic classification the vast majority is published by individuals which can be interpreted as data privacy discussion on Twitter in CRA context are dominated by complaints or questions of individuals. Although there are differences in the numbers, the results are consistent with each other. Data breaches, inaccurate personal information in credit files and the difficulty to correct them, finally third-party data access have been observed as the main privacy concerns of individuals. Considering the limitation of discussions on Twitter, we call for urgent more research into the interfaces between data protection law and the CRAs.

Since the ultimate goal of this study is to understand CRA- and GDPR-related discussions on Twitter, our data collection step might have led us to miss privacy discussions that lack explicit mentions of the GDPR or CRA elements. Our focus on only 3 large CRAs may have led to a lack of coverage of discussions on other CRAs. In our future work, we plan to broaden our scope and investigate more CRAs and look into tweets covering implicit discussions on the GDPR and CRAs and also general discussions on CRA-related privacy issues beyond the GDPR. We also plan to study CRA accounts from different countries to better understand cultural differences behind related discussions.

REFERENCES

[1] M. G. M. Rothemund, "The European Credit Information Landscape: An analysis of a survey of credit bureaus in Europe. European Credit Research Institute (ECRI) Industry Survey, commissioned by Association of Consumer Credit Information Suppliers (ACCIS)," 2011. [Online]. Available: https://www.ceps.eu/ceps-publications/european-credit-information-landscape/.

[2] "Equifax Limited, Experian Limited, TransUnion International UK Limited: Credit," 2020. [Online]. Available: https://www.equifax.co.uk/crain/. [Accessed 2020].

[3] *REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation).*

[4] "ICO, Information Comissioner's Office, UK: Do the CRAs need my consent to hold," [Online]. Available: https://ico.org.uk/your-data-matters/credit/#consent.

[5] "UK Parliament: Consumer Credit Act 1974, Part X: Ancillary credit businesses.," 2018. [Online]. Available: https://www.legislation.gov.uk/ukpga/1974/39/part/X.

[6] "Privacy International: Tell companies to stop exploiting your data," [Online]. Available: https://privacyinternational.org/campaigns/take-control-your-data.

[7] "Privacy International: Our complaints against Acxiom, Criteo, Equifax, Experian,Oracle, Quantcast, Tapad," 2018. [Online]. Available: https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.

[8] "Privacy International: Request for an assessment notice of data brokers: Experian & Equifax (the credit reference 'data brokers').," 2018. [Online]. Available: https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20Complaint%20Experian%20%26%20Equifax.pdf.

[9] "Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad | Privacy International," [Online]. Available: https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad. [Accessed 13 12 2020].

[10] R. B. Sağlam, Ç. B. Aslan, S. Li, L. Dickson and G. Pogrebna, "A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR," in *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, 2020.

[11] F. Kammueller, "Formal Modeling and Analysis of Data Protection for GDPR Compliance of IoT Healthcare Systems," in *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2018.

[12] S. Wachter, B. Mittelstadt and L. Floridi, "Transparent, explainable, and accountable AI for robotics," 2017.

[13] "Association of Consumer Credit Information Suppliers (ACCIS): ACCIS 2017 survey of members: Analysis of credit reporting in Europe.," 2018. [Online]. Available: https://accis.eu/wp-content/uploads/2018/11/AUG18_ACCIS-Survey-of-Members-2017_FINAL.pdf.

[14] T. E. C. O. /. B. E. d. U. d. C. (BEUC), "The never-ending European credit data mess.," 2018. [Online]. Available: https://www.beuc.eu/publications/beuc-x-2017-111_the-never-ending-european-credit-data-mess.pdf.

[15] I. C. O. U. ICO, "What should i do if my credit file is inaccurate?," [Online]. Available: https://ico.org.uk/your-data-matters/credit/#file.

[16] S. Gichimu, *Credit Reference Bureaus, Loans Advancement and Recovery Performance by the Higher Education Loans Board of Kenya,* Kenya: University of Nairobi, 2013.

[17] "The 3 major credit reporting agencies and what they do," [Online]. Available: https://www.thebalance.com/who-are-the-three-major-credit-bureaus-960416.

[18] *FINAL-External-facing-ACCIS-Contribution-2020-Evaluation-GDPR-Feb-2020.pdf.*

[19] A. Giachanou and F. Crestani, "Like it or not: A survey of twitter sentiment analysis methods," *ACM Computing Surveys (CSUR),* vol. 49, p. 1–41, 2016.

[20] "10 Twitter Statistics Every Marketer Should Know in 2020 [Infographic]," [Online]. Available: https://www.oberlo.com/blog/twitter-statistics#:~:text=Here's%20a%20summary%20of%20the,are%20between%2035%20and%2065.. [Accessed 27 12 2020].

[21] S. A. Salloum, M. Al-Emran, A. A. Monem and K. Shaalan, "A survey of text mining in social media: facebook and twitter perspectives," *Adv. Sci. Technol. Eng. Syst. J,* vol. 2, p. 127–133, 2017.

[22] A. Karami, M. Lundy, F. Webb and Y. K. Dwivedi, "Twitter and research: a systematic literature review through text mining," *IEEE Access,* vol. 8, p. 67698–67717, 2020.

[23] A. Tumasjan, T. Sprenger, P. Sandner and I. Welpe, "Predicting elections with twitter: What 140 characters reveal about political sentiment," in *Proceedings of the International AAAI Conference on Web and Social Media*, 2010.

[24] M. A. Bekafigo and A. McBride, "Who tweets about politics? Political participation of Twitter users during the 2011gubernatorial elections," *Social Science Computer Review,* vol. 31, p. 625–643, 2013.

[25] A. Reyes-Menendez, J. R. Saura and C. Alvarez-Alonso, "Understanding# WorldEnvironmentDay user opinions in Twitter: A topic-based sentiment analysis approach," *International journal of environmental research and public health,* vol. 15, p. 2537, 2018.

[26] J. R. Saura, A. Reyes-Menendez and P. Palos-Sanchez, "Are black Friday deals worth it? Mining Twitter users' sentiment and behavior response," *Journal of Open Innovation: Technology, Market, and Complexity,* vol. 5, p. 58, 2019.

[27] X. Zhou and L. Zhang, "Crowdsourcing functions of the living city from Twitter and Foursquare data," *Cartography and Geographic Information Science,* vol. 43, p. 393–404, 2016.

[28] N. N. Patel, F. R. Stevens, Z. Huang, A. E. Gaughan, I. Elyazar and A. J. Tatem, "Improving large area population mapping using geotweet densities," *Transactions in GIS,* vol. 21, p. 317–331, 2017.

[29] N. Mahroum, M. Adawi, K. Sharif, R. Waknin, H. Mahagna, B. Bisharat, M. Mahamid, A. Abu-Much, H. Amital, N. Luigi Bragazzi and others, "Public reaction to Chikungunya outbreaks in Italy—Insights from an extensive novel data streams-based structural equation modeling analysis," *PloS one,* vol. 13, p. e0197337, 2018.

[30] S. F. McGough, J. S. Brownstein, J. B. Hawkins and M. Santillana, "Forecasting Zika incidence in the 2016 Latin America outbreak combining traditional disease surveillance with search, social media, and news report data," *PLoS neglected tropical diseases,* vol. 11, p. e0005295, 2017.

[31] C. E. Lopez, M. Vasu and C. Gallemore, "Understanding the perception of COVID-19 policies by mining a multilanguage Twitter dataset," *arXiv preprint arXiv:2003.10359,* 2020.

[32] B. Sundstrom and A. B. Levenshus, "The art of engagement: Dialogic strategies on Twitter," *Journal of Communication Management,* 2017.

[33] W. Shin, A. Pang and H. J. Kim, "Building relationships through integrated online media: Global organizations’ use of brand web sites, Facebook, and Twitter," *Journal of Business and Technical Communication,* vol. 29, p. 184–220, 2015.

[34] J. H. Kim and H. W. Park, "Food policy in cyberspace: A webometric analysis of national food clusters in South Korea," *Government Information Quarterly,* vol. 31, p. 443–453, 2014.

[35] S. Yang, A. Quan-Haase and K. Rannenberg, "The changing public sphere on Twitter: Network structure, elites and topics of the# righttobeforgotten," *New media & society,* vol. 19, p. 1983–2002, 2017.

[36] A. Gruzd, D. Abul-Fottouh and A. Mashatan, "Who is Influencing the# GDPR Discussion on Twitter: Implications for Public Relations," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[37] C. Cadwalladr and E. Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The guardian,* vol. 17, p. 22, 2018.

[38] F. González, Y. Yu, A. Figueroa, C. López and C. Aragon, "Global reactions to the Cambridge analytica scandal: A cross-language social media study," in *Companion Proceedings of The 2019 World Wide Web Conference*, 2019.

[39] N. Vemprala and G. Dietrich, "A Social Network Analysis (SNA) Study On Data Breach Concerns Over Social Media," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[40] A. N. Novak and M. O. Vilceanu, "“The internet is not pleased”: twitter and the 2017 Equifax data breach," *The Communication Review,* vol. 22, p. 196–221, 2019.

[41] "How to Do Thematic Analysis | A Step-by-Step Guide & Examples," [Online]. Available: https://www.scribbr.com/methodology/thematic-analysis/. [Accessed 12 05 2020].

[42] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology,* vol. 3, pp. 77-101, 1 2006.

[43] U. Federal Trade Commission, "Credit Freeze FAQs | FTC Consumer Information," [Online]. Available: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs. [Accessed 26 11 2020].

CURRICULUM VITAE

PERSONAL INFORMATION

Name Surname : **Kübra AYDİN**
Date of Birth :
Phone :
E-mail :

Photo

Photo

EDUCATION

High School : **Ankara Öncü Anadolu High School**
Bachelor : **Ankara Yıldırım Beyazit University – Computer Engineer**

WORK EXPERIENCE

Computer Engineer: Tiga Information Technologies (October 2017 -)

January 2021
ANKARA

Department of Computer Engineering

Kübra AYDİN