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.

POLITECNICO DI TORINO

Data Ethics and Protection

Esame_20210625_Parte_1

[redacted]

Iniziato	venerdì, 25 giugno 2021, 17:03
Terminato	venerdì, 25 giugno 2021, 17:48
Tempo impiegato	45 min.
Valutazione	**14,50** su un massimo di 15,00 (**97**%)

Domanda 1

Completo

Punteggio ottenuto 7,50 su 7,50

What is the relationship between security requirements and risk management (Article 35) in the GDPR?

Data Security is a part of the risk managment procedure described in the GDPR and it is is mainly focused on the security requirements that have to be addressed in a technical sense. We can think to data security in a computer science meaning because when we are involved in a processing activity first of all we need ensure that all the aspect related to the security measure have been taken into account. When we talk about risk managment we need to focus on both data security risks and risk related on freedoms and rights of natural persons. When a company decides to collect,store, procces, manage, share, update and cancel data it must consider possible bad consequences in terms of data breaches. It could happen that data is unlawful or accidentally accessed, modified lost, distrupted. These things may be very dangerous especially if we are dealing with personal data and sensitive data. We need always asses the potential bad consequences of a data breach and we need to asses the likelihood and the severity of it. The company needs to care about a risk-cost analysis to establish what kind of technical and organizational measures must be taken in order to avoid accidents. When we talk about security measures we need to think to the proportionality concept so we need to decide the technical and organizational mesaures we need to ensure based on the likelihood and severity of the risk and on the cost of the implementation of such measures. Security measures are part of the risk managment and risk assessment because the GDPR decided not to provide a minimul level of security measures to be adopted. There is no a standard requirement because,as already said, companies need to asses the risk based on the context, so based on the nature of data they want to process, the purposes, the amount of data and the amount of persons that are involved and so on, for this reason,the establishment of a common stard would not been appropriate for all the

cases. When we talk about security measures we not only refer to technical aspects, like for instance an authentication system that ensure the access to data only to entities that have the right to access, but also to organization measures. Think for example to an employee that changes role in the processing activity, he may be not authorized anymore to access data once his role is changed, so we need to ensure that at the level of the organization all these changes are detected and informed. We need also think to security measures in terms of incident identification system and actions that must be taken to prperly react when data breaches happen, so we need to have efficient identification system that are able to promplty dected the incident but we also need to ensure that the processor notifies the data breach to the controller that on his hand to carefully evaluated the severity of the situation and decide if notify the breach to the SA only or also to data subject. Another very important concept is the one related to necessity of continuously update the security measures. The technologies change and so for example the technical system we decided to use may be not adequate anymore because its state of art is changed or maybe because the company is starting a further processing activity that require an higher level of security based on the nature of data and on the nature of the purpose. Therefore, like for the risk assessment on human rights and freedom, also the assessment on data security must follow a cyclic approach, we need to do a preliminary analysis to map all the process activities, the entities envolved, the data and the data subject envolved, the level of the risk, the necessity or not to provide a formal impact assessment, the necessity or not to ask for a prior consultation, the technical and organization measures that we want to ensure and then we need to continuoulsy update the risk assessment and verify that our decision are still adequate.

Commento:

Domanda 2

Completo

Punteggio ottenuto 7,00 su 7,50

A Portuguese AI company aims to create a large database for training image recognition algorithms, focusing on objects with different shapes and human bodies. The database will be accessible as a service to third parties on the basis of an annual fee.

To achieve this goal and populate the database the company collects worldwide images and videos from blogs, social media, and online media websites.

Please consider the characteristics of this case and provide an assessment of potential legal issues and possible related solutions.

When we talk about Artificial Intelligence algorithms we need to consider a lot of aspects due to the fact that this type of digital systems are much more complicated than traditional ones. Machine learning algorithms work with a big quantity of data so we are in the case of processing of a large scale of data. Moreover biometrical data are special cateogory of data so we fall in the scenario of

processing activity of sensitive data. According with the risk assesment part described in the GDPR but also with the Article 29 WP we have presumption of high risk so DPIA, so a formal impact assesment must be provided by the Portuguese company that is the controller of the processing activity. The AI company in fact decides which kind of data will be collected, for which purpose, for how long this data will be stored in its database, the measures to adopt to tackle the risk. It is not so easy to think to a collection of data in anonymous form because the shapes of human bodies are striclty connected with the identity of the person, for this reason the company need to process the activity being compliance with the GDPR regulation. Another crucial aspect is the consensus from the data subject, since the company wants collect sensitive data the consensus has to represent the legal ground for the processing activity. Regarding the access to data by the third parties we need to consider first of the possibility that the third party has a joint controllership with the Protuguese company (that is part of EU so compliant with the GDPR), in that case there must be provided detailed information about contractual documents. We need also to take into account two different scenarios: if the third party company is an European company or not. In the first case the flow of data from on company to another can happen without additional compliance than the one of the GDPR. In the case in which the third party company is not an European company we need to understand if its country adopts a level of data protections regulation whose level is acceptable for the GDPR, in that case we have adequacy and we can trust the flow of data. In the case in which the third party company is in US we have a bilateral agreement that force the American company to follow high level protections regulation when treating data from people in European territory. We can also have the case of binding corporate rules or contractual clauses that can be established in order to ensure that the processing activity by the company are compliant with the GDPR, in this case it could be not so easy to ensure a lawful flow and processing of data because the compliance with the clauses must be assesed by Supervisory authority (this could be difficult).

Commento:

Data Ethics and Protection

Esame_20210625_Parte_1

Iniziato	venerdì, 25 giugno 2021, 17:01
Terminato	venerdì, 25 giugno 2021, 17:46
Tempo impiegato	45 min. 1 secondo
Valutazione	**13,50** su un massimo di 15,00 (**90**%)

Domanda 1

Completo

Punteggio ottenuto 6,00 su 7,50

What is the relationship between security requirements and risk management (Article 35) in the GDPR?

Integrity and confidentiality as principles

In the GDPR's main principles (Article 6) we have data integrity and confidentiality. One of the regulation's

goals is to keep the data subject's data secure and reduce the risks of possible data breaches. This is

because of the possbile consequences of a breach on the subject's fundamental rights.

Data Protection Impact Assessment

In order to be accountable and to show that adequate security measures measures are used, it is useful,

and might be mandatory, to compile a Data Protection Impact Assessment, or DPIA. In this document, among

other information such as the name of the Data Protection Officer and a description of the data flows, we need to

explain which risks were considered and how we plan to address them.

Risk management techniques

It is possible to build a risk matrix containing the risk description, its likelihood, and its possible consequences

for both the data processing and the data subject's fundamental rights. Then, considering the product of the

likelihood and the impact severity, it is possible to evaluate the importance of this risk and decide how to address it.

Addressing security requirements and de-risking

For security requirements technical solutions such as encryption, hashing, salting and pseudoanonymization can be used.

We also have to estimate how difficult it would be to break the solutions we employed, considering the present and future state of the art.

Some organizational measures that address the security requirements are,for example, fine grained access control, and supervision.

Data protection by design

Other GDPR principles help in this aspect too, in particular data minimization and storage limitation. These two

help to obtain a system that is secure-by-design by reducing the attack surface.

Formal assessments

After having performed a risk assessment, if the risk is too high or if we fall in an application for which, a priori, the

risk is too high, a formal assessment with the Supervisory Authority has to start. In this process, the SA will help us

design measures and reduce the risk in our application.

Commento:

Domanda 2

Completo

Punteggio ottenuto 7,50 su 7,50

A Portuguese AI company aims to create a large database for training image recognition algorithms, focusing on objects with different shapes and human bodies. The database will be accessible as a service to third parties on the basis of an annual fee.

To achieve this goal and populate the database the company collects worldwide images and videos from blogs, social media, and online media websites.

Please consider the characteristics of this case and provide an assessment of potential legal issues and possible related solutions.

Actors

The Portuguese AI company as the data controller.

The people in the images collected by the company as the data subjects.

Material scope

The company collects images from the internet, in particular social media, thus we suppose that the data is personal since it concerns an identified or identifiable natural person.

Since this personal data, it may be about about EU citizens. For these reasons the GDPR applies.

Territorial Scope

Portugal is an EU member country and the company has an establishment there, so the GDPR applies.

Consent issues

The first issue that comes to mind is the one regarding consent. Even if the data subject has given consent to the social network for uploading the images to the open web, it is not clear if this particular usage was present and clearly stated in the data protection policy. And this would probably not be considered a legitimate interest of the website operator.

Terms of Service breach

Even if the social network's users had given consent for this particular application, this does not mean that the social network will let the AI company use these images for profit. In practice, this is forbidden by the terms of service of most websites.

Anonymous data and copyright issues

If the portuguese AI company pays particular attention in avoiding images that can be at all connected to a natural person, maybe by only collection 3D rendering of human bodies, then this data does not fall under the GDPR. Still, if the images are collected from websites, the AI company must make sure that copyright is not broken.

Applying GDPR's main principles to AI

Even if all of the previous issues are solved, it is not clear how GDPR's principles can be applied to this particular case. How can the data subjects know all of the uses this data will have? How can they express their right to deletion and the right to have accurate data, when this data has already been transformed in a black-box machine learning model?

Commento:

POLITECNICO DI TORINO

Data Ethics and Protection

Esame_202 [redacted] pello)

Iniziato	venerdì, 9 luglio 2021, 18:02
Terminato	venerdì, 9 luglio 2021, 18:47
Tempo impiegato	45 min.
Valutazione	Non ancora valutato

Domanda 1

Completo

Punteggio ottenuto 4,50 su 7,50

An Italian car insurance provider experimented the usage of machine learning for predicting the risk of repaying the costs of caused incidents in a year for a person. In case of high risk, a higher premium is offered to the applicant (who can accept the quote or not). The company used part of its own historical data (from 2010 to 2020) to train a classifier. During the experimentation, applicants could get their quote after filling a form with data about the car and themselves (fields filled are the same used by the classifier). In addition to that data, applicants were required to input information on their ethnic group: although this sensitive data was not used by the classification algorithm, it was collected in order to test the classifications against discrimination. In fact, national and international regulations require that prices should not vary depending on ethnic group, and they also forbid training of classification/prediction algorithms with it. The ethnic group had the following possible values: Caucasian, Black, Asiatic.

The features used by the classifier are the following ones.

A. Birthplace: driver's nation of birth (list of all possible countries in the world)

B. Age: driver's age (integer between 18 and 100)

C. City: driver's residence (list of all Italian cities)

D. Car: insured vehicle type, deduced from the car model and year (two possible values: small cars and large powerful cars)

E. Claim history: number of previous claims (values: less than 3, between 3 and 6, more than 6)

F. Yearly distance: estimation of kilometers driven in a year.

The analysis of the data gathered during the 6-months experimentation showed that offered prices varied significantly when only ethnic group differed while all other characteristics were equal.

Therefore, the company dismissed the development of the system, and kept applying insurance

costs with respect to traditional, static, risk models.

Please briefly answer to the following questions (GIVE A SEPARATE ANSWER FOR EAC H QUESTION):

1. Provide possible explanations for the results of the experimentation: clearly state you r own hypotheses, and any other information that you suppose in addition to the provid ed data, to coherently support your reasoning. (3p)

2. Which measurement issues do you observe? (3p)

3. Which changes in the experimentation data collection process would you introduce to check fairness in terms of separation? (1,5p)

1.

The following considerations are based on the assumption that it is likely that a non-Caucasian person is an immigrant in Italy.

we can look for possible explanations for the results in the correlation between the attributes used from the algorithm to make predictions and the ethicity of the person the data belong:

- Birthplace: this is likely a direct link between the person and its ethnical background.

- Age: although it is not always the case, it is reasonable to think that immigrant are quite young, as they usually move from their original place in search of job, with the aim to come back whenever possible.

- City: the italian residence does not have much correlation with ethnicity at a City level, even though it is possible to determines some italian area where the presence of non-Caucasian people is more relevant.

- Car: due to the economic conditions of immigrant people, it is likely for them to have more cheap cars, often old as they have been bought from previous owners.

- Claim history: this attribute does not have relevant correlation with the ethnicity of the data subject

- Yearly distance: we can assume that an immigrant (Black or Asiatic) is not near to family members, thus this exludes that kind of traveling, and it is also improbable that it has a job far away from home which needs to travel. In general, it is possible to have a light correlation between the yearly distance made with a car and the ethical group.

2.

For what concerns the measurement issues, we can say that the disparities coming out from the audit can be explained by considering the training dataset which consists in the historical of the insurance company from the last 10 years. In fact, we can suppose that it was highly dishomogeneus with respect to the ethnic group attribute, due to many factors. First of all it is reasonable to assume that the dataset would at least be coherent with the italian distribution of ethnic groups, which is not heterogeneus, and mainly represented by Caucasians. Moreover, this

disequilibrium can be increased by the fact that immigrant people, even though it is not true that all Black or Asiatic people are immigrant, lie in a situation of lower economical resources, which often are not enough for buying a car and maintain the insurance.

3.

First of all, it could be appropriate not to ask the birthplace, as it is directly related to ethinicity in many cases.

Commento:
1) very good

2) The whole answered is focused on imbalance, which is connected to Q1 and it is rather a consequence of the data collection rather than a measurement issue.

see the guide for some examples of measurement issues.

3) no

Domanda 2

Completo

Punteggio max.: 7,50

Comment the following statement: "technology is essentially the direct application of the results of fund amental science".

This statements, given the negative connotation hidden in the term "essentially", supports the idea that technology is subordinated to science as it is a mere application of its pure theoretical studies, devoted to the understanding of the natural world (and which deserves a higher respect as they are not directly transformed in material instruments).

However, we can think about technology as the direct application of the results of fundamental science, which itself contributes to the evolution of the latter. In fact, there is a strict relationship between these two side of the same medal that is the Science as a broader concept. While fundamental and theoretical science aims to deepen our understanding of the world and of its rules, the technology is able to leverage those discoveries and, by means of creativity and "savoir-faire", to invent and produce new instruments that are going to be fundamental for further science research.

For this reason, as Mauss wrote, there is a strict coevolution between those two worlds, differently from the traditional point of view, that has roots in the ancient greek philosophy and in particular with Aristotele's claims, which put the technology at a lower level with respect to science (techné as less pure than episteme). While the science is more vertical and focused to deppen the knowledge on a specific sector, the technology is more interdisciplinary, it looks at society issues too and tries to exploit that knowledge to produce new intruments that wil help in many fields.

POLITECNICO DI TORINO

Data Ethics and Protection

Exam_20230714_Part_1

	[redacted]
Iniziato	venerdì, 14 luglio 2023, 14:03
Terminato	venerdì, 14 luglio 2023, 14:43
Tempo impiegato	40 min.
Valutazione	**10,50** su un massimo di 15,00 (**70**%)

Domanda 1

Completo

Punteggio ottenuto 4,00 su 7,50

What is the main task of the Data Protection Officer (DPO) in the context of a Data Protection Impact Assessment?

Data protection officer in case of data breach should notify the data subject when there is a high risk of rights and freedoms.

DPO should have a document of technical and organisational measures in risk situation. a log of practices.

DPO is appointed in order to monitor the processing, collecting data and monitoring the job of data controler. DPO is not responsible for not complince with GDPR.

implementing the risk assessment process and if it is a high risk should prevent it to be launch into the market. but with precautionary principles the AI technology can be improved until mitigating its risk to the acceptance level.

when there is a high risk a DPO should be hired to monitor the data protection proccess and prevent the infringe from the GDPR.

should have another task in the companyjust being a DPO. have a plan for high risk situation .

Commento:

Domanda 2

Completo

Punteggio ottenuto 6,50 su 7,50

ABC srl, a Turin-based company, launches an online questionnaire on Italians' preferences regarding football.

Specifically, in the questionnaire, in addition to name and surname, various information of a purely sporting nature is asked, as well as questions relating to income, professional activity and even political preferences and sexual orientation.

The questionnaire was a success, thousands of persons answered.

With the answers obtained from the participants, ABC would like to train an artificial intelligence algorithm, based on its legitimate interest, capable of predicting people's favourite football team based on their income and political and sexual orientation.

However, ABC, having heard about GDPR, has some doubts about the feasibility of the project and, therefore, turns to you as legal counsel.

Can ABC carry out this processing activity relying on legitimate interest as a legal basis? Please, justify your answer

---

as it is said the consent of the participients is got because they freely complete the questionaire. but here should do a balance interest between right of the ABC to train the algorithm and data subject's interests and their rights and freedoms.

in term of consent the data subject they should have the right to access their data in portable format, right to be forgotten, right to rectify their data and right to limitation the access and object to the the data for the company. they should appoint a data protection officer because they are working with sensitive data, special category of data. risk assessment data protection should be held and have measure to tackle risk.

the variables income and professional activities are related to wealth of people that might be correlated with ethnic groups in term of discrimination that might be as a consequence of this questionare, like imigrant people in ITaly that might not have high income here.

political and sexual oreintation are special categories of data and they are sensitive data so they should not be in danger of publicity. they must be secured in an anonymous way that can not be identifiable' then it might not be under the GDPR rules.

for territory scope the company is in EU so should be under GDPR and also people of Italy should be under the protection of GDPR in term of human rights and freedom and data security.

there is nothing said about the time that data might be stored, limitation purpose should be considered and data should not be kept after collecting and proccessing for a long time. people should have the right to access, modify and erase their data whenever they want, that should be considered too.

in case of data breach because these are sensitive data if there were not organisational and technical measures and in case of high risk, data subject should be notified, as these data are so sensitive and private that might have dangerous consequences for data subject.

in my point of view under GDPR, natural person's interest prevails the legitimate interest of the ABC. there is no legal interest, scientific or historical in collecting these kind of data compare to risk.

If the latter observation holds, young candidates without university degree education that fall in the category 18-25 and with less skills are disadvantaged, regardless of the balance of the age categories.

3 Examples of possible improvements:

For a better gender balance (e.g., at least 35% female) in its current binary representation, it would be necessary to require a minimum IIR of 0.47 (approx. 0.50). Please notice that this intervention might not be sufficient to counterbalance the effect of the proxy variables, which depends on the correlations to be found.

in the data (between proxy variable and protected attribute, and between proxy variable and target variable).

Exam Answers

What is the relationship between security requirements and risk management (Article 35) in the GDPR?

(1) The European General Data Protection Regulation in its article 32 describe the security requirements that data controllers must perform when processing personal data in order to comply with the law. Recall that GDPR is a regulation setting a legal basis for the processing of personal data of European Union residents.

(2) The GDPR was developed under a risk-based approach. This means that data controllers must perform an evaluation of the risk posed by the data processing to the data subjects and take proportional and adequate measures for dealing with the risk. Those measures include the security of the data to be processed in terms of technology and procedures used.

However, the GDPR does not provide a specific technical requirement because it follows a tech-neutral approach and does not stick into a particular technology that could be disproportionate or not adequate in some cases also given technology development. Instead, it is the data controller that must evaluate the measures to be taken given the context.

(3,4) The data processing involves any operation performed on data linked to an identified or identifiable individual and the data controller must (5) respect the accountability principle. As said before it is the fact it took and adequate measures to minimize the risk by the processing.

First of all, a preliminary analysis of the data processing must be done in which the data strategy and management is defined. The risk assessment is done as a by-design approach which means it must be performed before any data processing takes place. Then a formal risk assessment is done, the Data Protection Impact Assessment (DPIA) , that although is not required in all cases (following the procedural approach) is strongly advised.

In it all the security measures proportionate to the data processing must be described. As suggested by the ENISAA those could be (but not limited to) the training of personal in cybersecurity issues, the physical security of informatic facilities, the procedural design, ...

In short, the data controller must ensure to take security measures, appropriate to the risk posed to the data subject. In particular by any unauthorized disclosure, alteration, erasure , . of the data.

Furthermore, the data controller must have (again, if retained necessary) a plan to follow in case of data breach since by the GDPR it is required to notify to the authorities the nature of the data breach and the measures taken.

What is a data breach? What is the procedure to follow in case of a data breach?

A data breach is whenever an unauthorized action such as disclosure erasure or modification happens on the personal data processed by a data controller.

The concept of data breach and the actions to be taken are discussed in the general data protection regulation of the EU (GDPR). In this regulation a legal framework for the processing of personal data is given. In particular, the responsibilities that a data controller must have in case of a data breach are specified.

Recall that the GDPR is a risk-based regulation, which means that no specific procedure is specified (except for a detail explained in the following about the time of report) and it depends on the context in which it happens. Therefore, in case of a data breach a company should assess the risk of the data breach and inform the Data Authority within 72 hours (this is the only detail specified) giving a report containing the nature of the data breach, its severity and the measures taken to reduce the damages to the data subjects. The data authority is the entity of a member state that ensures that the GDPR is respected.

Recall that the data subjects are the natural persons to which the data is referred (that is data that can be linked to an identified or identifiable data subject) and they must be informed about the data breach only in particular cases where the severity of the breach requires it, Note that this procedure should be done with the help of marketing and legal departments in order to not create excessive alarms and make the company lose money. As an example, we can think of the UniCredit case in which they exaggerated a data breach and lost many clients because it was not informed correctly.

The documentation to prepare is extensive and the report to the data authority must be done on time in order to allow it to warn other data controllers about the possibility of an attack (when itis necessary) 50:2 company should have already the documentation prepared in order to not risk receiving a sanction (that can be more or less severe depending on how accountable is the company). The sanction can be up to 20M EUR or 4% of the annual revenue of the company.

The data controller (the entity responsible for the processing of the personal data) must be able to demonstrate that it has taken the adequate security measures to ensure that the risk to the data subject minimized. As ENISAA suggests they must have acted in many fronts in order to ensure that there is an adequate level of physical and informatic security. Additionally, employees should have received training on issues about cybersecurity and good procedures must be adopted to ensure the risk of data breach is minimized.

In the data breach report, the controller must not minimize the data breach that happened. On the contrary it should explain in detail what happened, what are the risks and the measures taken (or to be taken).

Describe the main pillars of the GDPR and how they are related with the DPIA,

The GDPR is the General Data Protection Regulation in the EU. Its aim is to provide a legal framework for personal data processing by enforcing some rules in all EU member states.

SCOPE OF THE GDPR

The GDPR is applicable to the personal data of natural persons in EU soil (so not only EU citizens) (articles 3 and 4). The personal data is defined as any information liked to an identifies or identifiable person. This means that the personal data is referred to a person that could by any reasonable means be identified. It is stated that even if the person could be identifying in the future with technological development t should be considered. This is related to one of the pillars of the GDPR that, as we will see, is technology neutrality. The data processing is defined as any moderation such as collection, alteration and storage done on any personal data.

Notice that the territorial principle is not respected by the GDPR in the sense that it is enforcing laws indirectly on companies that can be based on another countries but process EU natural persons data.

MAIN PILLARS

1) Data-centric regulation : The aim of the regulation is to give the correct importance to the data of the people. So, data is in the centre of the regulation. It accepts that online identity is important.
2) Procedural regulation: The regulation does not specifically state what are the steps to be taken since it acknowledges that it might depend on the context. This point is strongly related with following points.
3) Risk based approach : The regulation is based on the accountability principle. That is an entity processing personal data must be responsible for the risk posed to the data subjects by its data processing and the balance of interest must be considered.
4) Tech-neutral approach : No specific technical measure to be takes is specified since the technology in constant development and writing a specific technology could be soon out-dated. Instead, the regulation goes to the risk-based approach.

DPIA

The DPIA is related to the risk-based approach. It is a formal assessment of the risk posed to the data subject by the processing of personal data. IN it the company has to clearly state what is the processing done, what are the risks to the data subject and the measures taken in order to minimize them, the company must also specify the assigned DPO (Data Protection Officer], so the person to verify that the processing is GPR compliant.

The company must be able to demonstrate that it complies with the GDPR principles:

a) Lawfulness of data processing : The processing of the data must be legal and transparent with respect to the data subject. Under this point we find the consent of the data subject that the data controller must be able to demonstrate it obtained following a correct procedure (knowledge of data subject and no asymmetric relationship between data subject and data controller), even if in some cases this is not enough for ensuring the lawfulness of the processing.
b) Data minimisation : The amount of data used must be only the strictly necessary one.
c) Security measures : Security measures (Art 32) must be sufficient to compensate for the risk. Adequate technical and procedural measures should be taken.
d) Purpose limitation : The data must be processed for the specific purpose for which it was collected.

The DPIA is not mandatory for all applications , however it is strongly suggested. It is mandatory for hi-risk applications thus applications involving millions of data or being done by public entities.

What are the main issues of regulating AI?

“The introduction of new technologies always comes with challenges for the law because problems arise, and it must be regulated. However, when we talk about Artificial Intelligence (AI) we observe that tis particularly problematic to regulate.

First, I will discuss the main problems introduced by the AI. With the introduction of this kind of information systems every piece of information becomes useful data. It can be called the datafication of the society. In fact, every information retrieved from every sensor might be used in the context of AI.

Take 2s an example the smart bands that monitor the health of the patient and give a huge amount of data to analyse. This fact itself introduces a challenge since we are monitoring the data and the data is shaping our society”. Another big issue is that before the processing of this data it is not possible to specifically know for which purpose, they will be used which is in contrast with the GDPR principles (principle of purpose specification). This is a problem when asking for consent of the users since at the moment of collection of the data it is not known the exact purpose for which tis collected. This can lead to legal issues with current regulations (like GDPR). Nonetheless problems with current regulations are not unique. Current regulations only focus on processing operations but not on individual and group rights (as discrimination, freedom of expression). Key issues of AI are the discrimination of certain groups.

This is exacerbated by the fact that those groups are not static, like in the past, but are dynamically defined which does not allow people to associate and fight for their rights. In addition, in most of the cases tis not possible to understand why a certain variable changes the result of the algorithm. The bias can happen because of. bias in the data, but also because of the procedure followed by the data scientist developing the algorithm that could introduce its own believing’s into the algorithm through the confirmation bias. Moreover, an AI system can become unreliable in contexts for which it was not trained. Therefore, it is necessary to introduce new laws regulating AI that address those problems.

‘The first challenge that comes with AI regulation is its definition. In fact, technologies of this field are constantly developing, and a narrow definition would lead to companies trying to fall out of the law.

It is also challenging to determine who is liable for the "behaviour" of an AI since it is a system that learns from data of users, so responsibility is not clear. Secondly, AI is not the same on every field, so it is not possible to give a unique law. Possible solutions are:

1) Coregulation : Hard-law combined with a soft-law in order cover different contexts.
2) Several hard laws for different contexts.

Off course this law must be consistent with existing laws. For example, creating a new EU.

Discuss how AI should be regulated.

Artificial Intelligence has changed the paradigm of data processing. It is technology that processes a lot of data and can be seen as a black box that learns from it and outputs a result or prediction. With the outcome of new technologies new problematics arise and this is the case of the AI. The extensive collection of data necessary for making these systems work contrast with the current regulations on personal data protection already existent that follow the "data minimisation” principle. In addition, there are several aspects not yet regulated about the transparency of those systems and the consequences they might have on society.

As a consequence, there will arise legal issues for which the court will not have the necessary laws to act properly. In fact, the first system that has to face the new technologies are the courts in which the first problems are treated. As an example, think about the HUD case against Facebook in the USA. The HUD is demanding Facebook for the systematic discrimination done by the AI that runs the targeting of the ads in the platform.

DEFINITION OF AI

The first problem we face when regulating AI systems is the definition of them. In fact, it is a technology constantly developing and if we give a narrow definition of it companies would try to fall out of this definition to avoid the regulation. Therefore, a sufficiently wide definition of it must be given.

DATA PROTECTION ISSUES

The AI systems require a huge quantity of information to properly work. However, current GDPR regulations require that the data collected is minimized. In addition, the data subject must explicitly give his consent in order for the data to be processed and he must know the purpose of the data collection.

However, at the moment of the collection it is not always known for which purpose the data will be collected with creates a problem that can lead to not GDPR compliance. A possible solution for this would be to use a broad consent (so a consent for many purposes but this would be hard to justify) or a dynamic consent.

TRANSPARENCY ISSUES

Most AI systems act as black box to which certain variables are given as input and an output is returned. However, even if we understand which variables have effect in the output it is not always clear why. This can lead to discrimination issues like in the COMPAS case. COMPAS is a system that has been employed in the penitentiary system of the USA to help judges in the decision of conviction of a defendant giving them a score with the probability of recidivism. However, the system systematically discriminates black defendants giving them higher scores (thus more probability of recidivism). Therefore, companies that develop these systems should perform impact assessments before deploying the system (by-design approach) to prevent those issues.

Notice that current regulations only focus on the regulation of how the data is processed and not on group rights (like non -segregation).

For the regulation of this aspect, we have to be careful of not regulating against the already existing laws. For example, creating another entity that supervise it would not be possible because it would conflict with already existent regulations (GDPR). Instead, an extension of the law should be proposed. In addition, we must consider the fact that not all scenarios are the same and measures to be taken highly depend on the context in which they are applied (the sector). There are two possible routed:

a) Co-regulation : Create a hard law (like GDPR) with several soft laws (like a code of conduct) for each sector.
b) Several hard laws for each sector. This option seems hard to implement on practice.

Data Ethics and Protection

Esame_20220715_Part_1_In-person

	LUCA MARCELLINO 292950
Iniziato	venerdì, 15 luglio 2022, 14:15
Terminato	venerdì, 15 luglio 2022, 15:00
Tempo impiegato	45 min.
Valutazione	**14,00** su un massimo di 15,00 (**93**%)

Domanda 1

Completo

Punteggio ottenuto 6,50 su 7,50

A company's data center is attacked with ransomware, and the attacker threatens to publish personal data of the company if a ransom of 20 bitcoins is not paid within 24 hours. What are the duties of the data controller? Please provide arguments for your answer, considering risk to the rights and freedom of individuals.

In this case the controller recived a **data breach,** in this case the data that are stolen are personal data, so data that can direct or indirect indetify a **natural person.**

We can have different kind of data breach:

- **Accidentally** : so someone for example send the data to another person putting the wrong email.
- **Unlawfully**: if someone modify or delete some data without authorization (like in this case).

Moreover we can divide it in another three categories:

- **Confidetiality**: someone take the data without authorization
- **Integrity**: someone modify the data without authorisation
- **Availability**: someone delete or lose the data without authorization

In case of data breach the company have to comunucate the data breach at the competent authorities until **72 Hours** from when the controller find the breach**.**

Moreover in case of data breach the company must give a communication to the people involved in which are present:

- How much and which data are taken unlawfull.
- Contact of DPO.

- Which are the conseguences of this data breach.
- Which are the measure to fight this data breach.

In this case the company is until the 72 hours so he can wait to communicate the data breach an try to get the data without give a communication.

Nevertheless in this case the data that are stolen are personal data so could be a good idea say to the person that are involved that their data are stolen, because with this data breach someone can identify a natural person so we have problem in rights and freedom, moreover because the thief said that want to pubblish the data.

The comunication is better if show how kind of measures were taken in order to avoid this kind of breach (so if the company has a magement risk plan is better, is not mandatory in all case but very suggested), which wil be the measures that will take in order to avoid this kind of issue in future, and a possible plan, if one exists, to regain or mitigate the possible impact. This could increase the trust to the company and avoid people ask to delete their data, like in unicredit case.

Commento: In this specific case, what kind of breach we are discussing?

- Confidentiality
- Integrity
- Availability

Domanda 2

Completo

Punteggio ottenuto 7,50 su 7,50

Please describe the role, tasks, and duties of the data processor.

Data processor is one of the main characters, with:

- **Data subject:** person that are in EU, and ower of his/her data.
- **Data controller:** who have the data and decide the process and take the decisions.
- **Data protection officer (DPO):** who can help in order to find possible issues in the application and help for the DPIA

The data processor role is analyze or conduct part or all the procces on behalf of data controller. We can distinguish between controller and processor because only the controller take the decison, the processor indeed, only, conduct the analysis. In some case controller and processor could be the same entity.

To make a deal between a controller and a processor there must to be a contract in which are present:

- The kind of process to conduct.
- For how many times the process will be conducted.
- Which data use.

The taks is provide the secutity measure for the data that process and the latter must be proportionate to the kind of data involved in the process and process the data following the guideliness provide by the contoller and in a lawfull manner.

The data processor almost always is not liable for the process, but if it will not respect the guideliness of the controller or it will process in unlawfull manner is itself liable. Indeed in this case the controller can aks for a damage.

At the end we can say that exist a sub controller. This figure is usefull, for example, to conduct specific tasks and a processor can choose but only after the permission of the controller, because also in this case the controller is liable.

Commento:

Data Ethics and Protection

Esame_20220623_Part_1_In-person

	ANAM UR REHMAN 283909
Iniziato	giovedì, 23 giugno 2022, 14:16
Terminato	giovedì, 23 giugno 2022, 15:01
Tempo impiegato	45 min.
Valutazione	**14,00** su un massimo di 15,00 (**93**%)

Domanda 1

Completo

Punteggio ottenuto 7,00 su 7,50

In an EU country, a company decides to use wearable robots for its employees. The robots have to fit the body and the company is considering several options, including the use of images generated by employees' body scans. In addition, the robots will be equipped with some sensors to collect certain parameters (body temperature, heart rate) during the work shift.

Can this technology be developed and used in a GDPR-compliant manner? Please provide arguments for your answer, considering different purposes, scenarios and possible technical solutions.

Subject-Matter

The company is collecting biomatric data about employees such as body measurements via body scan images. This information can not only identify the Data subject, but also they cannot easily change their body shape and sizes. This fall under the GDPR.

For other measurements, if a unique identifier is used to collect temprature and heart rate, then the data is pseudononymous but Data subject can still be identified using additionall information, Hence it is also under consituency of GDPR.

The company is already in EU so the territorial scope aspect is already met.

Purpose, scenarios

If the company is working in this project to increase the productivity of employees then it is a different context w.r.t if they are trying to help disabled or old-age employees who cannot work long hours due to their physical nature condition. In the later case, we have different

proportionality and balance of interest is also different.

The company cannot rely (only) on the Data subject consent because their might be a conflict of interest between employee and their company.

It is also not mentioned where the data about body temprature and heart rate is stored and for how long they will keep it in the form which allows directly or indirecltly identification of Data subject.

Possible technical solutions

As far as body shapes are concerend, company can avoid that buy designing robots for different categories, (small, mediam, large, Xlarge) and providing the possibility of adjusting some parts length, widht to fit better the employee. Keep in mind that this adjusments should disappear after the shift is over and robot should turn back to a "Default" shape.

To build these categories efficiently, they can perform a survey from employee where participation is totally optional and data is collected for very short period of time (even for 1 day). This is useful in the case when company has employees from different part of the world and using national level statistics of body measure is not optimal. (Even if it is for 1 day, It is still Personal data and it falls under GDPR. So all the GDPR compliance principles should be considered prior to this survey)

For the measurements about body temprature and heart rate, the data should be collected at each work shift and destroyed as soon as the shift is over.

Commento:

Domanda 2

Completo

Punteggio ottenuto 7,00 su 7,50

What is a DPIA (Data Protection Impact Assessment) and why is it important?

What is DPIA?

DPIA is a document containing the following information:

- Description of the nature of personal data being collected, processed. The legal basis for Data Controller to perform these actions (if any).

- Describes if the consent of involved data subject is taken before performing any operation on their personal data in easily accessible manner. How Data subject can achieve his rights related to personal data such as right to rectification, erasure, portability, object etc.

- It assess kind of risk to data subject (to their privacy, fundamental human rights or freedom) are present and what is their severity. If any protected attributes about data subjects are being collected or processed. If their is a risk of any sort of descrimination based on protected attributes such as their Sex, ethinicity, Political preferences, Religion or biometric information etc.

- The legitemate interests of Data controller and their balance with Fundamental rights and freedom of data subject.

- What is the purpose of this data collection and processing (purpose limitation), For how long the personal data will be stored, processed or tranmitted (Data retention policy), What other measure are taken to further safe guard any harmful impact on Data subject.

- Measure taken for data security such as encryption of user devices, pseudononymization.

- What is the impact on the society in terms of universal accessibilty, environmental sustainability and physical safety.

- In case of Data Breach, what is the Incident Response plan.

- In summary, it assesses if given system, product is in compliance with GDPR.

Why is it important?

DPIA is fundamental to shape the design of product or system. Since it can shape the design, it must be done at the begining of the project and not at the end.

It allows the seeker to mitigate any possible Bias and descrimination caused by their system by allowing them to make better subjective choices which are concentric on Public safety, freedom and fundamental human rights. Whenever there is a high Risk to Data subject rights or descrimination against them, the Data controller must perform DPIA.

Commento:

POLITECNICO DI TORINO

Data Ethics and Protection

Esame_20220207_Part_1_Remote

[redacted]

Iniziato	lunedì, 7 febbraio 2022, 14:22
Terminato	lunedì, 7 febbraio 2022, 15:07
Tempo impiegato	45 min.
Valutazione	**12,50** su un massimo di 15,00 (**83**%)

Domanda 1

Completo

Punteggio ottenuto 7,00 su 7,50

The role of the data subject's consent in data protection.

According to GDPR data subject is a natural person whose data is being processed. The general rule is that since the processing of the personal data may cause negative impact on the society, this processing is allowed only under the legal premises, So as a genral rule the data may only be processed only when compliant with rules of GDPR and under the suppervision authority.

The GDPR was designed considering the right based approach where the rights of the individuals is considered on a priority basis. In this regard we have have protection by default hence any application has to run with minimal data requirements by default. The idea here is to minimize the risk and provide maximum data protection and security on the default level.

The consent of the individual for the processing of data is important and moreover the right to withdraw the consent should be as easy as the consent was given. The natural persons must have also the right to ratification which mean to have wrong data corrected or deleted. With the recent economic developments, Personal data is being used for economic purposes and hence has value, the consent has been exploited as tool to extract this value for the company. There are several categories of personal data inculding name, ethnicity, race, religious beliefs, sexual orientation etc. All of this data requires maximum level of security due to the fact that this data can be used for descrimination. Consent is a legal ground for processing this kind of data but it comes with a limit in terms of necessity. In other words the importance and the extent of processing such kind of data must be clearly motivated. In short with the recent generation of GDPR, The responsibilty is not on the data subject but on the data controller or the processor.

The age of the data subject is important as well, in some memeber states it is 14 and in some it can be 14 or 15. Nevertheless the consent of the individual remains the top priority according to the GDPR's right based approach

Commento:

Domanda 2

Completo

Punteggio ottenuto 5,50 su 7,50

A company aims to provide its employers with robotic exoskeletons to support their most stressful tasks. To ensure a perfect fit, the company wants to adopt body-scanning technology, obtain biometric images of each employee and create a tailor-made exoskeleton. What are the challenges related to this project, in relation to data protection, to consider?

The statement does not mention the location of the company, hence we can not be sure if the company is with in the territorial scope of GDPR. On the other hand we know that the company is processing biometric data which is personal data and is considered to be a part of the material scope of the GDPR. Having said that, we can examin the possible options the company has regards to the processing of the data. We are not sure about the scale of the company and corresponding to this we can not be sure about the level of risk involved in this case. The company can decide to outsource this project to a third party. In that case the company itself will be considered data controller and the company working on the project shall be the data processor. The locationn of the data processing company is important and the required security measures are put forward accordingly. If the company working on the exoskeleton is within EU the tranfer of data shall have no restrictions according to GDPR. If the that company is outside EU, either that country has passed the adaquacy level or the country has a bilateral agreement with EU or else the two companies need to sign the contractual clauses. If the same company is assigning the project to one of its subsideries, it needs to have the binding corporate agrrement signed. Another aspect of this project is related to the security of the individual. The company as a data controller must get the consent of the employees of the company. The withdrawler of the consent should be as easy as the consent was given. Moreover the individual must be informed about the intent and the extent to which the data is being collected which means that the data must be erased after the exoskeleton model has been built. The company is advised to higher a data protection officer to deal with the legal issues that occur during the processing of the data. According to the level of risk, data protection authority may require data protection assessment which is necessary in case of high risk according to gdpr. In case of low risk the company still can show compliacne with GDPR throufgh certification.

Commento:

Issues related to the processing of biometric data have not been sufficiently processed