

# Obsah

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| O autorech.....                                                            | V   |
| Autory jednotlivých částí textu jsou.....                                  | VII |
| Předmluva .....                                                            | IX  |
| Seznam použitých zkratk.....                                               |     |
| Úvodem ke kybernetické bezpečnosti a významu její právní<br>regulace ..... | 1   |
| Oddíl I. Kybernetická bezpečnost a její pojetí.....                        | 5   |
| Kapitola 1. Úvodní poznámky .....                                          | 7   |
| Kapitola 2. Kyberprostor a jak jej chránit – východiska<br>a modely .....  | 9   |
| 2.1 Hrozby a nač směřují .....                                             | 9   |
| 2.1.1 Informační bezpečnost.....                                           | 9   |
| 2.1.2 Systémová bezpečnost (fyzická bezpečnost systémů) ..                 | 11  |
| 2.1.3 Bezpečnost versus ochrana .....                                      | 12  |
| 2.2.4 Bezpečnost jako řízení rizik .....                                   | 13  |
| 2.2 Jak přistupovat k útoku a k obraně proti němu .....                    | 14  |
| 2.2.1 Útočníci a jejich motivy.....                                        | 14  |
| 2.2.2 Jak se bránit.....                                                   | 15  |
| 2.2.3 <i>Cyber kill chain</i> a fáze útoku .....                           | 17  |
| 2.3 Hrozby v oblasti zabezpečení dat a jejich řešení .....                 | 17  |
| 2.3.1 Neoprávněné zveřejnění informací .....                               | 17  |
| 2.3.2 Neoprávněná úprava a falzifikace .....                               | 18  |
| 2.3.3 Asymetrická kryptografie .....                                       | 19  |
| 2.4 Hrozby malware a jejich řešení .....                                   | 19  |
| 2.4.1 Množení a doručování.....                                            | 20  |
| 2.4.2 <i>Payload</i> .....                                                 | 21  |
| 2.4.3 Nápravná opatření.....                                               | 22  |
| 2.5 Hrozby v oblasti bezpečnosti softwaru a jejich řešení .....            | 22  |
| 2.5.1 Nápravná opatření.....                                               | 23  |
| 2.6 Hrozby v oblasti síťové bezpečnosti a jejich řešení .....              | 24  |
| 2.6.1 Průzkum sítě .....                                                   | 24  |
| 2.6.2 Firewall.....                                                        | 25  |
| 2.6.3 Útoky typu „odmítnutí služby“ .....                                  | 26  |
| 2.6.4 Ochrana a protiopatření .....                                        | 27  |
| 2.7 Hrozby AI pro bezpečnost kyberprostoru .....                           | 29  |
| 2.7.1 Útoky sociálního inženýrství využívající umělou<br>inteligenci ..... | 29  |
| 2.7.2 Phishingové útoky řízené umělou inteligencí .....                    | 29  |
| 2.7.3 <i>Deepfakes</i> .....                                               | 30  |

|                                                                                                                                     |                                                                                                                  |           |
|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-----------|
| 2.7.4                                                                                                                               | <i>Adversarial AI/ML</i> .....                                                                                   | 30        |
| 2.7.5                                                                                                                               | Škodlivé GPT modely.....                                                                                         | 31        |
| 2.7.6                                                                                                                               | Útoky za použití ransomwaru.....                                                                                 | 31        |
| 2.7.7                                                                                                                               | Jak snížit riziko kybernetických útoků využívajících AI ..                                                       | 31        |
| 2.8                                                                                                                                 | Závěrečná doporučení.....                                                                                        | 32        |
| <b>Kapitola 3. Kybernetická bezpečnost – pojem a definice .....</b>                                                                 |                                                                                                                  | <b>35</b> |
| 3.1                                                                                                                                 | Úvod .....                                                                                                       | 35        |
| 3.2                                                                                                                                 | Obecné chápání pojmu kybernetická bezpečnost.....                                                                | 35        |
| 3.3                                                                                                                                 | Kybernetická bezpečnost v odborné literatuře .....                                                               | 36        |
| 3.4                                                                                                                                 | Aspekty promítající se do vymezení kybernetické bezpečnosti .....                                                | 38        |
| 3.4.1                                                                                                                               | Aspekt prevence.....                                                                                             | 38        |
| 3.4.2                                                                                                                               | Aspekt včasného odhalení .....                                                                                   | 39        |
| 3.4.3                                                                                                                               | Aspekt nápravy stavu .....                                                                                       | 40        |
| 3.5                                                                                                                                 | ENISA a definice kybernetické bezpečnosti v celkovém kontextu .....                                              | 40        |
| 3.6                                                                                                                                 | Kybernetická bezpečnost vs bezpečnost informací.....                                                             | 41        |
| 3.7                                                                                                                                 | Kybernetická bezpečnost vs počítačová bezpečnost .....                                                           | 42        |
| 3.8                                                                                                                                 | Jak celkově definovat kybernetickou bezpečnost.....                                                              | 43        |
| <b>Kapitola 4. Funkce právní úpravy při zajištění kybernetické bezpečnosti.....</b>                                                 |                                                                                                                  | <b>45</b> |
| 4.1                                                                                                                                 | Úloha právních norem v oblasti kybernetické bezpečnosti .....                                                    | 46        |
| 4.2                                                                                                                                 | Právo kybernetické bezpečnosti – charakteristika a cíle .....                                                    | 47        |
| <b>Oddíl II. Kybernetická bezpečnost v právní úpravě EU .....</b>                                                                   |                                                                                                                  | <b>51</b> |
| <b>Kapitola 1. Nejednotný koncept definice kybernetické bezpečnosti v EU.....</b>                                                   |                                                                                                                  | <b>53</b> |
| 1.1                                                                                                                                 | Vymezení kybernetické bezpečnosti v <i>acquis communautaire</i> .....                                            | 53        |
| <b>Kapitola 2. <i>Soft law</i> jako předchůdce i průvodce unijních právních předpisů o kybernetické bezpečnosti.....</b>            |                                                                                                                  | <b>57</b> |
| 2.1                                                                                                                                 | K významu unijního <i>soft law</i> .....                                                                         | 57        |
| 2.2                                                                                                                                 | Dokumenty <i>soft law</i> v oblasti kybernetické bezpečnosti.....                                                | 58        |
| 2.3                                                                                                                                 | Vývoj po přijetí Strategie EU pro kybernetickou bezpečnost....                                                   | 66        |
| <b>Kapitola 3. Rozsah unijních pravomocí jako důvod počátečního omezení rozsahu úpravy kybernetické bezpečnosti právem EU .....</b> |                                                                                                                  | <b>71</b> |
| <b>Kapitola 4. Stěžejní předpisy v oblasti kybernetické bezpečnosti.....</b>                                                        |                                                                                                                  | <b>75</b> |
| 4.1                                                                                                                                 | Nařízení (ES) 460/2004 a nařízení (EU) 526/2013 o Evropské agentuře pro bezpečnost sítí a informací (ENISA)..... | 76        |
| 4.2                                                                                                                                 | Směrnice 2016/ 1148 o bezpečnosti sítí a informačních systémů – NIS .....                                        | 78        |

|       |                                                                                                                                               |     |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 4.3   | Nařízení 2019/881 – CSA (Akt EU o kybernetické bezpečnosti a Agentuře ENISA).....                                                             | 80  |
| 4.3.1 | Certifikační systém.....                                                                                                                      | 82  |
| 4.3.2 | Certifikační orgány .....                                                                                                                     | 82  |
| 4.3.3 | Nařízení 2025/37 o řízených bezpečnostních službách – novela CSA .....                                                                        | 83  |
| 4.3.4 | Prováděcí nařízení k CSA 2024/482 – Evropský systém certifikace kybernetické bezpečnosti založený na společných kritériích (EUCC) .....       | 84  |
| 4.3.5 | Prováděcí nařízení k CSA 2024/3143 – postupy pro oznamování subjektů posuzování shody.....                                                    | 85  |
| 4.3.6 | Prováděcí nařízení k CSA 2025/2540 – plán pro vzájemné hodnocení .....                                                                        | 85  |
| 4.4   | Směrnice 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti – NIS 2.....                                      | 85  |
| 4.4.1 | Regulované subjekty a hlavní povinnosti .....                                                                                                 | 87  |
| 4.4.2 | Sdílení informací a spolupráce mezi státy.....                                                                                                | 88  |
| 4.4.3 | Spolupráce na úrovni Unie a unijní zpráva o stavu kybernetické bezpečnosti .....                                                              | 88  |
| 4.4.4 | Dohled a vymáhání .....                                                                                                                       | 89  |
| 4.4.5 | Prováděcí nařízení 2024/2690 k směrnici NIS 2 – technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik..... | 90  |
| 4.5   | Směrnice 2022/2557 o odolnosti kritických subjektů – CER ....                                                                                 | 91  |
| 4.5.1 | Kritické subjekty zvláštního evropského významu .....                                                                                         | 93  |
| 4.5.2 | Poradní mise .....                                                                                                                            | 93  |
| 4.5.3 | Kompetentní orgány, jednotná kontaktní místa a spolupráce mezi členskými státy EU.....                                                        | 94  |
| 4.5.4 | Vnitrostátní rámce pro odolnost kritických subjektů .....                                                                                     | 95  |
| 4.5.5 | Opatření v oblasti odolnosti kritických subjektů.....                                                                                         | 96  |
| 4.5.6 | Dohled a vymáhání .....                                                                                                                       | 97  |
| 4.5.7 | Prováděcí předpisy.....                                                                                                                       | 97  |
| 4.6   | Nařízení 2022/2554 o digitální provozní odolnosti finančního sektoru – DORA .....                                                             | 98  |
| 4.6.1 | Účel a rozsah úpravy.....                                                                                                                     | 98  |
| 4.6.2 | Řízení rizik v oblasti informačních a komunikačních technologií finančními subjekty .....                                                     | 100 |
| 4.6.3 | Řízení, klasifikace a hlášení incidentů souvisejících s IKT.....                                                                              | 101 |
| 4.6.4 | Testování digitální provozní odolnosti.....                                                                                                   | 102 |
| 4.6.5 | Řízení rizik třetích stran v oblasti informačních a komunikačních technologií .....                                                           | 103 |
| 4.6.6 | Dohled a vynucování .....                                                                                                                     | 105 |
| 4.6.7 | Regulační a prováděcí technické normy .....                                                                                                   | 105 |
| 4.7   | Nařízení 2024/2847 – Akt o kybernetické odolnosti (CRA) ....                                                                                  | 106 |
| 4.7.1 | Rozsah působnosti CRA .....                                                                                                                   | 107 |
| 4.7.2 | Povinnosti hospodářských subjektů .....                                                                                                       | 108 |
| 4.7.3 | Shoda produktu s digitálními prvky .....                                                                                                      | 109 |
| 4.7.4 | Oznamování subjektů posuzujících shodu.....                                                                                                   | 109 |

|       |                                                                                                                                                                 |     |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 4.7.5 | Dozor nad trhem a vymáhání práva .....                                                                                                                          | 110 |
| 4.7.6 | Zachování důvěrnosti a sankce .....                                                                                                                             | 111 |
| 4.7.7 | Výkon přenesené pravomoci .....                                                                                                                                 | 112 |
| 4.8   | Nařízení EU 2025/38 – Akt o kybernetické solidaritě .....                                                                                                       | 112 |
| 4.8.1 | Cíl nařízení .....                                                                                                                                              | 112 |
| 4.8.2 | Evropský kybernetický štít.....                                                                                                                                 | 113 |
| 4.8.3 | Mechanismus pro mimořádné události v oblasti<br>kybernetické bezpečnosti .....                                                                                  | 114 |
| 4.8.4 | Mechanismus přezkumu kybernetických<br>bezpečnostních incidentů .....                                                                                           | 115 |
| 4.9   | Nařízení 2023/2841 – opatření k zajištění vysoké společné<br>úrovně kybernetické bezpečnosti v orgánech, institucích<br>a jiných subjektech Evropské unie ..... | 115 |
| 4.9.1 | Opatření k zajištění vysoké společné úrovně<br>kybernetické bezpečnosti.....                                                                                    | 115 |
| 4.9.2 | Sdílení informací o kybernetické bezpečnosti,<br>oznamování, reakce na incidenty a řízení.....                                                                  | 116 |
| 4.9.3 | Dodržování .....                                                                                                                                                | 117 |
| 4.10  | Návrh nařízení o přepracovaném CSA – Akt o kybernetické<br>bezpečnosti 2 .....                                                                                  | 118 |

## **Kapitola 5. Další unijní předpisy přímo související se zajištěním kybernetické bezpečnosti .....**

|       |                                                                                                          |     |
|-------|----------------------------------------------------------------------------------------------------------|-----|
| 5.1   | Nařízení 2016/679 – obecné nařízení o ochraně osobních<br>údajů (GDPR) .....                             | 123 |
| 5.1.1 | Zásady zpracování osobních údajů (článek 5).....                                                         | 124 |
| 5.1.2 | Záměrná a standardní ochrana údajů (článek 25) .....                                                     | 124 |
| 5.1.3 | Zabezpečení zpracování údajů (článek 32) .....                                                           | 125 |
| 5.1.4 | Ohlašování případů porušení zabezpečení osobních<br>údajů (článek 33).....                               | 126 |
| 5.1.5 | Oznamování porušení subjektu údajů (článek 34) .....                                                     | 127 |
| 5.1.6 | Posouzení vlivu na ochranu osobních údajů<br>(článek 35) .....                                           | 127 |
| 5.1.7 | Souhrnně k propojení ustanovení GDPR a právní<br>úpravy zajištění kybernetické bezpečnosti .....         | 128 |
| 5.2   | Nařízení EU 2024/1689 o umělé inteligenci (AI) a vazby<br>na právní rámec kybernetické bezpečnosti ..... | 128 |
| 5.2.1 | Systém řízení rizik (článek 9) .....                                                                     | 129 |
| 5.2.2 | Správa dat (článek 10) .....                                                                             | 130 |
| 5.2.3 | Vedení záznamů (článek 12) .....                                                                         | 130 |
| 5.2.4 | Povinnosti v oblasti transparentnosti a protokolování<br>(článek 13) .....                               | 131 |
| 5.2.5 | Změna přístupu k povinnostem v oblasti řízení rizik<br>a bezpečnosti již od návrhu (článek 15).....      | 131 |
| 5.2.6 | Povinnosti poskytovatelů obecných modelů AI se<br>systémovým rizikem (článek 55) .....                   | 132 |
| 5.2.7 | Provázanost Aktu o AI a právní úpravy kybernetické<br>bezpečnosti .....                                  | 132 |
| 5.2.8 | Význam AI pro zajištění kybernetické bezpečnosti .....                                                   | 133 |

|       |                                                                                                                                                   |     |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 5.3   | Nařízení 2023/2854 o datech ( <i>Data Act</i> ).....                                                                                              | 135 |
| 5.3.1 | Bezpečnost již od návrhu – <i>Security by design</i><br>(článek 3) .....                                                                          | 135 |
| 5.3.2 | Omezení sdílení z důvodu bezpečnosti (článek 4 a 5). ..                                                                                           | 136 |
| 5.3.3 | Mechanismy ochrany dat při jejich nuceném sdílení<br>(kapitola V) .....                                                                           | 136 |
| 5.3.4 | Změna poskytovatele služeb zpracování dat<br>(kapitola VI) .....                                                                                  | 137 |
| 5.3.5 | Technické aspekty změny poskytovatele (článek 30)... ..                                                                                           | 137 |
| 5.4   | Směrnice (2002/58/ES) o zpracování osobních údajů<br>a ochraně soukromí v odvětví elektronických komunikací<br>(směrnice <i>e-Privacy</i> ) ..... | 138 |
| 5.4.1 | Bezpečnost (článek 4).....                                                                                                                        | 138 |
| 5.4.2 | Důvěrnost komunikací (článek 5).....                                                                                                              | 139 |
| 5.4.3 | Nevyžádaná sdělení (článek 13).....                                                                                                               | 140 |
| 5.4.4 | Technické vlastnosti a standardizace (článek 14) .....                                                                                            | 140 |
| 5.5   | Nařízení 910/2014 o elektronické identifikaci (eIDAS) .....                                                                                       | 140 |
| 5.5.1 | Poskytovatelé důvěryhodných služeb a základy<br>řízení rizik (článek 19).....                                                                     | 141 |
| 5.5.2 | Zvýšení nároků – zvýšená bezpečnost u kvalifikovaných<br>poskytovatelů (článek 24).....                                                           | 142 |
| 5.5.3 | Nová dimenze – kybernetická bezpečnost již od návrhu<br>v peněžence EUDI .....                                                                    | 143 |
| 5.5.4 | Vzájemné propojení s rámcem úpravy na ochranu<br>kybernetické bezpečnosti.....                                                                    | 144 |
| 5.5.5 | Nedostatky v propojení úprav eIDAS a zajištění<br>kybernetické bezpečnosti.....                                                                   | 145 |
| 5.6   | Regulační rámec pro jednotný digitální trh a zajištění<br>kybernetické bezpečnosti .....                                                          | 146 |
| 5.6.1 | Nařízení 2022/1925 o spravedlivých trzích otevřených<br>hospodářské soutěži v digitálním sektoru (DMA).....                                       | 146 |
| 5.6.2 | Nařízení 2022/2065 o jednotném trhu digitálních<br>služeb (DSA) .....                                                                             | 148 |
| 5.7   | Směrnice 2015/2366 o platebních službách na vnitřním trhu<br>a povinnosti v oblasti bezpečnosti (PSD 2) .....                                     | 148 |
| 5.7.1 | Řízení operačních a bezpečnostních rizik (článek 95) ..                                                                                           | 149 |
| 5.7.2 | Silné ověření klienta – SCA (článek 97) .....                                                                                                     | 150 |
| 5.7.3 | Hlášení incidentů (článek 96).....                                                                                                                | 150 |
| 5.7.4 | Ochrana bezpečnostních prvků (články 69 a 70) .....                                                                                               | 150 |
| 5.7.5 | Nová právní úprava platebních služeb .....                                                                                                        | 151 |

## **Kapitola 6. Institucionální rámec zajištění kybernetické bezpečnosti v EU.....**

|     |                                                                                                           |     |
|-----|-----------------------------------------------------------------------------------------------------------|-----|
| 6.1 | Spolupráce mezi orgány EU a agenturami, zapojenými<br>do procesu zajištění kybernetické bezpečnosti ..... | 153 |
| 6.2 | Agentury a další subjekty .....                                                                           | 153 |
| 6.3 | Koordinační sítě jako mechanismy spolupráce mezi<br>subjekty EU .....                                     | 155 |

|                                                                                                                              |                                                                                         |            |
|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|------------|
| 6.4                                                                                                                          | Spolupráce mezi národními úřady členských států EU a mezi národními úřady navzájem..... | 156        |
| <b>Kapitola 7. Možné nesoulady mezi jednotlivými úpravami kybernetické bezpečnosti.....</b>                                  |                                                                                         | <b>157</b> |
| <b>Oddíl III. Česká národní úprava kybernetické bezpečnosti .....</b>                                                        |                                                                                         | <b>161</b> |
| <b>Kapitola 1. Vývoj před současným zákonem o kybernetické bezpečnosti.....</b>                                              |                                                                                         | <b>163</b> |
| <b>Kapitola 2. Základní a důležité subjekty .....</b>                                                                        |                                                                                         | <b>165</b> |
| <b>Kapitola 3. Hlášení incidentů.....</b>                                                                                    |                                                                                         | <b>171</b> |
| 3.1                                                                                                                          | Vymezení některých pojmů užívaných zákonem o kybernetické bezpečnosti .....             | 172        |
| 3.2                                                                                                                          | Úprava ohlašovací povinnosti .....                                                      | 175        |
| 3.3                                                                                                                          | Proces hlášení kybernetických bezpečnostních incidentů ....                             | 177        |
| <b>Kapitola 4. Dozor, nápravná opatření a sankce .....</b>                                                                   |                                                                                         | <b>183</b> |
| 4.1                                                                                                                          | Kontrolní řád .....                                                                     | 184        |
| 4.2                                                                                                                          | Nápravná opatření podle zákona o kybernetické bezpečnosti .....                         | 185        |
| 4.3                                                                                                                          | Přestupky .....                                                                         | 192        |
| 4.4                                                                                                                          | Pořádková pokuta a výkon rozhodnutí.....                                                | 195        |
| <b>Kapitola 5. Ochrana osobních údajů a soukromí v zákoně o kybernetické bezpečnosti.....</b>                                |                                                                                         | <b>197</b> |
| 5.1                                                                                                                          | Osobní údaje v zákoně o kybernetické bezpečnosti .....                                  | 198        |
| 5.2                                                                                                                          | Právo na informace a kybernetická bezpečnost.....                                       | 204        |
| 5.3                                                                                                                          | Kybernetická bezpečnost a informační sebeurčení.....                                    | 205        |
| <b>Kapitola 6. Prováděcí předpisy k zákonu o kybernetické bezpečnosti.....</b>                                               |                                                                                         | <b>209</b> |
| 6.1                                                                                                                          | Portál NÚKIB .....                                                                      | 209        |
| 6.2                                                                                                                          | Ostatní prováděcí předpisy.....                                                         | 211        |
| <b>Kapitola 7. Certifikace kybernetické bezpečnosti: rozhraní mezi zákonem o kybernetické bezpečnosti a úpravou EU .....</b> |                                                                                         | <b>217</b> |
| 7.1                                                                                                                          | Proč je certifikace v kybernetické bezpečnosti samostatný regulační nástroj.....        | 217        |
| 7.2                                                                                                                          | Nadnárodní úroveň: CSA jako primární pramen evropské certifikace .....                  | 218        |
| 7.2.1                                                                                                                        | První plně přijaté evropské schéma: EUCC (Common Criteria) .....                        | 221        |
| 7.2.2                                                                                                                        | Schémata ve vývoji: EUCS (cloud), EU5G a další .....                                    | 222        |
| 7.3                                                                                                                          | Česká úroveň: co upravuje zákon o kybernetické bezpečnosti v oblasti certifikací .....  | 223        |

|       |                                                                                                |     |
|-------|------------------------------------------------------------------------------------------------|-----|
| 7.3.1 | Autorizace subjektů posuzování shody<br>(KybBez, § 47 an.).....                                | 223 |
| 7.4   | Praktický význam certifikace pro povinné osoby podle<br>zákona o kybernetické bezpečnosti..... | 223 |
| 7.5   | Přehledové srovnání: co je upraveno v zákoně a co<br>na nadnárodní úrovni (EU) .....           | 224 |

#### **Oddíl IV. Právní úprava kybernetické bezpečnosti – existující dilemata a jejich řešení uznáním práva na KB.....**

225

#### **Kapitola 1. Problémy vyvolané a související s právní úpravou KB v EU .....**

227

|     |                                                                            |     |
|-----|----------------------------------------------------------------------------|-----|
| 1.1 | Rozdrobenost a nedostatky v implementaci.....                              | 227 |
| 1.2 | Regulační přetížení a zátěž spojená s dodržováním<br>předpisů.....         | 228 |
| 1.3 | Rozevírání mezery mezi právem a technologickým<br>vývojem .....            | 231 |
| 1.4 | Nedostatky ve vymáhání a nedostatečné vyvozování<br>odpovědnosti .....     | 234 |
| 1.5 | Mezinárodní povaha kybernetických hrozeb a limity právní<br>úpravy EU..... | 236 |
| 1.6 | Napětí mezi zajišťováním KB a ochranou osobních údajů .....                | 237 |

#### **Kapitola 2. Řešení konfliktů mezi zajišťováním kybernetické bezpečnosti a zájmy na ochraně osobních údajů .....**

239

|      |                                                                                                                                    |     |
|------|------------------------------------------------------------------------------------------------------------------------------------|-----|
| 2.1  | Zadní vrátka pro šifrování – konflikt mezi úpravou úkonů<br>na obranu proti kyberútokům a ochranou soukromí údajů .....            | 240 |
| 2.2  | Právní úprava uchovávání údajů a střet mezi požadavkem<br>na uchovávání údajů a právem na ochranu soukromí .....                   | 241 |
| 2.3  | Přeshraniční předávání údajů a konflikt mezi potřebou<br>zajištění KB a předpisy na ochranu osobních údajů.....                    | 243 |
| 2.4  | Ohlašování porušení zabezpečení osobních údajů a rozpor<br>mezi požadavkem transparentností a bezpečnostními<br>obavami .....      | 245 |
| 2.5  | Dohled a sledování – postupy zajištění KB vs omezení<br>v předpisech na ochranu soukromí údajů.....                                | 246 |
| 2.6  | Právo na výmaz vs auditní protokoly – konflikt mezi právem<br>na výmaz osobních údajů a zajištěním bezpečnosti .....               | 247 |
| 2.7  | Zajištění KB vs omezení sběru dat – úprava ochrany<br>osobních údajů omezující zpracování dat z důvodu<br>bezpečnosti .....        | 249 |
| 2.8  | Suverenita cloudových dat a protichůdná pravidla<br>pro ukládání a přenos dat.....                                                 | 250 |
| 2.9  | Zveřejňování zranitelností vs právní předpisy o oznamování<br>narušení bezpečnosti – rozpor ohledně načasování<br>zveřejnění ..... | 252 |
| 2.10 | Rozpor mezi realizací zásad „privacy by design“<br>a „security by design“ při zajišťování KB a při ochraně<br>soukromí .....       | 253 |

|                                                                                                                                            |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Kapitola 3. Právo na kybernetickou bezpečnost jako výraz rovnoprávnosti ochrany KB se základním právem EU na ochranu soukromí .....</b> | <b>257</b> |
| 3.1 Lze kybernetickou bezpečnost podřadit do celkového konceptu bezpečnosti v právu EU? .....                                              | 258        |
| 3.2 Důvody pro zavedení nového základního práva na KB .....                                                                                | 260        |
| 3.3 Obsah nového základního práva na kybernetickou bezpečnost .....                                                                        | 262        |
| 3.4 Problémy se zavedením nového základního práva na kybernetickou bezpečnost .....                                                        | 263        |
| <b>Kapitola 4. Závěrečné poznámky .....</b>                                                                                                | <b>265</b> |
| 4.1 Jak z labyrintu legislativy EU v právu KB? .....                                                                                       | 265        |
| 4.2 Hledání podoby právní úpravy zajištění kybernetické bezpečnosti se zárukami pro ochranu osobních údajů .....                           | 267        |
| <b>Seznam citované literatury .....</b>                                                                                                    | <b>269</b> |
| <b>Věcný rejstřík .....</b>                                                                                                                | <b>291</b> |