Reflective Writing

1. Data Ethics & GDPR

My initial exposure to the issue of the European General Data Protection Regulation (GDPR) had a bureaucratic coloring as a set of rules that must be followed and are a burden to the business. Thanks to the work we have done in Module 2, the ZDNet article as well as the idea of thing called contextual integrity by Zimmer, I started to think about GDPR in a different light. It could not be reduced only to preventing fines or checking off lists; it reflects a philosophical change in the approach to personal data appreciation by societies. GDPR requirements to consent explicit consent, granted by individuals, the rights to forget and data minimization reshaped my perceptions on privacy as a human right, rather than a commodity that can be negotiated.

It further intensified the point of view when the case was analyzed with tools of ethics. I discovered that GDPR safeguards not only people against acute Data Risk (such as Identity Theft) but we are also safeguarded against the systemic undermining of sovereignty. The trust in the digital environment, which my initial opinion had not taken into consideration, is strengthened by GDPR that forces organizations to treat user data with respect.

Takeaways: Compliance with privacy laws should not be viewed as a checklist; privacy laws should be regarded as an ethical promise to honor individual freedom in an era of online interactions. I should promote privacy-by-design even when it is not legally appertinent in any future cybersecurity or technological position.

2. Professional Ethics & “The Code I’m Still Ashamed Of”

My first impression concerning the story by Bill Sourour, a pharmaceutical quiz as he claims, using unobtrusive advertisement in order to advertise a drug but at the same time downplaying its side effects, was actually a sorry tale about underestimating the project. I may have thought before this course that it is a misunderstanding between marketers and developers. However, after reviewing the Material of the Module 4 and the Codes of Ethics, I was reevaluating the nature of the personal responsibility of the developer. The case demonstrated to me that evil can be done in cases whereby one is technically doing the correct work but the motivation behind the correct work is evil.

Using the ethical reasoning, I understood that the actual problem was not only an abuse of code, but the neglect to the well being of the end user. The code by Sourour also led to deluding of patients who were put in physical danger. The Codes of Ethics clearly urge the professionals to thwart harm, not lie, and consider the greatest good of the people. The case taught me that the excuse of obeying orders is not an excuse in cases where that work can be used to deceive or harm other people.

Lesson: One has to be technically qualified, but also one should be ethically conscious in the context of his profession as a responsibility. I should be ready to challenge or reject engaging a project whose aim is against the responsibility of protecting the public.

3. Cyberconflict & Just War Theory

Module 6 looked at the issue of cyberwarfare in the context of Boylan and Taddeo models. When I was first hearing about cyberattacks, I believed that they were, first and foremost, less innocuous options consistent with kinetic warfare, which, naturally, could not be preferred due to creating physical casualties. However, study of power grid and emergency facilities attacks changed my predisposition. I also observed how cyber operations may have long-term impacts by lowering the trust of people, destabilizing infrastructure, and degrading the emergency response infrastructure.

The ideas of Taddeo, as the “Infosphere”, induced me to understand that the information systems themselves are also part of the ethical landscape of war. The values of the Just War Theory, such as distinction, proportionality, necessity, not only concern physical attacks, but also the information continuity of civilians. Although the general war may be acceptable, some cyber strategies (such as false missile warnings) are not acceptable since they become unethical as they affect individual capabilities to make intellectual and life-saving actions.

Learning Point: When assessing cyber operations, I have to be aware of both short term tactical impacts, as well as their long term effects on trust and stability. It is only natural that maintaining the integrity of the Infosphere is as distinct as preventing flesh wounds.

Conclusion

Reflectively, all these issues increased my professional and ethical responsibility to the digital domain. GDPR redefined privacy to be moral as opposed to legal. The Sourour case brought me back to the fact that technical skills need to be focused towards the ethical purpose. Through analyzing threats of cyberconflict, I have realized that ethics of the modern warfare contain the protection of the informational integrity of the civilian population as one of the fundamental tenets. The combination of these lessons supports the notion that in my future career, I should not be solely led by what is possible but what is right--as in technology, the two are not always in line.