

Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om forslag til Europa-Parlamentets og Rådets direktiv om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter og om erstatning af Rådets rammeafgørelse 2001/413/RIA

(COM(2017) 489 final — 2017/0226 (COD))

(2018/C 197/04)

Ordfører: **Victor ALISTAR**

Anmodning om udtalelse	Europa-Parlamentet, 2.10.2017 Rådet, 25.10.2017
Retsgrundlag	Artikel 83, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde
Kompetence	Sektionen for Det Indre Marked, Produktion og Forbrug
Vedtaget i sektionen	18.12.2017
Vedtaget på plenarforsamlingen	18.1.2018
Plenarforsamling nr.	531
Resultat af afstemningen	129/0/1
(for/imod/hverken for eller imod)	

1. Konklusioner og anbefalinger

1.1. EØSU glæder sig over, at Kommissionen har gjort det til en prioritet at bekæmpe cyberkriminalitet — et fænomen, som berører elektroniske betalingsmidler — selv om dette burde være blevet prioriteret for længst. Fordelene ved digitaliseringen bør ledsages af mekanismer, som kan udgøre et svar på de udfordringer, som digitaliseringen også indebærer, så den europæiske økonomi og de europæiske borgere kan få fuldt udbytte af informationsfundet. EØSU hilser Kommissionens forslag velkommen, da det har til formål at beskytte borgere og virksomheder mod cyberkriminelle netværk og omfatter foranstaltninger, der skal styrke tilliden til brugen af elektroniske betalingsmidler.

1.2. I forbindelse med sin gennemgang af forslaget til direktiv hæfter udvalget sig ved en række mangler, der bør undersøges nærmere og findes en løsning på:

1.2.1. I artikel 11, som omhandler fastlæggelse af straffemyndighed i forbindelse med efterforskningen, bør det med henblik på at undgå en positiv kompetencekonflikt præciseres, hvorvidt det grundlæggende princip er gerningsmandens eller det anvendte informationssystems tilstedeværelse på en medlemsstats område. I den forbindelse opfordrer EØSU til, at der indføres et nyt afsnit i artiklen, som omhandler løsning af kompetencekonflikter ifølge én af de to metoder, der foreslås i denne udtalelse.

1.2.2. Direktivforslaget behandler ikke fyldestgørende den situation, hvor andre jurisdiktioner uden for EU er impliceret, og ej heller betingelserne for henvisning til andre instrumenter for internationalt retligt samarbejde. Det er derfor påkrævet, at der etableres forudsigelige og veldefinerede proceduremæssige rammer.

1.2.3. Det er nødvendigt at supplere artikel 16, som omhandler forebyggelse, med specifikke foranstaltninger, der foreskrives i medlemsstaternes gennemførelseslovgivning, og som vedrører oplysningspligten, som påhviler enten de aktører, der udsteder elektroniske betalingsmidler, eller de nationale reguleringsmyndigheder, eller som ligger hos de instanser, der er ansvarlige for oplysning om finansielle spørgsmål.

1.2.4. Hvad angår artikel 12 og 13 bør der også fastsættes bestemmelser om udveksling af god praksis med hensyn til afsløring, efterforskning og opklaring af sager om cyberkriminalitet baseret på svig med elektroniske betalingsmidler.

1.3. Selv om det område, der behandles her, vedrører efterforskningssamarbejde og retsligt samarbejde om computerrelateret bedrageri, er det også vigtigt at oprette præventive mekanismer og mekanismer til oplysning af offentligheden om gerningsmændenes modus operandi ved hjælp af oplysningskampagner, der gennemføres af medlemsstaternes retshåndhævende myndigheder.

1.4. For at sikre at foranstaltningerne til beskyttelse af personer er effektive, og for at nå de mål, som ligger til grund for dette initiativ, dvs. styrke tilliden til elektroniske og digitale betalingsinstrumenter samt opnå et højere overholdelsesniveau og styrke forebyggelsen, bør bestemmelserne i artikel 15 også omfatte indførelse i national lovgivning af en forsikring mod økonomiske tab som følge af svig, der indebærer en forpligtelse til at holde ofrene 100 % skadesløse i tilfælde af computerrelateret bedrageri, som skader indehaverne af elektroniske betalingsmidler. En sådan godtgørelse vil blive udbetalt efter, at den udstedende enhed som berørt civil part i sagen har afsluttet sin undersøgelse.

1.5. For at sikre at politikken for bekæmpelse af forfalskning af elektroniske betalingsmidler er effektiv, bør direktivet indeholde en pligt til at anmelde tilfælde af forfalskede elektroniske betalingsmidler, der svarer til anmeldelsespligten i forbindelse med politikkerne for hvidvaskning af penge og forordningen om beskyttelse af personoplysninger.

1.6. EØSU understreger, at det er nødvendigt at udbygge kapaciteten med henblik på at øge forståelsen af svig med elektroniske og digitale betalingsmidler, ligesom dette fænomen bør forebygges ved at indføre en mekanisme for indsamling af statistiske oplysninger med henblik på at styrke strategierne for forebyggelse og afhjælpning af konsekvenserne af sådan svig. Samtidig bør analysen af virkningerne af gennemførelsesforanstaltningerne i medlemsstaterne være fortløbende, og der bør udsendes kvantitative rapporter en gang om året og en kvalitativ evaluering af konsekvenserne hvert andet eller tredje år, så man kan vurdere, hvor effektiv politikken er, og identificere nødvendige justeringer.

1.7. For på mellemlangt sigt at øge effektiviteten af bekæmpelsen af computerrelateret bedrageri og forfalskning af betalingsmidler bør artikel 16 styrkes, og det bør tydeligt præciseres, at medlemsstaterne har pligt til at udvikle specialviden på området ved at udnytte den ekspertise, de erhverver med hensyn til efterforskning, og benytte sig af erfaringsudveksling for at forbedre de færdiguddannedes generelle kvalifikationer (ved hjælp af valgfag) samt eksperters og efterforskernes generelle kvalifikationer (ved hjælp af løbende specialiseret uddannelse).

1.8. Udvalget er i øvrigt af den opfattelse, at samarbejde på området er helt og aldeles uundværligt, og at der bør tilskyndes hertil. Det gælder både nationalt og grænseoverskridende samarbejde såvel som samarbejde om at bekæmpe og forebygge denne form for kriminalitet. Alle berørte aktører fra både den offentlige og den private sektor bør inddrages heri.

1.9. For at undgå enhver forvirring med hensyn til direktivets formål foreslår vi, at »andre betalingsmidler end kontanter« udskiftes med »elektroniske og digitale betalingsmidler« i direktivets overskrift.

2. Kommissionens forslag

2.1. Formålet med direktivet er at sikre en harmonisering af instrumenterne og styrke medlemsstaternes evne til at efterforske svig i forbindelse med elektroniske eller digitale betalingsmidler. Den foreslåede regulering sigter mod at fremme grænseoverskridende samarbejde mellem de myndigheder, som står for efterforskningen, og indføre en række foranstaltninger vedrørende dette samarbejde samt fælles minimumsstandarder for forebyggelsesarbejde, for støtte til ofrene og for ansvarliggørelse af udstederne af sådanne betalingsinstrumenter. I den forbindelse er den valgte fremgangsmåde at definere anvendelsesområdet for instrumentet, som sigter mod at tilvejebringe et teknologineutralt perspektiv.

2.2. I lyset af den teknologiske udvikling og diversificeringen af modus operandi, når det gælder computerrelateret bedrageri, herunder de strategier, som anvendes af kriminelle grupper, erkender Kommissionen i meddelelsen *En strategi for et digitalt indre marked i EU* ⁽¹⁾, at rammeafgørelsen ikke i tilstrækkelig grad kan imødegå nye udfordringer og teknologiske nyskabelser såsom virtuelle valutaer og mobilbetaling.

2.3. Betalingskort er det vigtigste kontantløse betalingsinstrument i EU set ud fra antal transaktioner. I 2013 tegnede svig med kort udstedt i euroområdet sig ifølge en undersøgelse foretaget af den Europæiske Centralbank for 1,44 mia. EUR, og tallet er for opadgående ⁽²⁾. Der findes kun data om svig i forbindelse med kortbetalinger, men betalingskort er også det vigtigste kontantløse betalingsinstrument i EU set ud fra antal transaktioner ⁽³⁾.

2.4. Det fremgår af Kommissionens analyse, at et af de områder, der er mest sårbare over for bedrageri, er anvendelse af elektroniske betalingsmidler til betaling af rejseudgifter — togbilletter, flybilletter, indkvartering og andre tilsvarende transaktioner.

⁽¹⁾ COM(2015) 192 final.

⁽²⁾ Den Europæiske Centralbank, »Fourth report on card fraud«, juli 2015 (senest tilgængelige data).

⁽³⁾ Jf. fodnote 2.

2.5. Kommissionens forslag har til formål at sikre en robust og teknologisk neutral ramme, fjerne operationelle hindringer og styrke de forebyggende foranstaltninger mod svig i forbindelse med elektroniske betalingsmidler.

2.6. For at sikre at der er effektive midler til rådighed til bekæmpelse af svig i forbindelse med elektroniske betalingsmidler og computerrelateret kriminalitet, fastlægger direktivforslaget fælles regler for de nationale lovgivninger, som omhandler: strafferetlige lovovertrædelser vedrørende computerrelateret bedrageri i forbindelse med betalingsmidler, medvirken til strafferetlige lovovertrædelser og politikken vedrørende strafferetlige sanktioner, juridiske personers ansvar og harmonisering af sanktioner med henblik på afskrækkelse. EØSU understreger, at det er første gang, at virtuelle valutaer reguleres inden for rammerne af EU's lovgivning. Definitionen af lovovertrædelser omfatter handlinger, som, selv om der ikke direkte er tale om svig, begås som forberedelse til svig (tyveri og forfalskning men også salg og den blotte besiddelse af stjålne betalingsinstrumenter).

2.7. Med henblik på at gøre det europæiske samarbejde om bekæmpelse af computerrelateret kriminalitet og svig i forbindelse med elektroniske betalingsmidler mere effektivt, indeholder direktivet regler om indførelse af konkrete og relevante bestemmelser om institutionelle mekanismer og kompetencer vedrørende efterforskning på medlemsstatsniveau samt vedrørende den europæiske mekanisme for udveksling af oplysninger mellem nationale myndigheder.

2.8. Et yderst vigtigt element i forslaget er, at det indeholder en forpligtelse til at indføre effektive foranstaltninger til beskyttelse af ofrenes interesser og sikrer dem adgang til effektive retsmidler.

2.9. I Kommissionens forslag, som er helt i tråd med Den Europæiske Unions lovgivningsmæssige kompetencer, som defineret i artikel 83 i traktaten om Den Europæiske Unions funktionsmåde, slås der til lyd for en minimumsharmonisering i medlemsstaterne med en gennemførelsesfrist på 24 måneder.

3. Generelle bemærkninger

3.1. Det valgte lovgivningsinstrument er langt mere hensigtsmæssigt, da det ved hjælp af et direktiv er muligt at fastsætte juridisk bindende regler i alle de nationale jurisdiktioner (med undtagelse af Danmark, hvis landet ikke tilslutter sig frivilligt), hvilket er mere vidtgående end den standardisering af praksis, som foreskrives i rammeafgørelse 2001/413/RIA, uden at det dog berører rammeafgørelsens indhold.

3.2. EØSU konstaterer, at forslaget til direktiv er i synergi med andre lovgivningsmæssige instrumenter, som medlemsstaterne deltager i, og at det supplerer andre af Unionens politikker såsom de paneuropæiske strafferetlige samarbejdsmechanismer og retsakter om bekæmpelse af computerrelateret bedrageri og hvidvaskning af penge. I den forbindelse skal det også understreges, at det er nødvendigt at sikre, at der er en sammenhæng mellem dette forslag og foranstaltningerne til beskyttelse af personoplysninger, der indehaves af finansielle institutioner, og cybersikkerhedsforanstaltningerne.

3.3. Grundlæggende findes der på EU-niveau en række retsakter, som specificerer de nødvendige regler for de finansielle markeder og finansielle tjenester ved at fastsætte regler for rettidig omhu med hensyn til levering, forvaltning og sikring af betalingsinstrumenter, men direktivforslaget indeholder en nødvendig styrkelse af den juridiske infrastruktur, når det gælder rapportering, efterforskning og strafferetlige sanktioner med hensyn til computerrelateret bedrageri og betalingsmidler.

3.4. EØSU understreger, at det er nødvendigt at udbygge kapaciteten med henblik på at øge forståelsen af svig med elektroniske og digitale betalingsmidler, ligesom dette fænomen bør forebygges ved at indføre en mekanisme for indsamling af statistiske oplysninger med henblik på at styrke strategierne for forebyggelse og afhjælpning af konsekvenserne af sådan svig. Samtidig bør analysen af virkningerne af gennemførelsesforanstaltningerne i medlemsstaterne være fortløbende, og der bør udsendes kvantitative rapporter en gang om året og en kvalitativ evaluering af konsekvenserne hvert andet eller tredje år, så man kan vurdere, hvor effektiv politikken er, og identificere nødvendige justeringer.

3.5. Eftersom der inden for rammerne af en mere robust ordning for sikring af juridiske instrumenter indføres et ansvar for juridiske personer og strafferetlige sanktioner, mindes der om, at det er nødvendigt at indføre instrumenter til støtte for de aktører, som leverer elektroniske betalingstjenester eller anvender platforme til onlinebetalinger, så de kan leve op til de sektorspecifikke regler⁽⁴⁾.

⁽⁴⁾ EUT L 267 af 10.10.2009, s. 7.

3.6. Hvad angår den mekanisme, der fastsættes i direktivforslagets artikel 13 og 14 og vedrører udveksling af oplysninger om efterforskning af cyberkriminalitet, som involverer svig i forbindelse med elektroniske betalingsmidler, er det nødvendigt at delegerede beføjelser til Kommissionen, så denne ved hjælp af delegerede retsakter kan regulere såvel mekanismen for udveksling af oplysninger som de standardiserede rapporteringsdata om sager, der er under efterforskning.

3.7. Hvad angår forebyggelse henviser Kommissionen i sin meddelelse ganske vist til et lignende tiltag, der blev vedtaget i forbindelse med direktiv 2011/93/EU, men efter EØSU's opfattelse er det nødvendigt dels at skabe større klarhed om forpligtelserne i forbindelse med forebyggelsesforanstaltningerne, dels at indføre en række forpligtelser med hensyn til oplysning af offentligheden om årsager, risici og måder, hvorpå den enkelte kan beskytte sig med henblik på at undgå svig i forbindelse med finansielle betalingsinstrumenter begået af cyberkriminelle netværk, som lokker brugerne i en fælde.

3.8. Der bør udvikles specialviden på dette område ved at udnytte den ekspertise, der erhverves med hensyn til efterforskning, og benytte sig af erfaringsudveksling med henblik på dels at forbedre de generelle kvalifikationer hos færdiguddannede med en almen uddannelse ved hjælp af valgfag, dels at udvikle en kompetenceramme for eksperter og efterforskere ved hjælp af specialuddannelsesprogrammer.

3.9. Det er vigtigt at sikre et effektivt samarbejde på området for at bekæmpe denne form for kriminalitet. Dette samarbejde bør organiseres på flere forskellige områder, og alle berørte aktører bør så vidt muligt inddrages heri. Det handler ikke alene om at bekæmpe denne alvorlige form for kriminalitet, men også om at forebygge den, både nationalt og i grænseoverskridende sammenhæng.

3.10. Direktivforslaget behandler ikke fyldestgørende den situation, hvor andre jurisdiktioner uden for EU er impliceret, og ej heller betingelserne for henvisning til andre instrumenter for internationalt retligt samarbejde. Det er derfor påkrævet, at der etableres forudsigelige og veldefinerede proceduremæssige rammer.

3.11. Selv om det område, der behandles her, vedrører efterforskningssamarbejde og retsligt samarbejde om computerrelateret bedrageri, er det også vigtigt at oprette præventive mekanismer og mekanismer til oplysning af offentligheden om gerningsmændenes modus operandi ved hjælp af oplysningskampagner, der gennemføres af medlemsstaternes retshåndhævende myndigheder. I den forbindelse er det nødvendigt, at der i bestemmelserne sidst i lovgivningsforslaget henvises til de instrumenter for internationalt strafferetligt samarbejde, som der vil blive henvist til i ekstraterritoriale situationer, og den måde, hvorpå der vil blive efterforsket med udgangspunkt i disse instrumenter. Med hensyn til procedure er der tale om et nyttigt instrument, som skaber øget klarhed.

4. Specifikke forslag

4.1. I artikel 11, som omhandler fastlæggelse af straffemyndighed i forbindelse med efterforskningen, bør det præciseres, hvorvidt det grundlæggende princip er gerningsmandens eller det anvendte informationssystems tilstedeværelse på en medlemsstats område, så man undgår en positiv kompetencekonflikt mellem den situation, som beskrives i artikel 11, stk. 2, litra a), som henviser til gerningsmandens fysiske tilstedeværelse, og den i artikel 11, stk. 2, litra b), beskrevne situation, hvor gerningsmanden har begået lovovertrædelsen på en medlemsstats område, men fysisk befinder sig et andet sted (anvendelse af en mekanisme af typen »remote shell«). Dette ville nemlig kunne betyde, at begge de berørte EU-medlemsstater har kompetence. Det er nødvendigt, at der i artikel 11 indføres et nyt afsnit, som omhandler løsning af kompetencekonflikter, enten ved at der udpeges en enhed, der skal have dette som sin opgave (f.eks. Eurojust), eller ved at der henvises til en lignende mekanisme til løsning af konflikten (f.eks. rammeafgørelse 2009/948/RIA⁽⁵⁾).

4.2. Det er nødvendigt at supplere artikel 16, som omhandler forebyggelse, med specifikke foranstaltninger, der foreskrives i medlemsstaternes gennemførelseslovgivning, og som vedrører oplysningspligten, som påhviler enten de aktører, der udsteder elektroniske betalingsmidler, eller de nationale reguleringsmyndigheder, eller som ligger hos de instanser, der er ansvarlige for oplysning om finansielle spørgsmål.

4.3. Hvad angår den i direktivforslagets artikel 13 omhandlede pligt til at oprette en mekanisme til udveksling af oplysninger om efterforskning af svig er det nødvendigt at oprette et enkelt nationalt kontaktpunkt, som svarer til de kontaktpunkter, der findes inden for bekæmpelse af hvidvaskning af penge og fødevarerikkerhed, så der sikres ensartethed på europæisk niveau. Dette kontaktpunkt kunne i de fleste jurisdiktioner i EU enten være justitsministeriet eller et andet kompetent organ. EØSU mener, at formuleringen »passende anmeldelseskanaler« delvist kan leve op til kravet om effektivitet, men ikke til kravet om harmonisering.

(⁵) EUT L 328 af 15.12.2009, s. 42.

4.4. Hvad angår artikel 12 og 13 bør der også fastsættes bestemmelser om udveksling af god praksis med hensyn til afsløring, efterforskning og opklaring af sager om cyberkriminalitet baseret på svig med elektroniske betalingsmidler.

4.5. For at sikre at foranstaltningerne til beskyttelse af personer er effektive, og for at nå de mål, som ligger til grund for dette initiativ, dvs. styrke tilliden til elektroniske betalingsinstrumenter samt opnå et højere overholdelsesniveau og styrke forebyggelsen, bør bestemmelserne i artikel 15 også omfatte indførelse i national lovgivning af en forsikring mod økonomiske tab som følge af svig, der indebærer en forpligtelse til at holde ofrene 100 % skadesløse i tilfælde af computerrelateret bedrageri, som skader indehaverne af elektroniske betalingsmidler. En sådan godtgørelse vil blive udbetalt efter, at den udstedende enhed som berørt civil part i sagen har afsluttet sin undersøgelse. Disse garantier bør også dække den skade, som tilføjes handlende repræsenteret af SMV'er i tilfælde af manglende afregning af beløb op til et rimeligt loft, der fastsættes på medlemsstatsniveau.

4.6. For at sikre at politikken for bekæmpelse af forfalskning af elektroniske betalingsmidler er effektiv, bør direktivet indeholde en pligt til at anmelde tilfælde af forfalskede elektroniske betalingsmidler, der svarer til anmeldelsespligten i forbindelse med politikkerne for hvidvaskning af penge og forordningen om beskyttelse af personoplysninger.

Bruxelles, den 18. januar 2018.

Georges DASSIS
Formand
for Det Europæiske Økonomiske og Sociale Udvalg
