Computer-aided Analysis of Privacy Policies: Extraction of Data Subjects Rights According to GDPR

Sabrina Heinrich 25.03.2019

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

Motivation

- General Data Protection Regulation (GDPR)
- Extraction of Data Subjects Rights

Problem

- Existing Approaches
- Supervised Machine Learning
- Research Questions

Approach

- Sentence Classification
- Sequence Labeling
- Procedure

Time Schedule

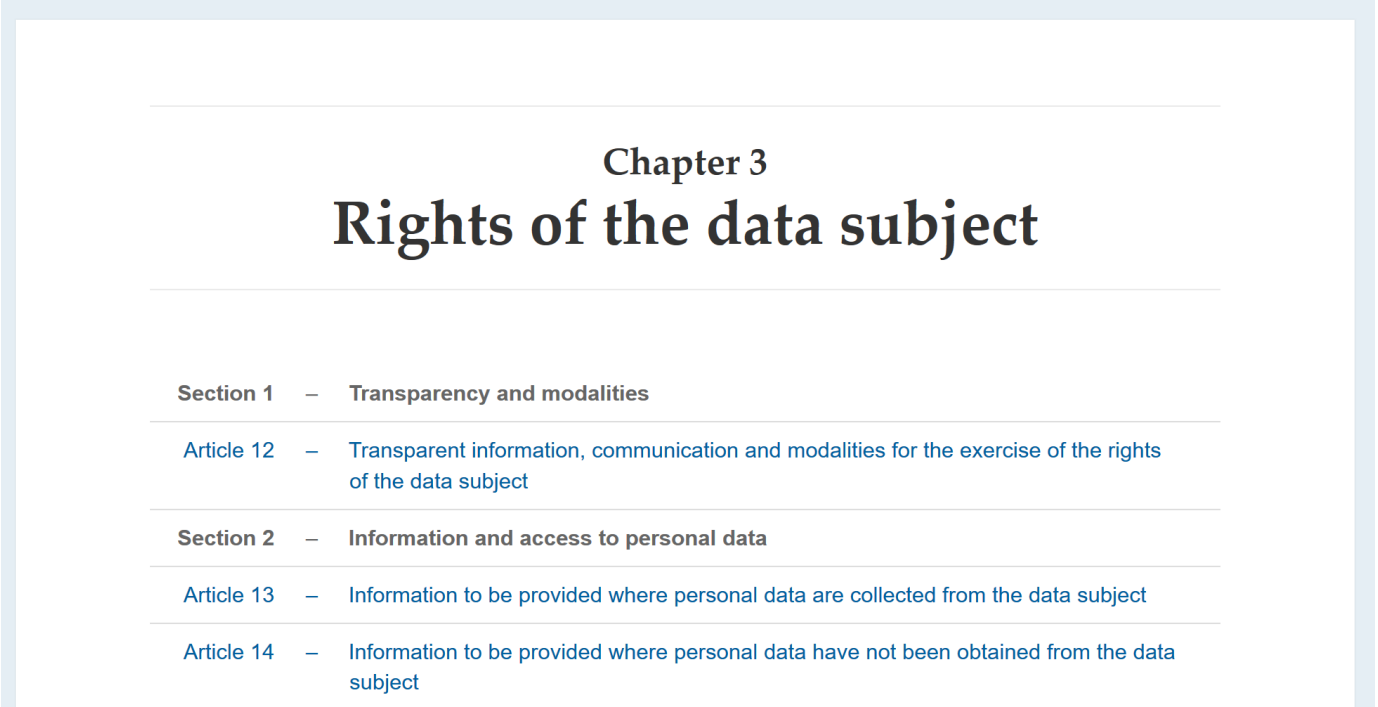
© sebis

Motivation

General Data Protection Regulation (GDPR)

- Implementation of GDPR in 2016 and applicable as of May 2018
  - In response to increasing digitalization
  - Regularization of processing of personal data within the EU

- One chapter deals with data subject rights



Chapter 3

Rights of the data subject

Section 1	–	**Transparency and modalities**
Article 12	–	Transparent information, communication and modalities for the exercise of the rights of the data subject
Section 2	–	**Information and access to personal data**
Article 13	–	Information to be provided where personal data are collected from the data subject
Article 14	–	Information to be provided where personal data have not been obtained from the data subject

Image: https://dsgvo-gesetz.de/kapitel-3/

© sebis

Motivation

Extraction of Data Subjects Rights

Privacy policies are most important source of information for data collection and usage

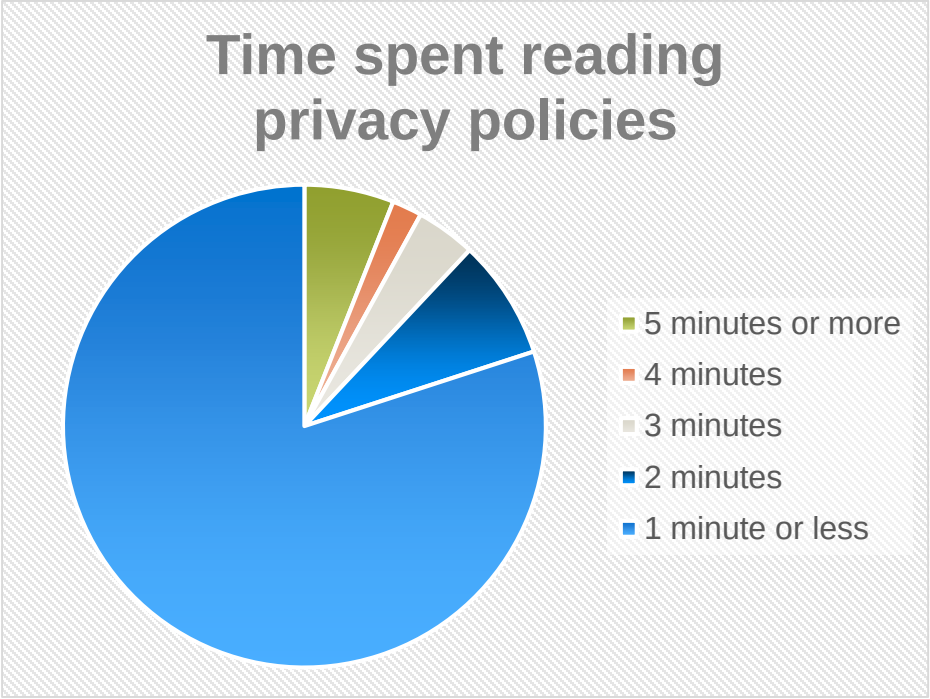
Problem:

Studies show that privacy policies

- are difficult to understand for non-experts
- cause an information overload

→ Little time is spent reading privacy policies

→ Hard to tell if all rights of the data subjetcs are included



Objective: Automatic analysis of privacy policies with regard to the coverage of these data subject rights

Outline

Motivation

- General Data Protection Regulation (GDPR)
- Extraction of Data Subjects Rights

Problem

- Existing Approaches
- Supervised Machine Learning
- Research Questions

Approach

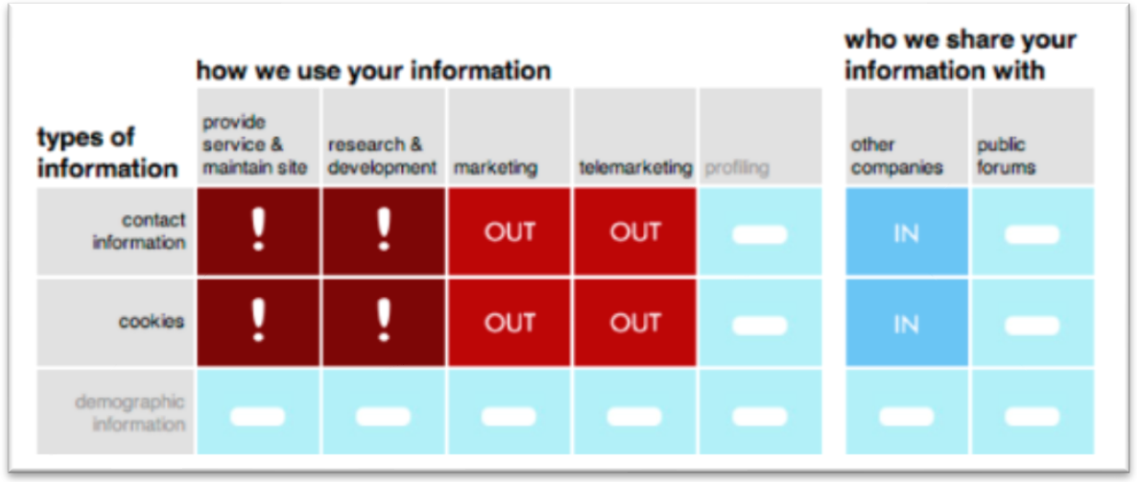
- Sentence Classification
- Sequence Labeling
- Procedure

Time Schedule

© sebis

Problem

Existing Approaches



types of information	how we use your information					who we share your information with	
	provide service & maintain site	research & development	marketing	telemarketing	profiling	other companies	public forums
contact information	!	!	OUT	OUT		IN	
cookies	!	!	OUT	OUT		IN	
demographic information							

Increase Usability

- Privacy Nutrition Labels
  - ➢ Summarize key points in standard form
- Layered privacy notices
  - ➢ Layers differ in detail

Technical Approaches

- Platform for Privacy Preferences P3P
  - ➢ web standard to enable browsers to read privacy policies
- Do not Track - DNT
  - ➢ Allows user to send a „Do not track“ signal

⟹ They have only shown limited success

Image: Kelley, Patrick Gage, et al. "A nutrition label for privacy."

© sebis

Problem

Supervised Machine Learning

Automated Understanding

- Analysis of privacy policies using NLP and **supervised machine learning** models

- Unsupervised Learning detects structures ⟶ hardly possible to specify the desired outcome
- Rule-Based approaches: A lot of expert-knowledge necessary and complex, manual creation of rules

⟶ For supervised machine learning an annotated dataset is needed

Existing Training Data

- 169 annotated privacy policies
- Easily extendable
- Annotation on different levels
  - Sentence-based (e.g. 126 containing ‘right to access’) ⟶ Models for **sentence classification**
  - Token-based (e.g. 148 tokens for ‘right to access’) ⟶ Models for **sequence labeling**

© sebis

Problem

Supervised Machine Learning

Annotation of Training Data

Sentence based labeling

Example:

Users are able to access and edit most of their Personal Data on the Site and if you have any queries or complaints we encourage you to contact us.

Right to access

Token based labeling

Example:

Users are able to access and edit most of their Personal Data on the Site and if you have any queries or complaints we encourage you to contact us.

Right to access

© sebis

Problem

Supervised Machine Learning

Annotation of Training Data

Sentence based labeling

Example:

Users are able to access and edit most of their Personal Data on the Site and if you have any queries or complaints we encourage you to contact us.

Right to access

Right to rectification

→ Multi-class labeling

Token based labeling

Example:

Users are able to access and edit most of their Personal Data on the Site and if you have any queries or complaints we encourage you to contact us.

Right to access

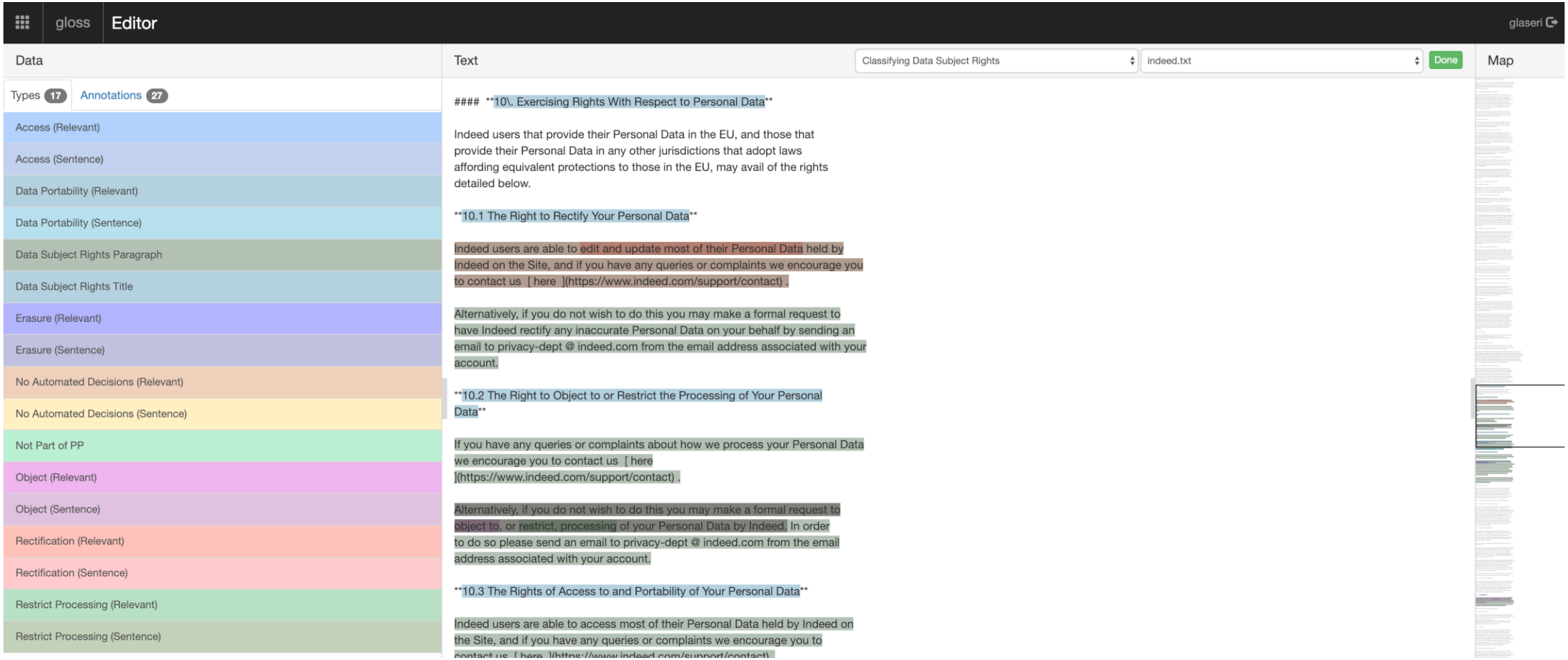
Right to rectification

© sebis

Problem

Supervised Machine Learning

Annotation of Training Data



Problem

Research Questions

- Which approaches exist to **automatically analyse** legal texts and privacy policies?
- Are **supervised machine learning** methods suitable to analyse privacy policies with regard to the coverage of these data subject rights?
- What are the strengths and weaknesses of **sentence classification** and **sequence labeling** based approaches?
- Which **supervised machine learning** approach performs best at extracting data subject rights from privacy policies?
- Which **performance** can be achieved on the test data and can the automated extraction **add value for private consumers** regarding the understanding of privacy policies?

© sebis

Outline

Motivation

- General Data Protection Regulation (GDPR)
- Extraction of Data Subjects Rights

Problem

- Existing Approaches
- Supervised Machine Learning
- Research Questions

Approach

- Sentence Classification
- Sequence Labeling
- Procedure

Time Schedule

© sebis

Sentence Classification

Implementation and validation of different classification methods of current literature

- Convolutional Neural Networks

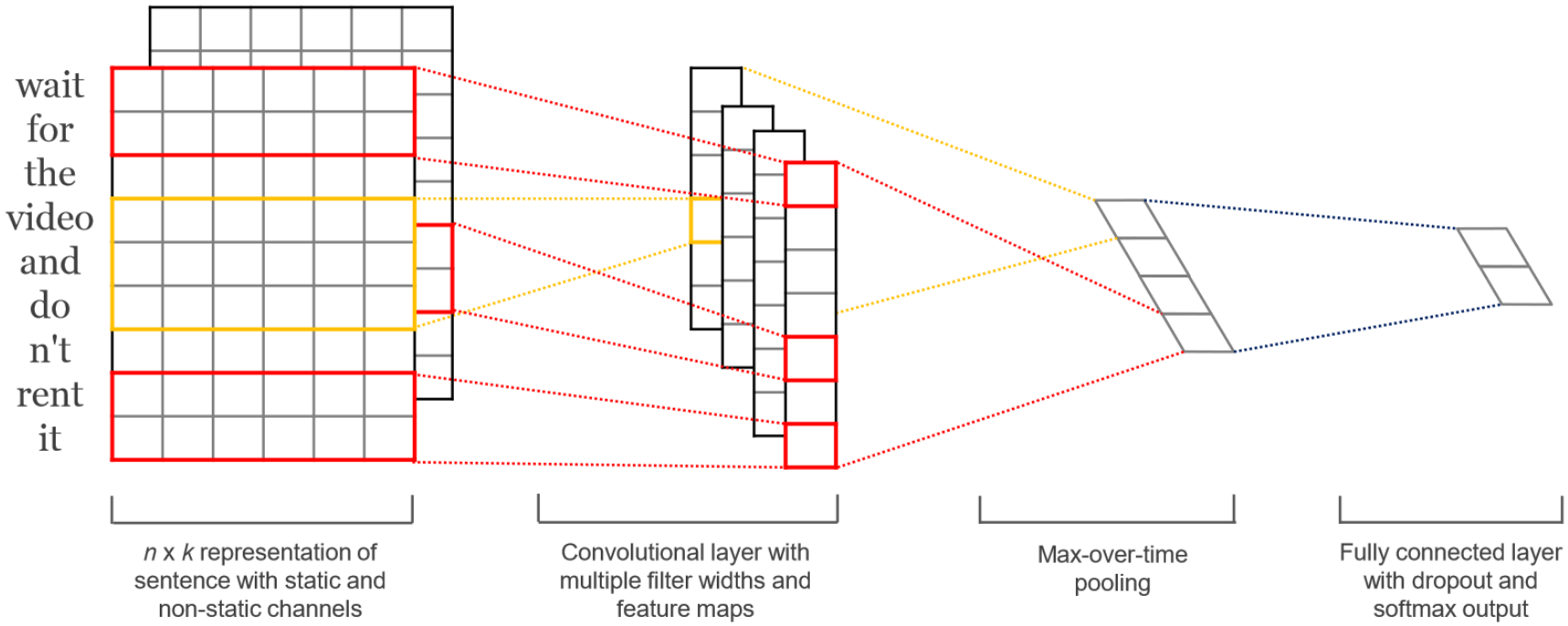


Image: Kim, Yoon. "Convolutional neural networks for sentence classification." arXiv preprint arXiv:1408.5882 (2014)

© sebis

Sentence Classification

Implementation and validation of different classification methods of current literature

- Support Vector Machines
  - Sequential, binary classification for multi-class classification
- Logistic Regression
- Naïve Bayes

$$p(\mathbf{x}|y=c,\boldsymbol{\theta}) = \prod_{j=1}^{D} p(x_j|y=c,\boldsymbol{\theta}_{jc})$$

- Decision Trees
  - E.g. used in spam filters

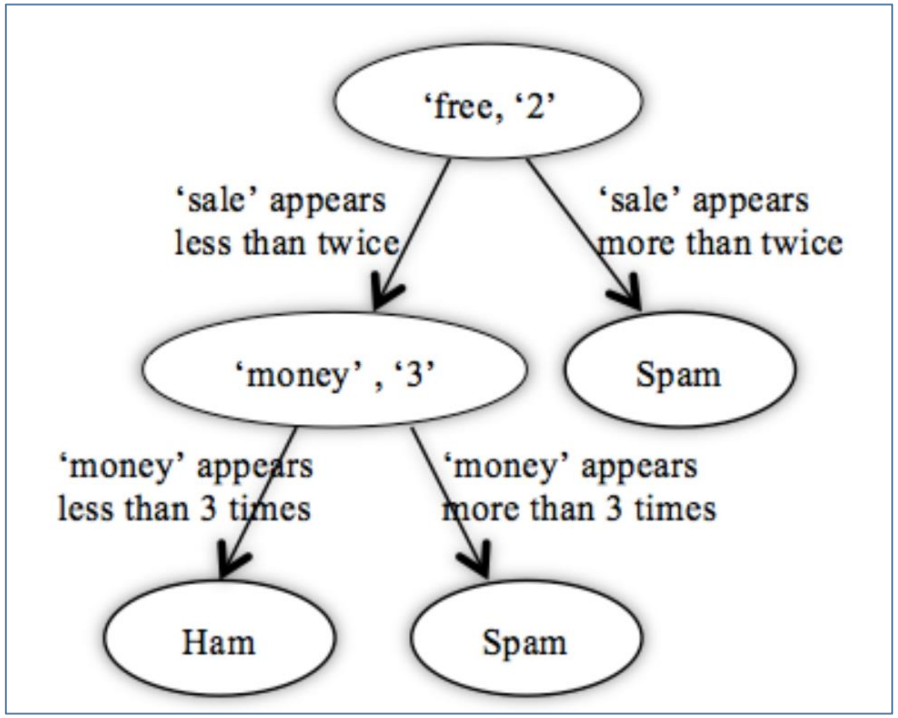
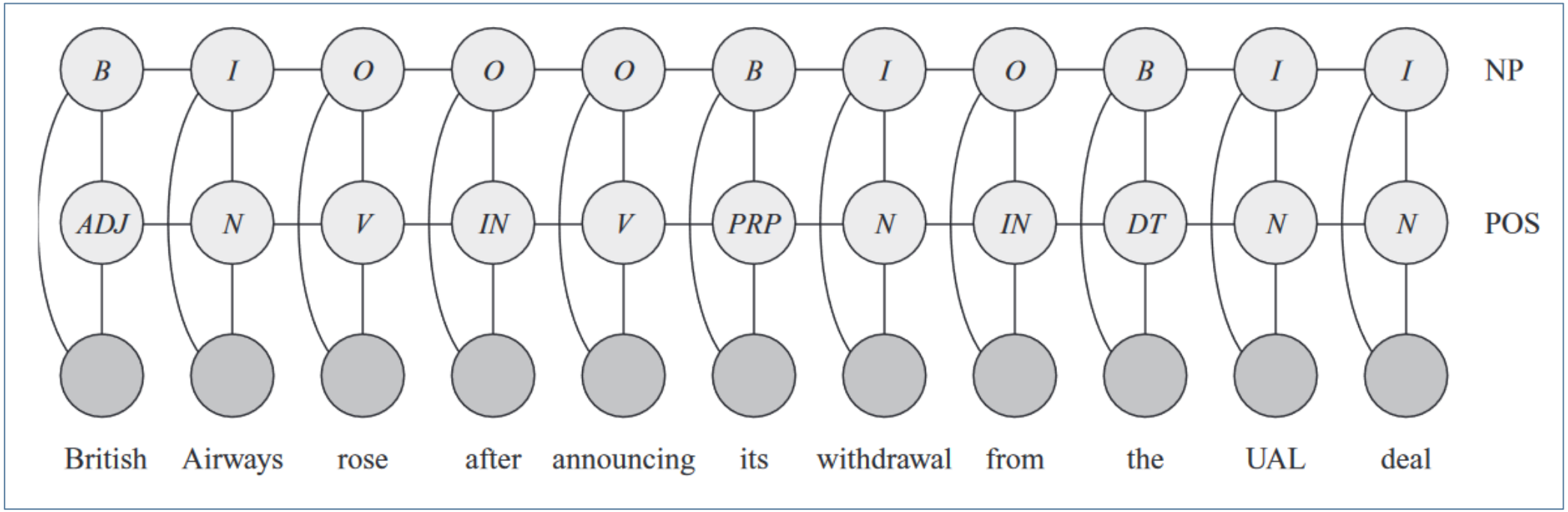


Image: https://ese.wustl.edu/ContentFiles/Research/UndergraduateResearch/CompletedProjects/WebPages/sp14/SongSteimle/WebPage/classifiers.html
© sebis

Sequence Labeling

Implementation and validation of different sequence labeling methods of current literature

- Conditional Random Fields
  - Well suited for processing sequences
  - Can take contextual information into account



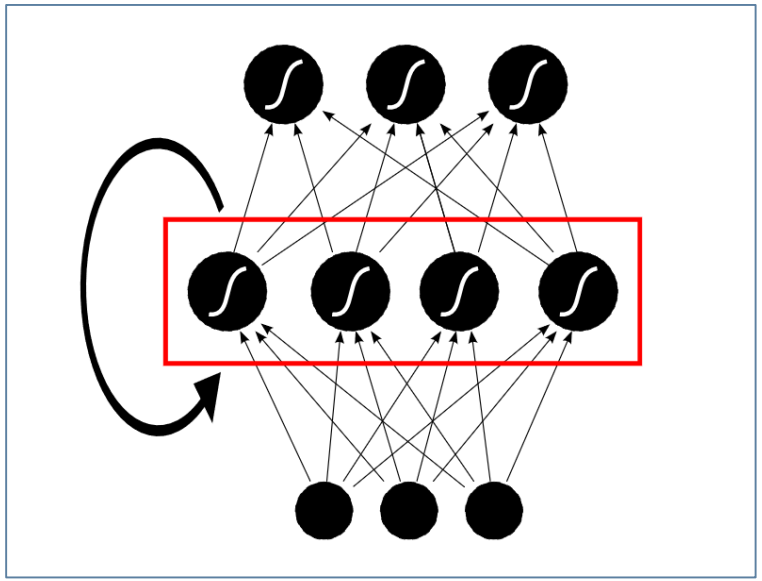
Images: MURPHY, Kevin P. Machine learning: a probabilistic perspective. 2012

© sebis

Sequence Labeling

Implementation and validation of different sequence labeling methods of current literature

- Support Vector Machines
- Recurrent Neural Network
  - Well suited for processing sequences
  - Long-Short-Term Memory



Images: Graves, Alex. "Supervised sequence labelling." Supervised sequence labelling with recurrent neural networks

© sebis

Procedure

- Literature research
  - Sentence classification approaches
  - Sequence labeling approaches

- Implementation
  - Promising sentence classification and sequence labeling approaches
  - User-interface for clearly displaying the results
  - If necessary: Extension of dataset

- Evaluation
  - Quantitative: Analysis by means of accuracy, precision and recall
  - Qualitative: Studies with potential end-users

© sebis

Outline

Motivation

- General Data Protection Regulation (GDPR)
- Extraction of Data Subjects Rights

Problem

- Existing Approaches
- Supervised Machine Learning
- Research Questions

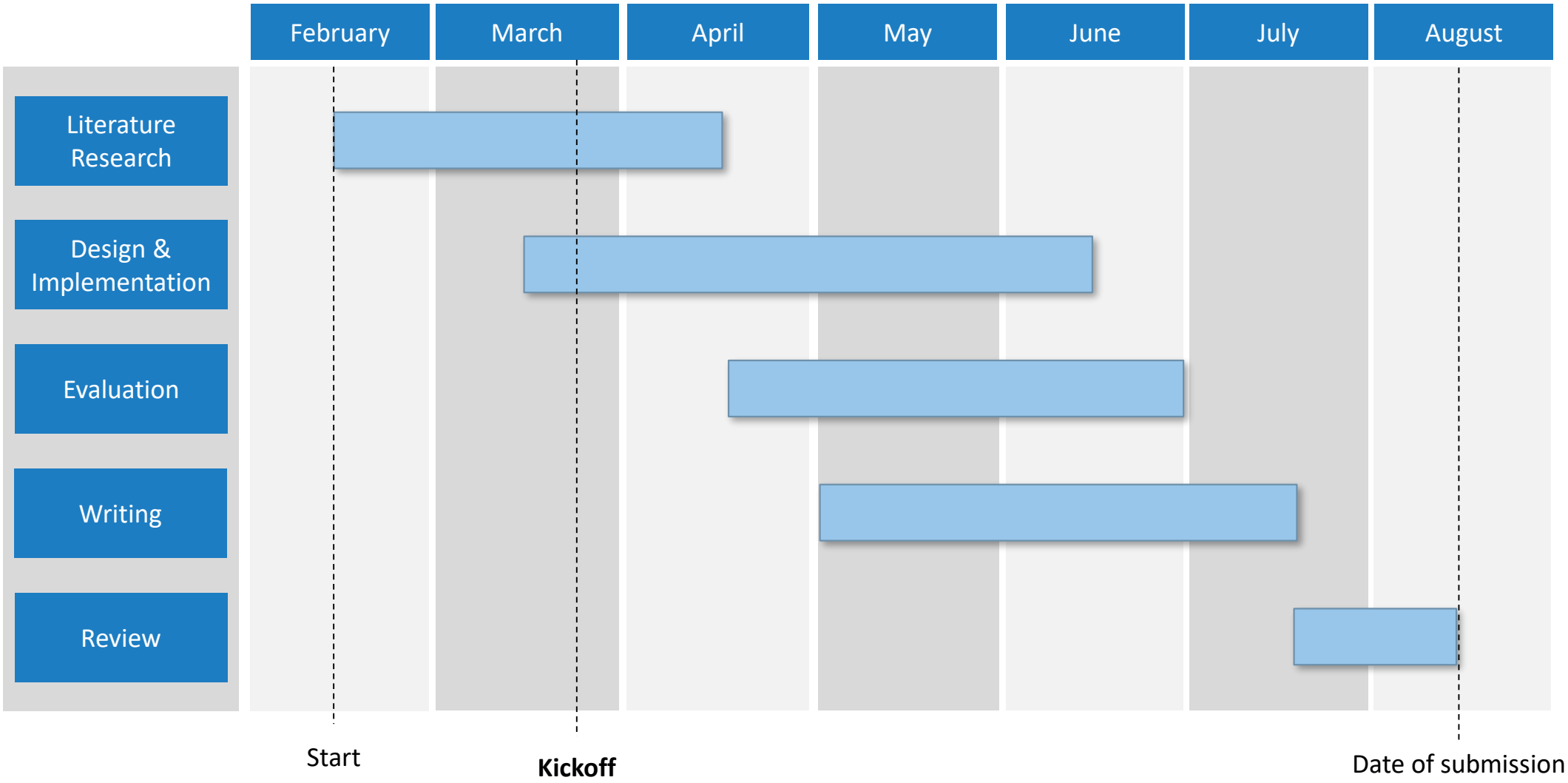
Approach

- Sentence Classification
- Sequence Labeling
- Procedure

Time Schedule

© sebis

Time Schedule



© sebis

References

- https://dsgvo-gesetz.de/kapitel-3/
- Obar, Jonathan A., and Anne Oeldorf-Hirsch. "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services." *Information, Communication & Society* (2018): 1-20.
- Reidenberg, Joel R., et al. "Disagreeable privacy policies: Mismatches between meaning and users' understanding." *Berkeley Tech. LJ* 30 (2015): 39.
- Manning, Christopher D., Christopher D. Manning, and Hinrich Schütze. *Foundations of statistical natural language processing*. MIT press, 1999.
- Kim, Yoon. "Convolutional neural networks for sentence classification." arXiv preprint arXiv:1408.5882 (2014)
- Khoo, Yuval Marom Anthony, and David Albrecht. "Experiments with sentence classification." *Proceedings of the Australasian Language Technology Workshop 2006*. 2006
- Graves, Alex. "Supervised sequence labelling." *Supervised sequence labelling with recurrent neural networks*. Springer, Berlin, Heidelberg, 2012. 5-13
- Bordes, Antoine, Nicolas Usunier, and Léon Bottou. "Sequence labelling SVMs trained in one pass." *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*. Springer, Berlin, Heidelberg, 2008
- Yang, Changhua, Kevin Hsin-Yih Lin, and Hsin-Hsi Chen. "Emotion classification using web blog corpora." *Web Intelligence, IEEE/WIC/ACM International Conference on*. IEEE, 2007.

Images:

- https://dsgvo-gesetz.de/kapitel-3/
- Kelley, Patrick Gage, et al. "A nutrition label for privacy." *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009.
- MURPHY, Kevin P. Machine learning: a probabilistic perspective. 2012https://ese.wustl.edu/ContentFiles/Research/UndergraduateResearch/CompletedProjects/WebPages/sp14/SongSteimle/WebPage/classifiers.html
- https://ese.wustl.edu/ContentFiles/Research/UndergraduateResearch/CompletedProjects/WebPages/sp14/SongSteimle/WebPage/classifiers.html

B. Sc.

Sabrina Heinrich

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289. 17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de

Training Data

- 169 privacy policies from Google PlayStore
- 1989 annotations in total
- 17 categories

	Sentence	Token
Right to access	126	148
Right to rectification	114	158
Right to erasure	120	158
Right to restrict processing	75	113
Right to data portability	66	98
Right to object	108	136
Right not to be subject to automated decisions	21	26
Not part of privacy policy	195	
Data subject rights paragraph	165	
Data subject rights title	162	

© sebis