# Shrnutí stanoviska evropského inspektora ochrany údajů ke sdělení Evropské komise Radě a Evropskému parlamentu o zřízení Evropského centra pro boj proti kyberkriminalitě

*(Úplné znění tohoto stanoviska je k dispozici v angličtině, francouzštině a němčině na internetových stránkách evropského inspektora ochrany údajů na adrese http://www.edps.europa.eu)*

(2012/C 336/05)

## 1. Úvod

### 1.1 *Konzultace evropského inspektora ochrany údajů (EIOÚ)*

1. Dne 28. března 2012 Komise přijala sdělení nazvané „Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě“ ([1]).

2. Evropský inspektor ochrany údajů bere na vědomí, že Rada zveřejnila ve dnech 7.–8. června 2012 své závěry o zřízení Evropského centra pro boj proti kyberkriminalitě ([2]). Rada schvaluje cíle sdělení, podporuje zřízení centra (uvádí se též jen „EC3“) v rámci Europolu a využívání stávajících struktur k boji proti dalším oblastem trestné činnosti, potvrzuje, že EC3 by mělo sloužit jako základna pro boj s kyberkriminalitou a že by toto centrum mělo úzce spolupracovat s příslušnými agenturami a aktéry na mezinárodní úrovni, a vyzývá Komisi, aby po konzultaci s Europolem dále rozšířila seznam konkrétních úkolů, které bude třeba provést k zajištění provozuschopnosti EC3 do roku 2013. Závěry nicméně nezmiňují, že je při zřizování EC3 velmi důležité dbát na základní práva a především na ochranu údajů.

3. Před přijetím sdělení Komise měl evropský inspektor ochrany údajů možnost vyjádřit neformální připomínky k návrhu tohoto sdělení. Ve svých neformálních připomínkách zdůraznil, že ochrana údajů je stěžejním aspektem, který je třeba vzít při zřizování Evropského centra pro boj proti kyberkriminalitě (dále jen „EC3“) v úvahu. Sdělení bohužel připomínky vznesené v této neformální fázi nezohlednilo. V závěrech Rady se kromě toho vyžadovalo zajištění toho, aby byl provoz centra zahájen již příští rok. Z tohoto důvodu by otázka ochrany údajů měla být zohledněna v následujících krocích, k nimž dojde již velmi brzy.

4. Toto stanovisko se zabývá důležitostí ochrany údajů při zřizování EC3 a představuje konkrétní návrhy, které by mohly být zohledněny při stanovování pravomocí EC3 a v legislativní revizi právního rámce Europolu. Evropský inspektor ochrany údajů jednal z vlastního podnětu, a přijal proto toto stanovisko na základě čl. 41 odst. 2 nařízení (ES) č. 45/2001.

### 1.2 *Obsah sdělení*

5. Komise ve svém sdělení uvádí, že hodlá v rámci strategie vnitřní bezpečnosti zřídit Evropské centrum pro boj proti kyberkriminalitě ([3]).

6. Sdělení obsahuje netaxativní seznam několika druhů kyberkriminality, na něž by se mělo EC3 soustředit: kybernetické trestné činy páchané organizovanými zločineckými skupinami, zejména pak činy vytvářející vysoké nezákonné zisky, např. podvody na internetu, kybernetické trestné činy působící závažnou újmu jejich obětem, např. pohlavní vykořisťování dětí na internetu, a dále kybernetické trestné činy vážně poškozující kritické systémy informační a komunikační technologie (IKT) v Unii.

7. Pokud jde o náplň práce centra, sdělení uvádí tyto čtyři hlavní úkoly ([4]):

— sloužit jako evropská základna pro informace o kyberkriminalitě,

— shromažďovat dostupné evropské odborné poznatky o kyberkriminalitě v zájmu podpory členských států při budování kapacit,

([1]) Kyberkriminalita není v právních předpisech EU definována.

([2]) Závěry Rady o zřízení Evropského centra pro boj proti kyberkriminalitě, 3172. zasedání Rady ve složení SPRAVEDLNOST a VNITŘNÍ VĚCI v Lucemburku ve dnech 7. a 8. června 2012.

([3]) Strategie vnitřní bezpečnosti Evropské unie: pět kroků směrem k bezpečnější Evropě. KOM(2010) 673 v konečném znění ze dne 22. listopadu 2010. Viz rovněž stanovisko EIOÚ k tomuto sdělení vydané dne 17. prosince 2010 (Úř. věst. C 101, 1.4.2011, s. 6).

([4]) Sdělení s. 4–5.

— poskytovat členským státům podporu při vyšetřování kyberkriminality,

— vystupovat za evropský kolektiv odborníků, kteří se v donucovacích a soudních orgánech zabývají vyšetřováním kyberkriminality.

8. Informace zpracovávané EC3 budou shromažďovány z *celé řady veřejných, soukromých a otevřených zdrojů*, a budou tak rozšiřovat dostupné policejní údaje, a budou se *týkat kybernetické trestné činnosti, metod a osob z této činnosti podezřelých*. Centrum bude také přímo spolupracovat s ostatními evropskými agenturami a institucemi. Tato spolupráce bude probíhat na základě účasti těchto subjektů na programové radě EC3 a rovněž prostřednictvím případné operativní spolupráce.

9. Komise navrhuje, aby EC3 bylo přirozeným rozhraním pro specializované činnosti Europolu a jiných mezinárodních policejních subjektů zabývajících se kyberkriminalitou. EC3 by rovněž mělo v partnerství s Interpolem a dalšími strategickými partnery ve světě usilovat o zlepšování koordinovaných odpovědí v boji proti kyberkriminalitě.

10. Z praktického hlediska Komise navrhuje vytvořit toto centrum jako součást Europolu. EC3 bude *součástí Europolu* ([1]), a tudíž se na něj bude vztahovat právní režim této agentury ([2]).

11. Podle Evropské komise ([3]) dojde v důsledku vytvoření EC3 k těmto hlavním změnám ve stávajících aktivitách Europolu: i) navýšení finančních zdrojů za účelem účinnějšího shromažďování informací z různých zdrojů, ii) výměna informací s partnery mimo donucovací orgány (především ze soukromého sektoru).

1.3 *Zaměření stanoviska*

12. Evropský inspektor ochrany údajů v tomto stanovisku:

— žádá Komisi, aby vyjasnila rozsah činností EC3, které se týkají ochrany údajů,

— posuzuje plánované činnosti v kontextu aktuálního právního rámce Europolu, zejména pak jejich slučitelnost s tímto rámcem,

— zdůrazňuje relevantní aspekty, u nichž by zákonodárný orgán měl uvést další podrobnosti s ohledem na budoucí revizi právního režimu Europolu s cílem zajistit vyšší úroveň ochrany údajů.

13. Struktura stanoviska je následující: část 2.1 se zabývá otázkou, proč ochrana údajů hraje zásadní úlohu při vytváření EC3; část 2.2 se zabývá slučitelností cílů stanovených ve sdělení pro EC3 s právním mandátem Europolu; část 2.3 se zaměřuje na spolupráci se soukromým sektorem a mezinárodními partnery.

## 3. **Závěry**

50. Evropský inspektor ochrany údajů považuje boj proti kyberkriminalitě za základní kámen při zajišťování bezpečnosti v digitálním prostoru a vytváření nezbytné důvěry. Rovněž upozorňuje, že dodržování režimů pro ochranu údajů by mělo být považováno za nedílnou součást boje proti kyberkriminalitě, a nikoli za překážku jeho účinnosti.

51. Ve sdělení je zmiňováno vytvoření nového Evropského centra pro boj proti kyberkriminalitě v rámci Europolu, přestože centrum pro boj proti kyberkriminalitě v Europolu funguje již několik let. Evropský inspektor ochrany údajů by uvítal, kdyby byly lépe objasněny nové kapacity a činnosti, které odliší nové EC3 od stávajícího centra pro boj proti kyberkriminalitě v rámci Europolu.

([1]) V souladu s doporučením studie proveditelnosti zveřejněné v únoru 2012, v níž jsou hodnoceny různé možnosti (status quo, fungování v rámci Europolu, vlastnictví/součást Europolu, virtuální centrum). http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf

([2]) Rozhodnutí Rady ze dne 6. dubna 2009 o zřízení Evropského policejního úřadu (Europol) (2009/371/SVV).

([3]) Tisková zpráva ze dne 28. března. Frequently Asked Questions: the new European Cybercrime Centre (Často kladené dotazy: nové Evropské centrum pro boj proti kyberkriminalitě) Referenční číslo: MEMO/12/221 Datum: 28.3.2012 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221

52. Evropský inspektor ochrany údajů doporučuje, aby pravomoci EC3 byly jasně definovány, a ne pouze vymezeny za pomoci odkazu na koncept „počítačové kriminality“ obsažený ve stávajících právních předpisech Europolu. Definice pravomocí EC3 a stanovení záruk ochrany údajů v rámci EC3 by rovněž měly být součástí přezkumu právních předpisů týkajících se agentury Europol. Evropský inspektor ochrany údajů doporučuje, aby na období před vstupem nových právních předpisů týkajících se Europolu v platnost Komise stanovila tyto pravomoci a záruky ochrany údajů v ustanoveních upravujících mandát centra. Tato ustanovení by mohla zahrnovat:

— jasnou definici toho, jaké úkoly zahrnující zpracování údajů (zejména vyšetřovací činnosti a činnosti provozní podpory) by zaměstnanci centra mohli vykonávat buď sami, nebo ve spolupráci se společnými vyšetřovacími týmy, a

— jasné postupy, které na jedné straně zajistí dodržování práv jednotlivce (včetně práva na ochranu údajů), a na straně druhé poskytnou záruky toho, že důkazy byly získány zákonným způsobem a mohou být použity u soudu.

53. Evropský inspektor ochrany údajů se domnívá, že výměna osobních údajů mezi EC3 a „celou řadou subjektů disponujících veřejnými, soukromými a otevřenými zdroji“ s sebou nese specifická rizika týkající se ochrany údajů, neboť bude často zahrnovat zpracovávání údajů shromážděných pro komerční účely a mezinárodní převody údajů. Tato rizika jsou řešena ve stávajícím rozhodnutí o Europolu, které stanoví, že Europol by zpravidla neměl přímo vyměňovat údaje se soukromým sektorem, a s určitými mezinárodními organizacemi by měl tuto výměnu provádět pouze za jasně vymezených okolností.

54. S ohledem na tyto skutečnosti a vzhledem k významu těchto dvou činností pro EC3 Evropský inspektor ochrany údajů doporučuje, aby příslušné záruky ochrany údajů byly stanoveny v souladu se stávajícími ustanoveními rozhodnutí o Europolu. Tyto záruky by měly být součástí mandátu, který bude pro EC3 vypracován zřizovacím týmem, (a později i revidovaného právního rámce Europolu) a v žádném případě by neměly vést ke snížení úrovně ochrany údajů.

V Bruselu dne 29. června 2012.

Peter HUSTINX

*evropský inspektor ochrany údajů*