National College of Ireland

Data Governance and Ethics (H9DGE)

MSc/PGD in Data Analytics

MSCDADJAN20A_O & MSCDADJAN20B_O

Continuous Assessment 1

Group: 24

Members:

Abdul Azadh Abdul Saleem	x18203621@student.ncirl.ie	**B**
Shikha Ojha	x19177151@student.ncirl.ie	**A**
Sudesh Kumar Narayanasamy Murali	x18199666@student.ncirl.ie	**B**

Lecturer: Dr. Vanessa Ayala-Rivera

1. i) LEGAL REQUIREMENTS IN DATA PROTECTION FOR CLEVERSOFT ORGANIZATION:

Organizations in Ireland or the countries under European Union which utilizes the users' personal details should follows the regulations implemented by the governing bodies of Data Protection in European Union and Ireland. Companies that works with the consumer data has to be under the compliance of **GDPR (General Data Protection Regulation)**, which has been signed in 25, May 2018 (UK Government, 2018). Though this regulation is applicable for states of European Union, the **Data Protection Act 2018** provides additional effect on this law of nation. This regulation is applicable for all the companies that sell, store, and process the demographic and personal information of the citizens of EU and EEA region. GDPR provides the residents of EU region greater control over their own personal data and provides the assurance that the collected personal data has been stored securely.

Following the legal requirements that CleverSoft organization must follow to process the data utilized for software development and for the protection of the data.

1. **General Data Protection Regulation (GDPR):**

   Organization that involve in development of software or application for mobile should fall under the direct complaint of GDPR. The data that the company has utilized in the process of software development has to be manipulated or encrypted in the format that the user information should never be exposed to unauthorized personal at any point of time. Below are the operational impacts of the GDPR to protect and use the data for software development.

   - **Mandatory notification on Data breach.**
     The companies that involve in processing personal and sensitive data has to notify the authorized regulators along and the individual person whose data has been breached. This can be prevented by conducting the end-to-end risk assessment and security enhancement and sourcing the security service from external service.
   - **Consumer's Right to be forgotten.**
     This regulation explains about the right that the owner of the personal detail possesses to control the usage of personal detail by other organization. The controller must erase the personal data of an individual without any delay, if the person concerns to provide the personal data, as explained in Article 17 in Data Protection Act, 2018 (UK Government, 2018).
   - **Assessment of Privacy Impact.**
     This mandates the company to conduct the data protection impact assessments, to make sure the operations of processing data are invasive. Further the regulators listed the scenarios which are subjected under this rule such as,
       i. Deploying new software or platform for data processing.
       ii. Collection of sensitive data in large public areas, which may affect the privacy of the individual.
       iii. Collection of information such as race, ethnics, religious opinions, political views, biometrics, health, criminal records, and health.

iv. Decision making project projects with the acquired data of the subjects which may affect the individual's life.

- **Privacy by design and default.**
  As mentioned in Article 25 in Data Protection Act, 2018, the products developed in the organization should have the ability to pseudonymization of the data for its protection while processing. This also makes sure the necessary data is utilized for process carried in the organization, and this prevention measure is designed to be in operation by default.
- **Management of external vendors.**
  GDPR also makes sure the company is responsible for the data processing, even if the operation has been sourced to the third-party vendors. Processors in the organization is responsible for making sure the liabilities of non-compliance by the organizations.
- **Portability of Data.**
  When the controllers in the organization process the data through automation the individual subject has the right to receive the data which is of their concern as stated in Article 20. Controllers are responsible for providing the data in commonly used in machine readable format and the subjects possess the right to transmit the data to any controllers. This regulation has increased the leverage of the user's choice to change the service provider.
- **Profiling.**
  This term of 'Profiling' in GDPR explains the process of recording and processing the personal data of an individual and evaluating the subject related to the natural traits. This includes the predicting the future actions of the subject with the past data recorded from the subject.

2. **Law Enforcement Directives.**
   Law Enforcement Directive (LED) is an official authorized body rather than a regulation, that controls the processing of data by the controllers for the purpose of enforcement of law (*Law Enforcement Directive | Data Protection Commissioner*, no date). This legislation is applicable only where the collection of data of citizens of EU countries is regulated by a data controller who must be a competent authority in accordance with section 69 of Data Protection Act and used for law enforcement purposes in accordance with section 70 of Data Protection Act, 2018 (UK Government, 2018).
3. **ePrivacy Regulations.**
   This act controls the collection and processing of data recorded from the electronic communication services in Ireland. ePrivacy directive is also said to the 'the cookie law' because this prevents the consumer to entering the website until the accept the cookies from that website (itgovernance, 2018). This act helps the end users to prevent the online privacy from being breached.
4. **Data Protection Act 1988 and 2003.**
   - **Data Protection Act 1988 and 2003.** (transposed to Data Protection Act, 2018 section 7 (4) and 8)**.** This act covers the complaints that were registered and investigations that have been registered under compliance before the Data Protection Act in 2018 (UK Government, 1998).

- **Data Protection Act 1988 and 2003.** (transposed to Data Protection Act, 2018 section 7)**.** This act covers the control over data processing and manipulation. The data related to national security, defense, classified information is secured from being exposed to other international states.

The above mentioned are the legal requirements that our organization has to follow in order to prevent the company from the privacy and data processing issues while operating in Ireland and European nations.

ii) ROLES AND RESPONSIBILITIES OF DATA CONTROLLER AND DATA PROCESSOR.

Establishment of Data Protection Act 2018 have mandated the importance of appointing Data Controller and Data Processor for an organization who takes the responsibility of controlling the organization over handling the sensitive data without any legal issues which could affect the organizations' position in the market. The role of Data Controller is critical in analyzing the data that has been used for processing by the company. This role caries out the responsibility of designing or verifying the process of data manipulating or storage carried out by the organization during the process of product development, and this role further extends to check the legal requirements and purpose for utilizing the data that the company has utilized during the process (*Data Protection Impact Assessments | Data Protection Commissioner*, no date).

ROLES AND RESPONSIBILITIES OF DATA CONTROLLER:

- Responsible to verify that the organization follow the regulations mentioned in Data Protection Act 2018, while collecting and processing the data in legalized, fair, and transparent manner to the authorized bodies.
- Responsible to make sure the organization utilize the collected and processed data for legit and lawful purpose.
- It is the duty of the controller to ensure that the data has not been processed or utilized of the any other reason contradicting for the purpose it has been recorded.
- Controller must conduct periodical Data Risk Assessments in the organization to ensure the technical protection measures, and the design for data protection were good, and the collected data does not have any irrelevant data of the user.
- The period of utilization of data of the user by the organization should not exceed the specified time mentioned in the agreement, this will be ensured by the Data Controller.
- Controller should verify whether the organization utilize a secured medium to transfer the data to any authorized network without external breach.
- Controllers must ensure that the data has been manipulated in the machine-readable format, by pseudonymization or data minimization and stored by the organization.
- Controllers must process the data of the users without any delay, if the subject concerns to change or delete their own data from the organization, or to transfer the data to any other online service.
- It is the duty of the Data Controller to document the GDPR compliance that the organization has followed regulation of Data Protection Act in processing the personal data with legitimate obligations.

- Data breach must be reported to the authorized body immediately and providing report of incidents happened during the occurrence.

Under the authority of the Data Controller, **Data Processor** has the responsibility to process the sensitive data collected by the organization, and to protect the purpose and the design of data processing carried by the organization, confidential. Data Processor is also subjected to be liable for data protection under the compliance of GDPR.

ROLES AND RESPONSIBILITIES OF DATA PROCESSOR:

- Processor holds the responsibility to follow various strategy and platforms to collect the personal data from subjects, controlled by the Data Controller.
- Ensure the implementation of secure and safety measures carried by the organization in recording the sensitive data and to confirm the GDPR compliance with these measures.
- Key responsible to report the breach in data protection to the Controller, and both the controller and processors holds the responsible to report the data breach to the authorities of GDPR compliance.
- Responsible to document the reports for GDPR compliance, Processor is responsible for the uncertainties in the record of user data, in case the breach occurs in the processing of the data.
- Modification and deletion of data has been carried by the processor, as per the instruction of the Controller.
- Processing of data must be carried by Processor, following the procedure proposed by the Data controller.
- It is the duty of the Processor to report or demonstrate the essential information requested by the Controller, for GDPR compliance.
- Processors are restricted from engaging with different processor or secondary processor without the authorization of Controller.
- In case of working under the joint controller, the processor should keep a record of the changes made in the data, as requested by each controller in the authorized body.

iii) DATA TRANSFER AGREEMENT EU-US:

All the organizations operating in Ireland or European Union nations has to abide to the legislation of the Privacy Shield as per the Articles 50, 49, 48, 47, 46, 44 and 45, that if the organization has to transfer the data of European residents to only the non-European countries listed under the third party countries. This regulation and protection helps to prevent the personal data of the individuals of European union to be confidential and secure (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016). With the effect of judgement of 'Schrems II', on July 2020, the data transfer from EU countries to US will not be based on Privacy Shield anymore. The transfer of data US must satisfy the rules mentioned in Article 44 in GDPR, to prove the required level of data protection to the European Union data

Transfer of Data based on Adequacy Decision:

The term 'Adequacy' refers to the required level of protection to the data provided by the organization in the countries mentioned in 'Official Journal of the European Union', to which there no specific authorization required to transfer data. These countries should also undergo periodic check of adequacy amendments every four years. The organization which satisfied the adequate protection requirement and transfers data from EU nations must undergo periodic review for every four years, providing the validation of level of protection satisfies the EU legal law.

By the judgement of Schrems II, which revoked the Privacy Shield Act between US and EU, the organization transferring data to US has to follow the regulations mentioned in Chapter V of GDPR, by Data Protection Act, 2018 (*THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016*) .

European Commission Controller – Processor Standard Contract Clauses (SCC) principles:

Since the Privacy Shield Act which provided the authority to transfer data from EU to US has been revoked, because the act fails to provide the required protection to the data of EU countries, organizations in EU has to follow the regulations mentioned in Art.44, 45, 46, 47, 48, 49, 50 of GDPR in order to transfer the data to US. Following will explain the legal requirements the organization has to follow to transfer data to US.

- Since US has failed to fulfill the requirements pf protection mentioned in the adequacy decision, the controller or processor must submit the required legal documents to the legislation to get authorization for every transfer of data.
- Controllers must maintain a record of transfer of data from EU, which will be inspected by the European Commission.
- During the process of transferring data, the controller must record all possible and required information about the process and submit it to European Commission.
- It is the duty of the controller to safety check the data of the individuals in EU before transferring it to US.
- Based on the intra-group binding rules authorized by the supervisory authority bodies in non-EU nations, the transfer of data has to be processed.
- Transfer of data can also be conducted on the code of contact approval mentioned in Art. 40 of GDPR.

Derogation for specific situations:

In cases where both the Art. 45 (3) (Adequacy decision) or Art.46 (Safeguard), then the transfer of data to third nations should follow derogation which specifies set of conditions to be applied (*THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016*).

- The transfer of data is possible only if the data subject consents for derogations, knowing the possible risk of transfer.
- Pre-contractual measures must be taken to the requests of subject, or contract has to be signed between controller and subject.
- Transfer if permitted in case of public interest and defense of legal claims.

2. ETHICAL ISSUES RAISED BY 'FAKE NEWS' AND ITS EFFECT ON RESEARCH STUDY.

"Fake news" has been described as the circulation by way of print, broadcast or social media of incorrect information for the purpose of malicious or politically motivated objectives. Selecting and summarizing the different ethical issues which raised with "fake news" and discussion of the challenges that fake news can create when conducting a research.

Fake news:

In our society information accuracy is paramount. Fake news refers to news messages containing inaccurate or false facts, but do not disclose the inaccuracy of the information. Fake news can be also understood as deliberately fabricated news. It is often noticed that fake news does not often publish reports of the non-existing news, in a very rare case scenario only there is a possibility of whole news story being a made-up story, however pure fabrication can still be taken as a potential source of false news (Wang, 2020).

The term fake news became very famous post U.S presidential election of year 2016 (Kim, Moravec and Dennis, 2019). It was noticed that people used social media platforms to deliberately spread misinformation which attracted extraordinary attention from the people across the globe. If we see the bigger picture, we can clearly notice that this is an area of concern because the attention received by the fake news resulted in decline of people's faith in public institutions and crippled democracy.

Ethical issues that arises due to fake news:

The major ethical concerns that can be discussed in a research project which is based on fake news is explained below (Zhang and Ghorbani, 2020):

- One of biggest issues is the prevalence of the misinformation that is "not only the easy availability of the misinformation" but also" the impact of the misinformation". Similar paradigm is created by the fake news as that of the real news which endangers free communication flow by generating false propaganda that may severely affect individual's mental health.
- Many ethical issues emerge on creation of the fake news. However, creation of the false news is not the only area of concern as it puts us under a state of confusion where we start considering even the valid news as a fake one. This creates a delusion between valid and the fake news when the news is simply stated fake.
- Not only does misinformation contribute to needless public fear and panic, but it can also generate hatred and prejudice. News and updates received from small community of the like-minded people with similar views and opinions that have access over a very limited range of resources may become easy victims of wrong and unvalidated information.
- While conducting a research study, ethical concerns related to fake news have high inference in forging and manipulating the data which is used for the study which can in turn change the produced result of the study.

Challenges posed by fake news while carrying out a research study:

- The purpose of the research study itself will fail as usage of the fake data will result in deviating from the research study. Wrong ideologies will be propagated by introduction of the fake news in the research study.
- Minimization and prevention of the fake news circulation proves to be challenging and may alter the direction of the research, as it will not yield a proper result if the biased information is taken for the research study.
- Fake news is being transmitted in many media outlets such as digital, physical and communication media. Fake news needs to be annihilated at these levels. Digital level checking can be performed by the identifying the news source in a fact checking website, at physical level author's integrity can be checked on a document paper, self-research would be a great help in distinguishing between real and fake news at communication level.
- Fact checking of all the information that is being spread should become compulsory which is really a difficult process that consumes a lot of time and is very expensive.
- One of the most interesting and challenging aspects about the fake news is the way it is identified on the social media. Social media has seen massive growth in its users in last few years as it changed the way people connected and perceived the information since it is open to everyone. This facilitates easy spread of the fake news resulting in people forming opinion based on the fake data and being inclined towards the wrong direction.
- During a research study it would be really challenging to control the amount of information or disinformation that is passed on to people. For example, Twitter which is a very famous social media platform is a great example where huge amount of uncontrolled information and misinformation are spread and where it becomes highly difficult to differentiate between valid news and fake news.
- Use of technology to create fake news has become one of the most prominent way for generation of misinformation. Use of artificial intelligence for creation of misinformation from the original source is disastrous due to the availability of the evidence that may prove the authenticity of the fake news. So, the research work which uses AI data are more prone to the fake news (Meel and Vishwakarma, 2020).

To recapitulate, in order to apply the right measures at the right time, it is important for governments and organizations to rely on accurate facts. In order to ensure a reliable and unbiased research outcome, it is necessary for researchers, scholars and data practitioners to capture information from authentic sources because the data speak (Allen *et al.*, 2020). While there is a need for ethical journalism for those engaged in the mass media, it is equally necessary for individuals using social media to carefully consider whether the distribution of information is of concern to the public or whether such information sharing is in the public interest. Worse still, it is difficult to ensure that members of the public act ethically. There is a growing need for the authorities to promote awareness regarding their ethical obligation to be responsible for what they publish on social media in order to prevent infodemics.

As the phrase implies that with great power comes great responsibility, there is a great deal of scope and responsibility on the part of governments, organizations, journalists, scholars,

technologists and individuals to demonstrate authentic leadership, integrity while at the same time being able to distinguish right from wrong.

3. DATA-INFORMED DUTIES IN AI DEVELOPMENT – Paper Review.

The artificial intelligence has been evolved in such a way that it has been replacing the human workforce in a lot of sectors and has even has the capability to think on its own and make decision if situation arises. However, as the efficiency and benefits has been laudable over the years and provided a significant benefit of reducing the over process cost, the challenges and negatives that has been associated with it possess quite a challenge to be addressed.

Although even in case of proper data being used for building an automated system the occurrence of bias is quite a possibility, so any mistake in the data usage or wrongful data will still worsen or become negative threat for Decision Model. So, in recent times, the Judiciary and Government Bodies has been trying to implement several laws and policies like the tort law to monitor and make sure that their Decision-making process are taking place in an ethical manner. Some experts argue that because of these negative implications the damage that happens could be very much severe and companies must take full responsibility of it. Now let us discuss about the negative effects or implication that could because of inaccurate or inappropriate data that has been used for analysis.

Implication caused by inaccurate Data Usage:

This type of data Implication happens because, the data that is used for building the model has been with the bias or the data is inaccurate and not verified properly. This type of case happens, if the data collection is done in a non-ethical manner like scrapping the data without proper authorization which leads verifying the authenticity of the data.

Let us take a case, where a company decides to build an Automatic decision-making tool for medical examination and uses the medical data from patients from the hospital's sources or from online websites that has been available. There is no proper channel or stream where these data can be verified or authenticated as it taken without any proper channel. In such instances there is a huge probability that the results obtained from the model could be biased and incorrect. Even if the Company decides to go ahead with its implementation in real time usage, the damages and negative impacts caused by the working system could be very humongous to get it sorted and even Manual work would provide better efficiency than Artificial intelligence. So, the main purpose of easing the job of humans gets nullified. This would not be case in every possible instant, but the consideration of data, its authenticity and originality play a significant role in building the Artificial intelligence Model.

Implications Caused by inappropriate Data Usage:

This implication happens because the data that has been used for analysis does not have proper or adequate representatives from all groups and particularly biased towards a certain group in the population. This is one of the most common problem while selecting data for analysis and could results in serious threats while going forward.

Let us consider an example of building an Automated model where the Male population are being at a large quantity than that of females, there is obvious case that the result could become biased slightly towards the males. So, this is one of the common cases that should be addressed at the initial stages of building the model and at regular intervals in time. Another example would be in case of medical results obtained from the Intelligence systems, by considering the data obtained from people of a particular group, age and ethnicity or region, and the model performs very well and produces excellent results in their prediction and the company decides to take to the another country or neighboring regions, then the inputs that are considered should be checked based on the expanding region, so that the results obtained from the system will not be biased and produces the results without supporting any particular group or region. And some companies check and rectify this issue by auditing the system at regular intervals and altering the model mechanism so that the results obtained are without any bias.

4. ACM PRINCIPLES FOR ALGORITHMIC TRANSPARENCY AND ACCOUNTABILITY – Paper Review

Application of algorithms in Automated decision-making systems have become an inevitable part in the Growing Digital world. The algorithmic aided decision-making systems have found application from weather prediction to automatic disease detection in humans, and the extent it has been growing and replacing the manual work of humans has been increasing at a rapid pace. As modern algorithm involves the application of techniques from Machine Learning, Big data and Deep learning, the way in which these algorithms operate is not exactly clear and their internal working is still kind of Blackbox for the developers as well. So, any mistake from erroneous results from these decision systems are bit of challenge to resolve and damage caused by the system involves hefty money and work to be rectify along with the loss of reputation for the organization as well.

So, Association for Computing Machinery US Public Policy control (USACM) have developed a set of 7 principles and guidelines that has to be followed for Transparency and accountability of the algorithms so these principles acts as a common base or pillar in designing the algorithm. Let us discuss 3 of the Principles in details along with examples below,

Awareness:

The Awareness principle explains about the main possible objective why the model is being built, and the entire set of people who are involved in the process like the Product owners, designers of the System, stakeholders like the end users of the product should be aware of the product functionality in the system. Good documentation of the entire Decision systems along with cases that are considered while building the model and their possible outcomes should be Noted and should be to the people who are Associated with the model. The Decision-making model does not have a capability to perceive the situation and provide a judgment it creates a Bias at that instant, which is a drawback and if affects the end-user altogether. So, suitable steps should be considered to tackle this problem as well.

Let us take an example of the Uber Case study, where surge pricing model is employed to the system. In a rare instance, where the person has been facing some emergency and the uber driver has to assist him to the nearby hospital, in this instance the Uber algorithm wouldn’t

consider the seriousness of the issue that is happening around and would still provide the same rules by providing the fee at the end of the Trip. So, at this instance, a feasible way should be considered, so that it would help the driver, passenger and uber management to get everything sorted in a peaceful manner. Although, the Factors considered by the model cannot be revealed, sufficient efforts should be taken to let people know about its working on holistic basis rather being a black box and mystery in obtaining the output.

Accountability:

Accountability is the principle where the institutions should take full responsibility of the results obtained from the Decision-system and would be accountable of the bias and possible damages caused because by the system. Sufficient steps and methods should be taken into account to check the entire working of the system and rigorous testing practice should be done before the implementation of the system as the results obtained from the system are completely accountable by the organization itself.

Let us take an example of the Food delivery company, which has a problem or bug like incase of delivery to some areas in the city, the application provides long distance routes to reach the destination. So, in this case the Delivery person is affected because of the extra travel time, customer might get annoyed because of the late delivery, so at this moment the Food delivery company has to take full responsibility of the delay rather than blaming on the delivery person and should compensate the people involved in the issue as customer reviews plays a very important role in the Firm's reputation and should also take steps to fix the bug as quick as possible.

Auditability:

Auditability is an instance where the entire process of the Decision-making using the algorithmic methods and the results obtained from the process are properly audited and verified. This process of auditability is done to ensure that the process takes place as per ethical standards and it also denotes the factors involved in the algorithmic decision making, data extraction and the Entire logic is as per the standards followed in the respective sector and country. This is of Great help if some process in the algorithm goes wrong or trust issues happens based on the results obtained from the algorithm.

Let us take an example of Airline firms, where they employ Dynamic pricing model in determining the price of Flight Travel tickets, based on various factors at the time of booking. Suppose in a case where flight Passenger thinks that he been cheated, Misused or being charge more than the other fellow passengers and decides it challenge it legally. The Airline Firm would not be able to reveal the source code, as it might be used be used by fellow competitors. So, at this juncture the Auditing Firms comes into picture where they evaluate the algorithm and provide a verifiable statement about their Pricing process which acts as a safety clause and acts like an insurer in this Process.

Reference:

Allen, J. *et al.* (2020) 'Evaluating the fake news problem at the scale of the information ecosystem', *Science Advances*. American Association for the Advancement of Science, 6(14), p. eaay3539. doi: 10.1126/sciadv.aay3539.

Data Protection Impact Assessments | Data Protection Commissioner (no date). Available at: https://www.dataprotection.ie/en/organisations/data-protection-basics (Accessed: 20 November 2020).

itgovernance (2018) *The EU ePrivacy Regulation (ePR) | IT Governance UK*, *itgovernance*. Available at: https://www.itgovernance.eu/en-ie/eprivacy-regulation-epr-ie (Accessed: 24 November 2020).

Kim, A., Moravec, P. L. and Dennis, A. R. (2019) 'Combating Fake News on Social Media with Source Ratings: The Effects of User and Expert Reputation Ratings', *Journal of Management Information Systems*. Routledge, 36(3), pp. 931–968. doi: 10.1080/07421222.2019.1628921.

Law Enforcement Directive | Data Protection Commissioner (no date). Available at: https://www.dataprotection.ie/en/organisations/resources-organisations/law-enforcement-directive (Accessed: 24 November 2020).

Meel, P. and Vishwakarma, D. K. (2020) 'Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities', *Expert Systems with Applications*. Elsevier Ltd, p. 112986. doi: 10.1016/j.eswa.2019.112986.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION (2016) *L_2016119EN.01000101.xml*, *THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e4227-1-1 (Accessed: 26 November 2020).

UK Government (1998) *Data Protection Act Section 7*. Available at: http://www.irishstatutebook.ie/eli/1988/act/25/section/7/enacted/en/html#sec7 (Accessed: 24 November 2020).

UK Government (2018) 'Data Protection Act 2018', *www.Gov.uk*, 2018(January), p. 338. Available at: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html (Accessed: 24 November 2020).

Wang, C. C. (2020) 'Fake news and related concepts: Definitions and recent research development', *Contemporary Management Research*. Academy of Taiwan Information Systems Research, 16(3), pp. 145–174. doi: 10.7903/CMR.20677.

Zhang, X. and Ghorbani, A. A. (2020) 'An overview of online fake news: Characterization, detection, and discussion', *Information Processing and Management*. Elsevier Ltd, 57(2), p. 102025. doi: 10.1016/j.ipm.2019.03.004.