Summaries

Justitiële verkenningen (Judicial explorations) is published nine times a year by the Research and Documentation Centre of the Dutch Ministry of Justice in cooperation with Boom Juridische uitgevers. 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 (vol. 30, nr. 8, 2004) is Cybercrime.

The permanent state of emergency; cybercritical reflections on the public space

M. Schuilenburg

This article shows how technological media (ICT) have changed penal enforcement in such a way that a state of emergency is always everywhere. It does so by first reviewing the influence of cameras and the usage of computernetworks on crime control by the police. In the pro-active approach of the police occurs a legal vacuum in which every civilian becomes an informant. As a consequence the difference between a civil subject and a juridical suspect becomes blurred. Secondly the article shows how in our informational society a new official penalty for fraud and environmental crime will be put forward: 'naming and shaming'. These two changes are presented as a new paradigm of governing today: a state of emergency in which every virtual danger is considered actual. In this permanent state, emergency is no longer an exception. Emergency is the law.

Vulnerability of the ICT-based society

E. Luiijf

Society increasingly depends on Information and Communication Technologies (ICT). This causes the ICT-based society to be vulnerable to threats against the trust by citizens, consumers, and businesses in the application of ICT in services and products on one hand, and threats against the critical infrastructures – which largely depend on ICT – on the other hand. The article discusses current threats and vulnerabilities and identifies future areas of concern like RFID and networking of embedded processors. Some weaknesses in the current legal framework – not limited to the Netherlands alone – to combat cyber crime are identified. These include deliberate attacks on ICT which is used to monitor and control infrastructures like power and

gas transport and distribution, water management, drinking water, and chemical processing plants.

Technology and the new dilemmas around identification, anonimity and privacy

J.E.J. Prins

This article focuses on issues arising in relation to identification and anonymity in an on-line society. It discusses the influence of both technological developments and recognised privacy principles on the limits of identification on the one hand and anonymity on the other. In doing so, the contribution covers developments in the area of surveillance and data retention as part of strengthening criminal enforcement and in fighting terrorism. In addition, the article outlines matters concerning identity and anonymity within the private sector. Identification in a commercial setting is clearly enhanced by technological developments such as domotica, RFID, personalised services and identity-based marketing. It is argued that in a society in which our behaviour and identities (i.e. not individual personal data as such), become the object of attention (for whatever reason or interest), the debate on privacy protection must be structured along other lines than those presently available. It requires that we shift our attention from protecting individual personal data to the role of legislation in providing the necessary instruments that will allow us to know and control how our behaviour, interests and social and cultural identities are 'created' and used in our present-day society.

Peer-to-peer vs. copyright

Chr. A. Alberdingk Thijm

This subject of discussion in this article is the rightfulness of peer-to-peer-programs (P2P) like Napster and KaZaA, which facilitate direct filesharing between program users. After a short explanation of the operating procedure of P2P-programs the author analyzes the lawsuits against Napster and KaZaA for violation of copyrights. The crucial point in this juridical struggle is wether the search function of the P2P program is provided from a central server operated by the provider. In that case proprietors can force the provider to stop passing on the location of files embodying a violation of copyrights. However the newest generation of P2P programs operates fully decentralised. Proprietors have no other option than to bring individual program users to court. In the next fase of this 'disastrous' struggle, says the author, proprietors will try to force internet providers to betray the identity of individual P2P program users.

The battle against cyber crime and the necessity of international regulations

H.W.K. Kaspersen

Today, an increasing number of incidents are reported of in principle criminal behaviour, such as computer hacking, distributed denial-of-service-attacks and other computer sabotage, spamming, spy ware and related acts. Although national Dutch law has already criminalised most of these acts, law enforcement seems to fail in taking appropriate actions to reduce and prevent criminal conduct in and around the internet. The article points at the global nature of the internet to tune national laws and to provide for effective international co-operation. As a first step the notion of *cyber crime* is discussed including some factors that have a strong impact on its occurrence and present growth. The need to collect electronic evidence requires adequate legal and technical powers. International cooperation is only achievable if there is a common understanding about the behaviour to be criminalized and if the law provides for adequate powers to investigate those crimes. Both elements require a more or less permanent form of international deliberations. The article thereto discusses the content, major features and merits of the Council of Europe Cyber Crime Convention (2001) and related measures taken by the European Union, including the implementation of these measures in the Dutch Criminal Code.

Trends in cybercrime

W. Ph. Stol

In the eyes of Dutch society the main problems concerning the Internet are the invasion of people's privacy (by other citizens and by the government), internet fraud, the distribution of child pornography and some crimes that are a threat to the system itself, like hacking, spam and viruses. Another major problem is the use of Internet by extremists and terrorists as a tool for their communication and organization. Priorities in law enforcement are the fight against extremism and terrorism, internet fraud and the distribution of child pornography. The working methods of 'cyber criminals' change over time. For example people trafficking in child pornography on the Internet promote their business via spam these days instead of via messages in newsgroups. The police should keep up with such developments. The main problem of the police is a lack of criminological knowledge concerning cyber crime.