

28. 8. 2025

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

# Kyberbezpečnost v civilním letectví a její právní rámec

Bezpečnost počítačových a informačních systémů je v současné době velkým tématem, a to i s ohledem na to, že rozvoj moderních technologií každoročně rapidně stoupá. Tento trend ukazuje i přijetí nového zákona 264/2025 Sb., o kybernetické bezpečnosti, který nabyde účinnosti 1. 11. 2025. Důraz na vyšší kyberbezpečnost můžeme najít i v oblasti civilního letectví, které může být snadným a zranitelným cílem kyberútoků. Náš článek si klade za cíl přiblížit základní specifika právní úpravy kyberbezpečnosti v civilním letectví, a to včetně možných důsledků vyplývajících z nedostatečné ochrany bezpečnosti počítačových a informačních systémů.

## Specifika kyberbezpečnosti v civilním letectví

Moderní technologie a jejich rozvoj přinesly do současné doby mnoho výzev, a to i v ochraně funkčnosti těchto technologií. Zvýšený důraz na ochranu těchto technologií je kladen i v oblasti civilního letectví, které se vyznačuje zvýšenou mírou své zranitelnosti, která může vyústit v nepříjemné důsledky pro osoby působící v tomto odvětví, a to jak v právní, tak v ekonomické rovině.

**O aktuálnosti** kybernetické bezpečnosti v civilním letectví svědčí nejen **rostoucí závislost na digitálních technologiích**, ale také **narůstající počet bezpečnostních incidentů**. V posledních letech jsme mohli zaznamenat případy útoků na letištní a letecké systémy, které vedly k výpadkům provozu (např. hackerský útok na letiště varšavského letiště Fryderyka Chopina v roce 2015), únikům citlivých dat (např. únik dat zákazníků British Airways v roce 2018) či narušení komunikačních nebo navigačních systémů (nejčastěji se vyskytující v oblasti Blízkého východu nebo východní Evropy[1]). Tyto události ukazují, že civilní letectví se stává atraktivním cílem kybernetických útoků a je nezbytné posilovat jeho odolnost.

## Právní rámec kyberbezpečnosti (bezpečnosti) v civilním letectví

Na zvýšenou potřebu chránit technologie v civilním letectví je reagováno i značným množstvím právní regulace, která se snaží uvedenou zranitelnost zmírnit, aby tak byla zajištěna co největší bezpečnost letectví.

Zmíněný právní rámec, který se zabývá otázkami kyberbezpečnosti, můžeme najít jak **na národní úrovni**, ale i **na úrovni mezinárodní**, včetně práva Evropské unie. Pro přehlednost tohoto článku se zaměříme na základní právní předpisy upravující leteckou kyberbezpečnost.

### Národní úprava

Mezi základní právní předpisy řešící na úrovni národní úpravy otázky kybernetické bezpečnosti patří zejména:

- zákon č. [181/2014 Sb.](#), zákon o kybernetické bezpečnosti a o změně souvisejících

**zákonů[2]** (dále jen „**ZKB**“), jehož pravidla mohou dopadat i na osoby působící v letecké dopravě, o kterých Národní úřad pro kybernetickou bezpečnost (dále jen „**Úřad**“) rozhodne, že jsou poskytovateli tzv. základní služby dle § 2 písm. i) bod 2. v oblasti dopravy v souladu s kritérii stanovenými vyhláškou č. [437/2017](#) Sb., o kritériích pro určení provozovatele základní služby bod 2.1. přílohy k vyhlášce,

- v současné době ještě neúčinný **zákon č. 264/2025 Sb., o kybernetické bezpečnosti** (dále jen „**NZKB**“), který implementuje tzv. směrnici NIS 2 a významným způsobem rozšiřuje okruh osob[3], které budou povinni k registraci podle tohoto zákona a budou povinni zavést potřebná a přiměřená bezpečnostní opatření, a to i v oblasti letectví a letecké dopravy (§ 4 odst. 1 písm. a) bod č. 8 NZKB[4], nebo
- **zákon č. 49/1997 Sb., o civilním letectví** (dále jen „**ZCL**“), který je základním právním předpisem v oblasti letectví, který upravuje mj. i aspekty obecné letecké bezpečnosti, a to i částečně s ohledem na kyberbezpečnost (např. § 85m ZCL, který stanovuje povinnost mít na letišti schválený bezpečnostní program Úřadem pro civilní letectví).

## Mezinárodní úprava

Vedle výše zmíněné národní úpravy jsou otázky bezpečnosti (včetně kyberbezpečnosti) v letectví řešeny i úpravou mezinárodní, kdy mezi nejdůležitější právní předpisy[5], kromě již zmíněné směrnice NIS 2 patří:

- **[Nařízení \(EU\) 2018/1139 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví](#)**, které upravuje obecné podmínky bezpečnosti v letectví, včetně zřízení EASA a zavedení Evropského programu pro bezpečnost letectví nebo Státního programu bezpečnosti[6] a něj navazující *nařízení Komise v přenesené působnosti EU) 2022/1645 ze dne 14. července 2022, resp. prováděcí nařízení Komise 2023/203 ze dne 27. října 2022*, nebo
- **[Nařízení Evropského parlamentu a Rady \(ES\) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení \(ES\) č. 2320/2002](#)**, které obecně řeší otázky bezpečnosti před protiprávními činy na území EU (např. čl. 12, který stanovuje požadavky na bezpečnostní program na letišti).

## Bezpečnostní opatření v letectví

Společným jmenovatelem uvedených právních předpisů (a dalších navazujících právních předpisů) je, že cílem této regulace je **snaha dosáhnout co nejlepší možné obrany**, jak proti vnějším, ale vnitřním nebezpečím, která by mohla leteckou bezpečnost jakýmkoliv způsobem ohrozit.

Z hlediska kyberbezpečnosti jsou kladeny na osoby působící v letectví takové povinnosti, aby byla co nejvíce zaručena ochrana informačních a komunikačních systémů proti útokům hackerů.

Jednotlivá opatření v oblasti kyberbezpečnosti lze ve smyslu NZKB[7] rozdělit na dva základní druhy opatření, a to opatření organizační a technické (§ 14 NZKB). Mezi tyto opatření patří v souladu § 14 NZKB například: řízení rizik, bezpečnost lidských zdrojů, řízení přístupu, detekce a zaznamenání kybernetických bezpečnostních událostí či použití kryptografických algoritmů[8][9].

Vedle zavedení konkrétních opatření mají osoby podléhající regulaci NZKB (ale koneckonců i dle ostatních předpisů, včetně ZKB) i další povinnosti, včetně povinnosti hlásit kybernetické bezpečnostní incidenty, a to buď národnímu týmu koordinace a zvládnání kybernetických bezpečnostních incidentů, událostí a hrozeb (v případě režimu nižších povinností - § 15 odst. 2 NZKB) nebo Úřadu (v případě režimu vyšších povinností - § 15 odst. 1 NZKB) či povinnost vůči

dodavatelům (§ 24 a násl. NZKB).

## Sankce

Důležitosti zavedení příslušných opatření a plnění zmíněných povinností odpovídají i **případné sankce za nedodržení těchto povinností** v souladu s NZKB. Tyto sankce mohou dosáhnout až 175.000.000, - Kč nebo 1,4 % ze světového obratu v případě režimu nižších povinností nebo až výše 250.000.000, - Kč nebo 2 % ze světového obratu, popř. pozastavení platnosti certifikace nebo dočasný zákaz výkonu funkce člena statutárního orgánu.

## Další právní a ekonomické důsledky

Vedle výše uvedených sankcí spojených porušením povinností v oblasti kybernetické bezpečnosti mohou do úvahy přicházet i **další negativní následky nastalé v důsledku bezpečnostního incidentu**,

a to nejen u osob podléhající výše zmíněné regulaci.

Mezi tyto důsledky patří např. **uložení pokuty** spojené s porušením ochrany osobních údajů<sup>[10]</sup> či **požadování náhrady škody** (v případě leteckých dopravců náhrady škody za zpoždění letu).

Kromě právních důsledků se mohou tyto bezpečnostní incidenty projevit i **v rovině ekonomické**, neboť případný bezpečnostní incident může ovlivnit, jak konkurenceschopnost (např. v případě získání obchodního tajemství či know-how ze strany konkurenta), tak i samotnou dobrou pověst osoby působící v letectví, což vzhledem k omezenému okruhu osob působící v letectví může vést až k fatálním ekonomickým následkům.

## Závěr

S ohledem na výše uvedené je patrné, že téma kyberbezpečnosti je v současné době značně aktuálním tématem. Z těchto důvodů je tak vhodné doporučit mít ochranu kyberbezpečnosti v letectví (ale i obecně leteckou bezpečnost) nastavenou tak, aby odpovídala nejvyšším bezpečnostním standardům a minimalizovala právní a ekonomická rizika.



**JUDr. Ing. Jan Vych,**  
advokát a partner



**Mgr. David Šnajdr,**  
advokátní koncipient



Advokátní kancelář Vych & Partners, s.r.o.

Lazarská 11/6  
120 00 Praha 2

Tel.: +420 222 517 466  
Fax: +420 222 517 478

---

[1] V reakci na tyto útoky přijaly Agentura Evropské unie pro bezpečnost letectví (EASA) a Mezinárodní asociace leteckých dopravců (IATA) plán, který stanovuje základní plán proti tomuto typu útoků >>> [zde](#).

[2] Je nutno zmínit, že pravidla stanovená v tomto zákoně budou platit do 1. 11. 2025, kdy nabyde účinnosti nový zákon o kybernetické bezpečnosti.

[3] Pod okruh těchto osob spadají osoby poskytující regulovanou službu (§ 4 odst. 1 písm. a) NZKB) a osoby, které jsou podle § 4 odst. 1 písm. b) NZKB středním nebo velkým podnikem ve smyslu doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků nebo jsou významní pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice.

[4] Konkrétní seznam služeb podle § 4 odstavce 1 písm. a) NZKB a vymezení podmínek významnosti poskytovatele těchto služeb podle § 4 odstavce 1 písm. b) NZKB budou stanoveny vyhláškou vydanou Úřadem (§ 4 odst. 2 NZKB).

[5] Ve výčtu právní úpravy budou uvedeny zejména právní předpisy, které stanovují určitá konkrétní pravidla v oblasti bezpečnosti letectví. Ve výčtu nebude tak zmíněna např. dohoda č. 147/1947 Sb., úmluva o mezinárodním civilním letectví (tzv. Chicagská úmluva).

[6] Státní plán bezpečnosti ČR pro roky 2023-2025 je dostupný na stránkách Ministerstva dopravy >>> [zde](#).

[7] Z důvodu blížící se účinnosti NZKB považují autoři za lepší se zaměřit v otázce bezpečnostních opatření na úpravu NZKB.

[8] Konkrétní opatření se liší podle tzv. režimu povinností dle NZKB (§ 8 NZKB). Autory byly vybrány

opatření, která budou využívány v obou těchto režimech.

[9] Konkrétní obsah těchto opatření bude doplněn vyhláškou vydanou Úřadem.

[10] Toto nastalo např. u výše zmíněného případu British Airways, kterému byla uložena pokuta za porušení pravidel GDPR ve výši přesahující 183 milionů liber.

© EPRAVO.CZ - Sběrka zákonů, judikatura, právo | [www.epravo.cz](http://www.epravo.cz)

## Další články:

- [Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše](#)
- [Zneužití práva na přístup podle GDPR](#)
- [Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona](#)
- [Právní povaha sítě elektronických komunikací - režim náhrady škody](#)
- [Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory](#)
- [Jak fungují plánovací smlouvy v reálných situacích \(2. díl\)](#)
- [Nejvyšší soud a forma smlouvy o smlouvě budoucí: krok zpět v ochraně právní jistoty?](#)
- [„Za každou kauzou je živý příběh“](#)
- [Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi](#)
- [Spoluvlastnictví a správa společné věci](#)
- [Doručování soudních písemností ze zahraničí do ČR](#)