Ochrana osobních dat a právní úprava v České republice

Jana ZEZULOVÁ

I.
Pojem informace

Informaci můžeme chápat jednak ve smyslu subjektivním (jako zvýšení znalosti něčeho), jednak ve smyslu objektivním (jako sdělení o něčem v písemné či jinak na hmotný předmět vázané podobě. Tento druhý typ informace nazýváme informací potencionální, technickou podobu této informace označujeme jako „data"[1].

Právní pojetí informace nespadá do pojmu majetek. Na informaci pohlížíme jako na nehmotný statek. Práva k informacím jsou považována za osobně majetková práva (jako např. práva k uměleckému dílu či vynálezu).

Z ekonomického hlediska se stává informace zbožím. Mohou se stát předmětem obchodu.

II.
Informace a právo na soukromí

Předmětem informace může být prakticky cokoliv. Zvláštní význam však mají informace, jejichž předmětem je občan. Jde jednak o informace statusové (o jménu občana, o jeho datu narození, o datu sňatku), informace o bydlišti občana, o jeho zaměstnání, o jeho zdravotním stavu, údaje policejních evidencí (tj. zda byl či nebyl trestně stíhán a za co byl trestán), údaje o jeho majetku např. pro potřeby finančních a daňových úřadů, vklady v peněžním ústavu atd. Tyto informace označujeme jako informace osobní nebo informace povahy intimní.

Pokud jde o tyto informace, dochází často ke střetu zájmů společnosti (reprezentované orgány státu) či organizací anebo i ostatních občanů na získání informace a zájmu občana, jehož se informace týká, tj. občana, jenž je (přímo či nepřímo) jejím předmětem, na utajení[2].

[1] Knapp, V.: Právo a informace. ČSAV 1988, Praha.

[2] viz odkaz 1).

V souvislosti s výše uvedeným vyvstává otázka, kdy zájem na získání či utajení informace bude zájmem oprávněným (tedy můžeme mluvit o právu na informaci, či o právu na utajení informace).

Základní okruh právních předpisů pro tuto oblast představuje čl. 10 Listiny základních práv a svobod a občanský zákoník.

Článek 10 odst. 3 Listiny základních práv a svobod stanoví: „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě."

Podle § 11 občanského zákoníku má fyzická osoba právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.

Osoba má právo se domáhat, aby bylo upuštěno od neoprávněných zásahů do sféry jejich osobnostních práv, odstraněny následky a poskytnuto zadostiučinění za materiální a nemateriální újmu, a to i v penězích.

Tato obecná úprava doplňuje speciální ochranu podle zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

III.
Ochrana osobních údajů v informačních systémech

Ochrana osobních údajů v informačních systémech se opírá o právo na osobní soukromí, právo na kontrolu informací o sobě samém, právo vymezit své vztahy k ostatním, právo být sám, právo na individuální autonomii, právo na tajemství či právo zůstat v anonymitě[3]. Ústředním právem však je právo na soukromí. Čl. 7 LZPS stanoví – nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

Právo na soukromí je základním občanským právem, zakotveným v ústavním zákoně, současně je i dílčím právem v rámci všeobecného osobnostního práva (podle naší právní nauky).

Otázkou zůstává vymezení soukromí, neboť pro každého bude soukromí něco jiného. Známá je definice Warrenova a Brandeisova „the right to be left alone", či Westinovo „the individual's right to determine what information about himself he is willing to share and with whom" or vymezení soukromí jako „in its most suggestive sense, privacy is a limitation of other's access to an individual".

Právě v souvislosti s rozvojem informačních systémů dochází k soustřeďování informací o občanovi, mající charakter osobních údajů o jeho osobě a soukromí. Vzrůstá nebezpečí úniku takovýchto informací, dále pak i přístupu k těmto informacím.

[3] Skála, J.: Právní ochrana osobních údajů v informačních systémech, Právník č. 1/1994.

Počátkem roku 1981 předložila Evropská rada členským státům EHS k podpisu Konvenci o ochraně dat osobnostní povahy v souvislosti s jejich elektronickým zpracováním.

V České republice se v této oblasti přijal zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, jehož účinnost se datuje od 29. dubna 1992.

Informační zákon představuje souhrn základních pravidel pro systematické nakládání s osobními údaji.

Ustanovení paragrafu druhého stanoví, že se Informační zákon vztahuje i na informační systémy založené zvláštním zákonem (např. zákon o živnostenském podnikání, zákon o účetnictví atd).

(Přijetí Informačního zákona vyvolalo nutnost novelizace dalších právních předpisů – zákon č. 154/1994Sb., o Bezpečnostní informační službě, zákon č. 153/1994 Sb., o zpravodajských službách České republiky.)

Informační zákon postihuje právem dosud neupravenou oblast. Proto bylo zcela nezbytné vytvořit pojmový aparát.

Za základní definici důležitou pro aplikaci celého zákona je ustanovení § 3, podle něhož informace, které se vztahují k určité osobě, jsou osobními údaji.

Zákon dále definuje v ustanovení § 15 pojem „zveřejněná informace". Za takovou informaci je nutno považovat informaci uvedenou na veřejnost prostřednictvím hromadných sdělovacích prostředků nebo prostřednictvím elektronických veřejně přístupných informačních služeb.

Fyzické a právnické osoby mohou vystupovat jako kterýkoli z „účastníků výměny informací". Fyzická osoba pak může dále také vystupovat jako „osoba dotčená", avšak za předpokladu, že o této osobě vypovídá informace.

Provozovatelem informačního systému, uživatelem i zprostředkovatelem může být jak fyzická, tak i právnická osoba.

Dále jsou Informačním zákonem definovány pojmy „informační systém", „informační služba", „zpracování informací", „likvidace informace", a „náležitý způsob sběru informací".

Za nejdůležitější ustanovení zákona je možno považovat stanovení povinností jednotlivých subjektů, podílejících se na provozování informačního systému. Jde o tyto subjekty: provozovatel, zprostředkovatel, dále pak fyzické osoby, které přicházejí do styku s informacemi, s nimiž informační systém nakládá.

Základní povinností provozovatele je rozlišovat mezi nakládáním s tzv. senzitivními informacemi a nakládáním s ostatními osobními údaji. Za tzv. senzitivní informace se podle ustanovení Informačního zákona považují ty informace, které vypovídají o osobnosti a soukromí dotčené osoby, jejím rasovém původu, národnosti, politických postojích a členství v politických stranách a hnutích, vztahu k náboženství, o její trestné činnosti, zdraví, sexuálním životě a majetkových poměrech.

Se senzitivními informacemi lze nakládat pouze stanoví-li tak zvláštní zákon, nebo se souhlasem žijící dotčené osoby (projev vůle). Pokud tuto podmínku souhlasu nelze splnit, lze s informací nakládat jen za předpokladu, že bude zachována lidská důstojnost, osobní čest, dobrá pověst a chráněno dobré jméno dotčené osoby. (Nelze toto ustanovení tedy chápat jako absolutní zákaz sběru vysoce senzitivních dat).

Tato omezení se vztahují na jakékoli nakládání se senzitivními informacemi ve smyslu tohoto zákona, tj. na shromažďování, zpracovávání, uchovávání i zpřístupňování informací.

Další povinností provozovatele informačního systému, z hlediska možnosti účinné ochrany práv jednotlivých subjektů před neoprávněným rozšiřováním osobních údajů, je povinnost poskytnout jednou do roka bezplatně, nebo za přiměřenou úplatu kdykoli, každé dotčené osobě na požádání zprávu o informacích o ní uchovávaných v informačním systému, pokud zvláštní zákon nestanoví jinak.

V zákoně jsou konstruovány dva druhy odpovědnosti. Odpovědnost provozovatele vzniká v případě porušení povinností uvedených v zákoně.

Odpovědnost fyzické osoby vzniká v rámci jejího pracovního nebo obdobného poměru nebo v rámci své veřejné či jiné funkce. Uvedené fyzické osoby mají uloženou povinnost mlčenlivosti o těchto informacích a nesmí je bez souhlasu provozovatele zpřístupnit jiným subjektům nebo je využít pro sebe, pokud zvláštní zákon nestanoví jinak. Povinnost mlčenlivosti přetrvává i po skončení pracovního nebo obdobného poměru mezi příslušnou fyzickou osobou a provozovatelem nebo po skončení výkonu funkce povinné osoby.

Informační zákon je orientován výlučně „civilně". Nezakládá trestní odpovědnost, avšak stanoví nároky dotčených osob v případě porušení povinností v zákoně stanovených.

Dotčené osoby se mohou obracet se žádostí o právní ochranu pouze na soudy a důkazy o porušení práva si musí zajistit samy. Postup soudu a účastníků příslušného řízení stanoví občanský soudní řád.

Je třeba zdůraznit, že informační systémy, nakládající s citlivými informacemi podléhají podle zákona povinné registraci, pokud neslouží výhradně pro vnitřní potřebu provozovatele. Z registrace jsou vyloučeny informační systémy nakládající výhradně se zveřejněnými informacemi (zveřejněné informace mohou být i osobní údaje, které zákon chrání, ale které již byly zveřejněny nebo zveřejněny budou).

To tedy znamená, že informační systémy, nakládající s citlivými informacemi podléhají povinné registraci u zvláštního orgánu, který však dosud v českém právu nebyl zřízen (formální požadavek pro zpracovávání osobních údajů – registrace na rozdíl od licence či koncese).

Návrh na zřízení České inspekce existuje již od roku 1992.

Česká inspekce (podle návrhu zákona) je na vládě nezávislý orgán – podobně jako Britský Data Protection Registrar.

Působnost Inspekce se vztahuje na všechny informační systémy provozované na území České republiky, pokrývá oblast státního i soukromého sektoru.

Základními pravomocemi Inspekce je pravomoc dozorová a registrační. Pokud se týče pravomoci dozorové, je inspektor oprávněn v rámci výkonu dozoru nařídit:

- provedení nápravy (pokud provozovatel informačního systému neplní své povinnosti, či zdržení se určitých činností pokud tyto činnosti jsou v rozporu se zákonem) – enforcement notice,
- nařídit ukončení provozu informačního systému – de-registration notice
- oznámit zákaz transferu (jde o zákaz transferu osobních dat za hranice, tj. do určité země, kde není dostatečně zajištěna ochrana dat) – transfer prohibition notice,
- uložit pokutu.

IV.
Závěr

Porovnáním Informačního zákona se Směrnicí[4] Výboru OECD z roku 1980, lze odvodit tyto následující principy:

- princip omezeného sběru
  – Collection-limitation
- princip právní kvality informací (§ 17 písm. c), d) e)
  – Data quality
- princip určitosti informací (§ 17 písm. a), b), g))
  – Purpose–specification
- princip omezeného užití
  – Use-limitation
- princip zabezpečení či ochrany informací (§ 17 písm. i))
  – Security safeguards
- princip individuální účasti (§ 17 písm. l))
  – Individual participation, the individual's right of access to „his" personal data (princip omezený – možnost žádat informace jednou do roka bezplatně nebo kdykoli za úplatu).

[4]Guidelines on the Protection of Privacy and Transborder Flows of Personal Date, 1980. (Guidelines obsahuje 8 principů stanovených pro vnitrostátní aplikaci. Směrnice se vztahuje na osoby fyzické, aplikovatelná v soukromém i státním sektoru).

Literatura:

[1.] **Skála, J.:** *Právní ochrana osobních údajů v informačních systémech,* Právník č. 1/1994.

[2.] **Knapp, V.:** *Právo a informace,* ČSAV Praha 1988.

[3.] **Kirstová, K.:** *Občanskoprávne aspekty slobody prejavu a ochrany individuálnych údajov,* Justičná revue, č. 12/1993.

[4.] *Ochrana dat a právní úprava v České republice,* Sborník referátů a sdělení ze semináře konaného 20. 4. 1993 v Praze, Praha 1993.

* * *

SUMMARY

Protection of Personal Data and Legal Regulation in the Czech Republic

The article deals with legal regulation concerning protection of personal data in the Czech Republic. The first part of the article is devoted to the definition of the term of information. As for the second part of the article, the author deals with the right of information and the protection of privacy in respect of the Charter of Fundamental Rights and Freedoms and the Civil Code. The third part of the work considers the protection of personal data in information systems as ruled by the Act No. 256/1992 Coll. on Protection of Personal Data in Information Systems. As for the concluding paragraphs, the author has tried to briefly compare our Information Act with the Directions of OECD of 1980.