The Essence of Ethics in A.I.

Individual Assessment

ECS7025P
Ethics, Regulation and Law in Advanced Digital Information Processing and Decision Making
2022/23

By Gargeya Sharma

220278025

MSc Artificial Intelligence

Queen Mary University of London

Executive Summary

"The Essence of Ethics in AI" puts emphasis on the use, practice, compliance and requirement of ethics and regulation in AI and the responsibilities of data scientists and AI developers in the context of the UK. A 2018 reported data breach case by Facebook-Cambridge Analytica is highlighted, and its relationship to GDPR principles and ICO rules is examined.

The report emphasises the significance of resolving ethical problems as well as the influence of AI on a number of UK sectors, including healthcare, education, finance, and public services. An analysis of the Facebook-Cambridge Analytica data breach shows how important it is to follow data protection laws and preserve personal information.

The report investigates ethical AI, data protection, and information governance within businesses using Globant as an example. Globant's approach to ethical AI, data protection, and information governance demonstrates a commitment to responsible AI practices and compliance with data protection laws and regulations, including GDPR. The company's approach serves as an example for other organizations aiming to implement AI ethically and responsibly.

In conclusion, the report offers valuable insights into the ethical considerations and regulatory compliance required for organizations to successfully harness the potential of AI while safeguarding data privacy and security.

Contents

List of Abbreviations

Short Form	Full Form
AI	Artificial Intelligence
UK	United Kingdom
EU	European Union
US	United States of America
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
GDP	Gross Domestic Product
R&D	Research and Development

Introduction

We all are familiar with the advancements and continuous developments in the field of Artificial Intelligence across the globe. The word has attached itself to almost all domains of human intervention. It has revolutionized businesses and changed how people interact with technology altogether. Parallelly, I find it crucial to ensure that AI causes as little harm to society as possible while addressing the ethical, governmental, and legal issues that will arise as it develops and is applied. The exponential expansion of AI has raised critical worries about potential negative consequences on privacy, security, employment, and even the foundation of our social structure. As a result, it is crucial to set moral standards, legal frameworks, and strict rules that direct the creation and application of AI technology. This report heavily discusses such issues and tackles a few questions that let us open our eyes before stepping another foot in the advancement of AI and ignorantly causing greater harm than imagined.

The amalgamation of ethically sound principles that guarantee AI systems to be developed and used ethically, transparently, and for the benefit of all is required since ethics plays and should remain to play a crucial role in AI. Such an intent aims to avoid discrimination, injury, and violation of human rights while embedding fundamental ethical concepts including justice, accountability, and transparency in the creation and application of AI systems. Similarly, we need regulations and legal frameworks to level the playing field for innovation in AI while minimizing negative societal impacts like issues regarding liability, intellectual property and most importantly privacy. These reforms should be acceptable by all in unison and need constant evolution to keep up with the pace of technological advancements. Let’s see how the UK is dealing with this issue with the help of the first question below.

Section A

As future data scientists and AI engineers/practitioners discuss the impact of AI in the UK (choice of the report) and how ethical dilemmas/issues can be handled.

Introduction

Before discussing the impacts of AI in the UK, the author is keen to put some light on "Why the report selected the UK to showcase the impact of AI on it?". The simplest and most straightforward answer would be its involvement in developing and researching to improve AI. It is one of the first countries in the world that envisioned AI to be part of our normal life and kept working towards making that goal a reality today. One of the godfathers of deep learning (a subset technique to build AI systems by letting them train themselves from the data and which today governs most of the advanced development in AI): Geoffrey Hinton (Wikipedia)[1] was born in London and completed his education from University of Cambridge and further PhD from University of Edinburgh. The UK is full of passionate researchers and has a rich history of strong contributions towards leading the development of AI to the position where it currently stands. Discussion about such a crucial contributor and how their own contributions have affected them over the period excites the author.

Unquestionably, the United Kingdom's industries have changed dramatically as a result of the quick development of AI technology, with notable advantages for the economy, healthcare, and education among others. However, the widespread use of AI applications has also given rise to moral conundrums and difficulties, especially regarding privacy, justice, and transparency. The influence of AI on the UK will be critically examined in this report, along with the ethical concerns raised by its application and suggestions for solutions. It will make use of examples from many industries, current thinking in the field, and the author's viewpoints on these problems.

Sector-wise Impacts of AI on the UK

1. Educational

As a student himself, the author wishes to put extra emphasis on the educational impact of AI. Almost everyone if not everyone uses 'Google' or different search engines to search and research about topics that either are part of their course of study or simply just a matter of curiosity. Search engines have been constantly improving in their task to take their users to the right place and cater to their individualistic needs (Nuning et al. 2018)[2]. This advancement cannot be possible without the use of AI behind the scenes. This common task of appropriate searching impacts all of our lives, call it educational or not. In order to improve accessibility and efficiency while also enhancing teaching and learning, AI technologies have been used in the UK's education sector. For instance, adaptive learning platforms can offer students individualized content and feedback, and AI-powered chatbots can provide immediate support and direction. However, the application of AI in education raises concerns about the likelihood of algorithmic bias and the effects of AI-driven choices on students' lives.

2. Economical

By innumerable people, AI is known to be a force that will steal our jobs or leave us useless in multiple sectors, but the author argues that this perception lacks not only the fundamental

quality that makes us intelligent and human beings: curiosity and creativity but also adjustability. Current AI is strong but not creative and critical as human beings, we are the ones who create jobs and work given our given available resources. According to a popular study by PwC (2017) [3], In the UK, AI has played a vital role in economic progress. They say that AI might boost the UK economy by up to £232 billion by 2030, or almost 10.3% of GDP (PwC, 2017). Increased efficiency and productivity as well as the opening of new work opportunities are the main drivers of this expansion. With AI's potential to replace people, particularly in mundane tasks and positions, this rise is not without risks, though.

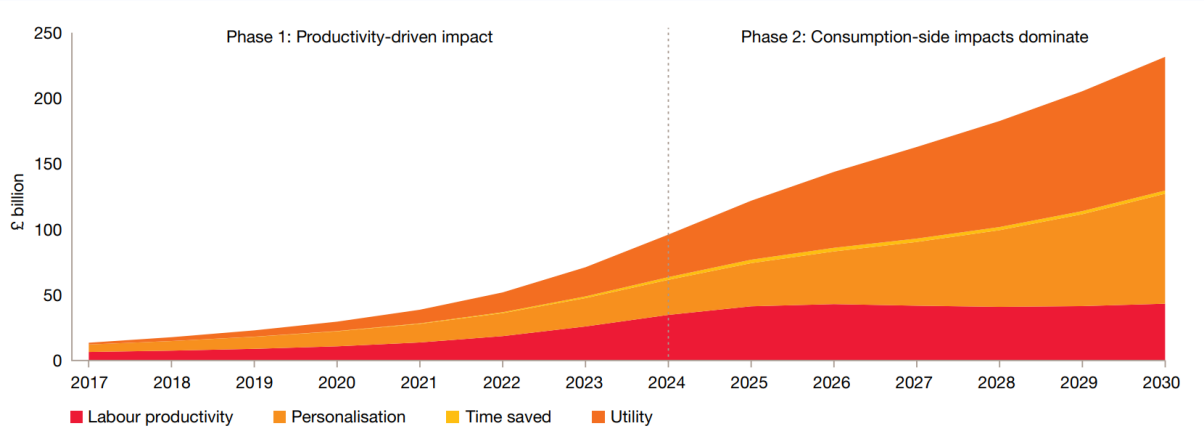

Figure 1: Where will the value gains come from with AI? (PwC, 2017)[3]

This study also supports the author's argument that the UK economy may be slightly more affected by artificial intelligence than Northern Europe is. AI has the potential to increase GDP in Northern Europe by up to 9.9% by 2030, and the UK may experience even greater advantages due to its stronger technological basis and access to talent. With the introduction of "no-human-in-loop" technology, some employment will eventually become obsolete, but AI will generate new ones in development, application, construction, maintenance, operation, and regulation. Additional economic demand brought on by AI will also result in the creation of occupations unrelated to AI.

3. Healthcare

One of the world's most renowned AI companies started in the UK: DeepMind is leading the development of agent-oriented artificial intelligence where they have created an AI system that can diagnose age-related macular degeneration and diabetic retinopathy more precisely than human experts (De Fauw et al., 2018)[4]. Healthcare in the UK could undergo a transformation like mentioned above due to AI. It has the potential to enhance patient outcomes and save healthcare costs through early disease diagnosis, drug discovery, and individualized treatment strategies. But from a holistic perspective, despite these developments, issues with patient data privacy and the moral implications of AI-driven healthcare decision-making continue to be raised.

Ethical Dilemmas and Challenges

1. Privacy

AI demands enormous amounts of personal data which as a result poses privacy issues. GDPR (EU, 2016)[5] imposes strict rules for collecting data, however, compliance while preserving AI effectiveness is difficult. AI systems might also expose confidential data or experience security breaches.

2. Equity and Bias

If developed with false assumptions or trained on biased data, AI algorithms can reinforce or generate prejudices. AI bias could lead to discrimination based on race, gender, or other distinctions. For instance, a US study (Angwin et al., 2016)[6] revealed a bias towards African Americans in an AI system used to assess criminal risk. For fair AI systems that don't aggravate inequality, addressing biases is essential.

3. Accountability and Transparency

Decision-making procedures are opaque, and accountability is challenging due to AI's "black box" nature. AI practitioners and developers will be impacted by the GDPR's requirement for justifications for automated choices (Art. 22 GDPR)[7]. For ethical deployment and adoption, it is essential to provide AI accountability and transparency.

4. Misuse and Surveillance

Concerns about privacy and civil liberties are raised by the use of AI in surveillance, such as facial recognition. The use of facial recognition by law enforcement in the UK is met with criticism, legal issues, and calls for stronger control (BBC, 2020)[8]. The ethical discussion is complicated by the possibility that governments or other bad actors will exploit AI.

Handling Ethical Dilemmas and Challenges

1. Education and Training

AI practitioners need to get continual education and training in order to address the ethical problems related to AI. This entails cultivating a solid grasp of ethical ideas as well as the abilities required to identify and handle ethical dilemmas in daily life. The complicated ethical environment around AI technology can be better negotiated by AI practitioners if ethics education is included in AI curricula and professional development programs. The author argues education is one of the strongest tools to achieve anything in this world, producing responsible and thoughtful professionals can prove to be that small yet strong wave that avoids creating a destructive tsunami of AI.

2. Responsible AI Development and Deployment

Related to the point mentioned above, corporate training and practices are someway similar to the educational side of AI hence, AI design, development, and evaluation must take ethical issues into account (Leslie, D., The Alan Turing Institute, 2019) [9]. A human-centric strategy makes sure AI systems respect societal norms, human rights, and values.

3. Legislation and Regulation

Some ethical issues relating to AI are addressed by existing laws such as GDPR (European Parliament and Council of the European Union, 2016) [5], the Equality Act 2010 [10], and the Data Protection Act 2018 [11]. The proposed AI legislation from the European Commission seeks to establish an open and accountable legal system (European Commission, 2021) [12].

4. Collaboration and Stakeholder Engagement

Regular open discussion through seminars, workshops, social media and so many other ways to connect to each other is one of the robust ways where we can train each other and complete each other's education on such topics. Also, engagement with decision-makers, regulators, civil society groups, and the general public encourages discussion and agreement on moral AI practices and concepts.

Conclusively, the report suggests that although AI has a major impact in the UK, ethical issues arise. The education, development and deployment of AI can be performed more responsibly and ethically by putting an emphasis on ethical issues, obeying laws and regulations, and prioritizing education and collaboration.

Section B

Select a recent or past data breach case and discuss the breach in relation to the GDPR principles and the ICO guidelines.

Introduction

This report will examine a past data break specifically the 2018 Facebook-Cambridge Analytica data breach in relation to GDPR and ICO guidelines. This report will explore the nature of the breach, its causes, and the GDPR standards it violated through a critical study of the breach as well as relevant literature. It will also provide vital insights into why these breaches keep happening.

What is meant by a breach?

According to the Merriam-Webster dictionary [13], a Breach is an infraction or violation of law, obligation, tie or standard. In the context of this report, we will be focusing on a specific type of breach: Data breach hence, the terms breach and data breach will be used interchangeably.

As a graduate of computer science engineering in cyber security and forensics, the author describes data breach as "the act of accessing, disclosing, or stealing private or protected information by unauthorised individuals either intentionally or *unintentionally*." Data breaches can happen for several reasons, such as system weaknesses, human error, or cyberattacks. A personal data breach is described in the GDPR as "a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed" (GDPR, Article 4 Point 12) [14]. Data breaches can have serious effects on people and organisations, including monetary loss, harm to their reputations, and legal issues.

Nature of the Facebook-Cambridge Analytica Breach

According to Granville (2018) [15] and (Isaak & Hanna, 2018) [16], the Facebook-Cambridge Analytica data breach resulted in the unauthorised gathering and use of personal data from about 87 million Facebook users. This data was obtained by the political consulting firm Cambridge Analytica from a researcher who had gathered it via the Facebook application "This Is Your Digital Life." The software, which claimed to be a personality test, secretly collected information not just from individuals who took the test but also from their Facebook connections. The 2016 US presidential election as well as the Brexit vote were then supported by Cambridge Analytica's creation of targeted political adverts.

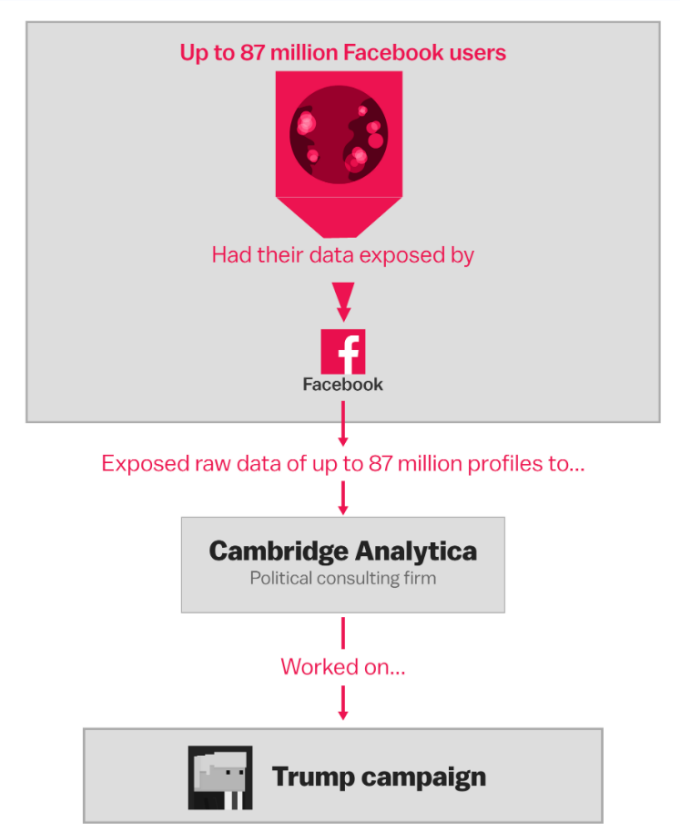

Figure 2: Visual version of the Facebook-Cambridge Analytica Breach (Chang, A, 2018) [19]

Why and how did this breach take place?

The major factors that contributed towards this incident were the lack of data protection rules, insufficient oversight, and a lack of openness among many others. Facebook provided substantial user data access to third-party app developers without adequate authorization or restrictions (Isaak & Hanna, 2018) [16]. Additionally, when Facebook learned of the problem in 2015, they did not monitor how this data was used and did not respond appropriately. By taking advantage of Facebook's API, the "This Is Your Digital Life" app was able to collect data from users who completed the quiz as well as their friends, resulting in a massive collection of personal data.

Relevant GDPR guidelines in accordance with this breach

Several of the GDPR regulations were broken by this data breach. Key clauses that have been broken include:

- Article 5(1)(a) GDPR (EU, 2016) [5] - Processing of personal data must be done lawfully, fairly, and openly. The author wants to emphasise on how these were exactly violated:
    - Lawfulness, fairness, and transparency: Facebook failed to obtain valid user consent before disclosing users' data to third parties and failed to give clear information regarding data collection and processing.
    - Purpose Limitation: Facebook uses users' personal information for purposes other than those for which it was intended, like targeted political advertising.
    - Data minimization: In comparison to the app's stated aim, the amount of data acquired by "This Is Your Digital Life" was excessive.
    - Accountability: Facebook failed to monitor the adherence to data protection regulations by third-party app developers and failed to take necessary precautions to protect user data.
- Article 6 GDPR (EU, 2016) [5] - Lawfulness of processing, in particular, Article 6(1)(a), requires that the user's consent be obtained before processing any data.
- Article 32 GDPR (EU, 2016) [5] – "Security of processing", which mandates the implementation of appropriate technical and organizational measures to ensure data security.

The breach not only broke GDPR regulations but also the UK's Information Commissioner's Office (ICO) [17] rules, particularly those related to the handling and security of personal data. The UK's Data Protection Act of 1998 [18] allows for a maximum fine of £500,000 (about $663,000), which is what the ICO stated it will impose on Facebook in July 2018.

It's crucial to remember that the hack happened before GDPR's implementation. According to Article 83 of the GDPR [5], which defines administrative sanctions for non-compliance, Facebook could have been subject to a substantially bigger charge if the breach had occurred after GDPR went into force. This fine could have been up to 4% of its annual global sales or €20 million (whichever is higher).

According to the author, even though the GDPR and ICO rules offer a framework to stop such breaches and enforce fines and penalties, it is vital for organisations to prioritise data protection and user privacy to prevent such situations in the future. He argues that humans shouldn't be ethical just because there are punishments but, they should rather do it as a moral duty to support harmony, growth, and respect for all the individual's choices in society.

Critical thoughts on why such breaches continue to take place.

Ideally, it should be a moral duty, but we should be aware that our world is neither ideal nor even close to one. Data breaches continue to happen for a variety of reasons despite the implementation of strict data protection legislation like GDPR:

a) **Insufficient enforcement**: Regulatory agencies might not have the resources or power necessary to properly enforce data protection laws, which could cause organisations to not comply.
b) **Technology and regulatory complexity**: Organisations may find it challenging to stay current with the most recent security precautions and regulatory standards, which can result in vulnerabilities and potential breaches.
c) **Lack of knowledge and training**: Organisations may not place a high priority on data protection, which leaves staff members with little to no training and an increased risk of unintended security breaches.
d) **Insufficient investment in cybersecurity**: Companies may not devote enough funds to cybersecurity, which leaves them vulnerable to online threats and potential data breaches.
e) **Profit-driven motivations**: Some businesses may put their financial interests ahead of data security, deciding to use user information for marketing purposes or other competitive advantages even at the risk of breaking data protection laws.

Section C

Use an interview or guest lecture to unpick these below-mentioned issues/topics based on AI in companies.

This report targets all the questions mentioned below in response to a guest session by Globant that the author attended through one of his modules regarding Ethics in AI which was hosted by Dr Mahesha Samaratunga, Director of Well-Being at the Queen Mary University of London (QMUL, Ethics, Regulation…, Lecture 4, 2023)[20].

Views on industries or companies using new technology or data to build state-of-the-art capabilities.

Globant's views on using new technologies and data to build state-of-the-art capabilities are solid and consistent right from when it started leaving its digital footprint in 2006. They have over 27,000 clients spread over more than 32 countries. They might not be well known for their new technology or state-of-the-art but that doesn't mean it's not happening, Globant claims that in some shape or form, we have interacted with something they have built, and this clearly shows they strong foot in this industry. In fact, they were the first outsourced partner of Google, One of the top Tech-Giants in the world.

Globant is aware of how machine learning and artificial intelligence (AI) technology may aid businesses to remain competitive and innovative. By utilizing these cutting-edge technologies, Globant hopes to provide its clients with innovative products and services like GlobantX and Reinvention Studios that can assist them in overcoming different business difficulties all with expertized guidance in their respective industry domains. They and others competing in this domain are trying to solve problems where humans or basic intelligence is required to get the predictions. The idea behind the use of such massive data and advanced technologies is to understand and improve how we communicate with the world.

Globant is committed to examining how artificial intelligence (AI) and data-driven technologies might help businesses grow, become more operationally efficient, and promote informed decision-making. They think that businesses that adopt and use these technologies will be far ahead of their rivals because they will be better able to respond to market trends and client requests. Globant's investment in R&D, strategic alliances, and commitment to building a culture of continuous learning and improvement all demonstrate its drive for innovation and technological advancement.

Company's Take on Using AI to transform organisational decision making

Globant's perspective on using AI to transform organizational decision-making is centred around the concept of augmenting human intelligence with the power of AI. They believe that AI can serve as an invaluable partner to decision-makers, providing insights and recommendations that are based on vast amounts of data and sophisticated algorithms while on the other side, also sourcing problems like information bubbles, different kinds of data-induced biases and bad algorithmic impacts on power dynamics in the decision making. For instance, Globant described bias by saying that "any algorithm by the nature of learning from past experience will have encoded or will have preferences that may or may not be related to what's called protected categories". These biases can be good or bad but what is more important according to them is how an organization handle them when working with information models, which decision should be let to be made autonomously, which of them should require human intervention and which of them should only be taken by expert professionals running the organization.

Some of the redundant and backend decision-making can be easily enhanced by incorporating AI into those decision-making processes, this way organizations can make better-informed choices and adapt more quickly to changes in the business environment. As such monotonous operations are automated, Globant believes that this will increase organizational effectiveness and free up valuable human resources for more strategic and innovative work. AI can also assist businesses in streamlining their operations to allocate resources as efficiently as feasible. Additionally, AI-powered analytics can offer insightful data on consumer behaviour, industry trends, and internal processes, empowering businesses to make data-driven decisions that promote success and growth.

Organisations harnessing the power of AI

Organizations like Globant have harnessed the power of AI in a variety of ways to address different business challenges and opportunities. Some of these include:

- Creating highly individualized client experiences: By utilizing AI-driven recommendations and insights, businesses can give their consumers a more individualized experience. This can boost customer satisfaction, loyalty, and revenue. But, In order to provide tailored promotions, goods, and services that are most pertinent to each individual client, firms like Netflix and others can utilize AI to analyze customer data and preferences which creates a unique information bubble for that client. This really is a big problem because if for example, Netflix doesn't give you what you are

more likely to click, it going to lose its impact on the user's experience hence, users can wander on other streaming platforms looking for more personal results. This dual-edged sword is the current reality of how AI is being harnessed by most of the companies out there.

- Enhancing internal operational efficiency: As mentioned above, By automating routine processes and streamlining workflows, AI may free up valuable human resources for more strategic and innovative projects. This may result in more productivity, lower operating expenses, and a more organized method of overseeing regular corporate operations.
- Implementing AI-powered analytics: AI could be used to examine enormous amounts of data in order to find hidden patterns and trends that human analysts might not see right away. These revelations can and are subsequently used in corporate strategy, innovation, and decision-making within businesses.
- Leveraging AI for security and fraud detection/prevention: By examining data for suspicious patterns or abnormalities, AI can be used to identify and stop possible security threats or fraud cases. This can assist businesses in protecting their priceless assets and guaranteeing the reliability of their systems and procedures.

Company's take on data privacy, information governance requirements in the UK and the relevant organisational and legislative data protection and data security standards that exist.

Globant boldly, honestly accepted the reality that ethics in AI is not something that can be solved (at least not just like that). They clearly mentioned that "How do we define what is correct, what's valuable" It's all very subjective. Their belief satisfies the principle of fairness in GDPR (Article 5) [5] "It is always related to difficult choices, there is a lot of trade-off going on every day where we can encounter this subjective nature of ethics, for example, when we are talking about the capacity of people publishing things online we are always balancing the idea of the self-expression versus the damage we believe that expression can generate on others." That being said they added "The same thing happens in terms of privacy and safety: when it's an invasion of privacy and when it's a necessity by states or whatever to provide security and safety, and what's the limit where this overlap is stepping over what we believe as right. That kind of choice is what we need to solve". The author also supports these ideas as one of his own because when it comes to dealing with people, there is no black or white, it all boils down to context with so many other human factors which define us in the most unique ways possible.

Globant maintains its data security/protection, and ethical standards by asking questions like: "How can I own the outcome of this process if I'm a company and I'm using a model? how do I limit the impact of my organizational decision on people's lives? (This specific question satisfies the principle of data minimization from GDPR (Article 5) [5]) How do I limit the damage that can be done with that? How can I change to frame my products in a more positive manner? We can see why these questions are important because the question is not if AI's good but rather how can I make its impact better, and the impact is going to be what matters most to us." Their concern and introspective question satisfy the principle of accountability in GDPR (Article 5) [5]. This report argues that these lines, these thoughts by Globant should be installed

in every process and organization of the digital world. All the ways we discussed in the above sections to aware and train professionals into improving their ethical practices, especially in AI; should have a base built on these introspective questions. These concerns and design decisions satisfy the principle of privacy by design and default from GDPR Article 25 [5]. In terms of governance, it is important that powerful companies like Globant and others should account for the power dynamics and how they maintain control over its aspects while responsibly reflecting upon the responsibilities or the points where they need to control and track what's going on.

In Summary of the guest lecture and author's understanding of Globant's perspective:

By abiding by UK data protection rules and regulations, such as GDPR and the UK Data Protection Act, Globant prioritizes data privacy, information governance, and data protection. The company's strategy includes developing a strong framework for information governance, putting in place organizational and technical security measures like secure data storage solutions and advanced encryption technologies, routinely updating policies and procedures to address emerging threats and technologies, encouraging a culture of data privacy awareness among employees through training and education, and working with customers, partners, and regulators to achieve a shared understanding. These approaches promote industry-wide consistency and maintain transparency in data-handling processes while ensuring compliance, security, and privacy.

Finally, their focus on responsible AI-driven decision-making and limiting its impact on people's lives satisfy Article 22 [5]: Automated individual decision-making, including profiling of GDPR. Additionally, the author appreciates and congratulates Globant for their focus on culture and team ethics, their BeKind fund of $10 Million which back-benches the companies that are looking to mitigate the negative impact of technology on the environment seems very admirable to the author.

References

1. Wikipedia Contributors (2019). Geoffrey Hinton. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Geoffrey_Hinton.
2. Kurniasih, N., Kurniawati, N., Yulianti, Rahim, R., Sujito, Ikhwan, A., Aimang, H.A., Haluti, F., Putri, L.D. and Napitupulu, D. (2018). The utilization of search engines by students of the Library and Information Science Program at Universitas Padjadjaran. Journal of Physics: Conference Series, 1114, p.012085. doi:https://doi.org/10.1088/1742-6596/1114/1/012085.
3. PwC (2017). The economic impact of artificial intelligence on the UK economy. [online] Available at: https://www.pwc.co.uk/economic-services/assets/ai-uk-report-v2.pdf.
4. De Fauw, J., Ledsam, J.R., Romera-Paredes, B., Nikolov, S., Tomasev, N., Blackwell, S., Askham, H., Glorot, X., O'Donoghue, B., Visentin, D., van den Driessche, G., Lakshminarayanan, B., Meyer, C., Mackinder, F., Bouton, S., Ayoub, K., Chopra, R., King, D., Karthikesalingam, A. and Hughes, C.O. (2018). Clinically applicable deep learning for diagnosis and referral in retinal disease. Nature Medicine, [online] 24(9), pp.1342–1350. doi:https://doi.org/10.1038/s41591-018-0107-6.
5. European Parliament and Council of the European Union. (2016) 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). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
6. Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016). Machine Bias. [online] ProPublica. Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
7. Intersoft Consulting (2013). Art. 22 GDPR – Automated individual decision-making, including profiling | General Data Protection Regulation (GDPR). [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/art-22-gdpr/.
8. Rees, J. (2020). Police force facial recognition use ruled unlawful. BBC News. [online] 11 Aug. Available at: https://www.bbc.co.uk/news/uk-wales-53734716.
9. Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute. https://doi.org/10.5281/zenodo.3240529
10. Equality Act (2010). Equality Act 2010. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2010/15/part/2/chapter/1.
11. legislation.gov.uk (2018). Data Protection Act 2018. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/2/enacted.
12. European Commission (2021). EUR-Lex - 52021PC0206 - EN - EUR-Lex. [online] Europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.
13. Merriam-webster.com. (2019). Definition of BREACH. [online] Available at: https://www.merriam-webster.com/dictionary/breach.

14. Intersoft consulting (2013). Art. 4 GDPR – Definitions | General Data Protection Regulation (GDPR). [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/art-4-gdpr/.
15. Granville, K. (2018). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. The New York Times. Retrieved from https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
16. Isaak, J. and Hanna, M.J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer, 51(8), pp.56–59. doi:https://doi.org/10.1109/mc.2018.3191268.
17. ICO (2019). Personal data breaches. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
18. GOV.UK (1998). Data Protection Act 1998. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1998/29/contents
19. Chang, A. (2018). The Facebook and Cambridge Analytica scandal, explained with a simple diagram. [online] Vox. Available at: https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.
20. QMUL (2023). Ethics, Regulation and Law in Advanced Digital Information Processing and Decision Making – 2022/23, Lecture 4 [online]