

# Mladá veda

## Young Science



# Mladá veda

## Young Science

### MEDZINÁRODNÝ VEDECKÝ ČASOPIS MLADÁ VEDA / YOUNG SCIENCE

Číslo 2, ročník 11., vydané v júni 2023

ISSN 1339-3189, EV 167/23/EPP

Kontakt: [info@mladaveda.sk](mailto:info@mladaveda.sk), tel.: +421 908 546 716, [www.mladaveda.sk](http://www.mladaveda.sk)

Fotografia na obálke: Saint-Tropez. © Branislav A. Švorc, [foto.branisko.at](http://foto.branisko.at)

#### REDAKČNÁ RADA

*doc. Ing. Peter Adamišín, PhD.* (Katedra environmentálneho manažmentu, Prešovská univerzita, Prešov)

*doc. Dr. Pavel Chromý, PhD.* (Katedra sociálnej geografie a regionálneho rozvoje, Univerzita Karlova, Praha)

*Mgr. Jakub Köry, PhD.* (School of Mathematics & Statistics, University of Glasgow, Glasgow)

*prof. Dr. Paul Robert Magocsi* (Chair of Ukrainian Studies, University of Toronto; Royal Society of Canada)

*Ing. Lucia Mikušová, PhD.* (Ústav biochémie, výživy a ochrany zdravia, Slovenská technická univerzita, Bratislava)

*doc. Ing. Peter Skok, CSc.* (Ekomos s. r. o., Prešov)

*prof. Ing. Róbert Štefko, Ph.D.* (Katedra marketingu a medzinárodného obchodu, Prešovská univerzita, Prešov)

*prof. PhDr. Peter Švorc, CSc.*, predseda (Inštitút histórie, Prešovská univerzita, Prešov)

*doc. Ing. Petr Tománek, CSc.* (Katedra verejnej ekonomiky, Vysoká škola báňská - Technická univerzita, Ostrava)

*Mgr. Michal Garaj, PhD.* (Katedra politických vied, Univerzita sv. Cyrila a Metoda, Trnava)

#### REDAKCIA

*Mgr. Branislav A. Švorc, PhD.*, šéfredaktor (Vydavateľstvo UNIVERSUM, Prešov)

*Mgr. Martin Hajduk, PhD.* (Banícke múzeum, Rožňava)

*PhDr. Magdaléna Keresztesová, PhD.* (Fakulta stredoeurópskych štúdií UKF, Nitra)

*RNDr. Richard Nikischer, Ph.D.* (Ministerstvo pro místní rozvoj ČR, Praha)

*PhDr. Veronika Trstianska, PhD.* (Ústav stredoeurópskych jazykov a kultúr FSS UKF, Nitra)

*Mgr. Veronika Zuskáčová* (Geografický ústav, Masarykova univerzita, Brno)

#### VYDAVATEĽ

Vydavateľstvo UNIVERSUM, spol. s r. o.

[www.universum-eu.sk](http://www.universum-eu.sk)

Javorinská 26, 080 01 Prešov

Slovenská republika

# RIZIKÁ PORUŠOVANIA PRÁVA NA OCHRANU OSOBNÝCH ÚDAJOV AKO SÚČASŤ KRÍZY DEMOKRACIE

THE RISKS OF VIOLATION OF THE RIGHT TO DATA PROTECTION AS PART  
OF THE CRISIS OF DEMOCRACY

**Viktória Ferková<sup>1</sup>**

Autorka pôsobí ako interná doktorandka na Fakulte verejnej správy Univerzity Pavla Jozefa Šafárika v Košiciach. Vo svojom výskume (resp. dizertačnej práci) sa venuje problematike ochrany osobných údajov v zmysle všeobecného nariadenia GDPR, predovšetkým v podmienkach územnej samosprávy Slovenskej republiky.

The author works as an internal doctoral student at the Faculty of Public Administration of the University of Pavel Jozef Šafárik in Košice. In her research (or dissertation thesis), she deals with the issue of personal data protection in the sense of the general GDPR regulation, especially in the conditions of the territorial self-government of the Slovak Republic.

## **Abstract**

By progressing the development of the cyber space and communication technologies, become personal data easily accessible and easily disseminated. It is important how the state and companies are able to process personal data so that the rights of individuals are not violated. Protection of personal data is closely related to security, respect and protection of the right to private and family life. Personal data belong to the elements that construct a person's social identity. All citizens have the right to protection against unauthorized publication, collection, or other misuse of information about them by the state or private individuals. In the context of the fact that politics is a tool that serves to expand freedom, but on the other hand to suppress it, the aim of this article will be to analyze the risks of violating the right to protect personal data in relation to democracy and its principles.

Key words: personal data protection, GDPR, democracy

## **Abstrakt**

Na základe pokroku vo vývoji kybernetického priestoru a komunikačných technológií sa osobné údaje stávajú ľahko dostupnými a jednoducho šíriteľnými. Je dôležité, ako štát a firmy dokážu spracúvať osobné údaje, aby nedochádzalo k porušovaniu práv fyzických osôb. Ochrana osobných údajov úzko súvisí s bezpečnosťou, rešpektovaním a ochranou práva na

---

<sup>1</sup> Adresa pracoviska: Mgr. Viktória Ferková, Katedra verejnoprávnych disciplín, Fakulta verejnej správy, Univerzita Pavla Jozefa Šafárika v Košiciach, Popradská 66, 040 11 Košice  
E-mail: viktoria.ferkova@student.upjs.sk

súkromný a rodinný život. Osobné údaje patria k prvkom, ktoré konštruujú sociálnu identitu človeka. Všetci občania majú právo na ochranu pred neoprávneným zverejňovaním, zhromažďovaním alebo iným zneužívaním informácií o nich zo strany štátu alebo súkromných osôb. V kontexte toho, že politika je nástrojom, ktorý slúži na rozširovanie slobody, no na druhej strane na jej potláčanie, cieľom tohto článku bude analyzovať riziká porušovania práva na ochranu osobných údajov vo vzťahu k demokracii a jej princípov.

**Kľúčové slová:** ochrana osobných údajov, GDPR, demokracia

## Úvod

*„Schopnosť človeka pre spravodlivosť umožňuje demokraciu, ale ľudský sklon k nespravodlivosti robí demokraciu nevyhnutnou.“ (Reinhold Niebuhr, 1944)*

Jedným z dôsledkov kontinuálneho progresu rozvoja informačno-komunikačných technológií a online priestoru sa stala jednoduchá dostupnosť a šíriteľnosť osobných údajov. Nakoľko je ochrana osobných údajov výzvou celospoločenského charakteru, obzvlášť dôležitá je schopnosť štátov i súkromných spoločností spracovať dotknuté údaje spôsobom nenarúšajúcim práva jednotlivcov. V kontexte toho, že politika má slúžiť k rozširovaniu slobody, ale na druhej strane predstavuje nástroj k jej potláčaniu, bude cieľom tohto článku analýza a ohodnotenie rizík nerešpektovania a porušovania práva na ochranu osobných údajov a legislatívy o GDPR vo vzťahu k demokracii a jej princípom.

Osobné údaje majú v poslednom desaťročí predovšetkým digitálny charakter. Tým, že sú ukladané, zdieľané a spracovávané v kyberpriestore, musia byť podrobené špecifickej kontrole, a ich spracovanie či ochranu ovplyvňujú na jednotlivých úrovniach rôzne inštitúcie a legislatíva.

Celá spoločnosť každodenne zdieľa osobné údaje – v kontexte nákupných zvykov, bankových informácií, lekárskeho záznamov až po súkromné fotografie. Dáta sa postupom času stali najcennejším zdrojom súčasného hospodárstva, nevyhnutnosťou každodenného života a sú zlatom 21. storočia (Jourová, 2018). Internet častokrát býva opisovaný pozitívnymi metaforami: ako digitálny priestor vytvárajúci z celého ľudstva veľkú, globálnu rodinu, ako estrádne a podmaňujúce miesto a ako svet neobmedzených možností. Táto deskripcia avšak zatajovaním negatívnych stránok internetu neodráža realitu.

Lektor kritického myslenia Ján Markoš charakterizoval internet takto: „Internet je teplý tropický oceán, na ktorého vlnách môžeme surfovať od rána do večera. Jemná a inteligentná sieť, ktorá pokrýva celý svet a spája v ňom aj tie najvzdialenejšie miesta do jediného celku. Globálna dedina, v ktorej sú si ľudia zo všetkých kontinentov a národov blízko. Kyberpriestor, nový rozmer existencie darovaný ľudskej rase. Virtuálne miesto podobné raju, v ktorom môžeme byť kýmkoľvek...internet je ako stoka. Každý z nás doň odhadzuje tisíce útržkov informácií, mnohé z nich celkom irelevantné, ale ďalšie veľmi osobné a citlivé. Tento informačný odpad pláva v kalnom prúde digitálneho kanála nevedno kam, do cudzích rúk. Možno klesne na dno a tam čaká. Mesiace, roky. Možno ho niekto vyloví z prúdu a starostlivo uschová. Internet má sloniú pamäť. Nezabúda“ (2019, s. 189).

V súčasnom globalizovanom svete plnom informácií tak potreba ochrany osobných údajov ako súčasť základných ľudských práv nadobúda stále dôležitejší rozmer vzhľadom na

to, že zneužívanie osobných údajov dokáže vo významnej miere narušiť demokraciu a jej fundamentálne princípy. Môže teda nastať situácia, že členské štáty budú častejšie zlyhávať pri ochrane ľudskej dôstojnosti, legitímnych záujmov a základných práv. O naštrbení demokracie môžeme hovoriť v kontexte toho, že kvôli vysokému stupňu digitalizácie a obchádzaniu právnych predpisov zo strany technologických gigantov a vlád môže dochádzať k nerešpektovaniu základných ľudských práv a slobôd voči používateľom internetu. Konkrétne môžeme poukázať na porušenie demokratických princípov takým spôsobom, že potenciálne môže dôjsť k narušeniu princípu slobody človeka, zásady rovnosti, k porušeniu pravidla služby štátnej moci všetkým občanom, či ochrany práv občanov zo strany štátu.

V nasledujúcich častiach článku si priblížime aspekty technologickej spoločnosti ohrozujúce demokratické fungovanie, zmysel ochrany osobných údajov, súčasné riziká spojené s ochranou osobných údajov a aktuálne legislatívne zmeny, týkajúce sa zvýšenia tejto ochrany na národnej úrovni a na úrovni Európskej únie.

### **Od postindustrializmu k technologickej spoločnosti**

Postindustriálne zmeny a inovácie stoja za významnými zmenami v spoločnosti ako celku. Inovácie majú významný vplyv aj na rozvoj informácií a vedomostí a rovnako aj na vznik interaktívnych kapacít počítačovej technológie, ktorá používa a spracováva informácie v predtým nepoznaných rozmeroch (Zuboff, 1988).

Je preto nevyhnutné sledovať aj to, ako a či sa v súvislosti s tým mení aj sloboda obyvateľstva. Kým sa v postindustriálnej spoločnosti hovorilo skôr zvyšovaní všeobecnej slobody jednotlivcov a o posilňovaní demokratických princípov, pri prechode na technologickú spoločnosť sa viac začali objavovať totalitaristické a iné tendencie, ktoré slobodu eliminujú alebo obmedzujú. Ľudia sú totiž kvôli technologickému pokroku, ktorý sa spája so spracovávaním rozličných dát bez regulácii, postupne zbavovaní svojej slobody (Nelson a Cooperman, 1998).

V tomto zmysle je potrebné poukázať na vzťah, ktorý vzniká medzi politickými štruktúrami a veľkými súkromnými organizáciami. Na jednej strane vzťahu stoja korporáty, ktoré majú na základe technologického rozvoja schopnosť robiť čím ďalej tým viac pre dosahovanie väčších ziskov, a to až na takej úrovni, že ovplyvňujú správanie sa občanov (spotrebiteľov). Na druhej strane vzťahu figuruje štát, ktorý zápasí s problémom prioritizácie - či uprednostniť budovanie priaznivých podmienok pre rozvoj ekonomického rastu a podporiť súkromný sektor alebo uprednostniť ochranu na druhej strane stojacej občianskej spoločnosti, ktorej sloboda je týmto spôsobom narúšaná.

Demokratická spoločnosť a slobodný priestor internetu predstavujú úrodnú pôdu pre smerovanie spoločnosti k zvyšovaniu kontroly nad občanmi a k ich všeobecnej manipulácii. Technológie a internet tak vychádzajúc z údajov virtuálneho sveta umožňujú kvantifikovanie rôznorodých aspektov o jedincoch a ich správaní. Vďaka technologickému napredovaniu a schopnosti čoraz efektívnejšie zbierať a spracovávať dáta cez internet, sa celá spoločnosť stáva manipulovanou, sledovanou a ovplyvňovanou (Zuboff, 2019).

Keď vezmeme do úvahy fungovanie internetových algoritmov platí, že čím viac vstupov - dát, používateľ poskytne, tým presnejšie a lepšie je možné tieto vstupy vyhodnotiť.

Následne sú dáta efektívnejšie využité v spoznávaní a predvídaní správania sa jednotlivcov a rovnako aj spoločnosti. Týmto spôsobom dokážu byť digitálne technológie rôznorodými spôsobmi intervenované do ekonomických a sociálnych štruktúr spoločnosti (Denny, 2020).

V prostredí existencie veľkých súborov dát a v prípade prístupu k nim len zo strany určitých skupín obyvateľstva, môžeme sledovať sukcesívne prehlbovanie závažného „defektu“ demokracie v nastavení spoločnosti, ktorá už ďalej nemá perspektívu manifestovať svoje hodnoty ako za normálnych a bežných podmienok.

Východiskovým problémom je, že v internetovom priestore a v priestore nových technológií dlhodobo absentovali dostačujúce regulácie, čo bolo dôvodom, kvôli ktorému sa jednotlivci a inštitúcie stali obeťou tých, ktorí si túto medzeru v slobodnom a demokratickom priestore všimli, a zúročili ju vo svoj prospech. Takýto nový spôsob práce s dátami je nezvratnou konzekvenciou technologického pokroku, ktorý v podstate prebieha mimo pravidiel spoločnosti. Následné neskoré reakcie štátnych inštitúcií na tento rozvoj majú nebezpečné dôsledky na celkové fungovanie spoločnosti či na demokraciu ako takú (Zuboff, 2015). Preto je nevyhnutné či už na úrovni Európskej únie alebo na národnej úrovni, venovať ochrane osobných údajov náležitú pozornosť.

### **Právo na ochranu osobných údajov a všeobecné nariadenie GDPR**

Ako sme naznačili už v úvode tohoto článku, právo na ochranu osobných údajov sa zaradzuje k základným ľudským právam, garantovaným primárnymi prameňmi práva Európskej únie. Ide konkrétne o čl. 6 a čl. 39 Zmluvy o Európskej únii, čl. 16 Zmluvy o fungovaní Európskej únie a čl. 8 Charty základných práv Európskej únie. Na úrovni Slovenskej republiky je právo na ochranu osobných údajov súčasťou čl. 19 Ústavy. Súčasná fundamentálna úprava tohto práva sa nachádza v Nariadení Európskeho parlamentu a Rady 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (General Data Protection Regulation), ktorým sa ruší smernica 95/46/ES. Okrem Ústavy na legislatívu Európskej únie suplementárne nadväzuje aj slovenská národná legislatíva v znení zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a Vyhláška úradu na ochranu osobných údajov SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov. Práve táto dvojica právnych predpisov sa na úrovni Slovenskej republiky stala základom ochrany osobných údajov.

Na Svetovom ekonomickom fóre v Davose vyslovil George Soros myšlienku o existencii eventuálnych prípadov straty slobody mysle, kedy by mohli mať ľudia vyrastajúci v digitálnom veku problémy pri jej opätovnom získavaní, čo by mohlo mať ďalekosiahle politické následky - keďže ľudia bez slobody mysle môžu byť veľmi ľahko manipulovaní (George Soros, 2018). V tomto čase však neočakával, že jeho slová sa stanú v roku 2018 „prorockými“, a svet prežije búrlivý technologický rozvoj, a to aj v podobe prijatia všeobecného nariadenia o ochrane osobných údajov.

General Data Protection Regulation (ďalej len „GDPR“), tzv. zlatý štandard ochrany osobných údajov nadobudol svoju platnosť 25. mája 2018 a je nariadením, ktorým sa občanom Európskej únie naskytuje väčšia vedomosť a kontrola nad tým, ktoré subjekty a akým spôsobom prístupujú k použitiu a spracovaniu dát o ich osobe.

GDPR platí pre každého, kto koncentruje a spracováva osobné údaje fyzických osôb (napríklad zamestnancov, zákazníkov, klientov, obyvateľov, žiakov, pacientov, návštevníkov internetových stránok a pod.). Ochrana osobných údajov sa teda vo všeobecnosti vzťahuje na všetkých, bez ohľadu na to, či majú status prevádzkovateľa spracovávajúceho osobné údaje, alebo sú v pozícii dotknutej osoby, ktorej osobné dáta sú spracúvané. Táto forma právnej ochrany teda zasahuje do väčšiny oblastí ľudského života (Mesarčík, 2020).

Základnou úlohou nariadenia GDPR, ako aj zákona o ochrane osobných údajov je, aby spracúvanie a ochrana osobných údajov v súlade s ich ustanoveniami neboli len reprezentantmi právnych pojmov, ale aj praktickou činnosťou viditeľnou v prostrediach sprostredkovateľov a prevádzkovateľov, bez ohľadu na to, či ide o súkromné spoločnosti alebo štátne orgány. Prostriedkom zabezpečujúcim plnenie tejto úlohy sú predovšetkým práva dotknutých osôb, ktoré boli nariadením konkretizované a spresnené, a ktoré dávajú každej dotknutej fyzickej osobe v prostredí konkrétneho sprostredkovateľa alebo prevádzkovateľa príležitosť aktívne sa zaujímať o spracovávanie ich osobných dát (Úrad pre ochranu osobných údajov Slovenskej republiky, 2021).

Európska únia prijala GDPR z adekvátnych a nevyhnutných dôvodov, pričom sa nastavením predvídateľných celosvetových pravidiel stala medzinárodným lídrom v presadzovaní ochrany osobných údajov pre európske spoločenstvo. Podmienkou nariadenia je, že ho všetky členské štáty i súkromné organizácie musia pri výkone svojej práce rešpektovať (Bonefeld-Dahl, 2021). Únia tiež spolu s jej členskými štátmi úpravou pravidiel vnútorného trhu hovorí o dátovej suverénite a poukazuje pri tom na fakt, že sa dáta v posledných rokoch stali významným zdrojom hospodárskeho rastu, konkurencieschopnosti, inovácií, vytvárania pracovných miest či spoločenského pokroku. Charakter toho, ako štáty a Európska únia ako celok organizujú prístup k údajom a k ich použitiu, taktiež determinuje ich inovačnú kapacitu do budúcnosti (Yar, 2021).

Aj napriek tomu, že sa GDPR stalo globálnym štandardom ochrany osobných údajov paralelne čelí problémom, ktoré by si žiadali revíziu nariadenia. Medzi najväčšie problémy možno zaradiť presadzovanie nariadenia. Rozsiahlejšia reforma centralizovanej kontroly a presadzovania najmä voči veľkým globálnym firmám by mohla túto situáciu výrazne napraviť.

Medzi problematiku môžeme zaradiť aj to, že v súčasnosti rieši prípady cezhraničného porušovania nariadenia národný alebo regionálny regulátor v štáte, v ktorom má daná firma oficiálne hlavné sídlo a uplatňuje sa pritom prístup one-stop-shop. Vedúci dozorný orgán v tomto prípade koordinuje úkony iných dotknutých dozorných orgánov v súlade s čl. 60 - 62 nariadenia (vzájomné poskytovanie informácií, vzájomná pomoc, vykonávanie spoločných operácií). Tento prístup býva považovaný za neefektívny, avšak viacero európskych hráčov nepovažuje „otváranie“ nariadenia po tak krátkom čase od nadobudnutia platnosti za vhodné riešenie (Manancourt, 2021).

Môžeme teda tvrdiť, že zákonná ochrana súkromia a osobných údajov občanov sa postupne zvyšuje, ale na druhej strane, schopnosť vlád či firiem zhromažďovať kolosálne množstvá dát a následne ich analyzovať sa zvyšuje tiež, ale podstatne rýchlejšie, čo môže spôsobiť významné problémy.

## **Riziká pri poskytovaní osobných údajov a známe prípady porušenia práva na ochranu osobných údajov potenciálne prispievajúce ku kríze demokracie**

Na Svetový deň ochrany osobných údajov priniesol Európsky výbor informácie o tom, ako sa od prijatia GDPR v Európskej únii modifikovalo vnímanie ich ochrany. Za najspornejšie je vnímané zneužívanie osobných dát v cielenej reklame, čoho sa v súčasnosti týka viac než 100 tisíc sťažností. Väčšina z nich súvisela s činnosťami ako rozposielanie propagačných emailov, telemarketing, či sledovanie užívateľov prostredníctvom videa alebo CCTV kamier (t.j. prostredníctvom uzavretého televízneho okruhu, kde sa signál z kamier prenáša na uzavretý počet užívateľov) (Yar a Stolton, 2019).

Fakt, že sú vlády a firmy schopné zhromaždiť kolosálne množstvo osobných dát, so sebou prináša mnoho rizík. Bežní používatelia internetu sú pritom vystavení trom hlavným hrozbám:

1. tendenciou vlád a firiem je na základe nadobudnutých informácií o konkrétnom človeku ukazovať hlavne to, čo daný človek chce vidieť (resp. si myslia, že to chce vidieť) - čím krivia jeho percepciu reality,
2. informácie získané o konkrétnom človeku prostredníctvom internetu môžu slúžiť ako kompromitačné materiály či nástroje na zastrasovanie,
3. tzv. „veľké dáta“ sú pre bežných používateľov nezrozumiteľné a neprehľadné natoľko, že sa zo strany informovanejších a mocnejších subjektov môžu stať prostriedkom rozličných manipulácií (Markoš, 2019).

## **Príklady najznámejších prípadov porušenia práva na ochranu osobných údajov**

Celoeurópsky známym problémom bolo v oblasti porušovania osobných údajov napríklad nezákonné využívanie údajov o voličoch, ktoré boli zneužitú na ovplyvňovanie volieb (hlasovanie o brexite vo Veľkej Británii v roku 2016). V tomto prípade došlo k psychologickému manipulácii voličov za pomoci ich vlastných osobných údajov, čo možno považovať za hrozbu pre demokraciu. Vo Veľkej Británii bol v tomto čase porušený britský Zákon o ochrane údajov a kreovali sa veľké, politicky významné databázy o voličoch, ktorí boli pred referendum neprestajne ovplyvňovaní. Pri tendenciách k zintenzívneniu personalizovaného zacielenia voličov bola odignorovaná nielen ochrana osobných údajov, ale rovnako aj zásady o financovaní politických kampaní. Od GDPR sa preto v súčasnosti očakáva, že sa bude zaoberať aj profitovaním zo získania osobných údajov s cieľom vyhrať voľby. Riešením by mohlo byť zvýšenie transparentnosti a efektívneho dohľadu pretože sankcie, aj keď sú vysoké, nie sú odstrašujúce v dostatočnej miere. Naopak, zvýhodňujú finančne nezávislých kandidátov či ich sponzorov. Nevyhnutné sú aj kroky pre kontrolu zahraničných aktérov, ktorí môžu rôznymi spôsobmi ovplyvniť parlamentné voľby - národné aj európske (vybudovaním rozsiahlych databáz voličov, vytváraním fiktívnych spoločností, poskytovaním darov a služieb a pod.), a ktorých motívy destabilizujú demokratické inštitúcie a spoločnosti, ovplyvňujú spôsob riadenia štátu a podporujú vlastné politické ciele (Byström, 2018).

Osobné údaje internetových používateľov poháňajú rovnako aj čoraz lukratívnejší miliardový obchod s online reklamou, v rámci ktorého sa strata súkromia považuje ako cena za bezplatné využívanie internetových služieb. Na druhej strane však incidenty s únikom



osobných dát, netransparentnou manipuláciou s dátami a so skrytou reklamou otvorili otázku poctivosti takéhoto obchodovania. Na lapsusy technologických gigantov často poukazujú aj spotrebiteľské organizácie. Sťažnosti sa týkajú napríklad sociálnej siete TikTok, ktorý nedostatočne chráni detských používateľov siete pred škodlivým obsahom a skrytou reklamou. Napríklad v Holandsku táto platforma čelí hromadnej žalobe za porušenie GDPR kvôli tomu, že neplnoletí používatelia sú nedostatočne informovaní o tom, ako sú využívané ich osobné údaje. TikTok tiež údajne porušuje zákon tým, že neoveruje vek svojich používateľov a nedáva rodičom nástroje na kontrolu obsahu, ktorý deti sledujú (Zmušková, 2021).

Sťažnosti sa týkajú taktiež napríklad mobilnej aplikácie WhatsApp, ktorý má príliš tlačiť na akceptovanie netransparentných podmienok používania. WhatsApp svojich užívateľov zaťažuje naliehavými notifikáciami o akceptácii nových zmluvných podmienok, pod dojmom, že aplikácia stratí niektoré z jej funkcionalít, ak ich jej užívatelia tieto podmienky neprijmú (Spoločnosť ochrany spotrebiteľov, 2021).

Najväčší problém s obchádzaním GDPR má spoločnosť Meta, ktorá pre porušenie nariadenia čelila niekoľkým žalobám. Posledné rozhodnutie pre porušenie všeobecného nariadenia voči tejto spoločnosti je zo 4. januára 2023 a týka sa rozporu personalizovanej reklamy s európskym právom. Meta nedodržala povinnosti transparentnosti GDPR, a z jej právneho základu podľa rozhodnutia nie je jasné, na aké účely sa využívajú osobné údaje používateľov (Data Protection Commission, 2023).

Na týchto príkladoch môžeme vidieť, že politici a aj jedny z najznámejších technologických spoločností pôsobiacich v online priestore obchádzajú pravidlá GDPR. Deje sa tak bez ohľadu na hrozbu miliónových sankcií. Zisk – či už politický alebo finančný býva primárnym cieľom dotknutých subjektov a ochrana ľudských práv v tejto oblasti nie je mnohokrát kladená na popredné miesta v rebríčku ich hodnôt (aj keď ju deklarujú).

### **Sledovanie občanov na základne poskytovania osobných údajov**

Poskytovanie osobných údajov sociálnym sieťam a šírenie fotografického obsahu na internete môže byť využité napríklad aj na sledovanie občanov. Konkrétne môžeme spomenúť detekciu tvári na fotografiách, ktorá rozpozná konkrétnu osobu na obrázku podľa jej predchádzajúcich fotografií (sociálna sieť Facebook túto funkciu využíva od roku 2017), a obdobný „projekt“, ktorý už prešiel pilotným testom v päťmiliónovom meste Ku-i-ang plánuje spustiť aj Čínska vláda, ktorá pripravuje databázu tvári svojich občanov. Na základe tejto databázy bude možné identifikovať kohokoľvek v priebehu niekoľkých sekúnd. Čínske úrady prínos projektu argumentujú tým, že databáza tváří v spolupráci s mnohopočetnou sieťou kamier umožní za krátky čas lokalizáciu a odhalenie páchatel'ov trestných činov v uliciach Číny. Otázkou je, či by bude tento projekt využívaný na deklarovaný účel, alebo bude len ďalším z nástrojov na sledovanie občanov v nedemokratických krajinách.

Pre organizácie spracúvajúce dáta je výsadou aj diferencovanie polohy používateľov mobilných telefónov - keďže sa smartfóny automaticky pripájajú k GPS, ktoré je najbližšie k vysielateľu mobilného operátora, či k blízkym Wifi sieťam. Následne, je po spracovaní týchto dát možné (na metre presne) zistiť, kde sa konkrétny mobilný telefón nachádza. Takéto

rozpoznávanie polohy napríklad napomohlo k zisteniu, že v hlavnom meste Slovenska, v Bratislave žije o 250 000 viac ľudí, ako v nej má oficiálny trvalý pobyt.

Ďalšími údajmi o používateľoch internetu disponujú trackingové programy zabudované na webových stránkach. Ako príklad môžeme uviesť BlueKai alebo DoubleClick Floodlight, ktoré asistujú pri efektívnejšej inzercii, ďalej napríklad Chart Beat, ScoreCard Research a Beacon modelujúce štatistiky o správaní internetových užívateľov, a programy ako je Facebook Connect, ktoré monitorujú užívateľskú činnosť vo vzťahu k sociálnym sieťam. „Špiónmi“ v smartfónoch sú aj rôzne nainštalované aplikácie. Až 70% mobilných aplikácií, posiela pravidelne údaje o ich užívateľoch tretej strane (napríklad Facebooku a Googlu) (Markoš, 2019).

Problémovými sú dokonca aj tie domáce spotrebiče, ktoré sú schopné pripojiť sa automaticky na internet. Kávovar napríklad napovedá o tom, kedy vstávame. Zapnutá televízia hovorí o tom, či sme doma a odкрýva aj zaužívané návyky o tom, čo a kedy v televízii sledujeme. Robotické vysávače vedia vytvoriť dôkladnú mapu bytu a elektrické zubné kefky napojené na Wifi, dokážu podať na sekundu presné informácie o tom, ako dlho si umývame zuby aj niekomu, kto je vzdialený tisícky kilometrov. Ide pri tom o informácie, ktoré sú užitočné pre reklamné agentúry. Bolo tiež zistené, že prístroje napojené na internet so svojimi centrálnymi komunikujú neustále, a to bez ohľadu na to, či sú ich používatelia doma alebo či sú zapnuté (Hill a Mattu, 2018).

### **Očakávané a súčasné legislatívne zmeny na úrovni Európskej únie a Slovenskej republiky v oblasti ochrany osobných údajov**

Veľké technologické firmy doposiaľ čelili žalobám za spomínané porušenie práva na ochranu osobných údajov a za porušenie iných ustanovení spotrebiteľského práva (napríklad za nekalé zmluvné podmienky a obchodné praktiky) iba v niekoľkých členských štátoch, avšak od polovice roka 2023 ich bude možné podávať vo všetkých štátoch Európskej únie, vrátane Slovenskej republiky, a to na základe smernice o kolektívnych žalobách. Kolektívna žaloba podľa novej smernice by mala byť najlepšou cestou, ako sa dostať k odškodnému za porušenie spomínaných práv (Európsky parlament a Rada, 2020).

Európska únia tiež prijala zákon o dátach (The Data Act), ktorý má zaistiť prístup pre využívanie dát za účelom výskumu alebo na tvorbu inovatívnych produktov a služieb. Cieľom Európskej dátovej stratégie je vytvorenie viacerých „dátových priestorov“ (napríklad pre energetiku, výrobný priemysel a zdravotníctvo), v ktorých bude zaručené zdieľanie dát medzi rôznymi aktérmi v rámci viacerých sektorov. Tento zákon o dátach dáva možnosť toku dát prostredníctvom vytvorených mechanizmov interoperability a zdieľania (Cullen International, 2022).

V Bruseli v súčasnosti rezonuje aj debata o pripravovanej regulácii o správe dát (Data Governance Act), ktorá predstavuje medziodvetvový nástroj. Jeho cieľom je sprístupniť v rámci Európskej únie viac údajov, a to reguláciou opätovného použitia verejne chránených dát, posilnením zdieľania údajov prostredníctvom regulácie nových sprostredkovateľov údajov a podporou zdieľania údajov na altruistické účely (Európska komisia, 2022).

Ak sa pozrieme na Slovenskú republiku, predovšetkým pandémie poukázala na problém, ktorý má štát s dátami. Rezorty pri otázkach o dátovej politike apelujú väčšinou na ministerstvo informatizácie, ktorému však chýbajú jasné kompetencie.

Značnou pomocou by mohol byť pripravovaný zákon o údajoch. V rámci Európskej únie ide o pomerne inovatívnu myšlienku v oblasti dátovej politiky, avšak na našej národnej úrovni čelí stovkám pripomienok. Zákon má reflektovať na aktuálny vývoj vo sfére informačných technológií verejnej správy v súlade s Európskou dátovou stratégiou, ktorú Európska Komisia predstavila v roku 2020. V porovnaní s GDPR táto legislatíva zvolila princíp zdola nahor a manažuje iba verejné dáta v správe štátu. Cieľom zákona bude okrem iného všeobecné nastavenie dátového manažmentu verejnej správy (MIRRI SR, 2021).

Ministerstvo informatizácie taktiež spustilo projekty, ktorých účelom je zjednodušiť výmenu a sprístupňovanie údajov. Konkrétne ide o angažovanie nových inštitúcií a zaisťovanie nových údajov, ktoré si budú medzi sebou vymieňať štátne orgány prostredníctvom Informačného systému Centrálnej správy referenčných údajov (IS CSRÚ), a teda o dátovú integráciu a vytvorenie nových integračných väzieb. Podstata CSRÚ spočíva v tom, že občan alebo firma poskytne svoje údaje štátu len raz (princíp „jedenkrát a dost“), pričom následnú distribúciu údajov inštitúciám, ktoré ich pre konkrétne konanie vyžadujú, zabezpečia informačné systémy verejnej správy zdieľajúce osobné údaje integráciou na služby systému CSRÚ (Centrálny metainformačný systém verejnej správy SR, 2021).

Ďalšími projektmi majú byť sprístupňovanie vybraných údajov občanom (údaje, ktoré o nich štát vedie), a tiež vývoj technologickej platformy, tzv. „konsolidovanej analytickej vrstvy“, cez ktorú budú analytické útvary v štáte vytvárať dátové analýzy a modely (Centrálny metainformačný systém verejnej správy SR, 2022).

Od novembra 2022 na Slovensku platí aj nový zákon o elektronických komunikáciách, ktorého cieľ spočíva vo výraznom obmedzení množstva nevyžiadaných telefonátov. Je ním implementovaná smernica Európskeho parlamentu a Rady EÚ o kódexe elektronickej komunikácie, ktorá zdôrazňuje ochranu koncových užívateľov a v prípade nesplnenia konkrétnych pravidiel posúva reklamné a iné nežiadúce hovory mimo zákon (NRSR, 2021). Takisto by mal vzniknúť aj register, na ktorý občania budú môcť registrovať svoje telefónne čísla, v prípade, že nebudú chcieť prijímať žiadne reklamné či iné obťažujúce telefonáty (Hochel, 2021).

Ako už bolo vyššie spomenuté, pre GDPR bola najväčšou skúškou pandémie Covid-19. Keďže veľká časť verejnosti považovala zásahy a obmedzenia zo strany štátu za nezákonné a problematické. V tejto časti článku si priblížime dôvody a argumenty vládnych obmedzení súvisiace s osobnými údajmi a ich ochranou počas pandémie.

GDPR pozná právne dôvody umožňujúce zamestnávateľom a oprávneným orgánom verejného zdravotníctva spracovávať osobné údaje v súvislosti s epidémiami bez toho, aby získali súhlas dotknutých osôb. Na to, aby bolo zaručené zákonné spracúvanie osobných údajov, bolo potrebné zohľadniť určité aspekty a vo všetkých prípadoch upozorniť na to, že akékoľvek opatrenie prijaté v súvislosti so spracovaním osobných údajov počas pandémie muselo rešpektovať všeobecné právne zásady a nemohlo byť nezvratné. Krízová situácia je totiž právnym stavom, ktorý môže legitimovať obmedzovanie slobôd, ale len za predpokladu,

že tieto obmedzenia sú primerané a obmedzené trvaním krízovej situácie (Úrad na ochranu osobných údajov Slovenskej republiky, 2021).

Článok č. 88 nariadenia GDPR, ktorý sa týka spracovania osobných údajov v súvislosti so zamestnaním poznamenáva, že členské štáty by mali chrániť ľudskú dôstojnosť dotknutej osoby, legitímne záujmy a základné práva. Údaje, ktoré sa týkajú zdravia zaradzujeme medzi tzv. osobitnú kategóriu osobných údajov. GDPR na jednej strane ustanovuje všeobecný zákaz pre spracúvanie tejto kategórie osobných údajov, zároveň však implikuje katalóg výnimiek, v ktorých je možné túto kategóriu spracovávať. Bez existencie výnimiek by spracúvanie údajov súvisiacich so zdravím zamestnancov nebolo považované za zákonné. To znamená, že by bolo realizované v rozpore s pravidlami GDPR (Konvit, 2020). Je teda potrebné poukázať na to, že osobné údaje môžu byť spracovávané len vtedy, ak je ich spracovanie argumentované vopred determinovaným účelom, za súčasnej existencie minimálne jedného zo šiestich vymedzených právnych základov, a to:

- a) súhlasu dotknutej osoby,
- b) splnenia zákonnej povinnosti,
- c) plnenia zmluvy s dotknutou osobou (plnenie povinností zamestnávateľa v oblasti pracovného práva v súvislosti s ochranou zdravia a bezpečnosti pri práci zamestnancov),
- d) existenciou životne závažného záujmu,
- e) existenciou oprávneného záujmu
- f) existenciou verejného záujmu v oblasti verejného zdravia (na základe práva Európskej únie alebo práva členského štátu, pričom v tejto situácii dokonca nie je potrebné vyžadovať súhlas jednotlivcov) (Ravas a Milošovič, 2021).

Na základe legislatívy o ePrivacy bola taktiež ustanovená zásada, že prevádzkovateľ (najčastejšie telekomunikačný operátor), môže využívať údaje o polohe ak sú anonymné, alebo ak mu bol poskytnutý súhlas dotknutej osoby. Iba v prípade, že to nie je možné, legislatíva ráta s výnimkou vo veci otázok verejnej a národnej bezpečnosti. Európska únia však žiadala členské štáty aby takto postupovali s prihliadnutím na predpoklady primeraných opatrení v demokratickej spoločnosti (Yar, 2020).

Na Slovensku došlo k legislatívnym zmenám predovšetkým počas tretej vlny pandémie ochorenia Covid-19, a to konkrétne v podobe zákona č. 412/2021 Z. z., ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s treťou vlnou pandémie ochorenia Covid-19. Zákon priniesol zmeny, ktoré sa týkali najmä Zákonníka práce a Zákona o ochrane, podpore a rozvoji verejného zdravia. Tieto zmeny sa priamo dotýkali aj spracúvania osobných údajov. Zákonník práce priniesol počas pandemickej situácie viacero zmien, čím sa stal primárnym právnym základom pre spracovanie citlivých osobných údajov, týkajúcich sa zdravotného stavu zamestnancov (Nagyová, 2021).

Legislatívne zmeny prijaté počas pandémie vyvolali množstvo otázok. Predovšetkým tých, ktoré sa týkali etiky využívania údajov občanov zdanlivo širokým spôsobom, keďže bol verejný záujem postavený na prvé miesto, pričom naopak súkromie jednotlivcov bolo na opačnom konci rebríčka. V prípade legislatívnych zmien, ktoré boli v Slovenskej republike prijaté ako nástroj riešenia dopadov pandémie na kvalitu života občanov v súvislosti

s ochranou osobných údajov, si však môžeme položiť otázku, či bola dosiahnutá rovnováha medzi hrozbami pre verejné zdravie, ktoré so sebou pandémia Covid-19 priniesla na jednej strane, a ochranou osobných údajov v zmysle GDPR na strane druhej. Naliehavosť presadzovať právo na ochranu osobných údajov a súčasne umožniť efektívnu reakciu na pandémiu bolo totiž jednou z kľúčových tém mnohých diskusií a obsahovalo tiež množstvo právnych otázok. Je teda vhodné pripomenúť, že aj napriek tomu, že je ochrana ľudského zdravia a života prvoradá, pri legislatívnom nastavení v zmysle zamedzenia šírenia ochorenia Covid-19 sa mali zásadné legislatívne úpravy prijímať tak, aby boli v súlade s legislatívou regulujúcou aj iné základné ľudské práva, kvôli zamedzeniu situáciám, kedy si právne normy vzájomne kolidovali alebo konkurovali.

Ak zhrnieme predložené legislatívne iniciatívy a zmeny, vzhľadom na ich ambicióznosť môžeme očakávať pozitívny vplyv na zvýšenie ochrany osobných údajov.

### **Záver**

Demokracia v súčasnosti prechádza transformáciou bezprecedentného charakteru. V článku sú okrem iného vyobrazené zmeny, ktoré prebiehajú pod vplyvom zvyšujúcej sa sily korporátnych spoločností a technologických gigantov, a taktiež hrozby z ovplyvňovania a manipulácie občanov, ktoré plynú zo schopnosti spracovania osobných údajov na základe technologickému progresu. Internet a sociálne siete v rukách veľkých spoločností totiž zjednodušujú systém udržiavania apatie v spoločnosti a prispievajú k riadeniu politických kampaní.

Otázkou je, či samotná demokracia predstavuje „prekážku“, ktorú treba odstrániť alebo ju v tomto spoločenskom procese berieme ako obeť, ktorú treba zachrániť pred deformáciou v dôsledku ekonomických tlakov. Podľa nášho názoru je potrebné upriamiť pozornosť spoločnosti jednoznačne na druhú možnosť. Keďže si spoločnosť nástrahy digitálneho priestoru plne neuvedomuje, je nevyhnutné neprestajne poukazovať na enormný dopad vznikajúcich protidemokratických tendencií na celú spoločnosť a tiež na urgenciu riešenia týchto problémov.

Sloboda občanov v demokratickom zriadení začína byť viac a viac limitovaná. Práve preto rastie potreba regulácie vplyvov technologických gigantov a nepochybne aj potreba ochrany osobných údajov občanov Európskej únie, k čomu má vo výraznej miere prispieť všeobecné nariadenie GDPR. V posledných rokoch sledujeme enormný posun v oblasti zefektívňovania a regulácie technológií a kyberpriestoru, a to aj vďaka GDPR. Stále však môžeme tvrdiť, že v porovnaní s rozvojom technológií a ich dosahu na spoločnosť, sú regulácie krok pozadu.

Internet predstavuje priestor pre efektívne umiestnenie reklamy, za ktorým stojí motivácia zisku. Google a aj mnoho iných organizácií na tomto princípe začali uľahčovať vyhľadávanie na internete a personalizovať reklamu. Z dátového prebytku o správaní sa ľudí sa tak v internetovom priestore stala vplyvná zbraň korporátov, akým je napríklad Google a zefektívnilo sa cielenie na zákazníkov. Avšak na tomto princípe nemusí fungovať na internete iba reklama na produkty, a preto poznatky o osobných údajoch jednotlivcov, o ich spracovaní a opätovnom využití začínajú vyvolávať obavy v spoločnosti, aj medzi vládnymi štruktúrami. Nebezpečenstvo tkvie v tom, že tak, ako technologickí giganti využívajú spracovávanie

užívateľských dát pre svoje potreby, ponúkajú rovnako aj štátu, alebo politickým stranám priestor na šírenie reklamy, názorov a na sebaaprezentáciu. Môžeme teda hovoriť o existencii paralely medzi tým, ako môžu byť napĺňané ekonomické a politické záujmy. V oboch prípadoch reprezentuje internet miesto, ktoré tomu vďaka schopnosti sofistikovaným spôsobom pracovať s dátami napomáha.

Evolúcia počítačových technológií postupuje nekontrolovateľne dopredu a schopnosť vlád a firiem zhromažďovať dáta o občanoch, ukladať ich a analyzovať sa explozívne zvyšuje. Ako spoločnosť sme vstúpili do éry veľkých dát a aj keď sa ich týkajúca sa legislatíva zlepšuje, súkromie občanov nie je chránené tak, ako by byť malo. Užívatelia internetu neodkážu mať stopercentnú vedomosť o tom, čo všetko o nich vlády a firmy vedia, či môžu zistiť. Takýto stav nie je možné akceptovať a nie je kompatibilný s demokraciou. V demokratickej spoločnosti majú rozhodovať občania, nie počítačový algoritmus, ktorý je ľahko zneužitelný.

Pre bežného občana je táto doba spojená so závažnými rizikami. Napríklad v súvislosti s tým, že internet personalizuje každému užívateľovi realitu, ktorá súvisí s tým, že každý na ňom vidí o niečo odlišný obsah. Naskytuje sa teda otázka, ako sa občania majú zhodnúť na dôležitých celospoločenských témach, keď sa nevedia dopracovať k rovnakým informáciám.

Každý občan tiež zdieľaním svojich osobných údajov zanecháva na internete nezmazateľné digitálne stopy, ktoré by proti nemu mohli pôsobiť ako kompromitačný materiál. Napríklad v nadväznosti na to, že vlády a firmy taja, čo sa deje s informáciami, ktoré o občanoch získali.

Zohľadňujúc všetko, čo bolo v článku analyzované, môžeme tvrdiť, že technologický pokrok a (možno aj nevedomý) únik osobných údajov nie len že porušujú právo na ochranu osobných údajov, ale aj zreteľne vstupujú do demokratického fungovania štátov a narúšajú ich základné mechanizmy, štruktúry a hodnoty.

*Tento článok odporúča na publikovanie vo vedeckom časopise Mladá veda:  
doc. JUDr. Mgr. Michal Jesenko, PhD.*

### **Použitá literatúra**

1. BYSTRŮM, N., 2018. Zneužitie osobných údajov podkopalo demokraciu – a môže znova [online]. 2018. [cit. 10. novembra 2022]. Dostupné z: <https://euractiv.sk/section/digitalizacia/opinion/zneužitie-osobnych-udajov-podkopalo-demokraciu-a-moze-znova/>
2. BONEFELD-DAHL, C., 2021. Obmedzenie prenosu dát ohrozí digitálnu transformáciu Únie [online]. 2021. [cit. 4. januára 2023]. Dostupné z: <https://euractiv.sk/section/digitalizacia/opinion/obmedzenie-prenosu-dat-ohrozi-digitalnu-transformaciju-unie/>
3. CENTRÁLNY METAINFORMAČNÝ SYSTÉM VEREJNEJ SPRÁVY SR, 2022. ISVS: Informačný systém centrálnej správy referenčných údajov verejnej správy [online]. 2022. [cit. 9. januára 2023] Dostupné z: <https://metais.vicempremier.gov.sk/detail/ISVS/ac011014-fb54-4257-9b77-ec47fe0b24e3/cimaster?tab=detailForm>
4. CENTRÁLNY METAINFORMAČNÝ SYSTÉM VEREJNEJ SPRÁVY SR, 2021. Projekt rozvoja IT: Konsolidovaná analytická vrstva [online]. 2021. [cit. 9. januára 2023] Dostupné z:

- <https://metais.vicpremier.gov.sk/detail/Projekt/15aae7d3-7149-4b5b-b606-9efd56cc8114/cimaster?tab=basicForm>
5. CULLEN INTERNATIONAL, 2022. The EU Data Act [online]. 2022. [cit. 9. januára 2023]. Dostupné z: <https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>
  6. DATA PROTECTION COMMISSION, 2023. Data Protection Commission announces conclusion of two inquiries into Meta Ireland [online]. 2023. [cit. 10. januára 2023] Dostupné z: <https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>
  7. DENNY, J., 2020. What is an algorithm? How computers know what to do with data online]. 2020. [cit. 10. januára 2023]. Dostupné z: <https://theconversation.com/what-is-an-algorithm-how-computers-know-what-to-do-with-data-146665>
  8. EUROPEAN COMMISSION, 2022. Data Governance Act explained [online]. 2022. [cit. 10. januára 2023]. Dostupné z: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained>
  9. HILL, K. a S. MATTU, 2018. The House That Spied on Me [online]. 2018. [cit. 9. januára 2023]. Dostupné z: <https://gizmodo.com/the-house-that-spied-on-me-1822429852>
  10. HOCHTEL, M. 2021. Blíži sa koniec nevyžiadaných telefonátov? Slovensko zapracuje staršiu európsku smernicu [online]. 2021. [cit. 10. januára 2023]. Dostupné z: <https://euractiv.sk/section/digitalizacia/news/blizi-sa-koniec-nevyziadanych-telefonatov-do-slovenskych-zakonov-konecne-pribudne-starsia-europska-smernica/>
  11. INTERSOFT CONSULTING, 2018. General Data Protection Regulation GDPR [online]. 2018. [cit. 16. novembra 2022]. Dostupné z: <https://gdpr-info.eu/>
  12. JOUROVÁ, V., 2018. Komisárka Jourová: O vaše osobné údaje sa starajú iní, mali by ste sa tiež [online]. 2018. [cit. 7. januára 2023]. Dostupné z: <https://euractiv.sk/section/digitalizacia/opinion/komisarka-jourova-o-vase-osobne-udaje-sa-staraju-ini-mali-by-ste-sa-tiez/>
  13. KONVIT, M., 2020. GDPR pre firmy v čase koronakrízy COVID-19 [online]. 2020. [cit. 10. januára 2023]. Dostupné z: <https://home.kpmg/sk/sk/home/insights/2020/05/gdpr-pre-firmy-v-case-koronakrizy-covid-19.html>
  14. MARKOŠ, J., 2019. *Sila rozumu v bláznivej dobe - Manuál kritického myslenia*. Bratislava: N Press. ISBN: 9788099925015.
  15. NAGYOVÁ, N., 2021. Aké zmeny je potrebné vykonať v dokumentácii GDPR z dôvodu zavedenia OTP režimu na pracovisku? [online]. 2021. [cit. 21. novembra 2022]. Dostupné z: <https://lanikovagroup.sk/ake-zmeny-je-potrebne-vykonat-v-dokumentacii-gdpr-z-dovodu-zavedenia-otp-rezimu-na-pracovisku/>
  16. NELSON, J., a D.COOPERMAN, 1998. Out of Utopia: The Paradox of Postindustrialization [online]. 1988. [cit. 10. januára 2023]. Dostupné z: [https://www.jstor.org/stable/4120829?searchText=Out%20of%20Utopia%20The%20Paradox%20of%20Postindustrialization&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DOut%2Bof%2BUtopia%253A%2BThe%2BParadox%2Bof%2BPostindustrialization&ab\\_segments=0%2FSYC-6744\\_basic\\_search%2Fcontrol&refreqid=fastly-default%3A29029990dce21cfefd415cb454f7a7c5](https://www.jstor.org/stable/4120829?searchText=Out%20of%20Utopia%20The%20Paradox%20of%20Postindustrialization&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DOut%2Bof%2BUtopia%253A%2BThe%2BParadox%2Bof%2BPostindustrialization&ab_segments=0%2FSYC-6744_basic_search%2Fcontrol&refreqid=fastly-default%3A29029990dce21cfefd415cb454f7a7c5)
  17. OXFORD REFERENCE, 2017. Oxford Essential Quotations\$ Oxford Essential Quotations [online]. 2021. [cit. 5. decembra 2022]. Dostupné z: <https://www.oxfordreference.com/display/10.1093/acref/9780191843730.001.0001/q-oro-ed5-00007882>
  18. POLITICO, 2021. EU privacy law's chief architect calls for its overhaul politika [online]. 2021. [cit. 5. januára 2023]. Dostupné z: <https://www.politico.eu/article/eu-privacy-laws-chief-architect-calls-for-its-overhaul/>
  19. RAVAS, F. a V. MILOŠOVIČ, 2021. Aktuálne: Kontrola OTP zamestnancov z pohľadu GDPR a ďalšie zmeny [online]. 2021. [cit. 21. januára 2023]. Dostupné z: <https://www.securion.sk/kontrola-otp-gdpr-zmeny-zakonnik-prace/>
  20. SOROS, G., 2018. Remarks delivered at the World Economic Forum [online]. 2018. [cit. 7. januára 2023]. Dostupné z:

- <https://www.georgesoros.com/2018/01/25/remarks-delivered-at-the-world-economic-forum/>
21. SPOLOČNOSŤ OCHRANY SPOTREBITEĽOV, 2021. Spotrebiteľské organizácie podali sťažnosť na WhatsApp za tlak na spotrebiteľov prijať ich nové podmienky [online]. 2021. [cit. 6. januára 2023]. Dostupné z:  
[https://www.sospotrebitelov.sk/aktuality/spotrebiteleske-organizacie-podali-staznost-na-whatsapp-za-tlak-na-spotrebitelov-prijat-ich-nove-podmienky/?doing\\_wp\\_cron=1673090535.3715929985046386718750](https://www.sospotrebitelov.sk/aktuality/spotrebiteleske-organizacie-podali-staznost-na-whatsapp-za-tlak-na-spotrebitelov-prijat-ich-nove-podmienky/?doing_wp_cron=1673090535.3715929985046386718750)
  22. ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY, 2021. 3. výročie uplatňovania všeobecného nariadenia o ochrane údajov (GDPR) a zákona č. 18/2018 Z. z. o ochrane osobných údajov v praxi [online]. 2021. [cit. 4. januára 2023]. Dostupné z:  
<https://dataprotection.gov.sk/uouu/sk/content/3-vyrocie-uplatnovania-vseobecneho-nariadenia-o-ochrane-udajov-gdpr-zakona-c-182018-z-z-o>
  23. ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV, 2021. Vyhlásenie EDPB o spracúvaní osobných údajov v súvislosti s prepuknutím ochorenia COVID-19 [online]. 2021. [cit. 10. januára 2023]. Dostupné z:  
<https://dataprotection.gov.sk/uouu/sk/content/vyhlasenie-edpb-o-spracuvani-osobnych-udajov-v-suvislosti-s-prepuknutim-ochorenia-covid-19>
  24. VALENTOVÁ, T., BIRNSTEIN, M. a J. GOLLAIS, 2018. *GDPR/Všeobecné nariadenie o ochrane osobných údajov: Zákon o ochrane osobných údajov*. Bratislava: Wolters Kluwer. ISBN: 978-80-8168-852-2.
  25. YAR, L. a S. STOLTON, 2019. Viac ako 95 tisíc Európanov sa sťažuje na zlé ochrany osobných údajov [online]. 2019. [cit. 6. januára 2023]. Dostupné z:  
<https://euractiv.sk/section/digitalizacia/news/viac-ako-95-tisic-europanov-sa-stazuje-na-zlu-ochranu-osobnych-udajov/>
  26. YAR, L. 2020. Čína zastavila šírenie koronavírusu aj vďaka zberu osobných dát. Môže ísť Únia touto cestou? [online]. 2020. [cit. 8. januára 2023] Dostupné z:  
<https://euractiv.sk/section/digitalizacia/news/cina-zastavila-sirenje-koronavirusu-aj-vdaka-zberu-osobnych-dat-moze-ist-unia-touto-cestou/>
  27. YAR, L., 2021. Dáta sú ropou 21. storočia. Ako sa o ne stará Slovensko? [online]. 2021. [cit. 11. decembra 2022]. Dostupné z:  
<https://euractiv.sk/section/digitalizacia/news/data-su-ropou-21-storocia-ako-sa-o-ne-stara-slovensko/>
  28. YAR, L., 2021. Národná, európska a transatlantická dátová politika [online]. 2021. [cit. 5. januára 2023]. Dostupné z: <https://euractiv.sk/section/digitalizacia/linksdossier/narodna-europska-a-transatlanticka-datova-politika/>
  29. ZMUŠKOVÁ, B. 2021. Technologické firmy bohatnú na dátach. Kolektívne odškodné môže ľuďom vrátiť moc [online]. 2021. [cit. 5. januára 2023]. Dostupné z:  
<https://euractiv.sk/section/spolocnost/news/technologicke-firmy-bohatnu-na-datach-kolektivne-odskodne-moze-ludom-vratit-moc/>
  30. ZUBOFF, S., 1988. *In the Age of the Smart Machine*. New York: Basic Books. ISBN: 139780465032112.
  31. ZUBOFF, S., 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization [online]. 2015. [cit. 9. januára 2023]. Dostupné z:  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2594754](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754)
  32. ZUBOFF, S., 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs. ISBN: 978-1610395694.
  33. LP/2021/55 Zákon o údajoch a o zmene a doplnení niektorých zákonov
  34. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES
  35. Smernica európskeho parlamentu a rady (EÚ) 2018/1972, ktorou sa stanovuje európsky kódex elektronických komunikácií
  36. Smernica európskeho parlamentu a rady (EÚ) 2020/1828 o žalobách v zastúpení na ochranu kolektívnych záujmov spotrebiteľov a o zrušení smernice 2009/22/ES
  37. Zákon č. 287/2021 Z. z., ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony



# **Mladá veda**

## **Young Science**

**ISSN 1339-3189**