Anglais

MP, PC, PSI

2020

CONCOURS CENTRALE•SUPÉLEC

4 heures

Calculatrice interdite

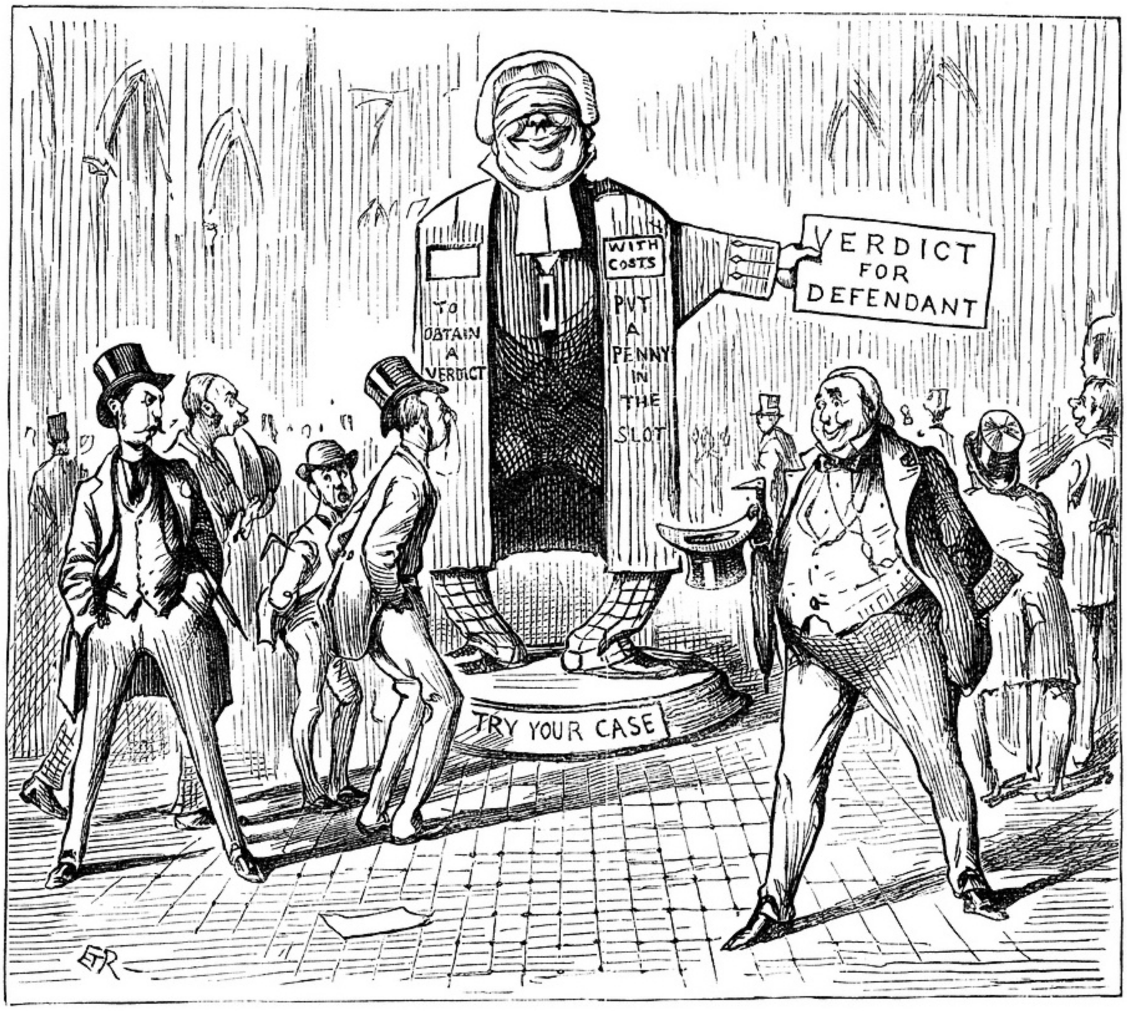
L'usage de tout système électronique ou informatique est interdit dans cette épreuve.

Rédiger en anglais et en 500 mots (plus ou moins 10 %) une synthèse des documents proposés, qui devra obligatoirement comporter un titre. Indiquer avec précision, à la fin du travail, le nombre de mots utilisés (titre inclus).

Ce sujet comporte les 4 documents suivants :

— un dessin paru dans *Punch Magazine* en 1890 ;
— un extrait de 'The Minority Report' de Philip K. Dick, nouvelle parue en 1956 ;
— un article de Hannah Fry publié dans *The Wall Street Journal* en 2018 ;
— un article de Vera Eidelman, publié sur le site de l'ACLU[1] en 2017.

L'ordre dans lequel se présentent les documents est arbitraire et ne revêt aucune signification.



AUTOMATIC ARBITRATION.

No more Exorbitant Fees! No more Law! No more Trials!

Source: *Punch Magazine* 1890

[1] The American Civil Liberties Union (ACLU) is a nonprofit organization whose stated mission is "to defend and preserve the rights and liberties guaranteed to every person in this country by the Constitution and laws of the Unites States". The ACLU provides legal assistance in cases when it considers civil liberties to be at risk.

Excerpt from Chapter I

"As I understand it," Anderton said cautiously, "you're going to be my assistant until I retire."

"That's my understanding, too," the other replied, without an instant's hesitation.

"Which may be this year, or next year — or ten years from now." The pipe in Anderton's hand trembled. "I'm under no compulsion to retire. I founded Precrime and I can stay on here as long as I want. It's purely my decision."

Witwer nodded, his expression still guileless. "Of course."

With an effort, Anderton cooled down a trifle. "I merely wanted to get things straight."

"From the start," Witwer agreed. "You're the boss. What you say goes." With every evidence of sincerity, he asked: "Would you care to show me the organisation? I'd like to familiarize myself with the general routine as soon as possible."

As they walked along the busy, yellow-lit tiers of offices, Anderton said: "You're acquainted with the theory of precrime, of course. I presume we can take that for granted."

"I have the information publicly available," Witwer replied. "With the aid of your precog mutants, you've boldly and successfully abolished the post-crime punitive system of jails and fines. As we all realise, punishment was never much of a deterrent, and could scarcely have afforded the comfort to a victim already dead."

They had come to the descent lift. As it carried them swiftly downward, Anderton said: "You've probably already grasped the basic legalistic drawback to precrime methodology. We're taking in individuals who have broken no law."

"But surely, they will," Witwer affirmed with conviction.

"Happily, they don't — because we get to them first, before they can commit an act of violence. So the commission of the crime itself is absolute metaphysics. We can claim they are culpable. They, on the other hand, can eternally claim they're innocent. And, in a sense, they are innocent."

The lift let them out, and they again paced down a yellow corridor. "In our society, we have no major crimes," Anderton went on, "but we do have a detention camp full of would-be criminals."

Doors opened and closed, and they were in the analytical wing. Ahead of them rose impressive banks of equipment — the data-receptors, and the computing mechanisms that studied and restructured the incoming material.

[...]

Witwer crossed the room to the machinery. From a slot he collected a stack of cards. "Are these names that have come up?" he asked.

"Obviously." Frowning, Anderton took the stack from him. "I haven't had a chance to examine them," he explained, impatiently concealing his annoyance.

Fascinated, Witwer watched the machinery pop a fresh card into the now empty slot. It was followed by a second — and a third. From the whirring disks came one card after another.

[...]

Automatically, Anderton collected the fresh cards which had been turned up by the spinning machinery. "Some of these names will be totally discarded. And most of the remainder record petty crimes: thefts, income tax evasion, assault, extortion. As I'm sure you know, Precrime has cut down felonies by ninety-nine and decimal point eight percent. We seldom get actual murder or treason. After all, the culprit knows we'll confined him in the detention camp a week before he gets a chance to commit the crime."

"When was the last time an actual murder was committed?" Witwer asked.

"Five years ago," Anderton said, pride in his voice.

"How did it happen?"

"The criminal escaped our teams. We had his name — in fact, we had all the details of the crime, including the victim's name. We knew the exact moment, the location of the planned act of violence. But in spite of us he was able to carry it out." Anderton shrugged. "After all, we can't get all of them." He riffled the cards. "But we do get most."

"One murder in five years." Witwer's confidence was returning. "Quite an impressive record... something to be proud of."

Quietly Anderton said: "I am proud. Thirty years ago I worked out the theory [...]. I saw something legitimate ahead — something of tremendous social value."

[...]

"Are you ever tempted to —" Witwer hesitated. "I mean, some of the men you pick up must offer you plenty."

"It wouldn't do any good. A duplicate file of cards pops out at the Army GHQ. It's check and balance. They can keep their eye on us as continuously as they wish." Anderton glanced briefly at the top card. "So even if we wanted to accept a —" He broke off, his lips tightening.

"What's the matter?" Witwer asked curiously.

Carefully, Anderton folded the top card and put it away in his pocket. "Nothing," he muttered. "Nothing at all."

[...]

On the card was his name. Line one — an already accused future murderer! According to the code punches, Precrime Commissioner John A. Anderton was going to kill a man — within the next week. With absolute, overwhelming conviction, he didn't believe it.

THE WALL STREET JOURNAL.

Don’t Believe the Algorithm

By Hannah Fry[2] | September 5, 2018

The Notting Hill Carnival is Europe’s largest street party. A celebration of black British culture, it attracts up to two million revelers, and thousands of police. At last year’s event, the Metropolitan Police Service of London deployed a new type of detective: a facial-recognition algorithm that searched the crowd for more than 500 people wanted for arrest or barred from attending. Driving around in a van rigged with closed-circuit TVs, the police hoped to catch potentially dangerous criminals and prevent future crimes.

It didn’t go well. Of the 96 people flagged by the algorithm, only one was a correct match. Some errors were obvious, such as the young woman identified as a bald male suspect. In those cases, the police dismissed the match and the carnival-goers never knew they had been flagged. But many were stopped and questioned before being released. And the one “correct” match? At the time of the carnival, the person had already been arrested and questioned, and was no longer wanted.

Given the paltry success rate, you might expect the Metropolitan Police Service to be sheepish about its experiment. On the contrary, Cressida Dick, the highest-ranking police officer in Britain, said she was “completely comfortable” with deploying such technology, arguing that the public expects law enforcement to use cutting-edge systems. For Dick, the appeal of the algorithm overshadowed its lack of efficacy.

She’s not alone. A similar system tested in Wales was correct only 7% of the time: Of 2,470 soccer fans flagged by the algorithm, only 173 were actual matches. The Welsh police defended the technology in a blog post, saying, “Of course no facial recognition system is 100% accurate under all conditions.” Britain’s police force is expanding the use of the technology in the coming months, and other police departments are following suit. The NYPD is said to be seeking access to the full database of drivers’ licenses to assist with its facial-recognition program.

Law enforcement’s eagerness to use an immature technology underscores a worrisome trend you may have noticed elsewhere: Humans have a habit of trusting the output of an algorithm without troubling themselves to think about the consequences. Take the errors we blame on spell check, or the tales of people who follow their GPS over a cliff. [...]

There’s no doubting the profound positive impact that algorithms have had on our lives. The ones we’ve built to date boast a bewilderingly impressive list of accomplishments. They can help us diagnose breast cancer, catch serial killers and avoid plane crashes. But in our hurry to automate, we seem to have swapped one problem for another. Algorithms — useful and impressive as they are — have already left us with a tangle of complications. [...]

Our reluctance to question the power of a machine has handed junk algorithms the power to make life-changing decisions [...].

Even the algorithms that (mostly) fulfill their promises have issues. The facial-recognition algorithm at the Manchester Airport failed to notice when a husband and wife accidentally presented each other’s passports to the scanners. Recidivism algorithms used in courtrooms overestimated black defendants’ likelihood to be repeat offenders, and underestimated the same likelihood for white defendants. Algorithms used by retailers to pinpoint pregnant women and serve them ads can’t be turned off, even after a miscarriage or a stillbirth. [...]

The inherent problems of algorithms are magnified when they are paired with humans and our ready acceptance of artificial authority.

But maybe that’s precisely the point. Perhaps thinking of algorithms as some kind of authority is where we went wrong.

Even when algorithms aren’t involved, there are few examples of perfectly fair, accurate systems. Wherever you look, in whatever sphere you examine, you’ll find some kind of bias if you delve deep enough. [...]

Imagine if we accepted that perfection doesn’t exist. Algorithms will make mistakes. Algorithms will be unfair. In time, they will improve. But admitting that algorithms, like humans, have flaws should diminish our blind trust of their authority and lead to fewer mistakes. [...]

The best results occur when humans and algorithms work together. Neural networks that screen breast cancer slides aren’t designed to diagnose tumors; they are designed to narrow down a vast array of cells to a handful of suspicious areas for the pathologist to check. The algorithm performs the lion’s share of the work, and the human comes in at the end to provide expertise. Machine and human work together in concert, exploiting each other’s strengths and embracing each other’s flaws.

This is the future I’m hoping for, one where arrogant, dictatorial algorithms are a thing of the past, and we stop seeing machines as objective masters and start treating them as we would any other source of power. We need to question algorithms’ decisions, scrutinize their motives, acknowledge our emotions, demand to know who stands to benefit, hold the machines accountable for their mistakes, and refuse to accept underperforming systems. This is the key to a future in which the net effect of algorithms is a positive force in society. The job rests squarely on our shoulders. Because one thing is for sure: In the age of the algorithm, humans have never been more important.

[2] Hannah Fry is British. She is an associate professor in the mathematics of cities at University College London. This essay is adapted from her book “Hello World: Being Human in the Age of Algorithms,” first published Sept. 18, 2018.

By Vera Eidelman, Staff Attorney | Published September 15, 2017 on www.aclu.org

Secret Algorithms Are Deciding Criminal Trials and We're Not Even Allowed to Test Their Accuracy

In today's world, computerized algorithms are everywhere: They can decide whether you get a job interview, how much credit you access, and what news you see. And, increasingly, it's not just private companies that use algorithms. The government, too, is turning to proprietary algorithms to make profound decisions about your life, from what level of health benefits you receive to whether or not you get charged with a crime.

This isn't necessarily good or bad. At their core, "algorithms" are just instructions, like a recipe or user manual, that use raw inputs to determine outcomes in all kinds of decision making. But it becomes a serious problem when the government keeps those algorithms — including the source code that executes the programs and the raw data that constitutes their inputs — secret from the public.

And that's exactly what is happening in criminal trials around the country.

Take, for example, the case of Billy Ray Johnson, who was sentenced to life in prison without parole for a series of burglaries and sexual assaults he says he did not commit, largely based on the results of a proprietary algorithm called TrueAllele. TrueAllele claims to identify the perpetrator of a crime from a tiny, degraded DNA sample swimming in a larger soup of multiple individuals' DNA. It's an experimental technology, not at all like the DNA tests that have developed over the past two decades, which also have serious flaws. At Mr. Johnson's trial, the court denied the defense team access to TrueAllele's source code — information crucial to the defense case — all because the company that owns it cried, "Trade secret!"

As we explained in an amicus brief we filed in the case on Wednesday, this is unconstitutional in a number of ways. Our Constitution gives a defendant the right to confront the witnesses against him, and it provides him with the right to a fundamentally fair trial that includes a meaningful opportunity to present a complete defense. It also gives the public a right of access to criminal proceedings, including evidence, so that we can serve as a check upon the judicial process.

Access to the source code of algorithms used in the criminal justice system is critical to ensure fairness and justice. Algorithms are human constructs that are subject to human bias and mistake, which can plague them throughout their design and use. For example, at the building stage, something as simple as a misplaced ampersand[3] can have profound implications. A coding error in another DNA algorithm was recently found to have produced incorrect results in 60 criminal cases in Australia, altering its reported statistics by a factor of 10 and forcing prosecutors to replace 24 expert statements.

Beyond random mistakes, people hold cognitive biases that can materially affect the variables they include in an algorithm, as well as how they interpret the results. Racial bias also often creeps into algorithms, both because the underlying data reflects existing racial disparities and because inaccurate results for smaller minority groups may be hidden in overall results.

And, of course, there's the possibility that financial incentives will pervert the goals of companies that build these algorithms. In the context of DNA typing, the prosecution, backed by the substantial resources of the state, is a company's most likely customer — and that customer is likely to be most satisfied with an algorithm that delivers a match. So companies may build programs to skew toward matches over the truth.

In Mr. Johnson's case, the trial court decided to ignore these potential pitfalls — and, more significantly, the defendant's constitutional rights — ruling in favor of TrueAllele's argument for secrecy. This is legally wrong and has troubling practical implications. Research shows that juries put too much trust in uncontested algorithms. Prosecutors and their expert witnesses present their results as infallible truth, which go "far beyond what the relevant science can justify." And juries, when given no other option, generally do not question them.

But the results need to be questioned, and this case demonstrates why. [...]

This isn't the first time we've been down this road with technology in criminal courts. There is a long history of junk science being used under the guise of technological advance. Public access to such evidence was a prerequisite to establishing its invalidity.

In the 1990s, "a series of high-profile legal challenges" and "increased scrutiny of forensic evidence" caused various long-standing methods — from bite-mark analysis to ballistics testing and from fingerprinting to microscopic-hair-comparison — to get "deflated or outright debunked." Similarly, after a New Yorker article exposed a flawed case based on arson science, the state responsible not only "reconsider[ed] old cases that had been improperly handled by the original investigators," but also "reinvented itself as a leader in arson science and investigation."

Scientific errors in the criminal justice system are a serious problem. But the examples above also reveal the power of adversarial testing and public scrutiny to correct those errors and create better science.

We hope the California appellate court agrees with us and orders disclosure of the algorithmic source code. An adversarial testing process is crucial to ensure that Mr. Johnson's constitutional rights are enforced.

[3] *ampersand* is the sign &.