POLITECNICO
DI TORINO

Data Ethics and Protection

Esame_20210709_Parte_1

	[redacted]
Iniziato	venerdì, 9 luglio 2021, 17:02
Terminato	venerdì, 9 luglio 2021, 17:47
Tempo impiegato	45 min.
Valutazione	**15,00** su un massimo di 15,00 (**100**%)

Domanda 1

Completo

Punteggio ottenuto 7,50 su 7,50

Which are the main approaches in regulating technology and what are their strengths and weaknesses?

First and foremost, one of the main issues in regulating technology comes with the Colingsridge dilemma, which in short states that "it is difficult to measure the impact of a new technology before it's wide use": considering this, the main approach that authorities engaged on in recent years was a precautionary one. Technology is not to be released freely on the market unless proven to be harmless to the rights and freedoms of natural persons and society, whithout impairing the technological advancement of human kind (ex. the GDPR regulates the rights of privacy (art 7 of the chart of fundamental rights of the EU) and data protection (art 8) of the EU citizens, but clearly states in its first article how the goal is to facilitate the flow of data). The strenght of this approach is that without an ample regulation that allows for a risk based approach, technology is not introduced in the market, and natural persons are never put under too much of a risk from it; on the other side, its main weakness is that regulating technology for which the risk is not know requires a lot of time and money from the entity developing it or from the regulating authorities, and might slow down the developement of it unless highly funded.

Another important point to consider concerns the so called "Law of the Horse". One of the possible approaches in regulating technology would be to create a new branch of law concerning cyber law, but this would come at the cost of a more confusing and maybe even contradicting regulation; despite being harder in its implementation, the adopted solution was to create specific provisions of existing regulations to cover never before seen cases, while having the possibility to create a new regulation altogether for technologies unrelated in any way to the existing regulation.

Lastly, technology could be regulated with either a bottom up (soft law) approach or a top down (hard law) approach. A bottom up approach sees the main players in a market regulating themselves, this allows for a very detailed regulation in the form of codes of conduct and requires little time and cost as the experts on the field work and have interest in it, but lacks the strenght of a strict law enforcement and might be subject to the phoenomena of the "bully-pulpit". On the other hand, a top down approach requires a lot of time and study from the regulating authorities and its the process of law making itself: its main strenght is to have a regulation that's backed by law enforcement, it's fair and equal and recognized in any case by the players in a given market, while its main weakness is the lack of adaptability, the time it requires to come into fruition and the lack of specific knowledge of the sector that's being regulated.

Commento:

Domanda 2

Completo

Punteggio ottenuto 7,50 su 7,50

A municipality decides to measure the level of crowding in the city centre, using sensors placed along the main streets. These sensors detect Wi-Fi signals from the mobile phones of passers-by, registering each phone separately with a unique code.

Each sensor works as a counter to measure how crowded different areas are by counting and recording the phones near the sensor at a given time.

Does this project have any relevant data protection issues to address? If yes, what measures should be adopted?

The main actors in this case are the municipality, which takes on the role of the controller for the collected data and the citizens, which are the data subjects. The collected data consist in a unique identifier for each phone, which in a general sense might be considered anonymous (or pseudonymous) and not linkable to any natural person. In the scenario i will consider, the sensor assigns the same unique identifier each time the specific device it belongs to is registered by it and the data is stored inside the EU.

Considering this premise, the main data protection issue that might arise is that of re-identification of the apparently anonymous data: by knowing where a natural person went in the city by other means, it would be possible to track said person along the route of the different sensors at any given time, thus violating his/her rights to privacy. This is very similar to the London bike sharing case, and if the collected data was ever to be made public, it would pose the citizens under a high risk.

Speaking of security measures that could be adopted, there are two possible routes. The first one is to comply with the GDPR by making the risk known to the citizens (the same way they are informed of cameras in a certain area), by providing a formal assessment (as per article 35) to the competent authorities and by taking the correct organizational and technical security measures to prevent a data breach or reduce the impact of it: this scenario is unlikely to happen as it would allow the municipality to track the citizens and the collection wouln't probably be justified. The second one would be to either randomize the identifiers each sensor assigns, to prevent re-identification and route tracking, or to use the identifier only as long as the device is in the vicinity of the sensor and then delete it as soon as said device leaves the area, only keeping a snapshot of the count of devices in a given area every xx:xx minutes for statistical purpose: this would be likely to happen and allow the municipality to make the data public as it would be completely anonymized.

Regarding the territorial scope, as article 3 states every data subject in the EU territory is under the GDPR, so if any tourist were to be tracked by the devices, it would still be fair under the existing regulation.

Commento: