JUSTITSMINISTERIET
Lovafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 2. februar 2016
Kontor: Databeskyttelseskontoret
Sagsbeh: Kristian Gyde Poulsen
Sagsnr.: 2016-0030-4061
Dok.: 1838722

Hermed sendes besvarelse af spørgsmål nr. 158 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 5. januar 2016. Spørgsmålet er stillet efter ønske fra Peter Skaarup (DF).

Søren Pind

/

Jakob Lundsager

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 158 (Alm. del) fra Folketingets Retsudvalg:

> "Vil ministeren kommentere artiklen "Kundeservicen var i top, da Politiken købte to danskeres personlige oplysninger" fra Politiken den 3. januar 2016, hvoraf det fremgår, hvor nemt det er at erhverve sig en danskers personlige oplysninger, som i det beskrevne tilfælde, hvor Politiken på hjemmesiden Alpha-Bay i løbet af få timer købte 2 danskeres personlige oplysninger omfattende navn, fødselsdato, adresse, telefonnummer, e-mailadresse, kodeord, ip-adresse oplysninger om pcstyresystem, kreditkortnummer, kontrolkode m.v., det der ifølge artiklen kaldes fullz på markedspladserne i undergrunden?"

Svar:

1. Justitsministeriet har til brug for besvarelse af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> "Rigspolitiet, Nationalt Cyber Crime Center (NC3), har - med forbehold for de opgaver, der varetages af Politiets Efterretningstjeneste - det overordnede politifaglige ansvar for politiets opgavevaretagelse vedrørende kriminalitet, hvor digitale spor indgår i efterforskningen, herunder salg af identiteter på internettet. I den forbindelse yder NC3 bl.a. efter anmodning bistand til politikredsene som led i politikredsenes efterforskning og forfølgning af denne kriminalitetsform, når efterforskningen kræver særlig avanceret teknologi, ekspertise eller rutine.
>
> Det er Rigspolitiets erfaring, at mulighederne for at efterforske og retsforfølge sager om ulovlig handel med personlige oplysninger på internettet varierer betydeligt.
>
> Når det konstateres, at der foregår ulovlig handel med identiteter på en dansk hjemmeside, er der mulighed for, at politiet kan iværksætte bevissikring med henblik på videre efterforskning og en strafferetlig vurdering.
>
> Imidlertid foregår denne handel dog i en vis udstrækning via servere placeret i udlandet, herunder i lande uden for EU. I forhold til efterforskning, hvor sådanne servere indgår, kan det være nødvendigt at rette henvendelse til de pågældende landes retshåndhævende myndigheder med henblik på, at der iværksættes relevante og nødvendige efterforskningsskridt i sagen. Det er Rigspolitiets erfaring, at de retshåndhævende myndigheders iværksættelse af efterforskningsskridt i en del lande kan tage lang tid. I visse tilfælde har Rigspolitiet tillige erfaring med, at efterforskning slet ikke indledes. Hertil kommer, at det er Rigspolitiets erfaring, at materialet i en del tilfælde kun be-

finder sig meget kortvarigt på en server, hvorefter det flyttes videre til en anden server eventuelt i et andet land. Dette kan vanskeliggøre iværksættelse af straffeprocessuelle tiltag med den fornødne hurtighed.

Da kriminalitetsfænomenet således ikke altid kan bekæmpes ved strafforfølgning, søger politiet ved en række initiativer mere generelt at imødegå den ulovlige handel med identiteter på internettet samt følgekriminalitet.

Rigspolitiet indgår således i et tæt samarbejde med Finansrådet, de danske pengeinstitutter samt betalingsvirksomheden Nets. I den forbindelse foretager Rigspolitiet - i det omfang Rigspolitiet bliver bekendt med, at der er større mængder af personoplysninger til salg på nettet - underretning af Nets og de relevante pengeinstitutter med henblik på spærring af eventuelle betalings- eller kreditkort samt kontakt til de personer, hvis identitet muligt vil blive eller allerede er blevet misbrugt.

Rigspolitiet kan endvidere oplyse, at Rigspolitiet har haft indledende drøftelser med Det Centrale Personregister vedrørende mulighederne for at etablere en såkaldt "blokeringsordning", hvormed en borger har mulighed for at "blokere" sit CPR-nummer. En sådan ordning vil kunne sikre en borger, der har blokeret sit CPR-nummer, mod yderligere misbrug af dette, ligesom det vil kunne sikre de erhvervsdrivende mod indgåelse af kreditaftaler med personer, der uretmæssigt benytter sig af stjålne identiteter, med tab til følge.

Det er Rigspolitiets vurdering, at selvom disse initiativer ikke i sig selv forhindrer handlen med identitetsoplysninger på internettet, så vil de dog kunne medvirke til at gøre handel med identitetsoplysninger mindre attraktivt, da det bliver sværere at anvende sådanne oplysninger efterfølgende til generering af et udbytte.

Rigspolitiet arbejder endvidere med at få etableret et særligt forum, hvor det private erhvervsliv og politiet kan have en løbende dialog og erfaringsudveksling om forebyggelse af hackerangreb og andre former for it-kriminalitet. Det er ligeledes tanken, at dette forum skal være et sted, hvor både erhvervslivet og politiet hurtigt kan få kompetente svar på spørgsmål vedrørende it-kriminalitet og generelle sikkerhedsforhold. Det er Rigspolitiets vurdering, at der igennem dette forum, som har særlig fokus på små og mellemstore virksomheder, vil kunne ske en generel højnelse af it-sikkerhedsniveauet i virksomhederne, hvilket vil kunne føre til, at det bliver sværere for de kriminelle at skaffe stjålne identiteter, der kan sælges videre.

Endelig kan Rigspolitiet oplyse, at Rigspolitiet har erfaring med blokering af internetsider med ulovligt indhold. Rigspoli-

tiet driver således i samarbejde med Red Barnet og størstedelen af de danske internetudbydere det såkaldte netfilter, hvis formål er på frivillig basis at blokere adgang til materiale med seksuelt misbrug af børn på internettet. I den forbindelse stiller Rigspolitiet løbende oplysninger til rådighed for internetudbyderne om internetadresser, som Rigspolitiet finder indeholder materiale, som er omfattet af straffelovens § 235. Det er herefter internetudbyderne, der blokerer for siderne i henhold til internetudbydernes forretningsbetingelser. Dette samarbejde har vist sig nyttigt og effektivt i en lang række sager, herunder særligt i sager med servere placeret i udlandet. Det er Rigspolitiets vurdering, at en sådan blokeringsordning også vil kunne anvendes i forhold til handel med personlige oplysninger på internettet. Dette forudsætter dog, at udbyderne vil være indstillet på at udvide samarbejdet til også at omfatte denne form for kriminalitet. Rigspolitiet vil tage initiativ til en dialog med branchen om at udvide den frivillige blokeringsordning til at omfatte handel med personoplysninger.

For så vidt angår statistiske oplysninger om kriminalitetsformen er Rigspolitiet ikke umiddelbart i besiddelse af oplysninger om antallet af sager om tilfælde, hvor en stjålen identitet er blevet solgt via internettet. Dette skyldes, at identitetstyveri og -misbrug ikke er selvstændigt kriminaliseret i dansk ret, hvorfor der ikke i Politiets Sagsstyringssystem er nogen selvstændig journalkode til sager vedrørende identitetstyveri. Sager vedrørende identitetstyveri oprettes med forskellige journalkoder, afhængig af hvordan identitetstyveriet og -misbruget er udført. Der kan således være begået en strafbar handling både i forbindelse med erhvervelsen af identiteten, eventuelt via hacking af en virksomheds kundedatabase, ligesom der kan tænkes begået strafbare handlinger i forbindelse med et eventuelt senere misbrug af den købte identitet til for eksempel indgåelse af kreditaftaler eller lignende. Størstedelen af sagerne vil således været oprettet under journalkoderne for dokumentfalsk, bedrageri eller databedrageri, men der kan også være oprettet sager vedrørende identitetstyveri under en række andre journalkoder.

På denne baggrund og til brug for besvarelsen af spørgsmålet om, hvor mange markedspladser, der i de senere år er blevet lukket, og hvor mange handlende, der er blevet anholdt, har Rigspolitiet anmodet politikredsene om oplysning herom. Ingen politikredse ses umiddelbart at have kendskab til sager, hvor ulovlige markedspladser er blevet lukket, eller at personer skulle være blevet anholdt i forbindelse med sådanne. Nordjyllands Politi har oplyst, at en person i en sag om handel med personoplysninger og andre forhold om kreditoplysninger den 15. januar 2013 blev idømt fængsel i 1 år og 3 måneder. Der skete ikke anholdelse eller varetægtsfængsling i sagen, idet den

pågældende begik forholdene i forbindelse med afsoning af en anden dom."

2. Justitsministeriet kan desuden oplyse, at det efter straffelovens § 263, stk. 2, er strafbart uberettiget at skaffe sig adgang til en andens oplysninger, der er bestemt til at bruges i et informationssystem. Bestemmelsen omfatter tilfælde, hvor en person f.eks. hacker en computer, server, tablet eller lignende og dermed uberettiget skaffer sig adgang til oplysninger, der normalt ikke er offentligt tilgængelige, såsom fødselsdato, e-mailadresse, kodeord, ip-adresse mv. Hacking af systematisk eller organiseret karakter kan straffes med op til 6 års fængsel.

Personer, der skaffer sig eller uberettiget udnytter oplysninger, som er fremkommet ved f.eks. de ovenfor nævnte tilfælde af hacking, kan ligeledes ifalde strafansvar, jf. straffelovens § 264 c. Det er således også strafbart at modtage eller udnytte oplysninger, der hidrører fra et tilfælde af (strafbar) hacking, selvom den, der modtager eller udnytter oplysningerne, ikke har medvirket til selve hackingen.

Straffelovens § 264 c om efterfølgende medvirken udstrækker således i princippet strafansvaret til alle de personer, der efterfølgende skaffer sig eller uberettiget udnytter oplysninger, der stammer fra et tilfælde af hacking. Både mellemmanden og modtageren, herunder køberen, af de konkrete oplysninger vil efter omstændighederne kunne straffes efter den nævnte bestemmelse i straffeloven.

Et eventuelt efterfølgende misbrug af oplysninger fra f.eks. kreditkort vil kunne udgøre en selvstændig strafbar handling. F.eks. vil det være strafbart efter straffelovens § 279 a om databedrageri, hvis den person, der uberettiget har skaffet sig oplysninger om et kreditkort, men som ikke selv har foretaget den oprindelige hacking, anvender oplysningerne på kreditkortet til at købe ting mv. over internettet.

3. Herudover indeholder persondatalovens kapitel 4 regler om, hvornår videregivelse og anden behandling af personoplysninger må finde sted, mens lovens kapitel 11 indeholder regler om beskyttelse af personoplysninger.

Persondatalovens kapitel 4 er opbygget således, at § 5 indeholder en række grundlæggende principper for behandling af personoplysninger, som altid skal iagttages, mens §§ 6-8 indeholder generelle betingelser for, hvornår behandling af ikke-følsomme og følsomme personoplysninger må finde sted. Endvidere indeholder § 11 generelle betingelser for, hvornår behand-

ling af oplysninger om personnummer må finde sted.

Indsamling af personoplysninger ved kriminelle handlinger og videregivelse af sådanne oplysninger i form af salg til brug ved kriminelle handlinger vil ikke være i overensstemmelse med behandlingsreglerne i persondatalovens kapitel 4.

Det fremgår af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Indehavere af hjemmesider, hvorfra der kan købes varer mod betaling med kreditkort, har således en pligt til at beskytte de personoplysninger, herunder kreditkortoplysninger, der indsamles fra kunder, mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Hvordan oplysninger nærmere skal beskyttes, vil i første omgang være op til den dataansvarlige at vurdere. Datatilsynet anbefaler dog, at private dataansvarlige i videst muligt omfang tilrettelægger deres sikkerhedsforanstaltninger i overensstemmelse med den såkaldte sikkerhedsbekendtgørelse (bekendtgørelse nr. 528 af 15. juni 2000), der ellers kun gælder for den offentlige forvaltning.

4. For så vidt angår spørgsmålet om beskyttelse af betalingskortoplysninger i forbindelse med internethandel, har Justitsministeriet indhentet en udtalelse fra Erhvervs- og Vækstministeriet, der bl.a. har oplyst følgende:

> ”Udbydere af betalingstjenester, fx udstedere af betalingskort, skal ifølge lov om betalingstjenester og elektroniske penge have betryggende kontrol- og sikkerhedsforanstaltninger på IT-området. Finanstilsynet offentliggjorde i januar 2015, at de fra 1. august 2015 vil anvende EBA’s retningslinjer for sikre internetbetalinger i deres tilsyn med ovennævnte virksomheder. Det indbefatter bl.a., at der skal anvendes såkaldt stærk kundeautentifikation ved brug af betalingskort på internettet, og at udbyderen af kortbetalinger skal forpligte internetforretninger, som modtager kort, kontraktuelt til at opbevare data forsvarligt.
>
> Stærk autentifikation indebærer, at en betaling skal godkendes med to faktorer, fx oplysninger, der fremgår af kortet, og en sms-kode, der sendes til købers mobiltelefon. Ved at anvende stærk autentifikation sikres det, at stjålne kreditkort ikke kunne

anvendes til at foretage køb på internettet, med mindre den kriminelle også har stjålet offerets mobiltelefon. Det nye krav har bl.a. medført, at Nets er begyndt at udvikle en sådan løsning for Dankort. Løsningen forventes at træde i kraft inden sommerferien 2016, hvilket forventes at reducere misbruget med Dankort betragteligt.

Derudover fastsætter det nyligt vedtagne 2. betalingstjenestedirektiv (PSD II) en række nye sikkerhedskrav, som skal styrke IT- og den operationelle sikkerhed for udbydere af betalingsløsninger. Direktivet skal være endeligt implementeret i medlemslandene senest 13. januar 2018. En række af sikkerhedskravene er dog meget overordnede, da den europæiske banktilsynsmyndighed, EBA, skal fastsætte retningslinjer for disse. De første af disse retningslinjer forventes ligeledes at træde i kraft fra januar 2018 og de sidste af disse i løbet af 2018. Samlet set vil det være med til at styrke sikkerheden ved betalinger og beskyttelsen af forbrugernes data."

5. Justitsministeriet kan i øvrigt oplyse, at ministeriet sammen med Erhvervs- og Vækstministeriet er ved at udarbejdet en kortlægning af beskyttelsen af oplysninger om borgernes elektroniske betalinger mv. Kortlægningen skal danne udgangspunkt for en politisk drøftelse af området.

For nærmere information herom henvises til Justitsministeriets besvarelse af 14. januar 2016 af spørgsmål nr. 147 (Alm. del) fra Folketingets Retsudvalg.