LAW OR ARTIFICIAL INTELLIGENCE?
NEW TRENDS IN THE DATA PROTECTION

by

BOHUMÍR ŠTĚDROŇ

The article deals with identity management and the new trends in the data protection in connection with the technological forecasts; new scenarios are presented. Key words and phrases: identity management, data protection, APEC model, technological forecast, artificial intelligence, RFID, brain gate chips.

Introduction [1]

According to Dataprotectionlaw & Policy (June 2006) forty-four percent of the United Kingdoms senior IT decision makers´ are using live customer data to test applications in breach of the Data Protection Act, according to a survey of 100 IT directors.

Francisco Garrido, bioethics and deputy for Seville, has presented a proposal to the Spanish parliament to obtain a commitment from the Spanish government to grant chimpanzees, gorillas, orangutans, and bonobos protection against "slavery, torture, death, and extinction." Second step for a human right for apes and monkeys has been made… (first step has been made in New Zealand in 1999).

Around five thousand miles from Spain according to CHICAGO TRIBUNE (7/13/2006) with a tiny, electronic chip implanted in the motor cortex of his brain, a 25-year-old man paralysed from the neck down for five years has learned to use his thoughts to operate a computer, turn on a TV set, open e-mail, play a video game and manipulate a robotic arm - the first successful steps toward using the mind to directly control machines.

These three seemingly unrelated facts represent common new development tendency in connection with the human rights and date protection. Analysing

the contemporary international conferences, regarding the data protection and annual reports of the data protection authorities, we can recognize two basic tendencies:

I. Linear or exponential Growth of Data Protection violation in the world.

II. Growth of using new technologies (RFID, modified SWIFT etc.), which are aimed at Artificial Intelligence. These new technological trends make impossible or very difficult to identify the source of date manipulation violating the Date Protection Acts, which were admitted not only in the EU countries.

III. New scientific disciplines mirrors the general development of the data protection

Identity Management [2]

The new scientific discipline Identity Management (IDM) has developed several interpretations in the IT industry and the focus on identity management goes back to the development of directories. Therefore we should consider identity management as the management of information (as held in a directory), which represents real life, identified items (users, devices, services, etc). Engineering such systems means that explicit information and identity engineering tasks become necessary.

The term Identity engineering is used where one puts engineering effort into managing large numbers of interrelated items (which have identifiers or names).

In the real world context of engineering online systems, Identity Management can be given two perspectives:

a) The user access (log-on) paradigm - A smart card and its associated data that a customer uses to log on to a service or services (a traditional view);

b) The service paradigm - A system that delivers personalized, role-based, online, on-demand, multimedia (content), presence-based services to users and their devices.

Identity Management in the user "log on" perspective would be an integrated system of business processes, policies and technologies that

enable organizations to facilitate and control their users' access to critical online applications and resources — while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access rights, access restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems.

Today many organizations are facing a major clean up in their systems to bring identity coherence to their world. This coherence is required in order to deliver unified services to very large numbers of users on demand - cheaply and with security and single customer view facilities.

a) IDM provides a significantly greater opportunity to an online business beyond the process of authenticating and authorizing users via cards, tokens and web access control systems.

b) User-based IDM is evolving from user/password and web access control systems to those that embrace preferences, parental controls, entitlements, policy based routing, presence and loyalty schemes.

c) IDM provides the focus to deal with system-wide data quality and integrity issues often encountered by fragmented databases and workflow processes.

d) IDM embraces what the user actually gets in terms of products and services and how and when they do that. Therefore IDM applies to the products and services of an organization such as health, media, insurance, travel or government services, as well as how these products are provisioned and assigned to (or removed from) "entitled" users.

e) IDM can deliver a single customer view that includes their presence and location, single product and services and single IT infrastructure and network views to the respective parties and therefore IDM is related intrinsically to information engineering and information security and privacy.

Technological Forecast [3]

Technological forecast of W.Halal from the George Washington University, BT Technology Timeline (Neidl, Pearson) or B. Stedron (FUTURIST March/2004) makes it possible to specify new segments in the

data protection markets, where human rights can be essentially in danger:

a) Voice command of computers

b) Intelligent Internet and distributed Artificial Intelligence (AI) including AI Judge (on-line dispute resolution as a first step)

c) Biosphere with AI.

Technology development is accelerating and an increasing number of new fields are being created and rapidly converted to establish new business segment Data Protection Area. The rapid growing of the personal data violation can be solved for the present by systematic increasing staff number of the Date Protection Authorities.

What's next for Law and ITC development and applications? Here are a few possible scenarios incorporating new trends and discontinuities (2010-2020):

a) All laws enacted by legislatures in Washington and Brussels rely heavily on AI-based expert systems.

b) Intelligent computers and telecommunication networks allow voice command for 3-D Internet, radio and television, mobile phones, medical care, and other services (intelligent RFID as a new generation of the today RFID).

c) The rapid growing of the personal data violation will be solved by new Laws: the personal date violation will be checked and financially penalized by private firms and robots, which will be certified by Data Protection Authorities. (The computer program, based on CLIPS AI Language from NASA, simulating the Date Protection Supervisor, will be tested in Autumn 2006 in the IT Department of the Faculty of Informatics and Management of the University of Hradec Kralove Czech Republic in cooperation with the Office for Personal Data Protection in Prague.).

d) Direct human-Internet communication is made possible with an implanted chip (later, without chips).

e) New discoveries lead to new materials incorporating low levels of intelligence and later materials with high levels of intelligence. Intelligent computers and telecommunications networks manage their own repairs, scientific research, and production.¨

f) Direct communication among humans, computers, and cetaceans (and primates) is possible using implanted chips (later, without chips).

g) New laws recognize human rights for Dolphins, Primates, Cetaceans and Pets. AI makes it possible to create a copy of any human being's intellect; laws regulating and protecting these copies quickly follow.

In connection with the above facts and predictions, only a system of new laws can guarantee human rights, better personal data protection and following much better social well-being:

a) Prohibition of the construction of AI computer programs with instinct of self-preservation;

b) Law for protection against electromagnetic smog and for protection against civilizations diseases;

c) Law regulation the usage of robots and biosphere and regulation of using ICT in some segments of culture and arts.

Currently the Internet will came to a new four-dimensional structure of post biological evolution of human civilization, which shows a features of artificial life, where particular dimensions are made up of consistent acceleration of components, artificial intelligence, global expansion, super convergence (energy and communication nets, legal systems, food production etc.). Instead of a current implementation of new scientific discoveries from an external environment, the Internet will grow into an autonomous civilization, symbiotically interconnected with a human civilization, where the interface is ensured by ecological information technologies in the future.

That is why two different strategic scenarios will be possible:

I. Following the publications LINKED we will be gradually connected to the one computer system (intelligent Swift Centrum), containing around 10 000 sensors for every human being (like Borg from Star Trek). Elimination of civil liberties is evident, undeniable and visible.

II. Very strict personal data protection Laws, guaranteeing the basic human rights.

Summarizing the current results and new trends, it seems obvious that it is necessary to change gradually the legal and political system. Otherwise all efforts to protect data will have the same results like Nikita Khrushchev efforts to increase the efficiency of the Soviet agriculture during the last century…

References

[1] BARABASI, Albert (2002). Laslo Linked ,Perseus Publishing Cambridge: Massachusetts.

[2] POLČÁK, Radim. (2005, 14, 4) Ke zneužití dominantního postavení v informačních sítích – případ Microsoft. Jurisprudence, vynutitelnost práva a právní praxe, Utrecht : Stichting EMP, 27-31.

[3] POLČÁK, Radim. (2006). Kingdom of IT and IP law and the Quest for Legitimacy. In KnowRight 2006. Vienna : Oesterreichische Computer Gesellschaft. 19-27.

[4] POLČÁK, Radim (2005). Normy w cyberprzestrzeni. Dlaczego? Studia Prawno Ekonomiczne, Lodz: Lodzkie Towarzystvwo Naukowe, 29-39.

[5] POLČÁK, Radim. (2005). Why norms in Cyberspace? In Cyberspace 2004: Normative framework. Brno : Masarykova univerzita v Brně, 2005. 3-8.

[6] STEDRON, Bohumir (2004, March-April). Forecast for Artificial Intelligence, Futurist (USA), 24-25.

[7] STEDRON, Bohumir (2005). Kunstliche Intelligenz; Problemlosung fur die Zukunft, Zukunfte (Berlin), 49.

[8] STEDRON, Bohumir. (2006, Februray) Law for the Future. Mezinárodní konference LEFIS, Firenze Italy, from http://www.lefis.it

[9] STEDRON, Bohumír (2003). Umělá inteligence: prognóza diskontinuity. Convergence 3. 14-15.