Stockholm den 6 maj 2020

R-2020/0313

Till Justitiedepartementet

Ju2020/00180/L5

Sveriges advokatsamfund har genom remiss den 13 februari 2020 beretts tillfälle att avge yttrande över departementspromemorian Ett nytt brott om olovlig befattning med betalningsinstrument − genomförande av non-cash-direktivet (Ds 2020:1).

Sammanfattning

Advokatsamfundet har i huvudsak ingen erinran mot en utvidgad kriminalisering enligt departementspromemorians förslag.

En utvidgad kriminalisering måste dock genomgående uppfylla erforderliga krav på nödvändighet, effektivitet och proportionalitet. Utformningen av de definitioner och avgränsningar av det straffbara området som föreslås i departementspromemorian bör därför övervägas ytterligare för att straffskyddet ska ges en rättssäker, ändamålsenlig och begriplig avgränsning, anpassad till anknytande regelverk och de missbruk av e-legitimationer och bankdosor som blivit allt vanligare.

Begreppet betalningsinstrument

Advokatsamfundet delar departementspromemorians bedömning (s. 146) att brottsobjektet – betalningsinstrumentet – bör beskrivas så tydligt som möjligt för att tillgodose rättssäkerhetsintresset. Det är viktigt att klarhet råder beträffande vad som faller inom ramen för legaldefinitionen enligt vilken berörda objekt ska ha vissa egenskaper (de ska utgöra ”skyddade utrustningar, föremål eller handlingar”) och ska vara möjliga att bruka för betalningar (de ska ”ge möjlighet att överföra pengar eller penningvärde”). Av lagmotiven och motsvarande definition i direktivet följer att betalningsinstrument kan

bestå av en kombination av skyddade utrustningar, föremål eller handlingar.[1] De närmare exempel som ges i departementspromemorian på icke-fysiska betalningsinstrument framstår emellertid som delvis motsägelsefulla.

I den allmänna motiveringen nämns kontokortsuppgifter och mobilapplikationer för överföring av pengar (s. 146). Samtidigt hänvisas till avsnitt 6.4.1 där som icke-fysiska betalningsinstrument pekas ut mobilapplikationer för överföring av pengar, t.ex. *Swish*, *Google Pay* eller andra liknande betalningslösningar, kontokortsuppgifter (dvs. de siffror, inklusive uppgift om månad, år och CVC/CVV-kod som anges på ett kontokort) samt digitala plånböcker som tillåter överföring av virtuella valutor (s. 68). I författnings-kommentaren exemplifieras på nytt icke-fysiska betalningsinstrument med mobilapplikationer för överföring av pengar, kontokortsuppgifter och digitala plånböcker, som kan användas för överföring av virtuella valutor (s. 168).

När departementspromemorian därefter redovisar att berörda objekt ska vara *”skyddade”* för att utgöra betalningsinstrument nämns att identifiering med mobilt BankID kan krävas exempelvis för överföring av pengar med en mobilapplikation. Tillgång till enbart applikationen möjliggör inte överföring av pengar. Härvid uttalas emellertid att betalningsinstrumentet då utgörs av den mobila applikationen (s. 147). När direktivets motsvarande definition redovisas i departementspromemorians nästa stycke framgår också att ett betalningsinstrument kan bestå av en kombination av skyddade utrustningar, föremål eller handlingar, som ensamma eller i förening med ett förfarande eller en uppsättning förfaranden ger innehavaren eller användaren möjlighet att överföra penningvärde. Enligt direktivets (EU 2019/713) skäl 8 är ett olovligt införskaffande av en applikation för mobila betalningar utan det nödvändiga godkännandet (t.ex. ett lösenord) inte att betrakta som olovligt införskaffande av ett icke-kontant betalningsinstrument, eftersom det inte ger en faktisk möjlighet att överföra pengar eller penningvärde (se även departementspromemorian s. 67).

Advokatsamfundet ansluter sig här till direktivets definition, där kombinationer av skyddade *utrustningar*, *föremål* och *handlingar* kan utgöra betalningsinstrument. E-legitimationer såsom BankID, (skyddade) identitetsintyg och andra liknande handlingar, som ställs ut vid legitimering eller underskrift, för att skapa exempelvis betalningsorder, utesluts inte från definitionen av betalningsinstrument, vilket dock departements-promemorian synes ge uttryck för. Till detta kommer de lösenord och liknande som (ofta tillsammans med en användaridentitet) samlas in genom dataintrång och liknande missbruk för att säljas på en svart marknad. Frågan är om även dessa kan ses som (skyddade) handlingar och omfattas av föreslaget straffskydd; jfr det andra betaltjänstdirektivets krav på säker kundautentisering. Nedan lämnas bl.a. ett förslag till

[1] I direktivet (EU 2019/713) definieras ”icke-kontanta betalningsinstrument” som 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. Vidare definieras där ”skyddade utrustningar, föremål eller handlingar” som utrustningar, föremål eller handlingar som är skyddade mot imitation eller bedräglig användning, till exempel genom utformning, kodning eller signatur (artikel 2).

ett tillägg till den föreslagna legaldefinitionen av betalningsinstrument, i syfte att tillse att en kombination av objekt och rena lösenord som samlats in inte exkluderas.

Här bör nämnas att begreppet ”betalningsinstrument” också används i lagen (2010:751) om betaltjänster, definierat som ”ett kontokort eller något annat personligt instrument eller en personlig rutin som enligt avtal används för att initiera en betalningsorder”, och att BankID nämnts i lagmotiven som exempel på sådana betalningsinstrument (se vidare prop. 2009/10:122 s. 24).

Advokatsamfundet redovisar i det följande närmare sin bedömning av begreppet betalningsinstrument, samordnat med de brottsliga förfaranden som enligt departementspromemorian ska kriminaliseras.

Det brottsliga förfarandet och betalningsinstrumenten

Med utgångspunkt i det förfarande som enligt 9 kap. 3 c § första stycket 1 brottsbalken föreslås bli straffbart genom att olovligen införskaffa ett betalningsinstrument, kan noteras att de i departementspromemorian nämnda exemplen, *Swish* och *Google Pay*, och de allmänt spridda applikationerna för bank på internet, får införskaffas av var och en genom att laddas ned från allmänt tillgängliga digitala tjänster (exempelvis *App Store*). Till detta kommer att det ofta är vanliga webbläsare och allmänt tillgängliga betaltjänster som missbrukas för bedrägerier. Visserligen är sådana applikationer och tjänster i sig skyddade mot manipulation av programkod och liknande, men detta skydd är inte utformat för att identifiera en viss användare av berörd betaltjänst. Vad som tidigare gav skydd mot obehöriga transaktioner var i stället vanligtvis användaridentiteter i förening med lösenord som användare skulle komma ihåg och skriva in vid varje transaktion. Departementspromemorian ger intryck av att alltjämt röra sig inom detta område och den traditionella hanteringen av kontokortsuppgifter, utan annat skydd än CVC-/CVV-kod. För att motverka det ökade missbruket av betaltjänster och liknande har emellertid nya instrument införts, förenade med förfaranden så att dessa instrument i sig faller inom ramen för ordalydelsen i den föreslagna definitionen av betalningsinstrument, jfr dock det andra betaltjänstdirektivets krav på säker kundautentisering.

Utifrån departementspromemorians exempel på missbruk av *Swish* eller från vanliga applikationer och webbtjänster för bank på internet − där de numera i media så uppmärksammade bedrägerierna mot exempelvis äldre personer äger rum − är det regelmässigt ett krav att

- *betalaren legitimerar* sig med *e-legitimation* i form av BankID, genom att *aktivera* den med en kod eller ett biometriskt kännetecken (exempelvis fingeravtryck eller ansiktsigenkänning) i en tjänst som utfärdaren eller en till denne anknuten aktör tillhandahåller (t.ex. BankID-applikation i förening med BankID-server och lösenord för e-legitimation), och
- *utfärdaren* av e-legitimationen (eller en till denne anknuten aktör) *kontrollerar identiteten* och utfärdar bevis om vem denne är, ett s.k. *identitetsintyg,* som

- *förlitande institut* använder för att kontrollera att behörig individ har godkänt transaktionen.

Både e-legitimationer och identitetsintyg är skyddade handlingar enligt departementspromemorians förslag till definition och direktivets definition (vanligtvis med digital stämpel),[2] men bara identitetsintyget kan vara av intresse att ensamt samla in för att *i sig* missbrukas.[3] Till en e-legitimation hör dels en kryptografisk privat nyckel (hemlig och finns på t.ex. ett chip eller i innehavarens BankID-applikation), dels aktiveringskod/fingeravtryck/ansiktsbild. En samling av *e-legitimationer* tillsammans med *privat nyckel* och *aktiveringskod,* som erbjuds på en svart marknad, skulle vara en synnerligen farlig kombination av skyddade handlingar som i förening med varandra och en uppsättning förfaranden möjliggör överföring av pengar eller pengars värde.

Både e-legitimation och privat nyckel är ”skyddade” i direktivets och lagförslagets mening, den första genom digital stämpel och den andra i t.ex. ett chip eller logiskt i en programvara/applikation genom kryptering.[4] Aktiveringskoder är däremot något användare minns, som inte får antecknas så att missbruk möjliggörs, medan fingeravtryck och ansiktsform utgör biometriska data, svåra att kopiera och sprida i brottssyfte. Enligt Advokatsamfundets uppfattning bör även här beskrivna skyddade handlingar (e-legitimationer och identitetsintyg) omfattas av begreppet betalningsinstrument i 9 kap. 3 c § andra stycket brottsbalken, ensamt eller i förening med exempelvis *Swish*-app eller liknande programvara.

Att samla in en allmänt tillgänglig applikation (utan manipulation av den) är emellertid utan betydelse för en gärningsman som själv kan ladda ned den. Av betydelse är i stället att aktiveringsdata, såsom lösenord och liknande som bara den behöriga användaren får känna till, anses vara innefattat i begreppet betalningsinstrument, tolkat som en kombination av skyddade utrustningar, föremål eller handlingar. Mot denna bakgrund delar inte Advokatsamfundet bedömningen i departementspromemorian (s. 68, 146 och 168) att till icke fysiska-betalningsinstrument *självständigt* hör mobilapplikationer för överföring av pengar. Det är endast i förening med andra uppgifter, exempelvis skyddade handlingar, som definitionen av icke-fysiskt betalningsinstrument kan anses vara uppfylld, vilket departementspromemorian ger uttryck för på annan plats (s. 147).

Skyddet för kontokortsuppgifter har varit lågt ställt och det har sannolikt uppfattats som självklart att dessa i sig ska ses som betalningsinstrument och omfattas av ett straffskydd för olovlig införskaffning av betalningsinstrument. Efter att skärpta krav införts genom det andra betaltjänstdirektivet bör detta emellertid övervägas ytterligare.

[2] Se vidare exempelvis eSams juridiska vägledning för införande av e-legitimering och e-underskrifter, 1.1.
[3] Eftersom intygen har mycket kort giltighetstid blir en samling av sådana dock knappast användbar.
[4] Kravet på skyddsnivå kan inte vara högt ställt, eftersom kontokortsuppgifter anses vara skyddade. Det som införs för e-legitimationer, identitetsintyg och privata nycklar erbjuder normalt en *mycket* högre skyddsnivå.

Bedräglig användning av olovligen införskaffat betalningsinstrument

I 9 kap. 3 c § första stycket 3 och 4 brottsbalken föreslås straffansvar för den som bedrägligen använder ett olovligen införskaffat betalningsinstrument eller anskaffar, överför, tar emot, förvarar, tillgängliggör, transporterar, distribuerar eller tar annan liknande befattning med ett olovligen införskaffat betalningsinstrument.

Inget sägs i departementspromemorian om tidsfaktorn när det gäller det olovliga införskaffandet och den bedrägliga användningen. Detta bör enligt Advokatsamfundet förtydligas. Behovet av ett klargörande har sin grund i att de skyddsmekanismer som införts genom kryptografi blivit så svåra att forcera att gärningsmännen i stället inriktar sig på att vilseleda behöriga innehavare av betalningsinstrument att bruka dem så att (ofta äkta) betalningsorder ges för transaktioner till bedragare (vanligtvis målvakter). Dessa missbruk berörs i departementspromemorian när det redovisas att vilseledande kan ske via telefon och att det är ”ett vanligt tillvägagångssätt är att gärningspersonen försöker få tillgång till målsägandens BankID för att kunna utföra transaktioner via dennes internetbank eller med hjälp av Swish”.

Det är emellertid som framgått inte en riktig beskrivning att gärningsmannen vill få tillgång till målsägandens BankID. I stället vilseleds den behöriga innehavaren (av exempelvis BankID-applikation och e-legitimation) att legitimera sig eller skriva under genom att aktivera sin privata nyckel med hjälp av sin aktiveringskod eller sina biometriska data, så att en identitetskontroll utförs och ett identitetsintyg produceras och skickas till använd digital tjänst hos berört finansiellt institut. I många fall släpps en gärningsman också in i berörd digital tjänst, som om gärningsmannen var den behöriga användaren, och utför åtgärder där obehörigen som den behöriga användaren sedan vilseleds att auktorisera. Här kan det lika gärna vara bankdosor som missbrukas − vilka i förening med aktiveringskoden också bör ses som betalningsinstrument i lagförslagets mening.

Förfaranden som de beskrivna sker naturligtvis ”bedrägligen”. Enligt Advokatsamfundets mening bör berörda (skyddade) applikationer och handlingar i förening med använda koder anses vara ”betalningsinstrument” i den föreslagna paragrafens mening. Att de ”införskaffats olovligen” framstår som klart, även om det sker momentant och utan annan aktiv åtgärd av en gärningsman än att lura den behöriga användaren att aktivera sin e-legitimation eller liknande. Förfarandet går oftast ut på att ett (skyddat) identitetsintyg ska bli producerat och översänt, så att icke avsedda betalningstransaktioner kommer till stånd. Om en svart marknad tillhandahålls med exempelvis privata nycklar i förening med deras aktiveringskoder, bör dessa objekt kunna omfattas av begreppet betalningsinstrument, även om de inte skulle vara kryptografiskt skyddade utan hos en behörig användare får sitt skydd genom att memoreras eller förvaras endast på t.ex. ett chip som en angripare bara med mycket speciella angreppssätt kan bereda sig tillgång till.

Att det vanligtvis är fråga om en kombination av objekt och att rena lösenord som samlats in inte bör exkluderas, kan t.ex. komma till uttryck i legaldefinitionen genom följande tillägg: ”Med betalningsinstrument avses skyddade utrustningar, föremål, handlingar *och*

kombinationer av dem och uppgifter för aktivering som ger möjlighet att överföra pengar eller penningvärde.”

Straffskyddet för missbruk av urkund har inte beaktats

I departementspromemorian uppmärksammas inte att den som sanningslöst åberopar pass, betyg, identitetshandling eller annan sådan för enskild person utställd urkund såsom gällande för sig eller annan person eller lämnar ut sådan urkund för att missbrukas på det sättet, om åtgärden innebär fara i bevishänseende, döms för *missbruk av urkund* (15 kap. 12 § första stycket brottsbalken).

Såväl använda e-legitimationer som identitetsintyg brukar förses med digital stämpel och är därmed att anse som urkunder. Ovan beskrivna förfaranden för digitala betalningar utgör ofta missbruk av urkund, se vidare Juridisk Tidskrift 2017-18 s. 517. Det bör enligt Advokatsamfundets mening övervägas i vilken mån denna bestämmelse ytterligare kan begränsa behovet av författningsändringar med anledning av non-cash-direktivet.

Ansvar för missbruk av urkund kräver varken att användningen ska vara bedräglig eller att urkunden ska vara ett betalningsinstrument. Det räcker att urkunden ”sanningslöst” åberopats, så att någon annan släppts in eller att urkunden lämnas ut för att missbrukas på det sättet, så att fara i bevishänseende uppkommer, jfr det i traditionell miljö vanliga fallet att en underårig lånar annans körkort för att bli insläppt på en tillställning med åldersgräns.

Även den kriminalisering som föreslås i en ny 9 kap. 3 a § brottsbalken ges emellertid ett vidsträckt tillämpningsområde. Det räcker att betalningsinstrumentet (som i många fall kan vara en urkund i brottsbalkens mening) införskaffas olovligen eller att ett olovligen införskaffat sådant tillgängliggörs, vilket ofta sker vid ovan beskrivna missbruk. Till detta kommer att det enligt definitionen av betalningsinstrument endast krävs att instrumentet ”ger möjlighet” att överföra ett penningvärde. Någon sådan överföring måste inte ha ägt rum eller vara avsedd i det enskilda fallet för att straffansvar ska kunna komma i fråga. E-legitimationer såsom BankID kan också alternativt användas för tillträde till eller underskrift i myndigheters e-tjänster. Oberoende av avsedd användning i ett konkret fall, bör den föreslagna straffbestämmelsen kunna tillämpas.

Straffskyddet bör inte begränsas till betalningar. Behovet av skydd mot olovligt införskaffande och tillgängliggörande av identitetsintyg har blivit alltmer angeläget på myndighetsområdet. Sådana handlingar ger möjlighet att överföra penningvärden, men de kan i det enskilda fallet i stället brukas exempelvis för att få tillträde till en e-tjänst. Detta behov har numera blivit starkt uttalat när hela tjänster tillhandahålls på nätet för att missbruka e-legitimationer och identitetsintyg så att någon annan släpps in (t.ex. ett företags robot) än den som anges i e-legitimation och identitetsintyg.

Betalningsinstrument har kommit att användas i betydande omfattning, inte bara för betalningsorder och liknande, utan också för att skydda myndigheter och företag mot att

obehöriga bereder sig olovlig tillgång till myndigheters eller företags digitala tjänster eller uppgifter som förvaras skyddat från olovlig åtkomst via nät.

De ansvars-, gränsdragnings- och konkurrensfrågor som härvid uppkommer, bör enligt Advokatsamfundets mening närmare belysas i lagstiftningsärendet.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander