Predictive policing in 2025: A scenario

Kevin Macnish, David Wright and Tilimbe Jiya

Introduction

Law enforcement authorities (LEAs) have begun using artificial intelligence and predictive policing applications that are likely to raise ethical, data protection, social, political and economic issues. What issues should policymakers be considering now in relation to such emerging technologies in order to be prepared for a future six or seven years hence, which can be assumed the time policymakers need to develop a policy addressing those issues (or, at least, some of them), to build support for it and to get their political masters to sponsor relevant legislation or regulation? That question impelled the development of the scenario detailed in the following pages.

The University of Twente in the Netherlands and the UK's Trilateral Research led the development of the scenario, which kicked off with a brainstorming workshop of 23 invited stakeholders. The partners drafted a scenario based on that brainstorming session, which they then sent to the workshop participants for comments. With those comments, the partners created a second iteration of the scenario, which they then sent to the SHERPA project[1] stakeholder board (27 experts) for their comments, whose comments, in turn, led to the third iteration of the scenario. The partners then invited the project's contact list of more than 1,000 people to comment on the scenario. The partners then posted the scenario on the project's website and invited visitors to comment on the scenario. In due course, the SHERPA project co-ordinator submitted the scenario to the European Commission. Hence, the scenario was not simply a mechanism to provide structured advice to

[1] See the last section of this chapter for more information about SHERPA, a 42-month, EU-funded project that began in May 2018.

policymakers, but also a process for engaging increasing numbers of stakeholders, a process intended to lend credibility and legitimacy to the scenario and in particular to its recommendations.

There were several good reasons for involving as many stakeholders as possible in the scenario construction process, which included the following. The involvement of stakeholders facilitated a participatory, deliberative approach to policy-making. It was also important because it helped to uncover issues that might otherwise be overlooked. Further, the involvement of various stakeholders was ideal for exploring possible consequences of current trends in smart information systems (the combination of AI and Big Data), considering desired and undesired futures as a result of such a combination. Furthermore, the stakeholder involvement helped decision-makers in the decision-making process aimed at determining what steps should be taken to reach the desired future and avoid an undesired future.

The partners aimed to develop a plausible scenario six or seven years from the initial brainstorming workshop (held in late 2018) to provide an early warning about how the use of AI and big data is likely to develop and inform policy (Wright et al., 2019). The agreed timeframe was seven years up to 2025, as it was sufficiently distant to merit some speculation, but not so distant that the project could indulge in science fiction. The wish was to create a *plausible* scenario that reflected the emergence of advanced technologies yet was sufficiently grounded that it could be justifiably used to tease out the ethical and human rights issues for policymakers and other stakeholders.

The brainstorming session followed a structured agenda which is reflected in the section headings in the scenario below. The partners structured the scenario to be of optimum use to policymakers i.e., and it addresses the questions policymakers would be expected to ask or be asked by their constituents. The authors describe the scenario as a “policy scenario” because it has been developed for policymakers and addresses the issues they would need to address before submitting a policy

proposal to their government ministers. The policy scenario methodology has been described elsewhere.[2]

The scenario

In 2025, many police forces across Europe are adopting predictive policing technologies in response to cuts in human resource budgets. Such cuts inevitably led to a rise in crime rates. Many LEAs began experimenting with different predictive policing technologies as a way of cutting crime before it happens. After some false starts, such technologies have evolved as remarkably as facial recognition technologies. Smart information systems, notably artificial intelligence (AI) algorithms, are within the reach of all European LEAs, who now can feed such systems with the vast swathes of data to which they have access. In a manner that is both intelligent and provides useful information in real-time, law enforcement authorities (LEAs) have been experimenting with different applications. Some of these have been developed in-house by the national forces, some have been developed through the European Commission's Horizon Europe research programme, but many are the result of collaborations with private sector players. In some cases, these private initiatives include or result in proprietary data of benefit to the private sector partners.

As one would expect, some approaches and technologies for predictive policing have proven to be better than others. The intelligence-led policing approaches trialled by Pol-Intel in Denmark (Bjørnholdt, 2016) have served as models of police access to and use of many disparate data sets. The more ambitious applications go beyond accessing data to using those data to make predictions regarding incidents of future crime. Most predictive policing applications have drawn on location-based data to define increasingly localised "hot spots" on which the police should focus attention at particular times, while others draw on personal data to identify likely offenders (Norwegian Board

[2] Wright, David, Bernd Stahl and Tally Hatzakis, "Policy scenarios as an instrument for policymakers", Technological Forecasting & Social Change [under review].

of Technology, 2015). Other applications aim to predict likely victims of crime in cases such as domestic violence, or those at risk of becoming offenders in the future. Still, other predictive policing applications have turned their attention from visible street crime to the less visible white-collar crimes, including money-laundering, tax evasion, fraud and cybercrime. Some researchers are using these technologies to draw together demographic, census and other social data to determine what factors are most likely to induce someone to commit a crime. The answers to such questions are expected to make possible early, large-scale interventions where communities and individuals are at risk.

Predictive policing applications must have measurable success factors. Typically, this is a matter of rising or falling reports of crime, but this is an unstable metric. At its heart is a mere correlation and does not prove a causal link between the application and the number of reports. Hence, a decline in reported crime might have come about through using the application, but it might equally be a result of demographic changes. It is possible that reliance on the application has reduced the efficacy of police responses such that many no longer bother reporting crimes as they know that they won't be acted upon. Equally, some applications have been reported as helping the police determine which crimes are worth a response. In some areas, thanks to local press reporting, it is widely known that burglaries will usually not merit a response, and so actual burglaries have increased in number while the number of reports of burglary has declined. On the other hand, the applications may be so successful that police are effectively anticipating crimes and arriving in time to deter the potential criminal from carrying through with their plans. This is plausible given efforts to streamline the online reporting process, itself aided by data analytics and AI allowing for a smooth and fast process for victims or others to report crimes.

While some of the public feared a move to “Minority Report” policing, in which a computer informs police who is about to commit a crime and then that person is arrested moments before the

act, this has not happened (Wright, 2008). Indeed, the police are adamant that any computer prediction regarding likely crime hot spots or offenders are fed as information to a team of analysts who then combine that with other information before advising patrols. This prevents policing by algorithm from becoming the norm. However, cuts in police funding have reduced the number of available analysts, and the remaining analysts have been noticing that the number of false positives (indications that a crime will occur in an area where no crime takes place) is falling with each year, and worry for the future of their jobs. In 2020, for example, there was only one information analyst working for the whole of the LA Police Department.

Furthermore, budget cuts have pushed many officers with good local knowledge into early retirement. New officers, lacking this knowledge, have come to rely upon the predictive policing system. This has led to fears of automation bias in which officers trust the system despite evidence to the contrary (Cummings, 2004; Wickens et al., 2015), and despite the training, introduced in 2020, to rectify this (Goddard et al., 2012). Nonetheless, there remains a tension as to how best to act when the system recommends one course of action and the officer disagrees with this recommendation, leading to some complaining that they are being treated like robots.

International comparisons do not end with the numbers of analysts. Many cities in the United States have been aggressive in pursuing predictive policing, particularly after funding to this end was increased shortly after the US 2020 presidential election. Incarcerations have increased, but there is no sign of a change in the demographic composition of the prison population, which is overwhelmingly African-American. China has also been aggressive in developing predictive technologies following the widespread integration of the Social Credit System which incorporates all data on a person, including bank records, medical records and educational attainments (Creemers, 2018). Facial recognition on CCTV is now standard in most Chinese cities, although there is insufficient recognition by the Chinese authorities of the problem of false positives. The

general approach is one of "better safe than sorry", leading again to a suspected (albeit unreported) rise in the prison population. Owing to Chinese information-sharing protocols, it is also not certain what the ethnic composition of that population looks like, but there are reports that some communities such as the Uighurs have been all but decimated in recent years as they are arrested on the basis of a likelihood of committing a crime (Rollet, 2018). Finally, efforts at introducing predictive policing in some South American cities, such as Bogota in Colombia, have exacerbated perceived biases as the focus remains on preventing crimes against the wealthy, while police ignore victims from less affluent areas.

Europe has been slower than China and the US in adopting predictive policing technologies, partly owing to the human rights frameworks such as the European Charter for Fundamental Rights and the European Convention on Human Rights, both of which are backed up by laws such as the General Data Protection Regulation, which is seen as an effective means of regulating the use of personal data across society. This regulatory framework has combined with the Horizon Europe research programme, begun in 2020, which continued to focus funding on counter-terrorism efforts, which in turn skewed investment in policing and predictive analytics towards identifying factors in radicalisation and away from more common crimes and even farther away from white-collar crime.

While there has been investment in police use of these technologies, criminals have not been idle. LEA cyber detectives have uncovered applications used by criminal gangs to predict where the police will be at any time of the day or night, often drawing on the same data sets used by the police, made public in the name of transparency and democratic accountability. Others have been found on the dark net offering significant sums to hackers who can reverse-engineer police systems to indicate which parameters are used to predict crimes in order that they can better avoid detection.

The police find themselves caught between a rock and a hard place. The press is critical of any reports of rising crime and cynical of reports to the contrary. The police do not need to be reminded of their duty to do all that is reasonable to prevent crime, but the debate within society as to what is reasonable, including which databases can be routinely accessed, rages on with opinion polls reflecting little more than responses to the latest scandal.

With such a postulated sequence of events on the social and ethical implications of using AI and Big Data in predictive policing are a number of drivers and inhibitors are identified. These are illustrated in Figure 1 below and explained further in later sections.

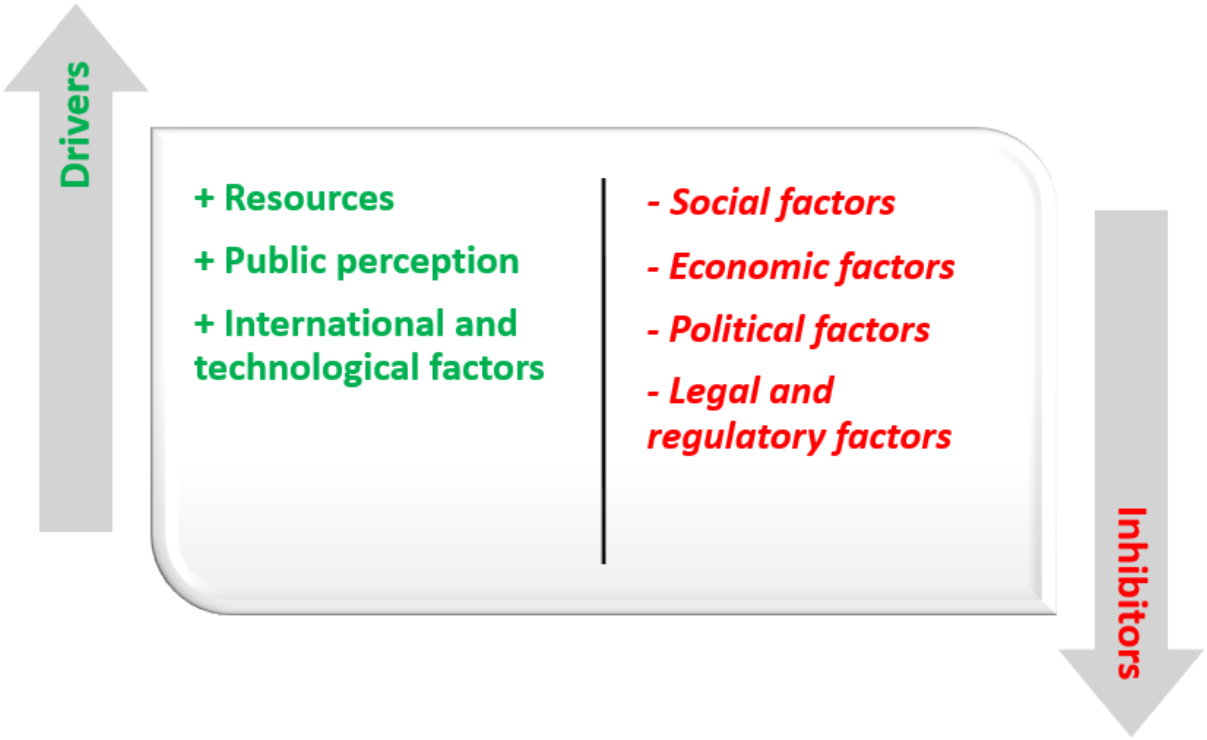

Figure 1: Drivers and inhibitors of predictive policing in 2025

Drivers to 2025

Various drivers have impelled the development of technologies used in predictive policing in 2025, as depicted in Figure 1 and are discussed below.

Resources

Ever tighter squeezes on funding have led to a decline in the number of officers over the past decade while investment in technology has increased. AI is often treated by politicians as a panacea to limited public funds. There is some dissension in the ranks, as many officers can see that while the police budgets are shrinking, the technology firms developing AI applications seem to be thriving. If police budget for human resources have been declining, the quantity and quality of data processed by the police have not. In fact, there is now so much data available from so many different sources that the police would be overwhelmed were it not for artificial intelligence.

Public perception

Given the increased data available, there is a concern that the police miss intervening in cases where they had the relevant information in advance but did not process it in time. This is widely seen as a dereliction of duty and one that no Chief Constable wants to see on her watch. The public view of the police is ambiguous at best, and there is a high level of expectation on the police and their use of technology. After all, if a member of the public can prove that her stolen phone is in her neighbour's house through using tracking apps like Prey, she wonders what is there to stop the police from entering the home and retrieving the phone? Her reasoning leads her to conclude that the police are either unwilling to help her or that they are hopelessly out of date.

International and technological factors

As noted above, Europe has been less aggressive in employing predictive technologies than other countries, notably the US and China, which have considerable resources and public support to invest in these technologies. Many European data scientists have already migrated to one of these countries to work on systems that European politicians see as being "too weak" to implement. These data scientists opine that we must follow where technology leads and if it can help capture bad guys, then you should use it. This divestment of talent, coupled with the mixed results of the

Horizon Europe research projects, has led some European police forces to buy technologies from US and Chinese companies, although they are uncomfortable with the fact that these were likely developed in a manner not consistent with European law. Furthermore, there is the ever-present fear that US or Chinese intelligence agencies will infiltrate these systems through backdoors to spy on their European counterparts.

Inhibitors to 2025

While there have been several drivers pushing the development of predictive policing technologies towards their current state in 2025, this development has not always been straightforward. There have been barriers that impede progress. These are discussed below.

Social factors

Media coverage of increasing use of technology has rarely been positive and, while the intended target was often politicians, it was the police who suffered from adverse coverage. In particular, the press noted the lack of change in the demographics of those arrested and imprisoned. While some have argued that a turn to computerisation in detecting and predicting crime would lead to reduced discrimination, this appears not to have been the case. Instead, data sets have been drawn from non-European countries to ascertain norms, and parameters have been developed by computer scientists unaware of European police priorities. At least one tool was developed in China using a Chinese data set and drawing on factors that were culturally predictive in China but not Europe. This led to a significant rise in immigrant arrests for the trial period when the application was first tested.

Even where the predictive capacities of the applications have been more effective, these were met by the equal capacities of criminals who were able to emulate the predictive tools and hack into them directly. This has become part of the continuing escalation of methods used by the police and criminals to stay one step ahead of each other. Most applications are in a constant phase of beta-

testing as by the time they are sufficiently stable to be rolled out on a wide basis their method has been cracked and they are no longer as effective.

There has also been some marked resistance to change from within the police forces themselves. This has largely been resolved through generational change as the post-millennial generation who grew up on smart phones have come of age and started to enter the workplace, but some resistance remains.

Economic factors

Resources have been a driving factor in the development of predictive applications but, paradoxically, they have also held back some aspects of development. There has been a chronic shortage of computer scientists developing tools, and a shortage of analysts with the abilities to effectively use those tools. This is largely due to the inability of the public services to compete with private organisations, especially those working in similar areas of technology in other countries. Limited funding has also led to datasets and tools being less reliable than would be ideal, with the result that their accuracy and efficiency sometimes leaves a lot to be desired. Despite this, for some, an 80% conviction rate is good enough, and many are becoming increasingly over-reliant on the systems that have led to a positive (although not a virtuous) feedback loop.

Political factors

The lack of funding is due to continued attempts to rein in public spending in the post-2008 world. Some politicians worry about the press drubbing them and the police for arresting people for crimes they haven't committed yet. Some sceptics have criticised the lack of effective and convincing metrics demonstrating the success of the technologies.

Legal and regulatory factors

To ensure accountability in the police use of data analytics and their databases, Parliament adopted laws and regulations that, among other things, made explainability the default mode for algorithms. Politicians had to balance concerns about individual privacy and data protection with the efficacy of police operations. The police were concerned that excessive transparency would give criminals better insight into police methods and, as it turned out, their concerns were justified. Consequently, a committee of the European Parliament has been investigating and debating whether algorithms developed for or used by LEAs should be compelled to have the same standards as others if organised crime benefits from the tiniest scrap of information.

One solution to the stricter regulations imposed by Brussels and national governments on artificial intelligence has been the outsourcing of some technologies to private companies. Google and Facebook have extensive databases of their users and have on occasion helped the police in exchange for access to police databases. Without such incentives, these companies only complied with the minimum requirements of the law, to the chagrin of many LEAs who believed these companies should be doing more to help them in the fight against organised crime. The press saw this outsourcing as having the effect of blurring the borders between policing and the corporate world even more than was already the case in the early 21st century.

Postulated impacts of predictive policing technologies

In 2025, the benefits of predictive policing technologies are starting to be felt, even though there is still considerable public discussion as to whether the benefits are strictly attributable to the technologies or other factors. Nonetheless, their use has been part of a marked shift in society and the number of impacts are noted as depicted in Figure 2 below.

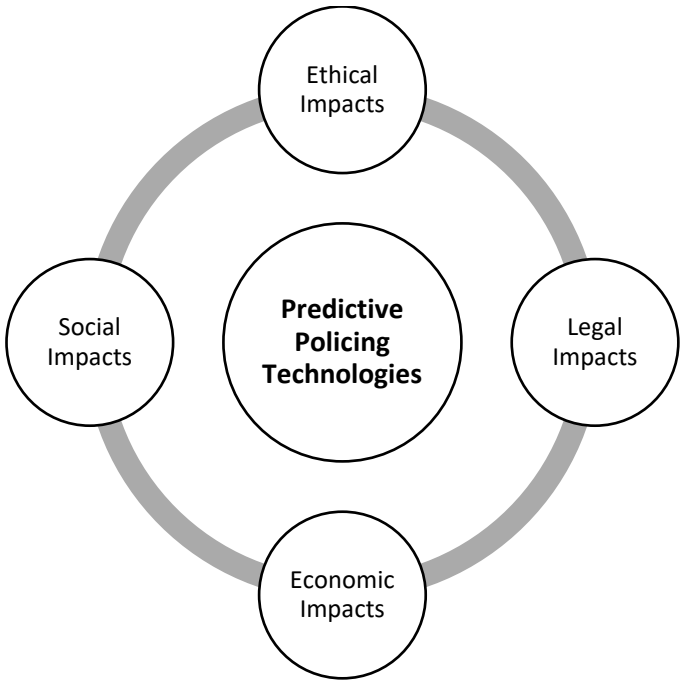

Figure 2: Postulated impacts of predictive policing in 2025

Ethical impacts

Older police officers resent the tighter constraints on their actions compared to when they started their careers. They feel the so-called "smart" information systems that tell them where to go and what to do, are undermining their own skills, experience and talents in responding to crime. Older policemen don't seem to recognise how organised crime has shifted away from street crime to more high-value crime in money-laundering and cybercrime. At the same time, there is clearly greater accountability and transparency in policing as bodycams record every move of every officer and individual officers are frequently held to account over why they did or did not intervene in a particular situation.

Civil society organisations protest that predictive policing technologies are an affront to Europeans' fundamental rights. There is much debate within police ranks and others about whether, when a police officer responds to an algorithm that has 80% predictive capabilities, she is infringing on a person's civil rights by treating him as a suspect on the basis of a statistical calculation rather than

his doing anything to warrant suspicion. At the same time, if she fails to act on the prediction, is she thereby failing to uphold the civil rights of potential victims? This debate is ongoing.

More positively, prior to the implementation of predictive technologies, individuals were already being stopped and searched, and arrested, sometimes for spurious reasons. The aforementioned increase in accountability has shed light on discriminatory stop-and-search practices. Overall, predictive policing technologies have reduced some discriminatory practices and embedded others.

The public discussion that accompanied the widespread introduction of these technologies helped ensure that the explainability regulations in Europe were fair, ethical and sensitive to privacy concerns. Public pressures led to the establishment of an independent oversight body to monitor police use of smart information systems.

While media attention has largely focused on the police use of predictive applications, some has focused on corporate responsibility. Since social media giants collect reams of data, they are frequently able to identify child sex offenders or people involved in domestic abuse. However, this information is rarely turned over to the police. Questions are being asked in national legislatures about the social responsibility of these organisations.

Legal impacts

A key problem with the development of legal and regulatory frameworks in keeping up with technological development is that policy and lawmakers often do not understand the technologies. Technological development is happening faster than the passage of laws and has been impeded by the time lawmakers need to understand recent developments and the subsequent legislative process. The GDPR, which came into effect in 2018, remains generally fit for purpose regarding personal data, but with the aggregation of databases, it is increasingly rare to find data that cannot in some

context or manner be used to identify a living person. The most applicable legislation for LEAs remains the Police Directive, which has meant that LEAs did not need to seek informed consent when they were investigating persons of interest. With so many AI-powered applications available online, prohibitions against automated decision-making affecting the rights of data subjects have become impossible to enforce except in a few high-profile cases like those against Google and Facebook in 2020-21. That so many enterprises see that it is impossible to enforce some provisions of the GDPR has had the predictable consequence of diminishing respect for the law even from law-abiding companies and citizens.

Social impacts

Criminals seek advantage over LEAs by taking advantage of new technologies before the police are able to put counter-measures in place. The nature of crime is changing. There is a shifting focus from street crime, which is particularly subject to some of the blunter forms of predictive policing technology, to organised crime and white-collar crimes, including money-laundering, fraud, online scams and hacking.

While organised crime gangs are aware of predictive policing technologies, the public generally has a low understanding of such technologies and their possible negative impacts. The public is bombarded with so much information (and disinformation) about new technologies that the public has become jaded. The powers of new technologies have ceased to spark wonder. The majority of the public accept these measures as just part of the cost of living. The public has already learned to cope with substantial levels of surveillance in society – on the streets and in cyberspace. Some people claim that they have altered their behaviour, to appear as conformist as possible, as these days, they do not know what will land them in some police database. “Better to play it safe,” they think.

Economic impacts

We have already noted the savage cuts in police budgets. Also of note is the shift in budgetary priorities from police officers to more data analysts. As the number of officers fall, so the reliance on AI grows, and as the reliance on AI grows, so the same work (or at least similar) is apparently achieved with fewer officers, and funding declines further. One solution has been to outsource certain tasks, such as facial recognition, to the private sector, as the US has done for several years.

Mitigating the negative and accentuating the positive influences of these technologies

For some people, predictive policing was an easy sell. While civil liberty organisations still complain about the bias in algorithms, the public is wary – neither trusting, nor distrusting, but conscious that crime rose several years in a row with cutbacks on police officers. Predictive policing was touted as the artificial intelligence that was going to make huge cuts in crime – which has not happened as organised crime gangs have upped their game too.

Politicians, recognising the need to boost their trust with the public, agreed to adopt a new regulation-making algorithms explainable to the public. Each algorithm was to include code saying who created the algorithm, who paid for it, its purpose, website and contact for more information. This dispelled concerns about the police wanting to keep their black boxes black, as it were, but led criminals to a better understanding of police methods and tactics and a spate of hacking attacks on police systems. Meanwhile, some “grey hat” hackers attempted to improve the algorithms to help eliminate bias.

A significant factor in gaining public acceptance was the establishment of trusted independent national bodies to oversee police use of algorithms in predictive technologies. Adequately funded, and staffed with known and respected figures such as Baroness Lawrence in the UK, these

independent bodies helped to build trust in the police system. These bodies looked at not only the algorithms themselves but all aspects of police use of data. They considered what data were collected, the purpose of their collection, how the data were processed and storied, and their eventual usage (including secondary use).

The findings of these bodies were, in the early days, significant in developing crucial training programmes for the police about the new technologies and their limitations. Politicians and senior police officials communicated these rules effectively to the public. They hosted regular stakeholder engagement meetings with the public to ascertain their concerns. Local police forces have also been hosting local meetings with residents and community leaders to explain their use of new predictive policing technologies, how these technologies were vital in offsetting the cuts in police staff numbers and, importantly, how accurate these algorithms were in predicting criminal acts.

Steps towards a desired future and avoidance of an undesired future

Civil society organisations, late-night talk-show hosts and some editorial writers articulated fears that the new predictive policing technologies would yield many false positives, that perfectly innocent citizens could be victimised by the new technologies and placed on a police register without knowing why. There were worries about positive feedback loops, in particular, locales targeted for attention leading to a greater number of arrests in these areas, leading in turn to algorithms predicting that these were the areas on which the police should be concentrating. Had there been a blind trust in the efficacy of the algorithms, then this may well have been the case, but fortunately, this concern had been raised so many times that the police and algorithm developers were on guard for such phenomena.

Addressing these concerns directly, by instituting transparency measures and empowering oversight bodies, the police increased public trust and strengthened social cohesion. Predictive policing technologies helped the police focus on previously invisible areas of crime. Data analysts uncovered these areas by training their algorithms with masses of information from disparate sources. This allowed the police to put more effort into tackling white-collar crime and online hate crime. This in turn has had a ripple impact on international crimes such as people trafficking and drug smuggling. In fighting such crimes, the police noticed positive effects in communities that were otherwise subject to the attention of such smugglers. Criminals and their would-be accomplices now recognise that if they commit a crime, the likelihood of getting caught is higher than ever, even though there are lingering worries about the inevitability of at least some false positives that could lead to the harassment of innocent people (Macnish, 2012).

The police also appreciated the new technologies as they found that effective intelligence-led to their approaching volatile situations with an enhanced awareness of how those situations were likely to play out. These days, it's rarely the case that a police officer finds himself unexpectedly in the middle of a riot and fearing for his life.

Predictive policing technologies have especially emphasised the prevention of crimes – not only by minutes or hours but also on the factors that lead to criminality. The initial emphasis on street crime led to an outcry by civil society organisations, the media and citizens that such technologies were ignoring corporate crime which has a much bigger impact on society. Always loving a challenge, data scientists recently developed new smart information systems that are expected to enhance the detection of corporate crime and malpractices significantly. These new technologies are bringing ethicists and data scientists together, which is expected to benefit European competitiveness greatly.

The SHERPA project

This chapter is informed by the research and work conducted by the EU-funded Horizon 2020 SHERPA project (SHERPA, 2018). SHERPA is a collaborative research project that was commissioned for 42 months, beginning in May 2018, by the EU to bring together a range of stakeholders to investigate, analyse and synthesise our understanding, and to make recommendations to policymakers regarding ethical and human rights issues raised by or likely to emerge from smart information systems, notably those embedded with algorithms and artificial intelligence.

The above scenario was one of five developed in the SHERPA project. The others concerned 'deepfake' technologies, information warfare, driverless vehicles and robots in education. Each of the five followed the same structure and process of engaging increasingly larger numbers of stakeholders. The five scenarios were submitted to the European Commission in June 2019.

With policy scenarios, we do not aim to predict a specific future. That is impossible. However, we can envisage a plausible future (the scenario) and the many factors – the drivers, barriers, impacts – that policymakers should take into account to enable or avoid a future like that envisaged in the scenario. We do not want a scenario with many variables and possible turns of event. Policymakers prefer a clear, single course of action that has stakeholder support. In addition to the structured approach to its development, our scenario shows the range of factors that policymakers should also take into account in the formulation of policy and recommendations.

One of the objectives of the scenario construction process was to reach a consensus on a plausible future. Participants were challenged to be creative, to leap ahead six or seven years and imagine how the technologies might evolve and what new applications might arise. The present often got in the way of the future in many of the discussions, but mostly the present provided a reality check on a story-telling exercise. We wanted more than the present, as it were, without getting trapped in science fiction. We sought to develop plausible scenarios with recommendations that would be

useful for policymakers. The scenario construction process is a way for policymakers to get "ahead of the curve", to develop policies now that will anticipate or pre-empt an undesired future and promote a desired future. In other words, the policy development process needs to begin now, as it usually takes several years before an identified policy requirement becomes legislation.

The scenarios were instrumental in spelling out ethical and social tensions and their role in the current human rights framework. The scenarios were one of the several methodologies that the SHERPA project used to understand and get to grips with ethics and use of big data and AI. Others included:

- Ten cases studies to explore the ethical and human rights tensions in different AI and big data application domains (Ryan et al., 2019).
- A large-scale online survey of 1,000 European citizens
- A Delphi study with 60 experts.

In these and other project methodologies, the partners sought to engage many stakeholders (Wright et al., 2019).

Recommendations

Following the scenario on the social and ethical consideration of using AI and Big Data in predictive policing are put forward. The recommendations are;

i. To boost their trust with the public, policymakers should adopt a regulation-making algorithms explainable to the public. Each algorithm should include code recording which created the algorithm, who paid for it, its purpose, website and contact for more information.

ii. Law enforcement authorities should ensure that criteria are clear and transparent for personal data to be entered into law enforcement databases.

iii. Policymakers should ensure there are independent regulatory authorities of sufficient size and clout to monitor the data in and use of law enforcement databases and offer commendations or impose penalties where appropriate.

iv. Decision-makers should ensure that measures in preventive policing and community investment supplement developments in predictive policing.

v. Law enforcement authorities should take a balanced approach to local, white-collar and online hate crimes.

vi. Law enforcement authorities should ensure effective training of police officers and database operators regarding the limitations of data analysis, particularly concerning the rates of false positives and automation bias.

vii. The EU should sponsor research on automatically detecting when an attack is being planned and discussed.

Conclusion

As AI penetrates further into our economies and societies, it is speeding up decision-making such that AI-powered decision-making becomes more needed. Human decision-makers cannot respond fast enough, especially in the instance of attacks on cities and critical infrastructure. AI-powered decision-making raises apprehensions about decisions gone wrong or without an appreciation of the consequences.

Our scenarios and the methodology we used to create them offer value to policymakers who wish to engage stakeholders in a structured process considering future developments and their ethical, data protection, social and economic impacts. To our knowledge, our structured approach to the scenario construction process is an innovation, yet it flows logically from the development of new technologies and applications to an illustrative vignette to the drivers, the inhibitors, and the ethical,

data protection, social and economic impacts. The scenarios conclude with some recommended measures to reach a desired future and avoid an undesired future. Our scenario construction methodology is based on engaging with stakeholders from the get-go, from an initial brainstorming workshop through several iterations of the scenario. Part of the reason to invite increasingly greater numbers of stakeholders to review and comment on the scenario is to prompt stakeholders to consider the implications of advanced new AI technologies, the risks and benefits. In other words, construction of a scenario is also an awareness-raising exercise. However, ultimately, a scenario is a policymaking tool, and our scenarios are constructed in a way so that policymakers can readily grasp their import and can use the scenario methodology themselves on other issues.

Acknowledgement

This chapter is based on research undertaken in the EU-funded SHERPA project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 786641. The authors hereby acknowledge with thanks the comments on the scenario from various stakeholders. The views expressed in this chapter are those of the authors and in no way are intended to reflect those of the European Commission.

References

Bjørnholdt, K., 2016. New IT should help police catch criminals. Copenhagen.

Creemers, R., 2018. China's Social Credit System: An Evolving Practice of Control (SSRN Scholarly Paper No. ID 3175792). Social Science Research Network, Rochester, NY.

Cummings, M.L., 2004. Automation Bias in Intelligent Time Critical Decision Support Systems, in: AIAA. Presented at the 1st Intelligent Systems Technical Conference, pp. 557–562.

European Economic and Social Committee, 2017. Artificial intelligence - The consequences of Artificial intelligence on the (digital) single market, production, consumption, employment and society. (Opinion No. INT/806). European Economic and Social Committee, Brussels.

Goddard, K., Roudsari, A., Wyatt, J.C., 2012. Automation bias: a systematic review of frequency, effect mediators, and mitigators. J Am Med Inform Assoc 19, 121–127. https://doi.org/10.1136/amiajnl-2011-000089

Jiya, T., 2019. Ethical Implications of Predictive Risk Intelligence. ORBIT 2. https://doi.org/10.29297/orbit.v2i2.112

Light, B., McGrath, K., 2010. Ethics and social networking sites: a disclosive analysis of Facebook. Information Technology & People 23, 290–311.

Macnish, K., 2012. Unblinking eyes: the ethics of automating surveillance. Ethics Inf Technol 14, 151–167. https://doi.org/10.1007/s10676-012-9291-0

Norwegian Board of Technology, 2015. Predictive policing – Can data analysis help the police to be in the right place at the right time? Oslo.

Rollet, C., 2018. In China's Far West, Companies Cash in on Surveillance Program That Targets Muslims. Foreign Policy. URL https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/ (accessed 12.8.19).

Ryan, M., Antoniou, J., Brooks, L., Jiya, T., Macnish, K., Stahl, B., 2019. Technofixing the Future: Ethical Side Effects of Using AI and Big Data to meet the SDGs, in: IEEE. Presented at the The 5thIEEE Smart World Congress (SmartWorld 2019), IEEE Smartworld, Leicester, p. 7.

Schwab, K., 2017. The Fourth Industrial Revolution. Crown Business 9.

SHERPA, 2018. SHERPA - Understanding and Analysing Smart Information Systems [WWW Document]. URL https://www.project-sherpa.eu/ (accessed 7.27.18).

Wickens, C.D., Clegg, B.A., Vieane, A.Z., Sebok, A.L., 2015. Complacency and Automation Bias in the Use of Imperfect Automation. Hum Factors 57, 728–739. https://doi.org/10.1177/0018720815581940

Wright, D., 2008. Alternative futures: AmI scenarios and Minority Report. Futures 40, 473–488. https://doi.org/10.1016/j.futures.2007.10.006

Wright, D., Rodrigues, R., Hatzakis, T., Pannofino, C., Macnish, K., Ryan, M., Stahl, B., Antoniou, J., 2019. Smart Information Scenarios (No. D1.2), Representation and visualization of ethical and human rights issues in SIS. SHERPA -EU Project, UK.