



Europeiska
unionens råd

Bryssel den 11 juli 2023
(OR. en)

11761/23

CYBER 184
DROIPEN 107
IA 180
JAI 998
MI 607
TELECOM 229

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	10 juli 2023
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2023) 363 final
Ärende:	RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET om bedömning av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa direktiv (EU) 2019/713 om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter och om ersättande av rådets rambeslut 2001/413/RIF

För delegationerna bifogas dokument – COM(2023) 363 final.

Bilaga: COM(2023) 363 final



EUROPEISKA
KOMMISSIONEN

Bryssel den 10.7.2023
COM(2023) 363 final

RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om bedömning av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa direktiv (EU) 2019/713 om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter och om ersättande av rådets rambeslut 2001/413/RIF

1. Inledning

Bedrägeri och förfalskning som rör andra betalningsmedel än kontanter, såsom kreditkort eller betalkort, är en inkomstkälla för organiserad brottslighet och möjliggör annan brottslig verksamhet, såsom terrorism, olaglig narkotikahandel och människohandel. Dessa brott orsakar betydande förluster: Det totala värdet av bedrägliga transaktioner med kort som utfärdats inom det gemensamma eurobetalningsområdet (Sepa) uppgick till 1,87 miljarder euro 2019¹. De flesta bedrägliga transaktioner är bedrägerier där kortet inte uppvisas: År 2019 berodde 80 % av kortbedrägeriernas värde på transaktioner utan fysiskt kort, dvs. betalningar via internet, post eller telefon². Bedrägerier där kortet inte uppvisas stod för 1,50 miljarder euro i bedrägeriförluster 2019, vilket var en ökning med 4,3 % jämfört med föregående år³.

Det finns en tydlig gränsöverskridande dimension: Mer än hälften av det totala värdet av bedrägeri under 2019 var kopplat till gränsöverskridande transaktioner inom Sepa. Ur ett geografiskt perspektiv stod inhemska transaktioner för 89 % av värdet på alla korttransaktioner 2019, men endast 35 % av bedrägliga transaktionerna. Gränsöverskridande transaktioner inom Sepa utgjorde 9 % av alla korttransaktioner i värde, men 51 % av rapporterade bedrägerier⁴.

För att effektivt bekämpa dessa brott måste medlemsstaterna gemensamt fastställa vilka handlingar som ska betraktas som bedrägeri och förfalskning av andra betalningsmedel än kontanter. De måste också ha likartade nivåer av påföljder och operativa möjligheter att rapportera brott och utbyta information mellan myndigheterna. Därför antog Europaparlamentet och rådet den 17 april 2019 direktiv 2019/713/EU (*direktivet*) om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter och om ersättande av rådets rambeslut 2001/413/RIF⁵. Denna rapport uppfyller kravet i artikel 21 i direktivet.

1.1 Direktivets mål och räckvidd

Målen för direktivet är att tillnärma medlemsstaternas straffrättsliga lagstiftning⁶ på området för bedrägeri och förfalskning som rör andra betalningsmedel än kontanter och att förbättra samarbetet mellan behöriga myndigheter. I detta syfte fastställer direktivet minimiregler för definitionen av brott och påföljder. Direktivets tillämpningsområde är brett och omfattar andra ”icke-fysiska eller fysiska skyddade utrustningar, föremål eller handlingar, eller en kombination av dessa, än lagliga betalningsmedel som, ensamma eller i förening med ett förfarande eller en uppsättning förfaranden, ger innehavaren eller användaren möjlighet att överföra pengar eller penningvärde, inbegripet med hjälp av digitala betalningsmedel”, artikel

¹ Europeiska centralbanken, sjunde rapporten om kortbedrägeri, tillgänglig på

<https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html>.

² Ibid.

³ Ibid.

⁴ Ibid.

⁵ <https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32019L0713>.

⁶ Från och med det här, såvida inget annat uttryckligen anges, avser ”medlemsstaterna” eller ”alla medlemsstater” de medlemsstater som är bundna av direktivet, dvs. alla EU-medlemsstater utom Danmark och Irland, som inte deltog i antagandet av direktivet, i enlighet med protokollet om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*) och i enlighet med protokoll 21 om Förenade kungarikets och Irlands ställning.

2 a⁷. Till exempel skulle en mobilbetalningsapp i samband med godkännandeförfarandet (t.ex. PIN-kod) omfattas av denna definition. Det omfattar även virtuella valutor, artiklarna 2 d och 6.

I direktivet definieras särskilda brott, nämligen följande:

- Bedräglig användning av icke-kontanta betalningsinstrument (artikel 3).
- Brott med anknytning till bedräglig användning av fysiska icke-kontanta betalningsinstrument (artikel 4).
- Brott med anknytning till bedräglig användning av icke-fysiska icke-kontanta betalningsinstrument (artikel 5).
- Bedrägeri med anknytning till informationssystem (artikel 6).
- Olagligt tillgängliggörande av verktyg som används för att begå de nämnda brotten (artikel 7).

I direktivet **utsträcks straffrättsligt ansvar** till anstiftan och medhjälp av fysiska och/eller juridiska personer för att begå, och deras försök att begå, brotten ovan (artikel 8).

De lägsta nivåerna av **maximistraff** för de brott som avses i direktivet finns i artikel 9.

De följande artiklarna fastställer minimivillkor för **juridiska personers ansvar** (artikel 10) och sanktioner som ska innefatta bötesstraff eller administrativa avgifter och ge en lista med exempel på andra sanktioner mot dem (artikel 11).

Syftet med artikel 12 är att säkerställa att gärningsmännen enligt direktivet åtalas för de brott som avses i artiklarna 3–8 i direktivet. En medlemsstats **behörighet** måste fastställas om a) brottet helt eller delvis begås på dess territorium, och/eller b) gärningsmannen är en av dess medborgare. Med andra ord fastställs territorialitetsprincipen i artikel 12.1 a i direktivet, medan led b leder till principen om aktivt medborgarskap.

Enligt artikel 13.1 i direktivet ska **utredningsverktygen** för att utreda och lagföra de brott som avses i artiklarna 3–8 vara effektiva, proportionella och tillgängliga för de ansvariga personerna, enheterna och avdelningarna. Information om de brott som avses i artiklarna 3–8 bör nå de myndigheter som utreder eller lagför dessa brott utan onödigt dröjsmål, enligt artikel 13.2 i direktivet.

Vad beträffar informationsutbyte föreskrivs i artikel 14 att medlemsstaterna ska se till att de har nationella operativa **kontaktpunkter** som kan nå dygnet runt alla dagar i veckan så att de kan besvara en brådskande begäran om bistånd från utlandet inom åtta timmar.

Enligt artikel 15.1 i direktivet ska medlemsstaterna dessutom inrätta lämpliga kanaler för att utan onödigt dröjsmål **rapportera de brott** som avses i artiklarna 3–8 till offentliga myndigheter. I synnerhet uppmanas finansinstitut att rapportera misstänkt bedrägeri till brottsbekämpande och juridiska myndigheter (artikel 15.2). Rapportering är ofta utgångspunkten för brottsutredningar (skäl 27).

Slutligen handlar artiklarna 16 och 17 i direktivet om **hjälp och stöd till brottsoffer** respektive **förebyggande åtgärder**.

⁷ Alla nämnda artiklar hänvisar till artiklar i direktivet om inget annat anges.

1.2 Rapportens syfte och metod

Enligt artikel 20 i direktivet ska medlemsstaterna sätta i kraft de lagar och andra författningar som är nödvändiga för att följa direktivet senast den 31 maj 2021 och underrätta kommissionen om dem.

Denna rapport svarar mot ett krav i artikel 21 i direktivet på att kommissionen ska överlämna en rapport till Europaparlamentet och rådet med en utvärdering av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa bestämmelserna i direktivet. Rapporten – som är den första enligt artikel 21 – ger en översikt över de viktigaste införlivandeåtgärder som vidtagits av medlemsstaterna.

Medlemsstaternas införlivande inbegrep att samla in information om relevant lagstiftning och administrativa åtgärder, analysera informationen, utarbeta ny lagstiftning eller – i de flesta fall – ändra befintlig, få den antagen och slutligen rapportera den till kommissionen.

Vid den tidpunkt då tidsfristen för införlivande löpte ut, (31 maj 2021), hade nio medlemsstater anmält till kommissionen att de hade införlivat direktivet till fullo och meddelat sina införlivandeåtgärder. I juli 2021 inledde kommissionen överträdelseförfaranden för utebliven anmälan om nationella införlivandeåtgärder mot de återstående 16 medlemsstaterna: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO och SI⁸. 15 medlemsstater har sedan dess meddelat sina införlivandeåtgärder, men den 30 april 2023 pågår fortfarande ett överträdelseförfarande mot Bulgarien för utebliven anmälan om nationella införlivandeåtgärder⁹.

Beskrivningen och analysen som följer i denna rapport bygger på de uppgifter om nationella införlivandeåtgärder som medlemsstaterna hade lämnat in senast den 31 januari 2023. Anmälningar som har inkommit efter detta datum har inte beaktats. Alla anmälda åtgärder angående nationella lagstiftningar beaktades såväl som domstolsbeslut och – i förekommande fall – gemensam rättslig teori. Dessutom kontaktade kommissionen under analysens gång medlemsstaterna direkt när det var lämpligt för att få ytterligare information eller förtydliganden. All insamlad information beaktades vid analysen.

Utöver de problem som konstateras i denna rapport kan det förekomma ytterligare utmaningar när det gäller införlivandet och andra bestämmelser som inte har rapporterats till kommissionen, eller framtida rättslig och icke-rättslig utveckling. Rapporten hindrar därför inte kommissionen från vidare utvärdering av vissa bestämmelser och från att fortsätta att stödja medlemsstaterna i införlivandet och genomförandet av direktivet.

⁸ Medlemsstaterna i detta dokument är förkortade enligt <http://publications.europa.eu/code/sv/sv-5000600.htm>).

⁹ Information om kommissionens beslut om överträdelseförfaranden finns här: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=en.

2 Införlivandeåtgärder:

2.1 Rättsliga definitioner

I artikel 2 anges definitionerna av de viktigaste begrepp som används i direktivet, nämligen icke-kontanta betalningsinstrument, skyddade utrustningar, föremål eller handlingar, digitala betalningsmedel, virtuell valuta, informationssystem, datorbehandlingsbara uppgifter och juridisk person.

Medlemsstaterna har i allmänhet införlivat definitionerna genom att förlita sig på lagar som föregick direktivet eller antogs efter dess ikraftträdande. I vissa fall, där det inte finns några särskilda bestämmelser om definitioner, införlivas brotten genom allmänna bestämmelser i strafflagen som har ett bredare tillämpningsområde, t.ex. bestämmelser om stöld. En utebliven anmälan om ett fullständigt införlivande av definitionen tyder därför inte nödvändigtvis på ofullständighet eller bristande överensstämmelse.

Till flera av definitionerna finns det korshänvisningar till definitioner i andra direktiv.

a) Icke-kontanta betalningsinstrument

Bedömningen har visat på minst ett fall av ofullständigt införlivande, eftersom definitionen i rådets rambeslut 2001/413/RIF inte hade uppdaterats. Följaktligen hänvisar den endast till fysiska betalningsinstrument och omfattar inte ”skyddade utrustningar, föremål eller handlingar, eller en kombination av dessa”, i enlighet med definitionen i direktivet.

b) Skyddade utrustningar, föremål eller handlingar

Flera medlemsstater har inte införlivat denna definition (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). Detta betraktas inte nödvändigtvis som ett fall av bristande efterlevnad, eftersom betydelsen vanligtvis är självförklarande eller kan härledas från ordalydelsen i definitionen av icke-kontanta betalningsinstrument. I vissa länder förklaras begreppet i förarbeten.

c) Digitala betalningsmedel och virtuell valuta

Dessa två definitioner är centrala i direktiv 2019/713, vars främsta mål var att ta itu med det faktum att rambeslut 2001/413/RIF inte längre återspeglade den nuvarande verkligheten och inte på ett tillfredsställande sätt hanterade nya utmaningar och teknisk utveckling, t.ex. virtuella valutor och mobilbetalningar, vilket behövde inkluderas för att säkerställa ett heltäckande svar på fenomenet och överbrygga oavsiktliga klyftor i kriminaliseringen.

Den viktigaste frågan som har uppstått vid införlivandet är täckningen av virtuell valuta enligt definitionen i artikel 2 d i direktivet. Även om elektroniska pengar definieras i alla medlemsstater, ofta till följd av införlivandet av direktivet om elektroniska pengar¹⁰, är definitionen och täckningen av virtuella pengar inte alltid enkel.

¹⁰ Europaparlamentets och rådets direktiv 2009/110/EG av den 16 september 2009 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet, om ändring av direktiven 2005/60/EG och 2006/48/EG och om upphävande av direktiv 2000/46/EG (EUT L 267, 10.10.2009, s. 7).

I Ungern betraktas virtuell valuta som egendom och elektroniska data och kan bli föremål för förverkande av egendom och beslag. På samma sätt definieras inte den virtuella valutan i lagstiftningen i Polen och det råder en viss osäkerhet om huruvida den skulle omfattas av de olika brott som är relevanta för införlivandet av direktivet, även om vissa upphovsmän anser att den virtuella valutan skulle kunna omfattas av bestämmelser i strafflagen som reglerar brott som rör information, databärare eller informationsuppgifter.

Många medlemsstater har införlivat dessa definitioner genom finansiella regler snarare än i straffrättsliga bestämmelser (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). Men det finns inte i alla dessa fall en korshänvisning till relevanta bestämmelser i den nationella lagstiftningen som fastställer brotten. Slutligen har båda definitionerna införlivats i strafflagen i tre medlemsstater (IT, MT, RO).

d) Informationssystem

I artikel 2 e definieras ”informationssystem” genom en korshänvisning till artikel 2 a i direktiv 2013/40/EU. Alla medlemsstater har införlivat definitionen i enlighet med direktivet.

e) Datorbehandlingsbara uppgifter

Datorbehandlingsbara uppgifter definieras i artikel 2 f genom en korshänvisning till artikel 2 b i direktiv 2013/40/EU. Alla medlemsstater har införlivat artikel 2 f i enlighet med direktivet.

f) Juridisk person

Slutligen definieras i artikel 2 g ”juridisk person”. Nästan alla medlemsstater har införlivat denna term i sin lagstiftning. Enda undantaget är Sverige, som inte definierar ”juridisk person”. Den närmaste termen som används i införlivandet är ”företag”. Denna term definieras i varken någon lagtext, rättslära eller rättspraxis.

2.2 Särskilda brott

a) Bedräglig användning av icke-kontanta betalningsinstrument

Enligt artikel 3 a i direktivet ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att bedräglig användning av ett stulet eller på annat sätt olovligen tillgripet eller införskaffat icke-kontant betalningsinstrument, när det sker uppsåtligen, utgör en straffbar gärning.

25 medlemsstater införlivade artikel 3 a i direktivet. Av de 25 länderna införlivade 14 direktivet genom en särskild bestämmelse om bedräglig användning av icke-kontanta betalningsinstrument (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). De återstående medlemsstaterna hänvisade till mer allmänna brott, t.ex. bedrägeri och datorförfalskning, eller bedrägeri med anknytning till betalningsmedel, som inte är begränsade till andra icke-kontanta betalningsinstrument (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

I Kroatiens lagstiftning hänvisas inte till användning av stulna eller på annat sätt rättsstridiga betalningsinstrument. Införlivandebestämmelsen i Ungern avser endast elektroniska icke-kontanta betalningsinstrument.

Enligt artikel 3 b i direktivet ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att bedräglig användning av ett helt eller delvis förfalskat icke-kontant betalningsinstrument, när det sker uppsåtligen, utgör en straffbar gärning.

Artikel 3 b införlivades i allmänhet på ett fullständigt sätt.

För att införliva direktivet hänvisar 15 medlemsstater till nationella bestämmelser om icke-kontanta betalningsinstrument (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), medan den nationella införlivandelagstiftningen i tio medlemsstater omfattar mer allmänna brott, t.ex. stöld eller bedrägeri, eller brott med anknytning till betalningsinstrument, men inte specifikt till icke-kontanta betalningsinstrument (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Brott med anknytning till bedräglig användning av fysiska icke-kontanta betalningsinstrument

Enligt artikel 4 i direktivet ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att de uppsåtliga gärningar som förtecknas i artikelns punkter är straffbara. Punkterna omfattar stöld eller annat olovligt tillgrepp av ett fysiskt icke-kontant betalningsinstrument (a), bedräglig hel- eller delförfalskning av ett fysiskt icke-kontant betalningsinstrument (b), innehav av ett stulet eller på annat sätt olovligen tillgripet, eller av ett helt eller delvis förfalskat fysiskt icke-kontant betalningsinstrument, för bedräglig användning (c), anskaffande för egen eller annans räkning, inbegripet mottagande, tillgrepp, inköp, överföring, import, export, försäljning, transport eller distribution av ett stulet eller ett helt eller delvis förfalskat fysiskt icke-kontant betalningsinstrument för bedräglig användning (d).

Artikel 4 tycks ha införlivats mer eller mindre bokstavligt, men i ett fåtal fall väcker det nationella införlivandet frågor där man för egen eller andras räkning anskaffar ett stulet, helt eller delvis förfalskat icke-kontant betalningsinstrument för bedräglig användning.

c) Brott med anknytning till bedräglig användning av icke-fysiska icke-kontanta betalningsinstrument

Artikel 5 i direktivet gör bedräglig användning av icke-fysiska icke-kontanta betalningsinstrument till en straffbar handling. Analysen visade att denna artikel inte verkar ha skapat några problem för införlivandet. I de flesta fall är den nationella bestämmelsen tillämplig på både fysiska och icke-fysiska icke-kontanta betalningsinstrument. Omkring hälften av medlemsstaterna har införlivat artikel 5 i direktivet genom mer allmänna bestämmelser (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK), och mer än hälften har införlivat artikeln genom en bestämmelse som särskilt avser bedräglig användning av icke-kontanta betalningsinstrument (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Bedrägeri med anknytning till informationssystem

Enligt artikel 6 i direktivet är medlemsstaterna skyldiga att se till att genomförande eller orsakande av en överföring av pengar, penningvärde eller virtuell valuta, som därigenom orsakar en olovlig förlust av egendom för en annan person i syfte att uppnå en olaglig vinst för gärningsmannen eller en tredje part, utgör en straffbar gärning om denna handling begås uppsåtligen genom att, utan rätt, hindra eller ingripa i ett informationssystemets funktion (artikel 6 a), eller utan rätt mata in, ändra, radera, överföra eller undertrycka datorbehandlingsbara uppgifter (artikel 6 b). Alla medlemsstater har införlivat artikel 6.

e) Verktyg som används för att begå brott

Artikel 7 i direktivet kräver att medlemsstaterna vidtar nödvändiga åtgärder för att säkerställa att framställning, anskaffande för egen eller annans räkning, eller tillgängliggörande av en utrustning eller ett instrument, datorbehandlingsbara uppgifter eller varje annat medel som i första hand är utformat eller särskilt har anpassats i syfte att begå något av de brott som avses i artikel 4 a–b, artikel 5 a–b eller artikel 6, åtminstone när brottet begås med avsikten att dessa medel ska användas, är straffbart.

De allra flesta medlemsstater har införlivat direktivets artikel 7 (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Sex länder har införlivat artikel 7 i direktivet genom bestämmelser som korshänvisar till mer omfattande bestämmelser, antingen om allmänna brott som stöld, eller om finansiella instrument och betalningsmedel (BG, FI, FR, LV, SE, SK). 17 länder har införlivat artikeln genom en särskild bestämmelse om verktyg som används för att begå de olika brotten i direktivet som rör fysiska och icke-fysiska icke-kontanta instrument (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Fem medlemsstater verkar ha stött på utmaningar i samband med införlivandet (BE, BG, HU, PL, PT).

2.3 Allmänna regler för de berörda brotten

a) Anstiftan, medhjälp och försök

Enligt artikel 8.1 i direktivet ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att anstiftan och medhjälp till ett brott som avses i artiklarna 3–7 är straffbart.

Alla medlemsstater har införlivat denna bestämmelse. De flesta medlemsstaterna har införlivat direktivet genom en redan befintlig artikel om anstiftan och medhjälp i allmänhet (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). Två medlemsstater beslutade dock att anta en ny bestämmelse, som endast är tillämplig inom ramen för brotten i direktivet (CY, MT).

Enligt artikel 8.2 första meningen i direktivet ska medlemsstaterna säkerställa att ett försök att begå ett brott som anges i artikel 3, artikel 4 a, b eller d, artikel 5 a eller b eller artikel 6 utgör en straffbar gärning. Alla medlemsstater verkar ha införlivat denna bestämmelse på ett fullständigt sätt, med undantag för BE, LU och SI.

Även här har majoriteten av medlemsstaterna införlivat direktivet genom en redan befintlig bestämmelse som gäller försök i allmänhet (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). Övriga har inkluderat det i en särskild införlivandeåtgärd (CY, DE, FI, MT, RO).

Medlemsstaterna ska också säkerställa att minsta försök till bedrägligt anskaffande av ett olovligt införskaftat eller helt eller delvis förfalskat icke-fysiskt icke-kontant betalningsinstrument för egen eller annans räkning (artikel 5 d) är straffbart, artikel 8.2 andra meningen.

Bedömningen visade att straffbeläggandet av försöket kan omfattas av begränsningar som inte föreskrivs i direktivet i två medlemsstater (HR, SI).

Övriga medlemsstater införlivade de relevanta bestämmelserna i direktivet. De gjorde detta antingen genom en artikel om försök i allmänhet (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK), eller genom en särskild införlivandeåtgärd (CY, DE, FI, MT, RO).

b) Påföljder

Artikel 9 föreskriver att brotten i artiklarna 3–8 ska vara belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder och anger vilka maximistraff som ska gälla för de olika brotten.

Medlemsstaterna har i allmänhet införlivat artikel 9 i direktivet, men i bedömningen identifierades möjliga frågor rörande definitionens räckvidd när det gäller artikel 9.2 i HR och 9.6 i BE, CZ, HR och HU.

Jämförelsen mellan medlemsstaternas påföljder för de olika brotten kompliceras av att brotten omfattas av både allmänna och särskilda bestämmelser. När medlemsstaterna införlivade direktivet genom bestämmelser om allmänna brott har de förlitat sig på flera nationella bestämmelser för att straffbelägga en av de gärningar som är förbjudna enligt direktivet. Detta leder till att flera maximistraff är tillämpliga för detta specifika brott och innebär att den faktiska maximala påföljden beror på varje enskilt fall, på domstolarnas tillvägagångssätt och på nationella bestämmelser om samtidiga påföljder. Som ett exempel, är regeln i Polen att en handling endast kan utgöra ett och samma brott. Om ett beteende motsvarar två eller flera straffrättsliga bestämmelser måste domstolen välja ett specifikt brott. Tvärtom ska domstolen i Bulgarien, i de fall där den särskilda delen av strafflagen föreskriver att två eller flera påföljder ska åläggas samtidigt för ett visst brott, fastställa omfattningen av varje påföljd så att summan överensstämmer med de allmänna målen för påföljden.

Dessutom kan vissa bestämmelser innehålla försvårande omständigheter som kan höja taket och leda till ökade påföljder. Maximistraffet beror därför på hur brottet begås. Den allmänna bestämmelsen om förskingring i Kroatien medför till exempel ett maximistraff på fem års fängelse. Om gärningsmannen använder våld är maximistraffet tio år, och om handlingen resulterar i en betydande materiell vinst riskerar gärningsmannen upp till 12 års fängelse. I Tyskland leder en förfalskning av fysiska icke-kontanta betalningsinstrument till högst fem års fängelse. Men om gärningsmannen agerade i kommersiellt syfte kommer straffet att vara högst tio år.

Bedömningen visade också att de tröskelvärden som fastställs i den nationella lagstiftningen i de flesta fall är strängare än de som fastställs i direktivet. Skillnaden kan vara betydande: Förfalskning av pengar är straffbart med upp till 15 år i Bulgarien och Luxemburg och upp till 25 år i Polen. Endast två medlemsstater föreskriver samma (eller mycket nära) maximistraff som i direktivet (AT, MT).

c) Juridiska personers ansvar

Bedömningen visade att 16 medlemsstater har införlivat artikel 10 i direktivet genom en redan befintlig allmän bestämmelse i sin strafflag (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), medan nio medlemsstater har införlivat den genom en särskild lag om juridiska personers ansvar inom ramen för direktivet (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sanktioner för juridiska personer

Enligt artikel 11 i direktivet ska medlemsstaterna fastställa effektiva, proportionella och avskräckande sanktioner i form av bötesstraff eller administrativa avgifter även för juridiska personer. Alla medlemsstater har fastställt sådana sanktioner.

I artikel 11 ges medlemsstaterna möjlighet att införa olika särskilda sanktioner för juridiska personer, t.ex. uteslutning från rätten till offentliga förmåner eller rättsligt beslut om upplösning av verksamheten. Sex medlemsstater utnyttjade inte möjligheten i artikel 11 i direktivet överhuvudtaget (AT, BG, EE, FI, NL, SE). De återstående 19 länderna har antingen införlivat hela artikel 11 eller delar av den (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Behörighet

Denna artikel, som ålägger medlemsstaterna att fastställa behörighet för brott som begås på deras territorium eller av en medborgare, införlivas i de allmänna bestämmelserna i den nationella strafflagen eller straffprocesslagen i alla medlemsstater. Territorialitetsprincipen och principen om aktivt medborgarskap har därför allmän giltighet och är inte specifika för de brott som regleras i detta direktiv. Dessutom införlivades artikel 12 av Cypern i den nationella lagen om bekämpning av bedrägerier och förfalskning av andra betalningsmedel än kontanter, och av Portugal i lagen om it-brottslighet.

Alla medlemsstater införlivade artikel 12.1 a och b.

Enligt artikel 12.3 får en medlemsstat fastställa sin behörighet över ett brott som avses i artiklarna 3–8 i direktivet vilket har begåtts utanför dess territorium, om bl.a. a) brottet begås av en person som har sin hemvist på dess territorium, b) brottet har begåtts till förmån för en juridisk person som är etablerad på dess territorium, eller c) brottet har begåtts mot en av dess medborgare eller mot en person som har hemvist på dess territorium. 14 medlemsstater (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) har utnyttjat den möjlighet som anges i artikel 12.3 a, 12 medlemsstater (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) införlivade artikel 12.3 b, och 16 medlemsstater (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) har utvidgat sin jurisdiktion i enlighet med artikel 12.3 c. När det gäller denna punkt c har det i Bulgarien, Tyskland, Estland, Ungern, Rumänien och Slovenien fastställts behörighet över ett brott som begåtts utanför landets territorium där brottet (endast) har begåtts mot en av landets medborgare – vilket utesluter personer med hemvist. Österrike föreskriver åtal enligt det österrikiska straffrättsliga systemet för brott som begåtts utomlands om gärningsmannen och brottsoffret är österrikare. CY, CZ, EL, FI, LV och MT har utnyttjat alla tre frivilliga bestämmelser i artikel 12.3.

2.4 Operativa uppgifter

a) Effektiva utredningar och samarbete

I alla medlemsstater ingår inte verktyg för att utreda och lagföra de brott som avses i artiklarna 3–8 uttryckligen i den lagstiftning som införlivar direktivet, utan snarare i mer allmän lagstiftning, t.ex. straffprocesslagar. Vanligtvis är möjligheten att använda ett utredningsverktyg i ett visst fall kopplad till påföljden för brottet i fråga. Såsom redan antyds i bestämmelsen i direktivet kommer de utredningsverktyg som används för att bekämpa organiserad brottslighet eller andra grova brott också att finnas tillgängliga för att utreda och lagföra de brott som fastställs i detta direktiv. Vissa utredningsverktygs exceptionella karaktär och vikten av proportionalitet till brottet ingår oftast i de relevanta rättsliga bestämmelserna och/eller i konstitutionen.

Information om de brott som avses i artiklarna 3–8 bör nå de myndigheter som utreder eller lagför dessa brott utan onödigt dröjsmål, enligt artikel 13.2 i direktivet. Därtill kommer att brottsbekämpande myndigheter och andra behöriga myndigheter i god tid bör få tillgång till relevant information för att utreda och lagföra de brott som avses i detta direktiv (skäl 22). Straffprocesslagen föreskriver ofta olika rapporteringssystem så att brott (i den mening som avses i artiklarna 3–8 i direktivet) kan rapporteras effektivt och snabbt. Dessa rapporteringssystem omfattar följande: en rapporteringsskyldighet för offentliga organ och myndigheter, ett visselblåsningssystem, ett klagomålsförfarande, en skyldighet för betaltjänstleverantörer att rapportera allvarliga operativa incidenter eller säkerhetsincidenter och privatpersoners rätt att rapportera incidenter. Dessutom kan vissa mer specifika lagar säkerställa att rapporter om säkerhetsincidenter (inklusive rapporter om allvarliga brott, t.ex. obehörigt förvärv, förfalskning och ändring av ett betalningsmedel) ges till de berörda myndigheterna så snart som möjligt. Sådana lagar rapporterades av AT, CZ, LT, FI, MT och PT.

Villkoret att den inlämnade informationen ska nå de berörda myndigheterna utan onödigt dröjsmål införlivas oftast inte uttryckligen.

b) Utbyte av information

Utbytet av information mellan nationella brottsbekämpande myndigheter i syfte att utreda och lagföra brott, inbegripet de som avses i artiklarna 3–8 i direktivet, kan underlättas genom operativa kontaktpunkter (skäl 26). Artikel 14.1 första meningen i direktivet säkerställer att medlemsstaterna faktiskt inrättar dessa kontaktpunkter och att de är tillgängliga dygnet runt alla dagar i veckan. Den andra meningen innebär dessutom en skyldighet för medlemsstaterna att ha förfaranden för att omgående behandla brådskande framställningar om bistånd och lämna svar inom åtta timmar, genom att åtminstone ange om begäran kommer att besvaras och i vilken form och den beräknade tid inom vilken svaret kommer att skickas.

Följande medlemsstater beslutade att använda sig av en befintlig operativ kontaktpunkt för de ändamål som beskrivs i detta direktiv: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

I tabell 1 ges en översikt över de etablerade kontaktpunkterna. Inga kontaktpunkter identifierades i BG, CZ, LU, SI, HR.

Tabell 1 operativa kontaktpunkter

Medlemsstat	Kontaktpunkt	Medlemsstat	Kontaktpunkt
AT	Federala kriminalpolisen	EE	Justitieministeriet
BE	Direktoratet för operativ polisinformation	FI	Centralkriminalpolisen
BG	ej tillämpligt	FR	Avdelningen för internationella förbindelser vid rättspolisens

			centraldirektorat
CY	Cyperns polis	HR	ej tillämpligt
CZ	ej tillämpligt	HU	Internationella centrumet för straffrättsligt samarbete (NEBEK)
DE	16 statliga kriminalpoliskontor och en federal kriminalpolisbyrå – centrala kontaktpunkter för it-brottslighet	MT	Maltas polis
EL	Grekiska polisen (avdelningen för internationellt polissamarbete)	ES	Krissamordningsenhet
IT	enhet för internationella operationer vid avdelningen för internationellt polissamarbete	NL	Nationellt centrum för internationell rättslig hjälp (LIRC)
LT	Andra divisionen i kårens styrelse vid polisens avdelning under republiken Litauens inrikesministerium och den litauiska kriminalpolisbyråns styrelse för internationella relationer	PL	Allmänna polishögkvarteret
LV	Nationella polisen	PT	Kriminalpolisen
RO	Åklagar- och brottsutredningsavdelningen vid den allmänna åklagarmyndigheten	SE	Polismyndigheten
SI	ej tillämpligt	SK	Kriminalpolisbyrån i polisens presidium i republiken Slovakien

Artikel 14.1 andra meningen i direktivet har i praktiken genomförts i ett fåtal medlemsstater. Information om de förfaranden som gäller för brådskande begäranden saknades i BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE, SK.

c) Rapportering av brott

Medlemsstaterna är också skyldiga att göra lämpliga rapporteringskanaler tillgängliga. Sådana kanaler för att rapportera misstänkt bedrägeri eller, mer allmänt, för att rapportera eventuella brott kan fastställas i lagstiftningsakter. Medlemsstaterna har ofta fastställt att rapportering av ett brott är en skyldighet för vissa kategorier (fysiska och juridiska) personer (vilket är i linje med artikel 15.2), medan brottsoffer och andra ”kringstående” ges möjlighet (men inte skyldighet) att rapportera. Dessa rättsliga bestämmelser kompletteras vanligtvis med praktiska genomföranden.

I alla medlemsstater kan skriftliga eller muntliga rapporter lämnas till polisen och/eller rättsväsendet. Dessutom har vissa medlemsstater tillhandahållit ytterligare rapporteringskanaler:

Den federala lagen i Österrike föreskriver olika rapporteringssystem så att brott (i den mening som avses i artiklarna 3–8 i direktivet) kan rapporteras effektivt och snabbt, nämligen följande: 1) en rapporteringsskyldighet för offentliga organ och myndigheter, 2) visselblåsarssystemet vid åklagarmyndigheten för ekonomiska frågor och korruption, 3) finansmarknadsmyndighetens system för visselblåsning och 4) betaltjänstleverantörernas skyldighet att rapportera allvarliga operativa incidenter eller säkerhetsincidenter. Ett särskilt rapporteringskontor för it-brottslighet har inrättats vid den federala kriminalpolisen. Dessutom samarbetar det federala inrikesministeriet med den federala ekonomiska kammaren. Till följd av detta sker olika utskick och kampanjer som motiverar och uppmuntrar allmänheten att rapportera relevanta lagöverträdelser.

I Belgien förvaltar ekonomiministeriet en enda kontaktpunkt för brottsoffer för bedrägerier, vilseledning och svindleri. Dessutom har en kanal för visselblåsning inrättats på laglig väg och gjorts tillgänglig av myndigheten för finansiella tjänster och marknader för alla klagomål som rör kredit- eller investeringsprodukter och -tjänster.

I Cypern utses Cyperns polis formellt, tillsammans med Cyperns centralbank och den nationella myndigheten för säkerhet i nätverks- och informationssystem, genom en lagstiftningsåtgärd till de behöriga nationella myndigheter som ansvarar för att inrätta lämpliga kanaler för rapportering och kommunikation.

I Tjeckien ålägger straffrätten statliga myndigheter att rapportera.

I Tyskland ska ansvariga enheter utan onödigt dröjsmål rapportera misstänkta transaktioner. Dessutom har icke-lagstiftningsåtgärder antagits på federal nivå, t.ex. ett institutionaliserat offentlig-privat partnerskap i syfte att upptäcka, förebygga, utreda eller lagföra brott som avses i artiklarna 3–8 i direktivet, och en plattform för informationsutbyte.

I Grekland har regeringen, utöver de allmänna rapporteringskanalerna, inrättat en statlig onlinetjänst där medborgare direkt kan lämna in klagomål för brott som begåtts på nätet. Dessutom måste kreditinstitut och andra betaltjänstleverantörer rapportera till Bank of Greece (som har behörighet när det gäller sådana klagomål) varje fall av bedrägeri direkt när de stöter på det.

I Spanien tillhandahåller Spaniens centralbank, förutom de allmänna kanalerna för rapportering av bedrägerier, en rapporteringskanal i samarbete med National Cybersecurity Institute.

Genom italiensk lagstiftning säkerställs att rättspolisens meddelande sker i tid till den allmänna åklagaren om nyheter om brott, som förvärvats på deras eget initiativ eller efter ett klagomål eller en stämning. Informationsutbyte uppmuntras också genom digitala plattformar.

Litauen har flera rapporteringskanaler för att rapportera brott som avses i artiklarna 3–8 i direktivet, via en webbsida (e-Police Portal), via det allmänna nödtelefonnumret 112, personligen, via e-post, via sms och via mobilapplikationen e-Police, och på andra automatiska sätt. Betaltjänstleverantörer, finansinstitut och andra ansvariga enheter, Litauens centralbank och utredningsavdelningen för ekonomisk brottslighet är skyldiga att underrätta de behöriga brottsbekämpande myndigheterna om rimliga misstankar om brottsliga och/eller andra olagliga handlingar.

I Luxemburg finns en webbplats som förklarar hur bedrägerier ska rapporteras. Kontrollkommissionen för finanssektorn fastställer riktlinjer för att upptäcka ekonomiska bedrägerier, men kräver också att alla verksamheter som står under dess tillsyn snarast ska rapportera alla bedrägerier och incidenter till följd av externa datorattacker.

I Rumänien finns det en rapporteringsskyldighet för offentliganställda och personer i ledande befattningar inom offentliga myndigheter, personer som utför tjänster i allmänhetens intresse och personer som agerar inom kontroll- och tillsynsorgan.

I Slovenien har alla statliga myndigheter och organisationer med myndighetsutövning en skyldighet att anmäla brott.

Enligt Perceval-plattformen i Frankrike, som inrättats genom en rättsakt, kan brottsoffer rapportera om bankkortsbedrägerier och förfalskningar. Det finns en liknande plattform för rapportering om it-brottslighet. Dessutom gäller påföljder för alla (fysiska eller juridiska) personer som inte genom en omedelbar handling förhindrar ett brott, vilket leder till en allmän rapporteringsskyldighet.

I Ungern fastställs skyldigheten att anmäla ett brott endast för personer knutna till myndigheten, offentliga tjänstemän och lagstadgade yrkesorganisationer. Den ungerska centralbanken uppmuntrar på sin webbplats finansinstitut att rapportera misstänkta bedrägerier i form av ett yttrande.

I Malta uppmanar den nationella kontaktpunkten till rapportering, särskilt av finansinstitut, om misstänkt bedrägeri och förfalskning av andra betalningsmedel än kontanter.

Förutom den rättsligt etablerade rapporteringskanalen för visselblåsare i Portugal finns det ett rapporteringssystem för it-brott, där det är möjligt att bara genom ett klick följa en länk som omedelbart öppnar ett e-postmeddelande som riktas till de behöriga myndigheterna.

I Sverige kan vissa typer av brott, t.ex. kreditkortsbedrägerier, även rapporteras via polisens e-tjänst. Aktörer inom bank- och finansverksamhet är också skyldiga att till polismyndigheten rapportera misstänkt verksamhet i samband med potentiella fall av penningtvätt eller finansiering av terrorism, eller egendom som på annat sätt härrör från en brottslig handling. Dessutom förs en fortlöpande dialog mellan bank- och finansverksamhet och polismyndighetens nationella bedrägericentrum.

I de rättsliga bestämmelserna i Slovakien fastställs ett krav på (samt förfaranden för) att offentliga myndigheter och andra juridiska personer skyndsamt ska anmäla brott till de brottsbekämpande myndigheterna. Det finns också rapporteringsskyldigheter när det gäller penningtvätt för ansvariga personer och särskilt banker.

Som ett alternativ har icke-lagstiftningsåtgärder som genomförs enligt artikel 15 i direktivet vidtagits i Nederländerna och Polen. Den nederländska polismyndighetens servicelinjer och polisens webbplats är lämpliga kanaler för att anmäla bedrägerier som inbegriper andra betalningsmedel än kontanter till myndigheterna. Den nederländska regeringen har dessutom åtagit sig att uppmana finansinstitut och andra juridiska personer till att rapportera varje misstanke om bedrägeri. Den ansatsen är bland annat tydlig genom att ett "front office" för ekonomiskt bedrägeri har inrättats vid alla polisenheter i Nederländerna. Dessutom har fyra större banker och ICS-kort undertecknat ett avtal med polisen för att gemensamt bekämpa (bank-)bedrägeri och nätfiske. I Polen godtas anmälningar om brott dygnet runt alla dagar i veckan av alla polisenheter. På grund av den typ av brott som begås med hjälp av datateknik är det också möjligt att direkt kontakta en specialiserad organisatorisk enhet vid polishögkvarteret. För att säkerställa snabbast möjliga samarbete med banksektorn har en samarbetskanal inrättats mellan byrån för bekämpning av it-brottslighet vid polishögkvarteret och det polska bankförbundets banksäkerhetscenter.

Artikel 15.2 i direktivet har inte införlivats i Bulgarien, Estland och Kroatien.

2.5 Stöd till brottsoffer och förebyggande åtgärder

a) Hjälp och stöd till brottsoffer

Hjälp och stöd till fysiska och juridiska personer vars personuppgifter har missbrukats säkerställs genom artikel 16.1 i direktivet. Sådana åtgärder skulle kunna omfatta: a) att de erbjuds särskild information och rådgivning om hur de kan skydda sig själva mot de negativa följderna av brotten och b) att de får en förteckning över särskilda institutioner som arbetar med olika aspekter av identitetsrelaterad brottslighet och stöd till brottsoffer.

I samma anda bör juridiska personer som är offer för de brott som avses i artiklarna 3–8 i detta direktiv ha tillgång till information om a) förfarandena för brottsanmälan, b) rätten att få information om ärendet, c) tillgängliga förfaranden för att inge klagomål om den behöriga myndigheten inte respekterar brottsoffrets rättigheter under ett straffrättsligt förfarande och d) kontaktuppgifter för information om det egna ärendet (artikel 16.3 i direktivet).

De flesta medlemsstaters straffprocesslag innehåller bestämmelser om brottsoffer och deras rättigheter, däribland vissa särskilda bestämmelser om offrens rätt till information och hjälp under förfaranden, rätten till rådgivning och rätten att inge klagomål. En särskild rättsakt som införlivar direktivet kompletterar ofta det som redan har fastställts i straffprocesslagen. Juridiska personer behandlas vanligtvis i separata rättsliga bestämmelser i straffprocesslagen eller någon annanstans. Dessutom finns olika informationskampanjer, broschyrer, särskilda webbplatser, cirkulär osv. tillgängliga för att hjälpa och stödja offer för de brott som avses i artiklarna 3–8 i direktivet. Detta är fallet i AT, BE (med avseende på artikel 16.1), CY, CZ, DE, IT, LT, LU (med avseende på artikel 16.1), LV (med avseende på artikel 16.3), RO, SI (med avseende på artikel 16.3), EE, FI (med avseende på artikel 16.1), FR (med avseende på artikel 16.1), HR, HU, NL, PL (med avseende på artikel 16.3), PT, SE och SK. Artikel 16.1 och/eller artikel 16.3 i direktivet har varken införlivats bokstavligen eller nästan bokstavligen, med undantag av MT.

Förteckningen över officiellt godkända rådgivningsorgan som ger stöd till brottsoffer, som avses i artikel 16.1 b i direktivet, finns vanligtvis tillgänglig online och genomförs därmed i praktiken.

b) Förebyggande insatser

Enligt artikel 17 om förebyggande åtgärder ska medlemsstaterna vidta lämpliga åtgärder, t.ex. kampanjer för information och medvetandegörande, forsknings- och utbildningsprogram. Detta avsnitt bygger på en bedömning av den information som medlemsstaterna har anmält till kommissionen samt en internetforskning med öppen källkod för att undersöka förekomsten av förebyggande åtgärder. Såsom beskrivs i tabell 2 nedan, när förebyggande åtgärder har identifierats, gäller dessa främst it-brottslighet och onlinebedrägeri. I vissa länder tillhandahålls dock också information om förebyggande av bedrägeri, vanligtvis av polisen.

Tabell 2 Förebyggande åtgärder

Medlemsstat	Åtgärder
AT	Den federala polisen tillhandahåller regelbundet information på sin webbplats och i sociala nätverk om hur man kan skydda sig mot bedrägerier. Samarbete med berörda parter, t.ex. handelskammaren stöds och genomförs inom ramen för e-handelsprojekt.
BE	Olika webbplatser med rådgivnings-/medvetandegörande material, t.ex. de som drivs av Centre for Cybersecurity Belgium (CCB). Ett visst samarbete med berörda parter kan identifieras genom internetsökning, t.ex. har den organisation som företräder finanssektorn samarbetat med den allmänna åklagarmyndigheten i Bryssel (Parquet) för att utveckla informationsmaterial.
BG	En kampanj för att bekämpa ”finansiella mulor” i Bulgarien inleddes 2021 av bankförbundet och genomfördes tillsammans med generaldirektoratet för bekämpning av organiserad brottslighet och åklagarmyndigheten. Generaldirektoratet har också inlett en kampanj om nätfiske.
CY	Polisens underavdelning för it-brottslighet tillhandahåller på sin webbplats information och råd om frågor som digitalt bedrägeri samt information om kommande evenemang, t.ex. informationskampanjer. Ett exempel är informationskampanjen om informationssäkerhet som genomförs av polisen, centralbankerna, bankförbundet och myndigheten för digital säkerhet.
DE	Den federala polisen (BKA) tillhandahåller på sin webbplats en översikt över de åtgärder som syftar till institutionaliserat offentlig-privat partnerskap i syfte att upptäcka, förebygga, utreda eller lagföra de brott som omfattas av direktivet, t.ex. partnerskapet mellan den federala kriminalpolisen (BKA), den federala myndigheten för informationssäkerhet (BSI) och det tyska kompetenscentrumet mot it-brottslighet (G4C), en sammanslutning av finansinstitut och företag inom it-säkerhetssektorn. BKA lanserade också konferensen om it-brottslighet C ³ , en plattform för utbyte mellan myndigheter, näringsliv, vetenskap och politik. G4C producerar också informationsbroschyrer och anordnar utbildning. Slutligen deltar BKA också i förebyggande åtgärder på området it-brottslighet på delstatsnivå, och på nationell nivå är BKA sammanlänkat med andra polismyndigheter och icke-polisiära organisationer (berörda parter) och intensifierar nu sitt samarbete, särskilt när det gäller trendfrågor.
FR	Inrikesministeriet offentliggör information om förebyggande av it-brottslighet. Plattformar som finns tillgängliga för att rapportera it-brottslighet omfattar även förebyggande budskap samt den nationella polisens informations- och kommunikationstjänst (SICoP). Andra exempel är vägledning från Frankrikes centralbank eller de riktlinjer om förebyggande av bedrägerier som offentliggjorts av nationella expertgruppen för bedrägeribekämpning, som samlar olika förvaltnings- och tillsynsmyndigheter.
EL	It-brottsavdelningen och polishögkvarteret är mycket aktiva när det gäller att informera allmänheten, öka medvetenheten och minska risken för att bli offer för bedrägerier, med tv-kampanjer, tal i utbildande syfte och information på nätet.
ES	Det spanska nationella cybersäkerhetsinstitutet och skattemyndigheten tillhandahåller på sin webbplats relevant information för att förhindra nätfiske, utpressningsprogram osv. i affärsmiljöer.
HR	Inrikesministeriet tillhandahåller onlineinformation om internetbedrägerier och sänder en Youtube-kanal avsedd för bedrägeri- och datorsäkerhet, som innehåller videor om it-bedrägerier.
IT	Finansdepartementet, som har till uppgift att förhindra bedrägerier med betalningsmedel, främjar redan en rad initiativ på lokal nivå, i samarbete med lokala förvaltningar och universitet, anordnar seminarier och workshoppar som riktar sig till de kategorier som är involverade i valutaförfalskning, inklusive medborgare.

LT	Information om förebyggande finns på webbplatsen för myndigheten för kommunikationsreglering om onlinebedrägeri och polisens webbplats om de vanligaste typerna av it-bedrägerier. Ett annat mål med den nationella strategin för it-brottslighet är att stärka förebyggande och kontroll av it-brottslighet, särskilt genom att utveckla ett effektivt samarbete mellan brottsbekämpande myndigheter och andra berörda parter.
LV	Finans- och kapitalmarknadskommissionen har utvecklat olika internetverktyg för att ge information och vägledning om frågor som rör ekonomisk säkerhet och bedrägerier. Dessutom har olika kampanjer anordnats i samarbete med den statliga polisen och centrumet för konsumentskydd.
NL	Åtgärder har vidtagits, t.ex. Fraudehelpdesk (hjälpplinen för bedrägerier) en organisation som subventioneras av den nederländska regeringen. När ett bedrägligt agerande kan rapporteras är Fraudehelpdesk en del av SAFECIN:s stichting, en stiftelse för att hantera finansiell och ekonomisk brottslighet i Nederländerna, med statlig medverkan.
SE	Det förs en fortlöpande dialog mellan bank- och finansverksamhet och polismyndighetens nationella bedrägericentrum NBC. Dessutom samarbetar NBC, även för brottsförebyggande ändamål, med t.ex. aktörer inom e-handel. Betydelsen av att anmäla bedrägerier till polisen betonas i dessa kontakter.

I tio medlemsstater (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK) hittades ingen information om lämpliga förebyggande åtgärder och praktiskt genomförande, även om lagstiftningen i Malta och Rumänien återspeglar denna skyldighet och ligger nära direktivets ordalydelse.

3. Slutsatser och nästa steg

Direktivet har lett till betydande framsteg när det gäller att straffbelägga bedrägerier och förfalskningar av andra betalningsmedel än kontanter på en jämförbar nivå i medlemsstaterna, vilket underlättar gränsöverskridande samarbete mellan brottsbekämpande myndigheter som utreder denna typ av brott. Medlemsstaterna har ändrat strafflagar och annan relevant lagstiftning, anpassat förfaranden och etablerat eller förbättrat samarbetssystem. Kommissionen är medveten om medlemsstaternas stora ansträngningar för att införliva direktivet.

Det finns dock ett stort utrymme kvar för att utnyttja direktivets potential till fullo om alla dess bestämmelser skulle genomföras fullt ut av medlemsstaterna. Analysen hittills tyder på att några av de viktigaste förbättringar som medlemsstaterna ska uppnå är artikel 2 d, där definitionen av virtuell valuta anges, artikel 7 om brott med anknytning till de verktyg som används för att begå brotten och artikel 8.2 om försök, artikel 9.6 om påföljder för fysiska personer om brottet begås inom ramen för en kriminell organisation, artikel 14 om informationsutbyte och artikel 16 om hjälp och stöd till brottsoffer.

Kommissionen kommer att fortsätta att stödja medlemsstaterna i deras genomförande av direktivet. I synnerhet kommer en särskild inbjudan att lämna förslag att offentliggöras 2023.

Kommissionen är angelägen om att säkerställa att införlivandet genomförs i hela EU och att bestämmelserna genomförs korrekt. I detta arbete ingår att övervaka att de nationella åtgärderna är förenliga med de relevanta bestämmelserna i direktivet. Vid behov kommer kommissionen att använda sina verkställandebefogenheter enligt fördragen genom överträdelseförfaranden.