Politi og information

Af Peter Blume

»*And although my eyes were open,*
they might as well have been closed«[1]

Mange samfundsmæssige funktioner er betinget af, at der er adgang til den information, som er nødvendig for funktionens udøvelse. Sådan har det altid været, men det er blevet mere tydeligt i informations- og netværkssamfundet, hvor mængden af information er eksponeret til ubeskrivelige højder med den risiko, at information virker kontraproduktivt ved ikke at skabe grundlaget for viden, men derimod for ikke viden. Den overvældende informationsmasse kan kaste et slør, der enten understøtter en illusion om viden, som ikke er med undertiden uheldige eller problematiske konsekvenser til følge, eller blot skabe den frustrerende oplevelse af uvidenhed selvom grundlaget for viden i og for sig er til stede. Man ser, men ser alligevel ikke, og selvom der skal være en høstak, for at der er en nål, kan man ikke finde nålen. Der kan foreligge en form for informationsdød, selvom denne karakteristik kan være for dramatiseret. Risikoen er dog til stede, og den er en vigtig advarsel, der sender et signal om, at "enough is enough".

Denne tilstand, der blander fordele og ulemper ved det digitaliserede liv, kan opleves mere eller mindre mærkbart afhængig af typen af den samfundsmæssige funktion og det formål, som den efterspurgte information tager sigte på. Der er forskel mellem funktioner, der er nødvendige for samfundet, og funktioner, der ganske vist er nyttige, men som ikke har en essentiel karakter. En informationel dysfunktion kan have større eller mindre negativ indflydelse på samfundet i almindelighed.

1. Gary Brooker, Keith Reid, Matthew Fisher: A whiter shade of pale. (Procol Harum 1967).

1. Politiets informationsbehov

I det følgende sættes fokus på den funktion, der udøves af politiet med det almindelige udgangspunkt, at uden (relevant) information kan et politi ikke fungere og leve op til de forventninger, der generelt kan stilles til et politi. Når politiet i denne sammenhæng er interessant, skyldes det, at der her udøves en samfundsmæssig funktion, som i almindelighed anses for nødvendig, og som der alt andet lige er enighed om ikke kan undværes. Mange andre offentlige institutioner kan der være forskellige meninger om, og måske kan de undværes, uden at samfundet fungerer på en mindre god måde. Det gælder ikke for politiet, selvom dette ikke nødvendigvis indebærer en tilslutning til, at et bestemt politi fungerer godt eller er indrammet på en tilfredsstillende måde. Det er politifunktionen som sådan, der karakteriseres ved at være nødvendig i forhold til opretholdelse og sikring af de grundlæggende normer og værdier i et samfund. Politiet udøver sin specifikke funktion og råder over midler, som naturligt altid vil påkalde sig kritisk opmærksomhed, hvilket sædvanligvis betragtes som sundt i demokratiske samfund, hvor politiet anses for påkrævet, men ikke skal være dominerende eller styrende (”politistat”).

Alle samfund har til alle tider haft en instans, der varetager politiets funktion. Det danske starter formelt i 1682, men politimæssige funktioner har altid været udøvet. Det gælder også i samfund, der kan være enighed om at karakterisere som demokratiske. Bortses der fra ordensmæssige funktioner, beror dette for så vidt på en sørgelig iagttagelse. Denne fortæller, at selvom der er fastsat regler, som borgere og virksomheder som retssubjekter skal følge, kan dette ikke tages for givet, og der er ikke samfund, hvor en almindelig respekt for retten medfører, at reglerne, uanset om man kan lide dem eller ej, i alle tilfælde og uden videre bliver overholdt. I et sådant lykkeligt samfund vil der ikke være behov for et kriminalitetsorienteret politi, men dette er en utopi, der ikke er eller bliver virkelighed.

Selv i såkaldte harmoniske samfund bliver reglerne ikke altid overholdt, og det gælder også for regler, som reproducerer anerkendte og nærmest internaliserede moralske normer. Dette er nok tydeligst for de af straffelovens regler, som er forbundet med religiøse bud, f.eks. om at man ikke må slå ihjel. Det ved alle, men det er ikke ensbetydende med, at alle ikke gør det. Lovovertrædelser af denne karakter er for så vidt ofte simple og er ikke normalt i synderlig grad direkte forbundet med informationssamfundet, men det forudsætter alligevel information for at klarlægge de

faktuelle omstændigheder. Informationsbehovet er selvsagt mere tydeligt, jo mere kompliceret den enkelte regelovertrædelse er. Der opstår spindelvæv og mønstre, der skal gennemtrænges for at opnå en kohærent forståelse af den specifikke sammenhæng.

Bastant udtrykt må politiet have information for at kunne sikre lov og orden. Denne information kan have en forskelligartet karakter, og visse hovedtyper må fremhæves. Først og fremmest må der skelnes mellem den personrelaterede og den øvrige information. Det er vanskeligt at foretage denne opdeling knivskarpt, fordi formålet med at indsamle den øvrige information i sidste instans er at finde eller understøtte et spor, der leder frem til en mulig gerningsperson. Selvom det er en virksomhed, der efterforskes, er genstanden reelt personer i virksomheden; betegnelsen juridisk person er som bekendt en fiktion, men den fremhæver dog det personelle aspekt. Bevæger politiet sig eksempelvis søgende rundt på IoT (Internet of Things), er formålet ikke kun, men dog også personorienteret. Dette betyder, at al den information, som politiet efterspørger under et formålsorienteret perspektiv, på et eller andet niveau er personrelateret.

Sondringen mellem de to informationstyper giver alligevel mening, fordi det er den egentlige personrelaterede information, som aktualiserer integritetsspørgsmål og derfor fremmaner særlig opmærksomhed. Det er her, politiretten møder persondataretten; et møde, som ikke altid er helt venskabeligt. Her noteres blot, at der et møde, idet der sættes mere fokus på dette nedenfor.

En anden central typeopdeling er relateret til informationens oprindelse. Der er information, som findes i Danmark, inden for det hjemlige politis jurisdiktion, og der er information, der for at findes også kan eller nogle gange skal søges uden for Danmark. Det er særligt karakteristisk for den udenlandske information, at den ofte er forbundet med efterforskning af grænseoverskridende forhold, som i mange tilfælde har interesse for flere landes politi. Den er international og opfordrer til samarbejde, som i praksis giver anledning til et forvitret spindelvæv af politiorganiseringer og ekstensive politidatabaser m.v., der repræsenterer et for de fleste uigennemskueligt mønster.[2] Den internationale information har en fremtrædende digital dimension knyttet til det forhold, at internettet, cy-

2. Se i denne forbindelse Bjarne Kvam, Politiets persondatarett (Oslo 2014), der redegør for de mange politidatabaser, der var aktuelle på dette tidspunkt. Dette er en krævende detektivopgave, og nu fire år senere er landskabet ikke blevet mere overskueligt.

berspace, er uden grænser og dermed i sig selv internationaliserer information. Der er og kan skrives meget om denne form information og dens strukturering, men her forbliver den blot et vigtigt opmærksomhedspunkt.

Politiet udøver forskellige typer af funktioner, og det kan overvejes, om der skal tages hensyn hertil ved den nærmere fastlæggelse af det legitime informationsbehov. Bredt formuleret bliver der skelnet mellem forskellige former for orienteringspunkter, idet der generelt er en proaktiv funktion, hvor den mulige forbrydelse ligger i fremtiden, og en reaktiv funktion, hvor forbrydelsen er et faktum. Den reaktive funktion er den mest præcise, fordi der her er et fast fokuspunkt, som vel ikke er fastlagt definitivt, men som dog indrammer informationsbehovet. Den proaktive funktion er derimod mindre demarkeret, idet den er baseret på mistanke eller på en begrundet fornemmelse af kriminel aktivitet. Den er ikke grebet ud af den blå luft, men dens informationsbehov er ikke klart afgrænset og dermed mere åben for de fristelser, som det digitale liv tilbyder. De informatoriske problemer er for så vidt de samme, men de er særligt accentuerede, når politifunktionen er proaktiv.

Så langt kan alle være med i hvert fald på det overordnede niveau, men det er ikke uden videre ensbetydende med, at politiet frit skal have adgang til enhver information, som politiet selv anser for relevant. Det er her, vanskelighederne opstår, og hvor der skal træffes valg, som ikke blot har betydning for politiet, men for samfundet som sådant. Retten træder ind på banen. Information kan være frit tilgængelig, eller forudsætter dens indsamling, at bestemte retlige betingelser opfyldes. Det er således ikke tilstrækkeligt, at politiet råder over den nødvendige teknologi og har evnen til at lokalisere den relevante information. Politiets almindelige karakteristika medfører retlig regulering, der overordnet tager sigte på, at poltiet fungerer, som det er ønskeligt i et demokratisk samfund. Politiet med dets legitimitet til anvendelse af fysisk tvang kan ikke være autonomt eller selvbestemmende. Der gælder således grænser for, hvad der kan indsamles, de midler, som kan bruges til indsamlingen, hvad informationen kan bruges til, og hvor længe den kan opbevares. Der er en retligt determineret ramme, som er samfundsmæssigt bestemt, og som søger at tage højde for den dragende kraft, som karakteriserer information.

Disse forskellige reguleringsspørgsmål, der tit kan være kontroversielle, besvares som udgangspunkt ud fra, hvilken type information der er tale om, og hvilken form for kriminalitet der udløser informationsbehovet. I alle tilfælde skal der træffes vanskelige valg, der er forbundet med

bestemte prioriteringer, og disse vanskeligheder er nok mest udtalte, når der er tale om personrelateret information, hvor der da også er den mest tætte regulering.

Retsplejeloven regulerer i almindelighed en række af de midler, der kan benyttes, idet fokus her er på indramningen af de straffeprocessuelle tvangsindgreb. Disse regler, der er i stadig bevægelse, er forholdsvis gamle, og de er udformet ud fra en vurdering af forholdet mellem effektiv efterforskning og retssikkerhed under hensyntagen til den specifikke mistankegrad og form for kriminalitet, som er efterforskningens tema. Reglerne har for så vidt en persondataretlig dimension, men deres udformning er ikke betinget af hensynet til databeskyttelse, der kun indirekte er et moment ved udformningen af den ordning, der er fastsat i retsplejeloven. Disse regler skal dog anvendes sammen med persondataretten, der aktiveres i de tilfælde, hvor tvangsindgrebet foretages. Reglerne legitimerer informationsindsamlingen, men udfylder ikke den persondataretlige ramme.[3]

2. Retshåndhævelsesdirektiv og lov

Persondataretten indrammer på væsentlig måde informationsanvendelsen. I det europæiske charter er databeskyttelse fastslået som en grundlæggende rettighed i artikel 8. Der er tale om en selvstændig rettighed og ikke blot, som det traditionelt har været tilfældet, en del af retten til privatlivets fred (EMRK artikel 8). I TEUF artikel 16 fastslås, at enhver har ret til databeskyttelse. Dette overordnede retsgrundlag har stor ideologisk betydning, og værdimæssigt indrammer det politiets persondataanvendelse. I takt med den teknologiske udvikling er persondataretten i det hele taget blevet en stadig mere fremtrædende del af retssystemet. Der er hermed skabt en forventning om at alle, der bruger personoplysninger, sikrer databeskyttelse. Dette må ske på forskellig måde afhængig af den funktion, der udøves, og ved den nærmere fastlæggelse af udformningen af regelgrundlaget og hvorledes fastsatte bestemmelser skal udfyldes, kan der derfor tages hensyn til politiets særlige opgaver.

3. Der findes vist nok ikke en undersøgelse af relationen mellem persondataretten og straffeprocesretten. Selvom retsplejelovens regler retsdogmatisk må antages at have forrang, er der tale om et felt, der har betydelig interesse.

Persondataforordningen, 2016:679, er et almindeligt udgangspunkt for databeskyttelsen, men det er anerkendt, at politiets funktion samfundsmæssigt er speciel samtidig med at en del af politiets funktion er særlig under et tværgående EU perspektiv. Hertil kommer, at brug af en forordning på dette område ikke harmonerer med det overordnede EU-retlige grundlag, og den tætte tilknytning retshåndhævelse, herunder politiets virksomhed, har til medlemsstaternes suverænitet.

Det er vel ikke nødvendigt at anfægte de særlige reguleringer eksempelvis af Europol, Eurojust, Frontex og Schengen, selvom et samlet regelsæt frem for det institutionelt betingede ville være befriende set under det databeskyttelsesmæssige perspektiv, men disse regler indicerer, at der er tale om specielle forhold og en egen tradition, som bør tages i betragtning. Dette taler for en flerhed af sui generis-reguleringer, der tager sigte på persondatabehandling med henblik på retshåndhævelse.

På denne baggrund blev der samtidig med persondataforordningen udstedt et direktiv, 2016:680, som specielt regulerer retshåndhævende myndigheders persondatabehandling.[4] Direktivet har erstattet rammeafgørelse 2008/977 (bekendtgørelse 1287/2010), der stammer tilbage fra den gamle søjlestruktur. Direktivet gælder forud for forordningen, jf. dennes artikel 2, men er inspireret af forordningen. Direktivet er gennemført ved lov 410/2017 og før databeskyttelsesloven (maj 2018), hvilket var nødvendigt for, at Danmark kunne opnå en tilslutningsaftale med Europol.

Det må indledningsvis fremhæves, at loven ikke omfatter al politivirksomhed, idet dens fokus er politiets kriminalitetsbekæmpende virksomhed, jf. § 1, stk.1,[5] og man kan konstatere, at politiet, man fristes til at sige vanen tro, skal forholde sig til tre regelsæt, persondataforordning, retshåndhævelseslov, databeskyttelseslov. Der er tegnet et komplekst retligt landskab, som det fremover sikkert ikke altid bliver helt enkelt at finde rundt i. I det følgende fremhæves enkelte aspekter af de specielle regler i retshåndhævelsesloven.

Den almindelige databeskyttelsesret karakteriseres ved at være centreret om en række generelle principper, jf. også forordningens artikel 5. Tilsvarende gælder her i § 4, hvor der er taget hensyn til retshåndhævelsens særlige karakter. Der er specielt grund til at pege på § 4, stk. 5, om vide-

4. Direktivet er omtalt i 1.udgave af Peter Blume: Den nye persondataret (København 2016).
5. Hverken direktivet eller forordningen gælder for efterretningstjenesterne

regivelse, der ikke indgår i forordningen. Efter denne regel skal der udvises særlig omsorg, når oplysninger bliver videregivet, idet dette bl.a. beror på, at videregivelse er en integritetsrisikabel form for persondatabehandling. Det skal sikres, at oplysninger er korrekte og ikke vildledende, og den afgivende myndighed skal verificere oplysningerne og ligeledes ledsage dem med anden information således at den modtagende myndighed har et grundlag til at bedømme oplysningernes korrekthed. Der skal være politimæssig disciplin baseret på kvalitetssikring. Dette er en interessant regel, da den mere intensivt end sædvanligt stiller krav til videregivelsen, der ofte er en kritisk del af persondatabehandlingen. Det er altid væsentligt, at der behandles korrekte oplysninger, men det kan med en vis ret hævdes, at dette er særligt vigtigt ved retshåndhævelse, hvor fejl kan få følelige konsekvenser for de implicerede personer. Især for oplysningens modtager, der ikke selv har indsamlet den pågældende oplysning kan det være svært at vurdere om den er korrekt.[6] Dette gælder ikke kun objektivt, men i nok højere grad i forhold til den sammenhæng, som oplysningen skal anvendes inden for. En oplysnings karakter er ikke altid stabil, men er derimod påvirket af konteksten. Det er positivt, at denne regel er medtaget, og den burde måske også indgå i den almindelige databeskyttelsesret.

En mere kritisk problemstilling aktualiseres af formålsbestemthedsprincippet, der angiver, at indsamlede oplysninger ikke på et senere tidspunkt må anvendes til et formål, som er uforeneligt med det oprindelige. Umiddelbart kan dette princip, der tager sigte på at sikre transparens, virke hæmmende på retshåndhævelsen. I § 4, stk. 2, henvises som ramme til de formål, der i almindelighed betinger loven, jf. § 1, stk. 1, men princippet kan fortsat virke begrænsende. På denne baggrund angiver § 5, stk. 1, at behandling til et andet formål kan ske "på baggrund af" af en lov, når det er nødvendigt og forholdsmæssigt. I forhold til hidtil gældende ret er dette en udtalt liberalisering, der er på linje med forordningens artikel 6(4). Det er svært på indeværende tidspunkt at vurdere, hvor stor en praktisk betydning denne nyordning vil få. Fleksibilitet er væsentlig for retshåndhævelsen, men den må ikke implementeres på bekostning

6. Denne iagttagelse er i øvrigt årsagen til, at mange amerikanske virksomheder er betænkelige ved en ret til indsigt i forhold til oplysninger indhentet fra andre kilder. Datakvaliteten er ikke kontrolleret og (store) erstatningskrav kan dermed blive konsekvensen.

af retssikkerhed eller medføre et unødvendigt tab af transparens. Der er tale om et opmærksomhedspunkt for fremtiden.[7]

Hensynet til transparens er i det hele taget centralt placeret i persondataretten, idet åbenhed og gennemskuelighed skaber grundlaget for tillid, der bl.a. understøtter anvendelsen af moderne teknologi. Oplysningspligten er et af de væsentlige midler, idet dette ikke mindst skyldes, at denne rettighed ikke forudsætter en anmodning fra den registrerede og praktisk ikke kun er forbeholdt de få stærke registrerede. Sædvanligvis er oplysningspligten struktureret ud fra to situationer, idet der skelnes imellem oplysninger fra den dataansvarlige, som har indsamlet persondata, og fra den dataansvarlige, der har modtaget data fra en anden dataansvarlig. Denne opdeling benyttes ikke her, idet der i § 13 er en samlet oplysningspligt. Det er ikke klart hvorfor dette er tilfældet, men det kan skyldes, at det er et forholdsvis begrænset antal oplysninger, der skal gives, hvorfor der ikke er praktisk grund til at særregulere den indirekte indsamling, som normalt opfattes som mest belastende for den dataansvarlige. Oplysningspligten er tvedelt, idet meddelelse af nogle oplysninger efter stk. 1 er obligatorisk, f.eks. den dataansvarliges identitet og behandlingsformålet, medens andre efter stk. 2 kun skal gives, når det er nødvendigt for, at den registrerede kan varetage sine interesser. Disse oplysninger omfatter retsgrundlaget, opbevaringstiden og kategorier af modtagere.

Det er under alle omstændigheder væsentligt, at der er oplysningspligt, men det er åbenbart, at den under bestemte omstændigheder kan virke negativt i forhold til det formål, som retshåndhævelsen tilsigter. Under dette perspektiv er åbenhed ikke et ubetinget gode. Det er interessant og en smule overraskende, at det ikke er muligt helt at undlade oplysningspligten, idet dette i § 14 kun er muligt af bestemte årsager i forhold til de oplysninger, der er omfattet af § 13, stk. 2. Dette er for så vidt positivt, eftersom en helt lukket og hemmelig retshåndhævelse dermed synes at være udelukket. Transparens kan begrænses, men ikke fjernes. Dette kan ses som tegn på, at persondata behandles inden for rammerne af et demokratisk samfund, og at der ikke må være kafkaske tilstande. Den ubetingede oplysningspligt i forhold til § 13, stk. 1, kan dog som nævnt også anskues som overraskende, idet der kan være situationer,

7. Under Folketingets behandling af forslaget til databeskyttelseslov (L 68, 25.10.2017) gav spørgsmålet om den nærmere udfyldning af formålsbestemthedsprincippet anledning til betydelig uenighed. Resultatet, § 5, stk. 3, er måske mindre restriktivt, da der ikke her stilles krav om lovhjemmel.

hvor disse oplysninger kan være en hæmsko for efterforskning og opklaring. Hensynet til databeskyttelse og hermed forbundet retssikkerhed har været mest tungtvejende.

Et væsentligt spørgsmål angår sikringen af, at den dataansvarlige har orden i sit eget hus. Det er vigtigt, at politiet har overblik over sin persondatabehandling, og at de hertil knyttede rutiner er indrettet således, at der tages hensyn til databeskyttelse. I direktivet og loven benyttes nogle af de instrumenter, der kendes fra forordningen.[8]

I lovens § 23 foreskrives, at den dataansvarlige politimyndighed skal udarbejde en fortegnelse, der bl.a. skal angive, hvilke kategorier personer og personoplysninger der registreres, hvilke kategorier modtagere oplysninger videregives til, eventuelle slettefrister, anvendelse af profilering, hvis dette benyttes, samt typer af dataoverførsler. Fortegnelsen er et internt arbejdsinstrument, der skal have en disciplinerende funktion i den dataansvarliges dagligdag ved at tilvejebringe et overblik over den persondatabehandling, der foretages. Da fortegnelsen ikke indeholder persondata, udløser den ikke rettigheder for de registrerede, der dog vil kunne anvende offentlighedsloven. I modsætning til forordningen (artikel 30(2)) er det ikke fastsat, at Datatilsynet i en konkret sag kan forlange fortegnelsen udleveret. Dette sender måske et signal, men har dog ikke stor betydning, da tilsynet kan rekvirere fortegnelsen i medfør af § 41, stk. 1, hvorefter tilsynet kan forlange enhver oplysning udleveret. Fortegnelsen vil være et nyttigt instrument, der i øvrigt skal opdateres, såfremt forholdene ændrer sig.

På samme måde som andre dataansvarlige foretager politiet forskellige former for persondatabehandlinger, der har varierende betydning for de registreredes integritetsbeskyttelse. Behandlinger, der kan indebære en høj risiko, påkalder sig særlig opmærksomhed. Dette kan bl.a. være behandlinger, hvor der anvendes ny teknologi, og hvor der er en sådan risiko som følge af ukendskab til, hvorledes teknologien vil virke. I § 25 bestemmes, at der i så fald skal gennemføres en konsekvensanalyse. Denne analyse tager sigte på at afdække risikoen og fastlægge de foranstaltninger, der vil medføre, at risikoen ikke aktualiseres. En sådan analyse kan føre til forskellige resultater. Det kan vise sige, at der alligevel ikke er en høj risiko. Der er en høj risiko og de kompenserende foranstaltninger vil være for krævende, hvorfor behandlingen bliver opgivet. Der er en høj

8. I modsætning til forordningens artikel 25 er der ikke fastsat en forpligtelse til databeskyttelse per design. Dette er for så vidt bemærkelsesværdigt.

risiko, men den kan reduceres eller fjernes ved brug af bestemte foranstaltninger. Alt i alt skal den dataansvarlige vide, hvad han gør, og indrette sig herpå.

Når der skal benyttes kompenserende foranstaltninger for at fjerne risikoen, skal Datatilsynet inddrages, jf. § 26. Tilsynet skal skriftligt rådgive den dataansvarlige og kan her anvise foranstaltninger, der bør foretages. Tilsynet kan påbyde disse og kan ligeledes forbyde behandlingen, når den ikke findes betryggende, jf. § 42. Selvom der ikke er en anmeldelsesordning, er der således en tilladelseskompetence. I denne forbindelse er det interessant i forhold til den ophævede persondatalov, der ikke åbnede en sådan mulighed, at Datatilsynet på dette uhyre, statslige område har denne kompetence. Kun fremtiden vil vise, i hvilken udstrækning forbud vil blive anvendt. Formodningen er, at det kun sjældent bliver tilfældet.

Databeskyttelse opnås ikke kun ved retlige regler, men forudsætter faktiske foranstaltninger, der sikrer personoplysningerne imod at blive brugt til uautoriserede formål eller blive ødelagt. Datasikkerhed er nødvendig både i forhold til eksterne trusler, herunder hacking, og interne angreb, der består i ansattes datamisbrug. Tilstrækkelig datasikkerhed er den dataansvarliges ansvar, jf. § 27, og dette er et vidtgående ansvar, der tit er ressourceudløsende. Ansvaret er krævende grundet den digitale teknologi, der tilbyder både sikkerhed ("PET") og usikkerhed ("PIT")[9]. Den dataansvarlige er nødt til at være oppe på mærkerne og være det konstant, da sikkerhedslandskabet hele tiden forandres. Den digitale virkelighed er konstant innovativ. Det er ikke altid nødvendigt at bruge de nyeste midler, state of the art, men det er godt at være opmærksom på dem, så der kan træffes rationelle valg. Dette gælder ikke mindst for politiet, der har en åbenbar interesse i god datasikkerhed. Politiet råder over oplysninger, der har stor interesse for andre med betydelig misbrugsrisiko, idet dette ikke kun gælder i forhold til dem, der direkte berøres negativt, de mistænkte. Erfaringsmæssigt gælder det også for den undertiden for nysgerrige offentlighed, og som nævnt også for de politiansatte selv.

Sædvanligvis angiver de almindelige persondataretlige regler ikke bestemte sikkerhedsforanstaltninger, da der er en risiko for forældelse under reglernes levetid. Den teknologineutrale form foretrækkes. Lovens § 24 gør i overensstemmelse med direktivet en bemærkelsesværdig und-

9. PET = Privacy Enhancing Technology; PIT = Privacy Invasive Technology.

tagelse, da det foreskrives, at der skal ske logning.[10] Herved registreres, hvilken computer der på et bestemt tidspunkt har søgt adgang til en bestemt oplysning. Denne fremgangsmåde sikrer intern disciplin og modvirker den fristelse, som enkelte oplysninger repræsenterer. Reguleringen tager herudover i vidt omfang sigte på at hindre det eksterne angreb, hvor bl.a. firewalls kan være et middel, ligesom maskering af oplysninger ved bl.a. pseudonymisering og kryptering kan fremhæves. Hacking er en svøbe, der hviler tungt over internettet, idet den ikke "blot" kan have en fjendtlig hensigt, men også er sport, hvor den ene hacker demonstrerer sin dygtighed over for andre hackere. Uanset motivet skal hackingen undgås.

Sikkerhed har høj prioritet, men selv den mest regelrette og omsorgsfulde dataansvarlige kan blive udsat for et sikkerhedsbrud, der medfører risiko for de registreredes integritet. Medmindre dette er en helt usandsynlig konsekvens, foreskriver §§ 28-29 en meddelelsespligt. Den dataansvarlige skal, senest 72 timer efter at bruddet er konstateret, meddele bruddet til Datatilsynet, herunder de reaktioner, der er iværksat. De registrerede skal, når risikoen er høj, orienteres direkte uden unødig forsinkelse, idet der dog er en række undtagelser fra denne ressourcekrævende forpligtelse. Meddelelsespligten skaber lys på et område, hvor der hidtil har været mørke. Et sikkerhedsbrud kan have en negativ indvirkning på den dataansvarlige politimyndigheds omdømme og kan vise, at der ikke har været tilstrækkelig omhyggelighed. Medmindre det ikke er muligt, kan det derfor være fristende at holde bruddet inden for murene. Dette gælder måske særligt for en myndighed som politiet, som ofte påkalder sig stor offentlig interesse. Mørket kan medføre, at der ikke sker en tilstrækkelig bearbejdning af sikkerhedshændelsen. Det er derfor både i forhold til det aktuelle brud og fremtidig sikkerhed væsentligt, at det skal meddeles. Det er endvidere i § 28, stk. 5, fastsat, at den dataansvarlige skal dokumentere alle sikkerhedsbrud og således have en historie, der kan læres af.

Meddelelsespligten medvirker til at skabe en god databeskyttelseskultur, men det må erkendes, at det for politiet og andre retshåndhævende myndigheder kan være svært at honorere de persondataretlige regler, der er komplekse og for mange er lidet tilgængelige. De repræsenterer en bar-

10. Jf. direktivets artikel 25 og i forbindelse hermed artikel 63(3), hvoraf fremgår, at dette krav ikke kan opfyldes af alle politimyndigheder i EU, således at der gælder en overgangsregel, der først udløber i 2026.

riere. På denne baggrund fastsættes i §§ 30-31, at der skal udpeges en databeskyttelsesrådgiver (DPO), hvis opgave er at bistå med, at der er den foreskrevne databeskyttelse, og herunder fungere som kontaktled til Datatilsynet. Rådgiverens funktion er primært intern, men omfatter som nævnt også en vigtig relation til tilsynsmyndigheden. Denne ordning vil bidrage til, at der udøves god skik, og selvom der ikke som i forordningen (artikel 37) stilles krav om, at rådgiveren skal have persondataretlig ekspertise, vil ordningen fremme en god databeskyttelsesmæssig orden.

Et afsluttende spørgsmål er, om det har konsekvenser for politiet, såfremt lovens regler ikke bliver overholdt. Dette spørgsmål er en særlig udgave af den almindelige problemstilling, om det giver mening at pålægge offentlige myndigheder et persondataretligt ansvar. I forordningens artikel 83(7) overlades spørgsmålet til medlemsstaterne, og i databeskyttelseslovens § 41, stk. 6, er der fastsat en sanktionsregel, der ifølge lovbemærkningerne i værste fald kan medføre en bøde på 16 mio. kr. Retshåndhævelsesdirektivets artikel 57 angiver, at der skal være sanktioner, men overlader udfyldningen til medlemsstaterne.

En ordning, der svarer til den ovenfor nævnte, gælder ikke på dette område, idet politiet efter § 50, stk. 2, alene kan pålægges en bøde, når det ikke efterkommer et påbud eller forbud udstedt af Datatilsynet. Der er således en meget begrænset sanktionering, idet det dog må anmærkes, at forvaltningsretligt disciplinæransvar kan bringes i anvendelse over for ansatte,[11] der ikke har levet op til deres persondataretlige forpligtelser. Når det tages i betragtning, hvor stor betydning persondataanvendelse har på dette område, er dette en skuffende ordning, idet der næppe er tvivl om, at en direkte sanktionering har betydning for den alvor, som de fastsatte regler mødes med. Selvom der er et legitimt hensyn til, at politiets effektivitet ikke begrænses, ville en direkte sanktionering, der kunne sættes lavere end de 16 mio. kr., derfor være ønskelig. Sagens alvor ville på den måde være betonet.

4. Den gode databeskyttelse.

Databeskyttelse i relation til retshåndhævelse og i forhold til politiets virksomhed har central betydning for borgerne og for retssamfundet. Po-

11. Se hertil Peter Blume, UFR 2014 p. 337-41.

litiet lever og må leve af persondata. Politiet må leve på en måde, der er samfundsmæssigt acceptabel, således at politiet kan udøve sin funktion, samtidig med at borgernes integritet er beskyttet. Der er som beskrevet en retlig regulering, og den er i hvert fald i et vist omfang specialiseret til den særlige situation, der omgiver politiet. Der er taget hensyn til, at politiet naturligvis må kunne fungere og må betragtes som en særlig type dataansvarlig, der på nogle punkter må have muligheder, som er tilpasset dets funktion. Bliver reguleringen respekteret, er der tilvejebragt et grundlag for tillid og tryghed, som måske ikke er optimal, men dog vil være betydelig. De kommende år vil vise, om denne ordning fungerer på en betryggende måde, og om den personlige integritet og privatlivet, der må beskyttes for enhver borger, faktisk bliver værnet på tilstrækkelig måde, således at der er god databeskyttelse. Det vil også vise sig, om ordningen understøtter, at politiet databeskyttelsesmæssigt kan virke i nutidens digitale samfund og her varetage sin centrale funktion.

Persondataretten skal understøtte et godt og effektivt politi, der udøver sine essentielle funktioner i et demokratisk samfund, og som gør dette inden for rammer, der fremmer tillid og tryghed på den måde, at de borgere, der får personoplysninger behandlet ikke kommer i situationer, hvor de møder datamisbrug. Denne situation skal borgerne opleve trygt, samtidig med at også politiet skal være trygt i det digitale miljø, der kan fremtræde som en urskov med en overvældende mængde information fra en uoverskuelig mængde digitale kilder, der løber alle mulige steder i skoven og aktualiserer en risiko for at såvel borgere som politi bringes i en tilstand, hvor de ser, men ikke ser, og dermed fremtræder som "a whiter shade of pale".