Curierul Judiciar

11/2021

Lista de întrebări:

1. Ce reprezintă conceptul de cybersecuritate şi care este scopul ei?
2. Care este obiectivul unei strategii de cybersecuritate?
3. Care sunt cele 8 dimensiuni din care poate fi abordat domeniul cybersecurităţii în era digitală?
4. Cum a evoluat legislativ conceptul de securitate cibernetică în România şi care este raportul cu legislaţia Europeană relevantă în materie?
5. Care sunt măsurile concrete de acţiune şi obiectivele cuprinse în Strategia de securitate a României şi în Planul de acţiune pentru 2021-2026?
6. Care sunt principalele ameninţări specifice la adresa securităţii cibernetice interne?
7. Se poate vorbi de un fenomen al criminalităţii informatice în România?
8. Cum a apărut, s-a consolidat şi a luat amploare?
9. Care sunt transformările ce le-a înregistrat?
10. Pot fi identificate anumite tipare în evoluţia fenomenului?
11. Care sunt caracteristicile fiecărei perioade / etape a acestei evoluţii?
12. Atrage atenţia / reclamă reflecţie anumite aspecte relevate de analiza cazuisticii înregistrate?
13. În ce măsură atât statele, cât şi actorii non-statali mai pot privi problematica conflictelor cibernetice doar dintr-o perspectivă etică, futuristă chiar?
14. Ar trebui să fie securitatea cibernetică o problemă care să îngrijoreze doar pe cetăţeni în mod individual sau mai degrabă pe factorii de decizie la nivel statal, fiind necesară o abordare globală la nivel internaţional?
15. Cât de mult poate impacta un stat o operaţiune cibernetică?
16. Este necesară o legislaţie în domeniul securităţii cibernetice la nivel internaţional?
17. Oare toate operaţiunile cibernetice au aceeaşi amploare, aceleaşi efecte? Implică toate acestea în mod automat o folosire a forţei?
18. Ar putea un stat să răspundă cu folosirea forţei la un atac cibernetic provenind din partea altui stat ce are drept consecinţe blocarea serverelor guvernului statului respectiv sau lăsarea unui oraş întreg fără lumină ore întregi?
19. Cum ne putem da seama de amploarea unei operaţiuni pentru a putea conchide că suntem în faţa unui război cibernetic?
20. Cum se manifestă ingerinţele statului în viaţa privată şi care sunt mijloacele de protecţie legale împotriva acestor ingerinţe?
21. Cine răspunde pentru prejudiciile născute în legătură cu colectarea şi stocarea datelor personale?
22. Care sunt principalele vulnerabilităţi în legătură cu securitatea datelor personale?
23. Cum este reglementată legătura dintre protecţia datelor şi mediul online în sistemul nostru de drept?
24. Care este standardul impus de Conv.EDO pentru folosirea metodelor speciale de supraveghere sau cercetare?
25. Ce constituie încălcări ale dreptului la viaţă privată în lumina jurisprudenţei CEDO referitor la metodele speciale de supraveghere sau cercetare?
26. Cum trebuie interpretate condiţiile de fond pentru autorizarea supravegherii tehnice pentru a fi în acord cu respectarea drepturilor fundamentale ale persoanei?
27. Cum se încadrează unele date informatice în noţiunea de corespondenţă, în special dacă ele aparţin unui avocat?
28. Ce condiţii trebuie să îndeplinească o supraveghere tehnică fără autorizare realizată de un privat?
29. Care sunt cele mai recente actualizări privind metodele speciale de supraveghere?
30. Există diferenţe între percheziţia informatică şii accesul la un sistem informatic?

31. Pot ţine organele instrucţiei penale pasul cu versatilitatea criminalităţii informatice aflată în continuă dezvoltare?
32. Ce este un blockchain?
33. Ce noţiuni trebuie cunoscute pentru o mai bună înţelegere a relaţiei blockchain - drept penal?
34. Care sunt beneficiile şi riscurile ecosistemului blockchain?
35. Care sunt cele mai frecvente conduite infracţionale ce vizează monedele virtuale?
36. Ce sunt portofelele digitale?
37. Care este importanţa cheilor criptografi ce şi a listei de cuvinte generate în mod aleatoriu („seed phrase”/„mnemonic phrase”)?
38. Ce sunt monedele virtuale şi criptoactivele?
39. Cum a influenţat pandemia de COVID-19 criminalitatea informatică?
40. Care sunt cele mai des întâlnite ameninţări cibernetice la nivel european?
41. De ce sunt firmele de avocatură ţinta preferată a hackerilor?
42. Care sunt vulnerabilităţile companiilor juridice şi cum le influenţează integritatea profesională?
43. Cât de expus este sectorul transportului aerian ameninţărilor cibernetice?
44. Cum a răspuns comunitatea internaţională pentru consolidarea securităţii şi rezilienţei cibernetice în domeniul aviaţiei civile?
45. Care sunt potenţialele efecte ale unui atac cibernetic, precum şi consecinţele asupra aviaţiei civile?
46. Se impune necesitatea existenţei unui cadru legal adecvat care să asigure incriminarea atacurilor cibernetice în domeniul aviaţiei civile internaţionale?
47. Care sunt principalele instrumente internaţionale de drept aerian care au rolul de a proteja aviaţia civilă?
48. Care sunt hotărârile obligatorii ale Înaltei Curţi de Casaţie şi Justiţie relevante în domeniul criminalităţii informatice?
49. Care este optica Înaltei Curţi de Casaţie şi Justiţie cu privire la accesul ilegal la un sistem informatic, frauda informatică şi falsul informatic?
50. Care sunt riscurile unei interpretări eronate ale hotărârilor obligatorii pronunţate de către Înalta Curte de Casaţie şi Justiţie, în ceea ce priveşte sfera de aplicabilitate a unor infracţiuni informatice?



www.curieruljudiciar.ro