INSTITUTO FEDERAL
ESPÍRITO SANTO
Campus Serra

Mestrado Profissional em Engenharia de Controle e Automação

PROCESSO SELETIVO N° 42/2019

PROVA 1 - LÍNGUA INGLESA

LEIA ATENTAMENTE AS INSTRUÇÕES ABAIXO

1. Você recebeu do fiscal o seguinte material:

   (a) Este caderno, com o enunciado das 20 (vinte) questões objetivas, sem repetições ou falhas.
   (b) O CARTAO-RESPOSTA destinado às respostas das questões objetivas formuladas nas provas.

2. Todas as questões valem 5 (cinco) pontos. Assim, a prova de língua inglesa vale 100 (cem) pontos.

3. Após a conferência, o candidato deverá assinar, no espaço próprio do CARTAO-RESPOSTA, a caneta esferográfica na cor azul ou preta.

4. Para cada uma das questões objetivas, são apresentadas 4 alternativas classificadas com as letras (a), (b), (c), (d); só uma responde adequadamente ao quesito proposto. Você só deve assinalar UMA RESPOSTA: a marcação em mais de uma alternativa anula a questão, MESMO QUE UMA DAS RESPOSTAS ESTEJA CORRETA.

5. SERA ELIMINADO do Processo Seletivo Público o candidato que:

   (a) Se utilizar, durante a realização das provas, de máquinas e/ou relógios de calcular, bem como de rádios gravadores, headphones, telefones celulares ou fontes de consulta de qualquer espécie;
   (b) Se ausentar da sala em que se realizam as provas levando consigo o CADERNO DE QUESTOES e/ou o CARTAO-RESPOSTA.
   (c) Não assinar a LISTA DE PRESENÇA e/ou o CARTAO-RESPOSTA.

   Obs.: O candidato só poderá se ausentar do recinto das provas após 1 (uma) hora contada a partir do efetivo início das mesmas. Por motivos de segurança, o candidato só poderá levar o CADERNO DE QUESTOES, depois de 2 (duas) horas contadas a partir de efetivo início da prova.

6. Reserve os 30 (trinta) minutos finais para marcar seu CARTAO-RESPOSTA.

7. Quando terminar, entregue ao fiscal, o CARTAO-RESPOSTA e ASSINE A LISTA DE PRESENÇA.

8. O TEMPO DISPONÍVEL PARA ESTAS PROVAS DE QUESTOES OBJETIVAS É DE 2h 30min (DUAS HORAS e TRINTA MINUTOS), incluído o tempo para a marcação do seu CARTAO-RESPOSTA.

TEXT 1

Why San Francisco’s ban on face recognition is only the start of a long fight

The city government can’t use the technology, but private companies still can, and regulating those uses is a thornier problem.

by Angela Chen
May 16, 2019

San Francisco has become the first US city to ban the use of facial recognition by its government. But though privacy advocates are celebrating, the ordinance doesn’t stop private companies from using facial ID in ways that many people find creepy.

It might, however, be a first step.

The use of face recognition technology has become increasingly common, despite evidence that it frequently misidentifies people of color. Activists warn that it could lead to false arrests, or be used to track people’s whereabouts and target dissenters who have done nothing wrong.

In recent years, San Francisco officials have had to second-guess their use of high-tech surveillance tools. In 2009, police pulled over a driver, Denise Green, and held her at gunpoint while searching her car, all because a license plate reader wrongly said it had been stolen. Green sued and the city ended up paying her $495,000. Such episodes undoubtedly contributed to the pressure for a ban, though San Francisco’s police don’t currently use face recognition tech.

In many ways, though, it’s unsurprising that the tech-obsessed city is the first to restrict the technology. “[It's like how] Silicon Valley parents are the most likely to ban screen time for their kids,” says Laura Noren, a data ethicist and vice president of privacy and trust at Obsidian Security. Other tech-savvy cities are likely to follow its lead, Noren says, which explains why nearby Oakland and Somerville in Massachusetts have already proposed similar bans. Still, she thinks a federal ban is unlikely under the Trump administration.

Public vs. Private

However, most people’s experience with facial analysis and recognition won’t happen because of police monitoring. Rather, it’ll be because of non-government endeavors, like school security cameras or stores that show consumers targeted ads. These uses come with the same risks of misidentification and discrimination, but bans like the one in San Francisco won’t prohibit them.

In one example of the problems that could arise, an 18-year-old sued Apple last month because, he alleged, a face recognition system in one of its stores falsely linked him to thefts. (According to Apple, it doesn’t use such systems in its stores.) In another case, tenants at Atlantic Plaza Towers, an apartment building in New York City, are fighting their landlord’s plan to replace a key-fob entry system with a face recognition system. The technology is discriminatory, the tenants say, because the tower residents are mostly people of color. “Why did [the landlord] choose our building to try this system out? Versus 11 other buildings that have a different makeup?” asks Icemae Downes, one of the residents.

A full ban in the private sector is unlikely, though. Many consumers are already using FaceID to unlock their iPhones or buying video doorbells, like Google’s Nest Hello, that identify familiar people. “When your narrative is ‘government surveillance,’ that tends to have powerful resonance," says Joseph Jerome, policy counsel for the Privacy & Data Project at the Center for Democracy and Technology. "When you're dealing with the private sector, we start having debates about what constitutes beneficial innovation."

Such debates get complicated fast. If companies use face recognition technology, how should they notify customers? What rights should people have to opt out, and how easy should that process be? Should the data ever be given or sold to third parties? These were some of the questions that came up during discussion of a Washington state privacy bill that failed earlier this year, according to Jevan Hutson, a technology policy researcher at the University of Washington. The two sides were unable to agree on how strong the privacy restrictions should be.

Still, restrictions on commercial uses have begun to appear, says Jennifer Lynch, surveillance litigation director at the Electronic Frontier Foundation. For example, a law in Illinois requires companies to get consent before collecting any kind of biometric data. A bipartisan bill with a narrower requirement, the Commercial Facial Recognition Privacy Act, is currently in committee hearings in Congress.

For her part, Noren believes companies will pursue an "accuracy threshold" requirement—in effect, proposing that face recognition be allowed so long as they can prove it doesn't make too many mistakes.

Ultimately, says Jerome, it's too early to tell how much the SF ordinance will influence commercial regulation. "I think it will juice the debate that states and the federal government are having around facial recognition, but whether that leads to action is unclear," he says. There was a similar public/private split over drones a few years back, Jerome adds: many local cities restricted their use by law enforcement, but did little to regulate them for commercial purposes.

Source: https://www.technologyreview.com/s/613536/facial-recognition-ban-san-francisco-surveillance-privacy-private-corporate-interests/

1) What is the downside of the decree passed by the city of San Francisco?

a. It has banned the use of facial recognition entirely.
b. The ban of facial recognition will hinder research developments.
c. The ban does nothing to prevent corporations from using facial recognition.
d. The decree only affects commercial use of facial recognition.

2) According to the text, one of the problems with the current facial recognition technology is that there is evidence "that it frequently misidentifies people of color" (line 6). Which of the options below is a direct consequence of that?

a. Misidentifications may lead to unlawful detentions.
b. Misidentifications are so common that they become an evidence of racism.
c. Although misidentifications do occur, there is no reason for concern.
d. The possibility of tracking offenders' whereabouts or dissenters is debatable.

3) When we read that "San Francisco officials have had to second-guess their use of high-tech surveillance tools" (lines 9-10), it means that:

a. High-tech surveillance tools have helped officials enormously in their work.
b. High-tech surveillance tools have somewhat helped officials in their work.
c. Officials have been able to fully trust the use of high-tech surveillance tools.
d. Officials have had to question and criticize their use of high-tech surveillance tools.

4) How does the author feel about the ban of facial recognition technology by the San Francisco government?

a. She is astonished, given that San Francisco is a tech-obsessed city.
b. She feels ambivalent, given that Silicon Valley parents often restrict their kids screen time.
c. She is saddened, given that the restriction will undoubtedly prove counterproductive.
d. She expected it, given that it is not an unprecedented position in California.

5) **Which of the options bellow best rephrases the sentence “Other tech-savvy cities are likely to follow its lead” (line 18)?**
a. Other cities that do not use technology as efficiently are likely to follow San Francisco.
b. Other cities that are learning to cope with technology are likely to do what San Francisco did.
c. Other cities that are very much familiarized with technology are likely to approve similar bans.
d. Other cities that are very much familiarized with technology might be interested in taking a different stand.

6) **How does the author believe most people will come into contact with face analysis technology?**
a. By being monitored by the law enforcement forces.
b. By being monitored by privately owned systems.
c. By being observed by local government surveillance systems.
d. By being watched by traffic and security cameras.

7) **What difference is drawn in the article between banning government facial recognition surveillance and banning facial recognition use by the private sector?**
a. It is far more likely for people to agree on banning government facial recognition surveillance than its use by the private sector because the latter brings beneficial innovations to the table.
b. People are more likely to have strong opinions against the private sector because they fell their privacy is being breached.
c. People are less likely to have a powerfully resonant opinion against government surveillance because they feel it improves security.
d. There isn’t much difference because most people will cherish their privacy over any beneficial innovations the technology might bring.

8) **Which of the options below best summarize the current state of privacy restrictions in the state of Washington?**
a. Companies and the government haven’t settled on how customers should be notified.
b. The government wants people to be able easily to opt out of face recognition technology.
c. Both government and private companies have not reached a consensus on how severe privacy restrictions should be.
d. Both government and private companies agree that data could be made available to third parties.

9) **According to Laura Noren, what will companies do to ensure that face recognition technology be implemented?**
a. Companies will prove that the technology conforms to desirable standards and that any misinterpretations will be minimized to acceptable levels.
b. Companies will make it clear to users that their data is being collected and made available to third parties.

c. Companies will negotiate with local government to make sure their innovations are implemented, despite any citizen complaints.
d. Companies will make it easy for people to opt out of the technology and restrict data circulation to third parties.

10) In the last paragraph we read that the San Francisco ordinance "will juice the debate that states and federal government are having around facial recognition" (lines 60-62). Which of the options below best explain what that sentence means?

a. The law passed by the San Francisco government will discourage other states from doing the same.
b. Other states and the federal government will not follow the example set by San Francisco.
c. Other states and the federal government will consider the example set by San Francisco when discussing what to do concerning facial recognition regulations.
d. The example set by San Francisco will influence other cities to do the same.

TEXT 2

When algorithms mess up, the nearest human gets the blame

A look at historical case studies shows us how we handle the liability of automated systems.
by **Karen Hao**
May 28, 2019

Earlier this month, Bloomberg published an article about an unfolding lawsuit over investments lost by an algorithm. A Hong Kong tycoon lost more than $20 million after entrusting part of his fortune to an automated platform. Without a legal framework to sue the technology, he placed the blame on the nearest human: the man who sold it to him.

It's the first known case over automated investment losses, but not the first involving the liability of algorithms. In March of 2018, a self-driving Uber struck and killed a pedestrian in Tempe, Arizona, sending another case to court. A year later, Uber was exonerated of all criminal liability, but the safety driver could face charges of vehicular manslaughter instead.

Both cases tackle one of the central questions we face as automated systems trickle into every aspect of society: Who or what deserves the blame when an algorithm causes harm? Who or what actually gets the blame is a different yet equally important question. Madeleine Clare Elish, a researcher at Data & Society and a cultural anthropologist by training, has spent the last few years studying the latter question to see how it can help answer the former. To do so, she has looked back at historical case studies. While modern AI systems haven't been around for long, the questions surrounding their liability are not new.

The self-driving Uber crash parallels the 2009 crash of Air France flight 447, for example, and a look at how we treated liability then offers clues for what we might do now. In that tragic accident, the plane crashed into the Atlantic Ocean en route from Brazil to France, killing all 228 people on board. The plane's automated system was designed to be a completely "foolproof," capable of handling nearly all scenarios except for the rare edge cases when it needed a human pilot to take over. In that sense, the pilots were much like today's safety drivers for self-driving cars—meant to passively monitor the flight the vast majority of the time but leap into action during extreme scenarios.

What happened the night of the crash is, at this point, a well-known story. About an hour and a half into the flight, the plane's air speed sensors stopped working because of ice formation. After the autopilot system transferred control back to the pilots, confusion and miscommunication led the plane to stall. While one of the pilots attempted to reverse the stall by pointing the plane's nose down, the other, likely in a panic, raised the nose to continue climbing. The system was designed for one pilot to be in control at all times, however, and didn't provide any signals or haptic feedback to indicate which one was actually in control and what the other was doing. Ultimately, the plane climbed to an angle so steep that the system deemed it invalid and stopped providing feedback entirely. The pilots, flying completely blind, continued to fumble until the plane plunged into the sea.

In a recent paper, Elish examined the aftermath of the tragedy and identified an important pattern in the way the public came to understand what happened. While a federal investigation of the incident concluded that a mix of poor systems design and insufficient pilot training had caused the catastrophic failure, the public quickly latched onto a narrative that placed the sole blame on the latter. Media portrayals, in particular, perpetuated the belief that the sophisticated autopilot system bore no fault in the matter despite significant human-factors research demonstrating that humans have always been rather inept at leaping into emergency situations at the last minute with a level head and clear mind.

In other case studies, Elish found the same pattern to hold true: even in a highly automated system where humans have limited control of its behavior, they still bear most of the blame for its failures. Elish calls this phenomenon a "moral crumple zone." "While the crumple zone in a car is meant to protect the human driver," she writes in her paper, "the moral crumple zone protects the integrity of the technological system, at the expense of the nearest human operator." Humans act like a "liability sponge," she says, absorbing all legal and moral responsibility in algorithmic accidents no matter how little or unintentionally they are involved.

This pattern offers important insight into the troubling way we speak about the liability of modern AI systems. In the immediate aftermath of the Uber accident, headlines pointed fingers at Uber, but less than a few days later, the narrative shifted to focus on the distraction of the driver.

"We need to start asking who bears the risk of [tech companies'] technological experiments," says Elish. Safety drivers and other human operators often have little power or influence over the design of the technology platforms they interact with. Yet in the current regulatory vacuum, they will continue to pay the steepest cost.

Regulators should also have more nuanced conversations about what kind of framework would help distribute liability fairly. "They need to think carefully about regulating sociotechnical systems and not just algorithmic black boxes," Elish says. In other words, they should consider whether the system's design works within the context it's operating in and whether it sets up human operators along the way for failure or success. Self-driving cars, for example, should be regulated in a way that factors in whether the role safety drivers are being asked to play is reasonable.

"At stake in the concept of the moral crumple zone is not only how accountability may be distributed in any robotic or autonomous system," she writes, "but also how the value and potential of humans may be allowed to develop in the context of human-machine teams."

Source: https://www.technologyreview.com/s/613578/ai-algorithms-liability-human-blame/

11) **What is the problem set forth in the first paragraph and that will be discussed throughout the article?**

a. The $20 million investment lost by a Hong Kong tycoon who trusted an automated platform.
b. A lawsuit over investment lost by an algorithm.
c. Algorithms that run automated platforms that do not require human intervention.
d. People being held accountable for mistakes made by automated systems.

12) **The author states that, although it is the first known case over automated investment losses, it is not the first involving the liability of algorithms (lines 7-8). Which of the options below best explain the concept of "liability of algorithms" according to the text?**

a. A liable algorithm would be subject by law to answer for its mistakes.
b. A liable algorithm would blame the person who created it.
c. A liable algorithm is an algorithm that is likely to make mistakes.
d. A liable algorithm is an algorithm that is likely to experience problems.

13) **Which is "one of the central questions we face as automated systems trickle into every aspect of society"?**

a. People are being blamed for mistakes made by automated systems.
b. A person will always be held responsible for harm caused by automated systems.
c. Someone or something must be held accountable for harm caused by automated systems.
d. People should not have to answer for mistakes made by automated systems.

14) **What comparison is made between the Air France flight 447 accident and today's self-driving cars?**

a. In both cases humans are fully responsible for the mistakes they made.
b. In both cases the automated systems failed and there was nothing humans could do to prevent the accidents.
c. In both cases people were blamed for their mistakes because the automated systems were "foolproof".
d. In both cases, humans were expected to monitor and interfere in extreme circumstances only.

15) **Which is the pattern identified by Madeleine Clare Elish in her recent paper concerning how the public perceives what happens after an accident involving automated systems?**

a. Investigations found several factors that caused the accidents, blaming both humans and automated systems for them, which was portrayed accurately by the media.
b. Investigations found several factors that caused the accidents, blaming both humans and automated systems for them, but the media portrayals reinforced the belief that only humans were to blame for not being able to respond accordingly.
c. The public will always blame the human factor, despite media coverage and investigations proving otherwise.
d. The public will always blame the automated systems, despite investigations proving only humans were to blame.

16) **The phenomenon called "moral crumple zone" by Elish is best described as:**

a. Humans will always have to make the final decision, even when dealing with highly automated systems over which they have limited control.
b. Humans must not be blamed for the failures of highly automated systems because humans have limited control over them.

c. Humans have limited control over the behavior of automated systems and therefore should not bear the blame for their failures.
d. Humans will be blamed even when dealing with highly automated systems over which they have limited control.

17) What does Elish mean when she says that humans act like a "liability sponge"?

a. Humans absorb most of the moral responsibility but are not legally accountable for the accidents.
b. Humans are held legally and morally responsible for the failures of automated systems even when they have little involvement in the accidents.
c. Humans are held morally responsible and absorb the blame for creating and misusing the automated systems.
d. Humans absorb all legal and moral responsibility when they are intentionally involved in the accidents.

18) Why does Elish state that "We need to start asking who bears the risk of [tech companies'] technological experiments" (lies 60-61)?

a. Because the blame must be place in those who create the automated systems people are going to interact with.
b. Because tech companies are not responsible for the failures caused by people not responding accordingly when interacting with automated systems.
c. Because the people who interact with the automated systems usually are not directly involved with their development.
d. Because the people who interact with automated systems are directly responsible for not responding in accordance with what the automated systems expect of them.

19) What advice does the author, based on what Elish's opinions, have for those responsible for deciding who or what is to be held responsible for automated system failures?

a. They should pass laws that put the blame solely on the automated systems, since people have no control over how they behave.
b. They should discuss at length how to find the people responsible for the failures, since the system is not a sentient entity and, therefore, cannot be blamed for its actions.
c. They should have nuanced conversations in order to come to an agreement that only benefits humans because they are the ones who pay the steepest cost.
d. They should talk openly and consider all aspects of the problem so that liability is distributed in a way that is not unjust.

20) In the statement "At stake in the concept of the moral crumple zone is not only how accountability may be distributed in any robotic or autonomous system […] but also how the value and potential of humans may be allowed to develop in the context of human-machine teams" (lines 71-74), the phrase "At stake" could NOT be replace by:

a. At first
b. In jeopardy.
c. At risk.
d. In question.