GELLERT, R.: *THE RISK-BASED APPROACH TO DATA PROTECTION*

JAN TOMÍŠEK[1]

GELLERT, R.: The Risk-based Approach to Data Protection. Oxford University Press, 2020, 304 s. **ISBN: 9780198837718**

Kniha Raphaëla Gellerta The Risk-Based Approach to Data Protection, publikovaná v roce 2020 v nakladatelství Oxford University Press, se věnuje problematice regulatorních metod v právu ochrany osobních údajů a představuje rozšířenou a aktualizovanou podobu disertační práce autora. Hlavním tématem publikace je zkoumání vztahu regulace založené na právech (*right-based approach) a* regulace založené na riziku (*risk-based approach)*. Toto téma je čtyři roky po účinnosti nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDPR“) vysoce aktuální, což potvrzuje i prostor, který mu věnuje domácí doktrína.[2]

Kniha je přehledně rozčleněna do sedmi kapitol doplněných úvodem a závěrem. V úvodu práce autor především vymezuje vztah mezi rizikem a regulací. V první kapitole pak podrobně rozebírá základní koncepty rizika

[1] Mgr. et Mgr. Ing Jan Tomíšek je externím doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy Univerzity. Působí jako advokát v ROWAN LEGAL, advokátní kancelář s.r.o. Kontakt: jantomisek@gmail.com

[2] Obecně srov. MÍŠEK, Jakub. Moderní regulatorní metody ochrany osobních údajů. Brno: Masarykova univerzita, 2020. s. 169 a násl. Aktuálně srov. NONNEMANN, František. Je načase začít diskutovat o GDPR 2.0? *Právní rozhledy.* 2022, roč. 30, č. 1, s. 23.

a regulace. Druhá kapitola popisuje ochranu osobních údajů jako formu regulace založenou na příkazech a kontrole jejich plnění. Třetí kapitola rozebírá problémy tohoto modelu regulace ochrany osobních údajů. Čtvrtá kapitola se věnuje změně regulatorního modelu z příkazů a kontroly na metaregulaci stanovící pouze regulatorní cíle a ponechávající na regulovaných subjektech nastavení konkrétních standardů a způsobů jejich implementace. V páté kapitole autor rozebírá projevy metaregulace, resp. přístupu založeného na riziku v ochraně osobních údajů. Šestá kapitola rozebírá konkrétní postupy řízení rizik v oblasti ochrany osobních údajů a jejich odraz v GDPR. Sedmá kapitola diskutuje úskalí přístupu založeného na riziku. V závěru knihy se autor vrací ke vztahu přístupu k regulaci založenému na právech a přístupu založenému na riziku.

Hlavní přínosy knihy shledávám v důkladném rozboru samotného přístupu založeného na riziku, jeho zasazení do širšího kontextu moderních postupů řízení korporací, resp. organizací obecně, analýzu jeho projevů v GDPR a také kritické zhodnocení tohoto přístupu vč. poukazů na jeho limity.

Autor knihy v prvé řadě blíže rozebírá samotný koncept řízení rizik, jak jej popisuje věda managementu. Poukazuje na známé problémy současných přístupů k řízení rizik. V rámci procesu hodnocení rizik je to hodnotitel, který rozhoduje, jaká rizika pro účely hodnocení vůbec vezme v úvahu. Dále pak hodnotitel těmto rizikům přisuzuje určité váhy zpravidla na základě pravděpodobnosti realizace rizika a závažnosti jeho dopadů, toto přiřazení však opět často není možné provést na základě objektivních rizik. Gellert tak správně poukazuje na nevyhnutelné subjektivní prvky v procesu řízení rizik, které se promítají i do oblasti ochrany osobních údajů.[3]

Stejně tak kniha příhodně zasazuje koncept řízení rizik do kontextu řízení korporací a disciplíny *corporate governance*.[4] Vnímání řízení v oblasti ochrany osobních údajů jako součásti běžných korporátních procesů je přitom podle mého názoru prvkem, který v aktuální praxi ochrany osobních

[3] Srov. GELLERT, Raphaël. The Risk-based Approach to Data Protection. Oxford University Press, 2020. s. 37.

[4] Srov. tamtéž, s. 110 a násl.

údajů v řadě případů chybí (tento typ rizik je řízen samostatně od rizik obecných), a jeho doktrinální uchopení je tak velmi žádoucí.

Vedle těchto obecných úvah se však kniha nevyhýbá ani analýze platné právní úpravy v podobě GDPR. Projevy přístupu založeného na riziku autor spatřuje zejména v principu odpovědnosti dle jeho čl. 5 odst. 2 a čl. 24, povinnosti standardní ochrany osobních údajů (*data protection by design*) dle čl. 25 a konkrétních institutech v kapitole IV GDPR.[5] Poukazuje však na dvě zásadní skutečnosti. V prvé řadě přístup založený na riziku není v GDPR doveden zcela do důsledku v tom smyslu, že by povinné subjekty v oblasti ochrany osobních údajů podle rizik konkrétního případu zpracování zcela volně volily příhodná opatření. Tato opatření jsou naopak do značené míry předem stanovena na úrovni základních zásad GDPR v čl. 5 GDPR (např. nezbytnost právního titulu, minimalizace rozsahu údajů či minimalizace doby uložení) a jeho konkrétních institutů (např. informační povinnost podle čl. 13 a 14 či bezpečnostní opatření podle čl. 32). Podle rizik konkrétního případu nemůže povinný subjekt volit, zda bude tato opatření provádět, ale pouze způsob jejich provádění.[6]

Tento přístup není třeba dle Gellerta hodnotit a *priori* negativně, naopak má své opodstatnění s ohledem na nutnost zajištění ochrany osobních údajů jako základního práva, kde může mít určení jistého minimálního obecného standardu své odůvodnění. Správně však upozorňuje, že je vhodné se v tomto kontextu kriticky zamýšlet nad jednotlivými základními zásadami, jejichž platnost nemusí být natolik univerzální, jak se na první pohled zdá. Současně je třeba tento přístup zákonodárce vést v patrnosti při výkladu jednotlivých institutů GDPR opírajících se o přístup založený na riziku.[7]

V kontextu tohoto přístupu se totiž mění samotný charakter posuzování rizik podle jednotlivých institutů. Gellert tak přesvědčivě argumentuje, že jelikož instituty jako posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR mají vést k identifikaci vhodných opatření pro implementaci

[5] Srov. tamtéž, s. 160 a 165.

[6] Srov. tamtéž, s. 155.

[7] Srov. tamtéž.

základních zásad a jednotlivých institutů ochrany osobních údajů,[8] je třeba v odpovídajícím procesu hodnocení rizik zkoumat rizika, že tyto zásady, resp. instituty budou porušeny, resp. nebudou řádně provedeny. Dle Gellerta tedy nejde v procesu hodnocení rizik dle GDPR o hodnocení bezprostředních rizik pro základní práva a svobody subjektu údajů, ale o hodnocení *compliance* rizik nesouladu s právní úpravou. Rizika pro základní práva subjektu údajů se do tohoto procesu promítají až sekundárně jako dopad jednotlivých uvažovaných porušení právní úpravy ochrany osobních údajů.[9]

Za velmi přínosné považuji také kritické zhodnocení přístupu založeného na riziku v ochraně osobních údajů. Vedle poukázání na vždy přítomný subjektivní prvek Gellert také poukazuje na problematičnost některých jeho východisek, zejména předpokladu, že povinné subjekty jsou vždy nejlépe vybaveny k tomu, aby v oblasti ochrany osobních údajů posoudily rizika plynoucí z jejich činnosti (zpracování osobních údajů) a zvolily vhodná opatření.[10] Praktická zkušenost ukazuje, že s ohledem na široký záběr právní úpravy naopak řada povinných subjektů nedisponuje odbornými znalostmi ani finančními zdroji, aby příslušná rizika posoudila a řídila. Dále poukazuje na negativní zkušenosti s příliš liberální aplikací a vymáháním tohoto přístupu ve finančním sektoru.[11]

Nosná je i závěrečná myšlenka autora, že v rovině konkrétních praktických postupů se mohou rozdíly mezi přístupem založeným na právech a přístupem založeným na riziku stírat a skutečný rozdíl mezi nimi může spočívat především v podkladových idejích určujících celkový způsob uskutečňování ochrany osobních údajů.[12]

Celkově knihu hodnotím jako velmi aktuální a přínosnou. Lze ji doporučit jak akademikům, kteří se věnují zkoumání v oblasti ochrany osobních údajů, tak čtenářům z praxe, kteří aplikují konkrétní postupy v této oblasti.

---

[8] Obdobně srov. Míšek, 2020, op. cit., s. 176.

[9] Srov. Gellert, 2020, op. cit., s. 198.

[10] Srov. tamtéž, s. 233.

[11] Srov. tamtéž, s. 236.

[12] Srov. tamtéž, s. 250.

Akademicky zaměřený čtenář nalezne v knize přehledné shrnutí základních premis ochrany osobních údajů a rozbor dominantních přístupů k její regulaci, vč. relevantních zdrojů pro další studium. Praktik pak může z knihy čerpat lepší pochopení jednotlivých institutů GDPR odrážejících přístup založený na riziku (zejména zásady odpovědnosti a institutu posouzení vlivu na ochranu osobních údajů) a jejich zasazení do kontextu korporátních procesů řízení rizik.
