

Summaries

Justitiële verkenningen (Judicial explorations) is published six times a year by the Research and Documentation Centre of the Dutch Ministry of Security and Justice in cooperation with Boom juridisch. Each issue focuses on a central theme related to judicial policy. The section Summaries contains abstracts of the internationally most relevant articles of each issue. The central theme of this issue (no. 3, 2016) is *New technologies in law enforcement and public security*.

From predictive policing to prescriptive policing

A. de Vries and S. Smit

Law enforcement around the world, including the Netherlands, is currently experimenting with *predictive policing*: policing based on crime predictions. Big Data on past crimes and the help of sophisticated machine learning enable police to use reliable predictions about when and where the next offense will take place. If the effectiveness of policing actions is stored in the system, it can also predict which intervention is most effective. This is called *prescriptive policing*. The authors explain how these methods work, how reliable and effective they are and which associated risks can be identified. The authors emphasize that legal, ethical and organizational safeguards are necessary for a responsible implementation.

Data-driven urbanism and the creation of smart cities

R. Kitchin

The article provides a critical overview of data-driven urbanism and smart cities focusing in particular on the relationship between data and the city, and critically examines a number of urban data issues, including: the politics of urban data; data ownership and control, data protection and privacy, dataveillance, and data uses such as social sorting and anticipatory governance; and technical data issues such as data quality and veracity of data models and data analytics. Whilst data-driven urbanism provides a set of solutions for urban problems, it does so within limitations and in the service of particular interests.

Data Protection by Design as an argument in the FBI vs. Apple debate

C. Cuijpers and S. van Schendel

Adhering to a strict interpretation, Data Protection by Design (DPbD) can conflict with the needs of law enforcement in their fight against terrorism and criminality. An illustration of this tension can be found in the case of FBI vs. Apple, where the FBI wants Apple to help bypass security on an iPhone in order to gain access to data. The FBI needs the help of Apple – or third parties – to get such access, for which they might need to create new legal mandates. However, private parties like Apple, may want to design their products in such a way that evading and breaking the security of the system is not possible, as consumers demand secure and privacy friendly devices. This article adds to this debate by posing DPbD as an argument in favor of private parties not to cooperate in making their products less secure and less privacy friendly. This argument is especially relevant when a similar case unfolds in the EU under the new regime of the General Data Protection Regulation in which DPbD is explicitly embedded.

Promising policing technologies. Experiences, obstacles and police needs regarding law enforcement technologies

B. Custers and B. Vergouw

Police forces and law enforcement agencies in many countries are continuously trying to optimize the use of technologies in policing and law enforcement. Efforts are being made to remove existing technological, legal and organizational obstacles to create more opportunities of promising technologies, both existing and new. This contribution describes the results of a survey among 46 police forces and other law enforcement agencies in eleven countries. Their experiences with policing technologies and their needs and preferences in this regard are described. The prevalence and satisfaction of existing technologies, including wiretapping, fingerprints, DNA research, database coupling, data mining and profiling, camera surveillance and network analyses were investigated. Legal, technological and organizational obstacles for the use of technology in policing were mapped and the extent to which policing technologies are evaluated and yield success stories was investigated. The main obstacles, according to the respondents, are insufficient financial resources and insufficient availability of technology. One in four organizations is lacking any clear,

appealing success stories and half of the respondents indicated they were not performing any evaluations on the effectiveness of using particular technologies in policing. As a result, the information available on whether technologies in policing are actually working is very limited.

Police and video technology

S. Flight

The Dutch National Police deploys video technology, for instance body-worn video camera (bodycams), drones, helicopters with cameras, and mobile units for surveillance. Four types of video technology are discussed: CCTV, bodycams, smart cameras and automatic number plate recognition (ANPR). These four types will be the most prominent applications of visual technology in the coming years, according to 'Vision on sensing', published in 2015 by the National Police. The potential benefits of video images for prosecution and in the courtroom are discussed in a separate paragraph, followed by a survey of recent changes in the laws regulating this technology.

Drones: a blessing or a curse?

P.J.M. Elands

This article discusses the risks of the use of drones in airspace. The author describes the various applications of drones and the impact of drones on society. Which laws and rules apply in the Netherlands for the use of drones? What changes should be made so that public safety is guaranteed while the development of beneficial forms of drone use can continue to flourish?

Reflections on the responsible use of artificial intelligence

M.V. Dignum and J. van den Hoven

The potential perils of robots and other forms of artificial intelligence (AI) have been a subject for discussion since the 1950s. Nevertheless it seems that society is still not prepared for the great impact of the rapid advancement of AI in the last decennium and the many ethical dilemmas involved. How can moral, social and legal values be integrated in the designing process of AI technologies? Is it imaginable that these AI systems would ever be considered as ethical entities? How to control these systems? The authors argue that we should not only analyze these problems, but also reflect on ethics itself. AI has the potential to

change the way we live and work. But it is important to introduce restrictions and controls to guarantee our freedom, autonomy and fundamental human rights.