Notat vedrørende Folketingets Administrations søgning efter e-mails til medlemmer af Folketinget og partiansatte

1. INDLEDNING OG PROBLEMSTILLING

Folketingets Administration blev kort før påsken 2024 opmærksom på, at et medlem af Folketinget havde modtaget en e-mail fra en borger, hvori fremgik både navn og billede på en sigtet i en verserende straffesag om drab. Folketingets Administration var fejlagtigt af den opfattelse, at der var nedlagt navneforbud i sagen, således at videredeling af informationen i e-mailen ville være strafbart.

Folketingets Administration foretog en søgning på, hvilke folketingsmedlemmer og partiansatte der havde modtaget en lignende e-mail fra borgeren med henblik på at underrette de respektive personer om, at indholdet af e-mailen var ulovligt, og at e-mailen skulle slettes.

På denne baggrund har Folketingets Administration den 5. april 2024 anmodet om vores vurdering af, hvorvidt Folketingets Administration i sagen har overtrådt straffelovens § 263, stk. 1 og 2, om at skaffe sig uberettiget adgang til andres data og brud på brevhemmeligheden, Den Europæiske Menneskerettighedskonventions artikel 8 om retten til respekt for privatliv og korrespondance samt gældende databeskyttelsesretlige regler i databeskyttelsesforordningen og -loven.

2. KONKLUSION OG ANBEFALINGER

Som nærmere beskrevet i vurderingen i afsnit 5 nedenfor kan vores konklusioner og anbefalinger sammenfattes som følger:

- Det er samlet set vores vurdering, at Folketingets Administrations udsøgning af e-mails ikke var foreneligt med straffelovens § 263, stk. 1, eller med EMRK artikel 8.
- Det er endvidere vores vurdering, at Folketingets Administrations udsøgning af e-mails ikke skete i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra a, om god databehandlingsskik, artikel 5, stk. 1, litra c, om dataminimering samt databeskyttelsesforordningens artikel 6, stk. 1, litra e.
- Der gælder en række formildende omstændigheder i sagen: I formildende retning taler, *at* formålet med søgningen – at advare modtagerne af e-mailen – tjente et sagligt formål,

idet Folketingets Administration befandt sig i en faktisk vildfarelse, *at* medarbejderen, der foretog udsøgningen af e-mails, havde en berettiget adgang til spam-filtret og var sikkerhedsgodkendt og underlagt tavshedspligt, *at* søgningen blev gennemført som en "nålestiksoperation", hvor der alene blev søgt på den pågældende e-mail og ikke bredt, og hvor Folketingets Administration ikke forsøgte eller fik adgang til modtagernes e-mailindbakker eller indholdet i de fremfundne e-mails, *at* Folketingets Administration straks slettede listen efter søgningen, *at* Folketingets Administration i to e-mails informerede modtagerne om søgningen og formålet hermed samme dag, som søgningen blev foretaget, *at* Folketingets Administration involverede politiet i sagen, samt *at* der var fastsat retningslinjer om brugen af e-mails, og at it-brugerne var blevet gjort bekendt med, at Folketingets Administration ville kunne have adgang til e-mails under særlige omstændigheder, og at Folketingets Administration agerede i henhold hertil, om end de som nævnt efter vores vurdering ikke gav grundlag for at skaffe sig berettiget adgang til informationer om de 33 personers private e-mails.

- Det er på denne baggrund ikke vores opfattelse, at Folketingets Administration har pligt til at politianmelde forholdet.
- Det bemærkes endvidere, at vurderingen af, om et strafbart forhold er begået, udelukkende henhører under domstolene, og at det inden da også beror på, hvilke oplysninger der fremkommer under politiets efterforskning af et muligt strafbart forhold samt af politiets og anklagemyndighedens vurdering af forsætsgraden og sagens beviser på tidspunktet for eventuel anmeldelse, sigtelse og tiltalerejsning.
- Vi anbefaler, at Folketingets Administration retter henvendelse til de implicerede folketingsmedlemmer og partiansatte, der var genstand for søgningen, og anfører, at søgningen på e-mails ikke var i overensstemmelse med gældende regler, som Folketingets Administration beklager. Meddelelsen skal endvidere indeholde de forhold, der er omfattet af oplysningspligten i databeskyttelsesforordningens artikel 14. Tilsvarende gælder i forhold til borgeren, der sendte e-mailen til de pågældende personer. Da Folketingets Administration har slettet listen fra søgningen over de omhandlede personers e-mailadresser, kan Folketingets Administration orientere om sagen ved at sende samtlige partiansatte og medlemmer af Folketinget samt borgeren en e-mail med de ovenfor angivne informationer.
- Vi anbefaler desuden, at Folketingets Administration overvejer ansættelsesretlige sanktioner i forhold til de implicerede medarbejdere, som iværksatte søgningen. Der foreligger ikke i sagen informationer om, at hverken Folketingets Administrations direktion – defineret som direktøren og de to vicedirektører – eller Folketingets formand var vidende om eller involveret i selve fremsøgningen af de omhandlede e-mails eller har afgivet instruktioner herom. På denne baggrund er der ikke grundlag for et strafferetligt ansvar for denne personkreds, endsige ansættelsesretlige sanktioner.

- Vi anbefaler endelig, at Folketingets Administration reviderer sine procedurer og arbejdsgange med henblik på at undgå lignende tilfælde fremadrettet. Vi kan forstå, at Folketingets Administration allerede har iværksat dette arbejde.

Vi har ikke foretaget en vurdering af, hvorvidt Folketingets Administrations søgning udgjorde et brud på persondatasikkerheden, der skal anmeldes til Datatilsynet – og som de berørte registrerede skal underrettes om – efter de gældende regler herom i henholdsvis databeskyttelsesforordningens artikel 33-34.

3. SAGENS FAKTISKE OMSTÆNDIGHEDER

3.1 Folketingets Administration

Det fremgår af Folketingets hjemmeside, at Folketingets Administrations primære opgave er at skabe rammerne for, at folketingsmedlemmerne kan koncentrere sig om deres politiske arbejde i Folketingssalen og i udvalgene. Medarbejderne bidrager til lovgivningsarbejdet og varetager derudover en lang række administrative og praktiske opgaver, der dels understøtter de politiske aktiviteter, dels holder de fysiske rammer på Christiansborg i orden.

Der er cirka 465 medarbejdere i Folketingets Administration, der ledes af Folketingets direktør. Folketingets formand er den øverste chef for Folketingets Administration.

Folketingets Administration består af 16 forskellige enheder med hver deres funktion og arbejdsområde. Enhederne er organiseret under direktionen, der består af Folketingets direktør og to vicedirektører.

3.2 Hændelsesforløbet vedrørende Folketingets Administrations søgning på e-mails

Et folketingsmedlem modtog den 12. marts 2024 en e-mail fra en borger, hvori fremgik både navn og billede på en sigtet i en verserende straffesag om drabet på en 13-årig pige i Hjallerup. Det pågældende medlem af Folketinget videresendte e-mailen fra borgeren til Folketingets formand og et medlem af Præsidiet. Folketingsmedlemmet anførte i e-mailen, at han (fejlagtigt) var af den opfattelse, at der var nedlagt navneforbud i sagen, og han ønskede råd til, hvordan han skulle forholde sig til e-mailen fra borgeren.

Formandens sekretariat videresendte to dage senere e-mailen fra folketingsmedlemmet til Folketingets Administration, It-systemer, den 14. marts 2024.

Folketingets Administration besluttede herefter samme dag at foretage en søgning på, hvilke andre ansatte eller medlemmer af Folketinget, der havde modtaget en tilsvarende e-mail.

Folketingets Administration var af den (forkerte) opfattelse, at der var nedlagt navneforbud i sagen, og formålet med søgningen var således at finde ud af, hvilke øvrige personer der havde modtaget e-mailen. På denne måde kunne Folketingets Administration kontakte de pågældende modtagere for at gøre opmærksom på e-mailen, som Folketingets Administration anså for at bryde et navneforbud, og bede modtagerne om at slette e-mailen, så den ikke lå i brugernes indbakker, uden de vidste det. Der var således ikke tale om en it-sikkerhedshændelse.

Folketingets Administration søgte alene efter denne e-mail og ikke øvrige e-mails. Søgningen foregik i spamfilteret og blev foretaget af en medarbejder, som var sikkerhedsgodkendt og underlagt tavshedspligt. Søgningen foregik på den måde, at medarbejderen alene søgte på det konkrete afsendernavn og tidspunktet for modtagelsen. I søgningen i spamfilteret fremgik alene følgende felter:

- Mailens navn (emnefelt),
- afsenderen (e-mail/navn),
- modtageren (e-mail/navn),
- dato for e-mailens afsendelse,
- tidspunktet for e-mailens afsendelse, samt
- nogle tekniske felter.

Medarbejderen har således ikke tilgået eller set andre informationer eller læst indholdet af de fremsøgte e-mails. Folketingets Administration har oplyst, at det via den valgte brugergrænseflade ikke er teknisk muligt at åbne eller læse de fremsøgte e-mails. Hvis man havde forsøgt at tilgå indholdet, ville man havde fået en fejlmeddelelse. Det er kun e-mails, som er blevet tilbageholdt, som man kan se indholdet af. Dvs. i dette tilfælde var det ikke muligt, da e-mailen ikke var tilbageholdt i filteret.

Søgningen viste, at 33 personer – heraf 17 folketingsmedlemmer og 16 ansatte i partierne – havde fået en e-mail fra den pågældende borger. Folketingets Administration formodede, at der var tale om den samme e-mail, som Folketingets Administration oprindeligt havde modtaget af medlemmet af Folketinget gennem Formandens sekretariat. Folketingets Administration slettede omgående listen fra søgningen, efter at den havde tjent sit konkrete formål.

Efter at Folketingets Administration, It-systemer, havde konstateret, at e-mailen var sendt til flere modtagere, tog [redacted] kontakt til Efterforskningsvagten i Folketinget. I en kort telefonsamtale spurgte [redacted] til den verserende straffesag og blev bekræftet i sin (forkerte) opfattelse, at der var nedlagt navneforbud i straffesagen. [redacted] drøftede ikke vejledning af medlemmer og fremsøgning af e-mails med politiet.

Politiet ønskede at efterforske sagen, og bad [redacted] om at videresende metadata (data fra mailheader) på den pågældende e-mail til brug for efterforskningen. [redacted] var ikke i besiddelse af den originale e-mail, så det kunne ikke umiddelbart lade sig gøre. Politiet spurgte ikke til, hvilke it-brugere der havde modtaget mailen. Politiet var udelukkende interesseret i metadata for mailen, ikke hvem og hvor mange, der havde modtaget den.

[redacted] anmeldte af egen drift sagen til politiet. Anmeldelsen blev efterfølgende trukket tilbage og metadata blev ikke sendt til Politiet.

Folketingets Administration, It-systemer, sendte herefter to e-mails til de pågældende modtagere af e-mailen fra borgeren.

Den *første* e-mail fra Folketingets Administration, It-systemer, blev sendt den 14. marts 2024 kl. 12:47 til de pågældende modtagere af e-mailen fra borgeren. I e-mailen fra Folketingets Administration, It-systemer anføres følgende:

> *"Kære modtager af denne mail*
>
> *Vi er blevet gjort opmærksom på, at du og flere andre har modtaget en e-mail, der indeholder grafik og informationer om en aktuel straffesag, hvor der er nedlagt navneforbud.*
>
> *Vi skal bede dig om at slette den pågældende mail fra din Indbakke og dernæst fra din mappe til Slettet post.*
>
> *Du kan kende mailen på afsenderen [fornavn og efternavn på borgeren] <[borgerens fulde e-mail]> samt at mailen er ankommet 12. marts kl. 22:35.*
>
> *Hvis du har spørgsmål til dette, er du velkommen til at kontakte mig eller ringe til It-Hotline på tlf. 3000.*
>
> *Med venlig hilsen*
>
> *[NN]*
> [redacted]"

Den *anden* e-mail fra Folketingets Administration, It-systemer, blev sendt den 14. marts 2024 kl. 14:36 til de pågældende modtagere af e-mailen fra borgeren. I e-mailen fra Folketingets Administration, It-systemer, anføres følgende:

> *"Kære modtager af denne mail*
>
> *Som opfølgning på den tidligere sendte mail, hvor vi bad jer slette en specifik mail, uddybes baggrunden herfor:*
>
> *Vi er blevet kontaktet af en bruger, der havde modtaget den pågældende mail, som indeholder et navn i en sag, hvor der er nedlagt navneforbud. Vi har været i kontakt med politiet, der har bekræftet at sagen skal anmeldes, da den anklagedes navn og billede fremgår. Sagen behandles derfor nu af politiet.*
>
> *Vi har derefter søgt på vores mailservere efter modtagere af den specifikke mail. Alle modtagere er derefter blevet orienteret per mail.*
>
> *I er fortsat velkomne til at vende tilbage til mig eller ringe 3000 (hotline) ved yderligere spørgsmål.*
>
> *Med venlig hilsen*
>
> *[NN]*
> [redacted]"

Dansk Folkeparti rettede efterfølgende henvendelse til Folketingets formand, Søren Gade, med en række opklarende spørgsmål til det konkrete sagsforløb. Folketingets Administration svarede efterfølgende på disse spørgsmål, men det blev i svaret fra Folketingets Administration fejlagtigt oplyst, at der var nedlagt et navneforbud i sagen. Dette har Folketingets Administration erkendt var en klar fejl og undskyldt over for Dansk Folkeparti. Folketingets Administration har oplyst, at det først var den 28. marts 2024, at det gik op for Folketingets Administration, at der ikke var nedlagt navneforbud i sagen.

Den 3. april 2024 sendte Folketingets formand en e-mail til de berørte medlemmer af Folketinget, hvor formanden orienterede om hændelsesforløbet samt anførte, at han har bedt Folketingets Administration om at give Præsidiet en redegørelse om sagsforløbet.

Formanden informerede i e-mailen også om, at sagen har ført til, at Folketingets Administration har besluttet at gennemgå sine nuværende regler og procedurer med henblik på, dels om en lignende sag kan undgås fremover, dels om der generelt kan strammes op og udvises yderligere forsigtighed med hensyn til medlemmernes e-mails. I dette arbejde vil det også indgå, om Folketingets Administration kan kommunikere bedre om politikker og regler på området.

3.3 Folketingets Administrations retningslinjer for brug af it-udstyr, herunder overvågning af e-mails

Folketingets Administration drifter og vedligeholder it-udstyr (hardware), herunder smartphones og laptops, og it-systemer og infrastruktur, herunder e-mailprogram, netværk og servere til opbevaring af data, som stilles til rådighed for medlemmerne af Folketinget samt til partierne, der befinder sig på Christiansborg.

Fra Folketingets Administration har vi modtaget kopi af "Folketingets overordnede informationssikkerhedspolitik 2020", version 1.0. Folketingets Administration har oplyst, at målgruppen for denne politik er alle it-brugere, herunder ansatte i Folketingets Administration, ansatte i partierne og folketingsmedlemmer.

Informationssikkerhedspolitikken udleveres ved udleveringen af it-udstyr, når brugeren starter i Folketinget. Folketingsmedlemmer får obligatorisk 1-1 undervisning af en it-supporter, og dokumenterne udleveres som tryksag. Folketingsmedlemmer og ansatte i partier skal dog – i modsætning til ansatte i Folketingets Administration – dog ikke underskrive for modtagelsen af materialet.

Af informationssikkerhedspolitikkens punkt 2 vedrørende "Gyldighedsområde" fremgår bl.a. følgende:

> *"Informationssikkerhedspolitikken gælder for alle former for behandling af informationer i Folketingets regi – herunder persondata – og ved udvikling, implementering og anvendelse af it. Beskyttelse af informationer gælder både for fysiske og digitale data. Informationssikkerhedspolitikken gælder for alle it-brugere, dvs. alle, der har adgang til Folketingets it-systemer.* [...]"

Af informationssikkerhedspolitikkens punkt 3 vedrørende "Dokumentation" fremgår følgende:

> *"Folketingets arbejde med informationssikkerhed beskrives i følgende dokumenter:*
>
> 1. *Informationssikkerhedspolitikken (dette dokument), som udstikker de overordnede målsætninger, principper og retningslinjer.*

2. "Folketingets regler for informationssikkerhed", som er rettet mod alle it-brugere af it-systemer i Folketinget.

3. Procedurer og instrukser, der sikrer en vedtaget, ensartet udførelse af en række driftsopgaver og sikkerhedsmæssige opgaver."

Fra Folketingets Administration har vi endvidere modtaget kopi af "Folketingets regler for informationssikkerhed" fra marts 2023. Folketingets Administration har oplyst, at målgruppen for disse regler er alle it-brugere, herunder ansatte i Folketingets Administration, ansatte i partierne og folketingsmedlemmer.

Reglerne udleveres ved udleveringen af it-udstyr, når brugeren starter i Folketinget. Folketingsmedlemmer får obligatorisk 1-1 undervisning af en it-supporter, og dokumenterne udleveres som tryksag. Folketingsmedlemmer og ansatte i partier skal dog – i modsætning til ansatte i Folketingets Administration – ikke underskrive for modtagelsen af materialet.

Af reglernes s. 3 under afsnittet "Sikring af it-udstyr" fremgår bl.a. følgende:

"Samtidig gøres opmærksom på, at Folketinget kun kan se følgende på din iPhone/iPad: Model, serienummer, ejer, enhedsnavn, operativsystem, appnavne og udstyrets placering.

Folketinget kan ikke se opkalds- og internetoversigt, mail og sms-beskeder, kontakter og kalender, adgangskoder eller fotos på din iPhone/iPad."

Af reglernes s. 5 f. vedrørende "Adfærdsregler ved brug af e-mail" fremgår bl.a. følgende:

"Indhold af e-mail
Folketingets e-mailsystem må ikke bruges til at sende materiale, hvis indhold strider mod gældende lovgivning eller ophavsret.

Ejerskab af e-mail
Folketinget betragter som udgangspunkt alle e-mail som tilhørende Folketinget, medmindre den i emnefeltet er mærket: "Personligt", "Privat" el.lign.

Privat brug af e-mail
Folketinget accepterer, at e-mailsystemet i begrænset omfang benyttes i privat øjemed, men det må ikke benyttes til erhvervsmæssige formål.

Ved brug af Folketingets e-mailsystem i privat øjemed må der ikke herske tvivl om, at e-mailen er privat og ikke har nogen relation til Folketinget.

Folketinget forbeholder sig ret til at skaffe sig adgang til data og e-mail hos medarbejdere, når dette sker af drifts- eller sikkerhedshensyn eller ved henvendelser fra politiet, PET og lignende myndigheder i forbindelse med opklaring af strafbare forhold eller i tilfælde, hvor Folketinget er retligt forpligtet til at udlevere det pågældende materiale til andre

E-mail slettes, når brugerens tilknytning til Folketinget ophører, og e-mailkontoen spærres for modtagelse. Folketingsmedlemmer kan i op til 6 måneder efter ophør få indsat et autosvar og eventuelt en videresendelse af mail.

[...]

Spam, phishing og bedrageri
Folketinget scanner alle e-mail for spam og andet skadeligt indhold. Du skal selv efterkontrollere i spamoversigten, der modtages på mail, om der fejlagtigt er frasorteret reelle e-mail.

Vær opmærksom på, om en e-mail kan være et forsøg på phishing eller social engineering. Slet mistænkelige e-mail. Er du i tvivl, om en mail er phishing, eller er kommet til at klikke på et 'farligt' link, så kontakt It-hotline."

Af reglernes s. 9 f. vedrørende "Overvågning og logning" fremgår følgende:

"Der bliver foretaget en central logning af alle ind- og udgående internetforbindelser. Logningsdata benyttes udelukkende i forbindelse med fejlsøgning eller ved mistanke om misbrug.

Overvågning og begrænsning
Folketinget filtrerer og begrænser internetadgangen baseret på trusselsniveauet. Det betyder, at hjemmesider, der indeholder virus eller på andre måder udgør en sikkerhedstrussel, bliver blokeret af forskellige automatiske sikkerhedssystemer.

Monitorering
Folketinget har automatiseret overvågning af al ind- og udgående datatrafik for at forebygge it-sikkerhedshændelser. I tilfælde af alarmer fra overvågningen eller ved anden mistanke, der indikerer tegn på aktive it-sikkerhedshændelser, tillades det at foretage en analyse af den pågældende datatrafik."

3.4 Databehandleraftale mellem Dansk Folkepartis Landsorganisation og Folketingets Administration

Jeg har endvidere modtaget kopi af en databehandleraftale indgået mellem Dansk Folkepartis Landsorganisation som dataansvarlig og Folketingets Administration som databehandler den 2. juli 2019.

I aftalens underbilag A, punkt 2, anføres formålet med behandlingen af personoplysninger, at den dataansvarlige kan anvende det it-udstyr, smartphones og infrastruktur (netværk og servere), som ejes og administreres af databehandleren. Det anføres videre, at den dataansvarlige kan anvende it-udstyret til at indsamle og behandle oplysninger om den dataansvarliges medlemmer og alle andre, som den dataansvarlige måtte få behov for at behandle personoplysninger om.

Databehandleraftalens underbilag B indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Folketingets Administration som databehandler skal foretage i medfør af databeskyttelsesforordningens artikel 32.

I aftalens punkt 7.1 (e) vedrørende organisatorisk sikkerhed anføres det, at databehandleren har en it-sikkerhedspolitik, som tages op til revidering minimum én gang årligt.

I aftalens punkt 7.1. (i) anføres følgende:

> *"Databehandlerens medarbejdere er bekendt med, at databehandleren har ret til at skaffe sig adgang til data og e-mail hos medarbejderne, når dette sker af drifts- eller sikkerhedshensyn eller ved henvendelser fra politiet i forbindelse med opklaring af kriminalsager. Databehandleren har forbeholdt sig ret til at analysere mailloggen med henblik på undersøgelse af og forebyggelse for, it-sikkerhedsrelaterede hændelser."*

I aftalens punkt 8.1 (r) vedrørende teknisk og logisk sikkerhed fastsættes det, at databehandleren har automatiseret overvågning af al ind- og udgående datatrafik med henblik på opdagelse af, og forebyggelse mod, it-sikkerhedshændelser. Det anføres videre, at i tilfælde af alarmer fra overvågningen, eller ved mistanke på anden vis, der indikerer tegn på aktive it-sikkerhedshændelser, analyseres den pågældende datatrafik.

4. RETSGRUNDLAG

4.1 Reglerne om navneforbud i retsplejeloven

Efter retsplejelovens § 31, stk. 1, kan retten i straffesager forbyde, at der sker offentlig gengivelse af navn, stilling eller bopæl for sigtede (tiltalte) eller andre under sagen nævnte personer, eller at den pågældendes identitet på anden måde offentliggøres (navneforbud), når offentlig gengivelse må antages at bringe nogens sikkerhed i fare, eller når offentlig gengivelse vil udsætte nogen for unødvendig krænkelse.

Det fremgår af de specielle bemærkninger til bestemmelsen, at der er tale om et egentligt identifikationsforbud, jf. Folketingstidende 1998-99, tillæg A, side 2033. Det indebærer, at offentlig gengivelse af oplysninger om den pågældendes identitet vil udgøre en overtrædelse af retsplejelovens § 31, stk. 1, hvis det ud fra oplysningerne vil være muligt at identificere den sigtede.

Det følger af retsplejelovens § 32 b, stk. 2, at overtrædelse af rettens forbud efter § 31 straffes med bøde, hvis den pågældende var bekendt med forbuddet. Det samme gælder, hvis den pågældende vidste eller burde vide, at sagen verserede ved retten, eller at politiet efterforskede sagen, og den pågældende ikke havde forhørt sig hos politiet, anklagemyndigheden eller retten om, hvorvidt der var nedlagt navneforbud.

4.2 Reglerne om indgivelse af politianmeldelse og politiets opgaver i anledning heraf i retsplejeloven og politiloven

Det følger af retsplejelovens § 742 at anmeldelser om strafbare forhold indgives til politiet. Politiet iværksætter efter anmeldelse eller af egen drift efterforskning, når der er rimelig formodning om, at et strafbart forhold, som forfølges af det offentlige, er begået.

Det følger videre af politilovens § 2, nr. 3, at politiet har til opgave at bringe strafbar virksomhed til ophør samt efterforske og forfølge strafbare forhold.

4.3 Straffelovens bestemmelser om uberettiget adgang til andres data

Det følger af straffelovens § 263, stk. 1, at den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem, straffes med bøde eller fængsel indtil 1 år og 6 måneder.

Det følger af forarbejderne til straffelovens § 263, stk. 1, at bestemmelsen angår den, der på en hvilken som helst måde uberettiget skaffer sig adgang til et datasystem eller data, jf. Folketingstidende 2018-19

(1. samling), tillæg A, L 20 som fremsat, side 46. Bestemmelsen tager udgangspunkt i, at meddelelser i stadigt stigende omfang sendes og opbevares elektronisk.

Indholdet af beskyttelsen af "*datasystem eller data*" er beskrevet i forarbejderne til bestemmelsen, jf. Folketingstidende 2018-19 (1. samling), tillæg A, L 20 som fremsat, side 8, hvoraf det fremgår, at:

> *"Beskyttelsen af datasystemer og data bør ligesom i dag gælde alle former for data, dvs. både programmer, indholdsdata og metadata. Det er således ikke alene indholdet af eksempelvis elektronisk kommunikation, der er beskyttet, men også eksempelvis oplysninger om afsender og modtager af en e-mail, antallet af udvekslede e-mails mellem bestemte personer, størrelsen af vedhæftede filer mv. Og ligesom i dag er f.eks. elektronisk kommunikation beskyttet både før afsendelsen, under forsendelsen (transmissionen) og efter modtagelsen, herunder efter at være blevet læst af rette modtager."*

Det følger videre af de specielle bemærkninger til § 263, stk. 1, at der ikke gælder særlige krav til de pågældende datas indhold:

> *"Den foreslåede bestemmelse vil omfatte alle former for data, og det er således ikke et krav, at disse er af en sådan karakter, at de er omfattet af straffelovens § 264 d om private forhold."*

Det fremgår af de specielle bemærkninger til straffelovens § 263, stk. 1, hvad der forstås ved udtrykket "*en andens*", jf. Folketingstidende 2018-19 (1. samling), tillæg A, L 20 som fremsat, side 46:

> *"Udtrykket »en andens« relaterer sig både til datasystem og data. Det vil således være et krav, at man enten skaffer sig adgang til en andens datasystem, eller at man skaffer sig adgang til en andens data, uanset om systemet tilhører gerningsmanden eller en anden. Der vil således kunne foreligge en strafbar krænkelse ved brug af eget datasystem, hvis f.eks. udlejeren af et datasystem uberettiget skaffer sig adgang til lejerens data, som er indkodet i datasystemet."*

Det fremgår af de specielle bemærkninger til straffelovens § 263, stk. 1, hvad der forstås ved udtrykket "*skaffer sig adgang*", jf. Folketingstidende 2018-19 (1. samling), tillæg A, L 20 som fremsat, side 46:

> *"Udtrykket »skaffer sig adgang« skal forstås bredt og dækker bl.a. hel eller delvis kontrol over et datasystem, som f.eks. giver adgang til data eller til at tilføje, ændre eller slette data eller programmer i datasystemet, uanset om der skaffes adgang direkte via det pågældende datasystem eller via et andet system.*

Den foreslåede bestemmelse vil således omfatte meget forskelligartede forhold, herunder at en gerningsmand skaffer sig adgang til en andens computer eller smartphone (uanset om man bruger den pågældende computer mv., eller om adgangen skaffes via en anden computer mv.), at en gerningsmand logger på en andens e-mailsystem (uanset hvilken computer mv. det sker fra), eller at en gerningsmand skaffer sig adgang til et usb-stik.

Bestemmelsen vil eksempelvis også omfatte tilfælde, hvor en gerningsmand udnytter en svaghed i et datasystem, der giver en videre adgang til oplysninger eller programmer end tilsigtet, for at kopiere, ændre eller slette oplysninger eller programmer.

Ligesom de øvrige bestemmelser om krænkelse af privatlivets fred i § 263, stk. 2, § 263 a og §§ 264-264 d afgrænses § 263, stk. 1, fortsat af det generelle forbehold om, at der skal være tale om uberettiget adgang. Hermed tilkendegives det, at bestemmelsen er formuleret så bredt, at der helt regelmæssigt skal ske en udskillelse af legale handlinger, der falder ind under bestemmelsens ordlyd.

Der kan således forekomme tilfælde, hvor man kun ved et konkret skøn kan afgøre, om en handling, der sprogligt omfattes af bestemmelsens ordlyd, skal anses som strafbar. Dette vil navnlig få betydning i forhold til personer, der har en berettiget adgang til et datasystem, men som anvender denne adgang til andre formål end dem, som adgangen er givet til.

Et eksempel herpå kan efter omstændighederne være en medarbejder, der har en berettiget adgang til arbejdsgiverens datasystem, men som anvender denne adgang til at tilgå data, som der ikke er arbejdsmæssigt behov for at tilgå, herunder navnlig hvis medarbejderen har et videregående forsæt til at videregive eller anvende disse data i en sammenhæng, der er arbejdsgiveren uvedkommende.

Endvidere vil den foreslåede bestemmelse eksempelvis omfatte en kunde, der har en berettiget adgang til en brugerflade på internettet eller en computer, men som f.eks. udnytter en fejl, svaghed eller utilsigtet adgang i systemet til at kopiere, ændre eller slette data eller anvende datasystemet på en måde, som ligger uden for det sædvanlige og aftalte."

Bestemmelsens gerningsindhold vil være fuldbyrdet, når gerningsmanden skaffer sig adgang til systemet eller dataene, og det er således uden betydning, hvad den pågældende efterfølgende foretager sig i relation til systemet eller dataene, jf. Folketingstidende 2018-19 (1. samling), tillæg A, L 20 som fremsat, side 47.

Under det lovforberedende arbejde blev det overvejet, under hvilke omstændigheder det kunne være berettiget for en arbejdsgiver at tilgå en medarbejders private oplysninger, jf. Folketingstidende 2018-19 (1. samling), tillæg A, L 20 som fremsat, side 8-9:

> *"For så vidt angår den omvendte situation – arbejdsgiverens adgang til en medarbejders private oplysninger, som måtte være placeret i arbejdsgiverens datasystem, herunder navnlig private e-mails – må udgangspunktet være, at arbejdsgiveren ikke er berettiget til at tilgå en medarbejders private oplysninger, selv om disse findes i arbejdsgiverens datasystem. Det er imidlertid vanskeligt i generel form at fastslå, under hvilke omstændigheder dette udgangspunkt kan fraviges. Afgrænsningen af, hvornår arbejdsgiverens adgang er berettiget, må således bero på en konkret vurdering af sagens omstændigheder, herunder navnlig af hvad der eventuelt er aftalt mellem arbejdsgiveren og medarbejderen om brugen af arbejdsgiverens systemer til private formål."*

Straffelovrådet har i sin betænkning nr. 1563/2017, side 28, om freds- og ærekrænkelser beskrevet forholdet om, at "*handlingen skal være uberettiget*" mere generelt:

> *"Bestemmelserne i straffelovens §§ 263 og 264-264 d indeholder alle det forbehold, at en handling for at være omfattet af bestemmelserne skal være "uberettiget". (I § 263 c er ordet "uberettiget" placeret, så det sprogligt kun er knyttet til "udnytter" og ikke til "skaffer sig". Det fremgår ikke af forarbejderne, om der er tale om en tilsigtet skelnen mellem de to led i bestemmelsen).*
>
> *Dette forbehold om, at handlingen skal være uberettiget har sammenhæng med princippet om material atypicitet, dvs. det forhold, at en strafbestemmelse kan fortolkes, så den ikke omfatter handlinger, der sprogligt falder ind under gerningsbeskrivelsen, men er ganske atypiske i forhold til det, der er bestemmelsens sigte. Når man i bestemmelserne om krænkelse af privatlivets fred ved udtrykkeligt forbehold gør opmærksom på, at ikke enhver handling, der er omfattet af (den øvrige del af) gerningsbeskrivelsen, bør falde ind under det strafbare område, skyldes det ifølge forarbejderne, at man her har at gøre med bestemmelser, man har måttet give en så bred udformning, at der helt regelmæssigt skal ske en udskillelse af legale handlinger, der i øvrigt ville falde ind under bestemmelsens ordlyd, jf. Straffelovrådets betænkning nr. 601/1971 om privatlivets fred, side 58.*
>
> *Der kan generelt gives diskulperende samtykke til de handlinger, der er omfattet af §§ 263 og 264-264 d, og handlingen er i så fald selvfølgelig ikke uberettiget. Det er som udgangspunkt den, der har rådigheden over det pågældende forhold, der i givet fald kan give samtykke.*

For lukkede meddelelser er det afsenderen indtil afsendelsen og dernæst modtageren. For lukkede optegnelser og gemmer er det den, der har rådigheden over disse."

Der foreligger en række domme, som indikerer det nærmere indhold af "*uberettiget*" i straffelovens § 263, stk. 1.

Højesteret har ved dom af 4. februar 2015 i en civil sag gengivet i UfR 2015.1525 H udtalt sig om en situation, hvor en arbejdsgiver – under fortrolige forhold – havde gennemgået en tidligere medarbejders korrespondance med en ekstern person på grundlag af en mistanke om læk af oplysninger til den pågældende person. Højesteret kom frem til, at gennemgangen ikke var en krænkelse af medarbejderens privatliv, der kunne begrunde godtgørelse efter erstatningsansvarslovens § 26. Højesteret anførte, at den pågældende gennemgang ikke var uberettiget, og det må heraf efter vores vurdering kunne udledes af dommen, at gennemgangen heller ikke ville have været i strid med den nugældende straffelovs § 263, stk. 1 (den dagældende straffelovs § 263, stk. 2). I den tidligere medarbejders ansættelseskontrakt var det fastsat, at arbejdsgiveren kunne gøre sig bekendt med mailkorrespondance på arbejdsgiverens system, men dog således at medarbejdere burde markere private mails i meddelelsesfeltet, hvilket den tidligere medarbejder ikke havde gjort med de i sagen omhandlede mails. Højesteret udtalte, at gennemgangen af den tidligere medarbejders mails var foretaget på grundlag af en mistanke om læk af oplysninger til en ekstern person og under fortrolige forhold. Højesteret bemærkede, at gennemgangen af mailkorrespondancen blev i henhold til en beslutning på ledelsesniveau foretaget af en nærmere afgrænset personkreds, som bestod af personer med fornøden faglig indsigt til at vurdere, om der var tale om forretningshemmeligheder, og de pågældende blev pålagt at underskrive en fortrolighedserklæring for at sikre, at de ikke videregav fortrolige oplysninger, og gennemgangen blev målrettet efter formålet med undersøgelsen. Ingen af de pågældende mails var markeret som private og måtte derfor som udgangspunkt anses for korrespondance tilhørende arbejdsgiveren, som arbejdsgiveren kunne gøre sig bekendt med, ligesom det ikke på forhånd var muligt at afgøre, om de havde et privat indhold. De pågældende mails mellem den tidligere medarbejder og den eksterne person indeholdt endvidere både private og arbejdsrelaterede meddelelser, og det var ikke godtgjort, at arbejdsgiveren havde søgt i og gennemlæst mails af privat karakter i videre omfang, end det var nødvendigt for at udskille den del af mailkorrespondancen, der var relevant i forhold til undersøgelsens formål. Der var herefter ikke grundlag for at fastslå, at der forelå en krænkelse af den tidligere medarbejders privatliv, der kunne begrunde godtgørelse for tort efter erstatningsansvarslovens § 26.

Dommen er kommenteret af Peter Blume i UfR 2015B.229 ff., der opsummerer præmisserne i dommen således:

"For det første kan præmisserne læses som en bekræftelse af, at der skal være givet en forudgående meddelelse til de ansatte om, at arbejdsgiveren kan læse e-post. Det er ganske vist

ikke klart, om ansættelseskontrakten tillægges afgørende betydning, men dette er mest nærliggende. For det andet kan det konstateres, at Højesteret lægger vægt på, at arbejdsgiveren havde tilrettelagt en fremgangsmåde, der var orienteret imod beskyttelse af privatliv og fortrolighed. For det tredje har det betydning, at den ansatte ikke havde benyttet muligheden for at markere mails og således ikke selv havde gjort noget for at beskytte sit privatliv i denne sammenhæng, jf. herom yderligere nedenfor. For det fjerde kan dommen læses således, at der skal foreligge en rimelig grad af mistanke, hvilket ansås opfyldt i dette tilfælde."

I en dom fra Vestre Landsret af 26. april 2016 gengivet i UfR 2016.2666 V var der tale om bl.a. en arbejdsgiver, der havde læst private sms'er på en mobiltelefon, som tilhørte arbejdsgiveren, men som en medarbejder, der var sikkerhedsrepræsentant, havde haft udleveret til både arbejdsmæssig og privat brug. Landsrettens flertal tog ikke stilling til forholdets forenelighed med straffelovens § 263, fordi der var indgået en fratrædelsesaftale mellem parterne, og denne aftale måtte fortolkes sådan, at medarbejderen havde givet afkald på sin ret til at anmode om offentlig påtale. Det var imidlertid byrettens og den dissentierende landsdommers opfattelse, at arbejdsgivernes gennemgang af sms'erne var i strid med straffelovens § 263. Der blev herved lagt vægt på, at arbejdsgiveren ikke havde udstukket retningslinjer for den nærmere private brug af mobiltelefonen, ligesom der ikke var indgået aftale herom, at medarbejderen ikke havde grund til at forvente, at arbejdsgiveren ville læse private sms'er, at arbejdsgiveren havde grund til at antage, at en del af medarbejderens korrespondance med kolleger havde et fortroligt og i nogle sammenhænge privat indhold, men at denne korrespondance alligevel blev gennemgået, at muligheden for at undersøge medarbejderens mobiltelefon opstod tilfældigt, og at gennemgangen ikke skete på baggrund af en generel ledelsesbeslutning om at undersøge et anstrengt forhold mellem medarbejdere og ledelse, ligesom det ikke kunne lægges til grund, at udlæsningen af korrespondancen var udtryk for en nøje planlagt proces fra havnens ledelse, og at der ikke var en nærmere konkret mistanke mod medarbejderen.

Det følger herudover af straffelovens § 263, stk. 2, nr. 1, at den, der, uden at forholdet er omfattet af stk. 1, uberettiget åbner et brev eller en anden lukket meddelelse eller optegnelse eller gør sig bekendt med indholdet straffes med bøde eller fængsel indtil 6 måneder.

Bestemmelsen er efter sin ordlyd subsidiær i forhold til § 263, stk. 1, og det følger også eksplicit af forarbejderne, at den ikke vil finde anvendelse, hvis et forhold omfattes af § 263, stk. 1, jf. Folketingstidende 2018-19 (1. samling), tillæg A, L 20 som fremsat, side 47.

Ved udtrykket »lukket meddelelse eller fortegnelse« forstås bl.a. breve, dagbøger, regnskabsbøger og skriftlige eller mundtlige meddelelser i elektronisk form, herunder e-mails, sms'er og telebeskeder. Omvendt omfatter det bl.a. ikke åbne postkort eller angivelser uden på en lukket forsendelse (eksempelvis angivelse af modtager og afsender).

Som en konsekvens af, at bestemmelsen er subsidiær i forhold til § 263, stk. 1, vil bl.a. åbning af en lukket meddelelse, f.eks. en e-mail eller sms, der sker ved uberettiget at skaffe sig adgang til et datasystem, ikke omfattes af bestemmelsen, i det omfang forholdet omfattes af § 263, stk. 1, jf. Folketingstidende 2018-19 (1. samling), tillæg A, L 20 som fremsat, side 48.

4.4 Den Europæiske Menneskerettighedskonvention

4.4.1 Konventionens anvendelsesområde

Det følger af Den Europæiske Menneskerettighedskonvention (EMRK) artikel 1, at det er medlemsstaterne, der er pligtsubjekter. Det følger Den Europæiske Menneskerettighedsdomstols (Domstolen) praksis, at der er tale om et bredt statsbegreb, og at staten kan ifalde ansvar efter konventionen for handlinger begået af alle statens organer, repræsentanter ("agents") og ansatte ("servants"), og vedkommendes hierarkiske placering er som udgangspunkt uden betydning, idet handlinger, der udføres i en offentlig egenskab, tilregnes staten. Det betyder, at konventionen kan krænkes af enhver person, der udøver en offentlig funktion, som er blevet betroet vedkommende, og af enhver national myndighed, der udøver offentlige funktioner. Der henvises til Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 35-36.

For så vidt angår Danmark påhviler pligten til at sikre opfyldelsen af konventionen både regering, Folketing, forvaltning og domstole. Det er uden betydning, om der er tale om en statslig, regional eller kommunal myndighed. Det er uden betydning, om der er tale om centrale, regionale eller lokale myndigheder. Det er endvidere uden betydning, om der er tale om en mere eller mindre uafhængig myndighed. Det er endvidere uden betydning, om myndigheden optræder som myndighedsudøver eller på anden måde, jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 36.

Ved vurdering af statens ansvar er det som udgangspunkt uden betydning, i hvilken egenskab staten handler. Staten er f.eks. ansvarlig, når den optræder som arbejdsgiver, og karakteren af ansættelsesforholdet er som udgangspunkt uden betydning, herunder om det efter national ret reguleres af offentligretlige eller privatretlige regler. Staten kan ifalde ansvar, hvad enten statens organer handler som myndighedsudøver eller privat kontrahent, jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 39.

4.4.2 Retten til respekt for privatliv og korrespondance

Efter EMRK artikel 8, stk. 1, har enhver ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.

Retten til respekt for korrespondance ifølge artikel 8 indebærer som udgangspunkt en ret til meddelelseshemmelighed i forbindelse med samtlige former for kommunikation. Udtrykket er bredt og omfatter middelbar kommunikation med andre. Der kan f.eks. være tale om skriftlige meddelelser, der formidles ved hjælp af brev, telefax, telegram, telex, e-mail, sms eller andet fysisk eller elektronisk læsbart medie, herunder diskette eller harddisk samt telefonopkald og -samtaler, radiokommunikation og anden internetkommunikation. Det må som udgangspunkt være et krav, at der er tale om kommunikation, som afsenderen og modtageren kan forvente formidlet, uden at andre gøres bekendt med indholdet.

Retten til respekt for sin korrespondance omfatter også e-mails sendt fra arbejdspladsen, og Domstolen har bl.a. vurderet, at overvågning af en ansats brug af e-mail på arbejdet udgør et indgreb i retten til korrespondance, når den ansatte ikke med rimelighed kunne forvente at blive overvåget, jf. præmis 41-42 i sagen Copland mod Storbritannien, dom af 3. april 2007. Det følger også af Domstolens praksis, at overvågning og registrering af en ansats brug af internet på arbejdspladsen, herunder programmer til kommunikation, kan være omfattet af retten til respekt for privatliv, selv om den ansatte er gjort bekendt med forbud mod privat brug af computer og internet, jf. præmis 74-81 i sagen Barbulescu mod Rumænien, dom af 5. september 2017. Se også Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 872 og 889 og Peer Lorenzen m.fl., Den Europæiske Menneskerettighedskonvention med kommentarer, 3. udg., 2011, DJØF Forlag, s. 755.

Ved indgreb forstås en enhver form for forstyrrelse eller overvågning – i form af f.eks. brevåbning, brevstandsning, aflytning, registrering – af personers kommunikation uden forudgående tilladelse fra den berørte afsender, modtager eller efter omstændighederne fra begge. Indgreb i korrespondance omfatter bl.a. tilfælde, hvor myndigheder gøres bekendt med privates kommunikation med andre (hvornår der er kommunikeret, hvordan der er kommunikeret, hvem der har kommunikeret m.v.) eller indholdet heraf (aflytning eller optagelse af samtaler, standsning, tilbageholdelse, åbning, gennemlæsning, afskrift eller kopiering af breve m.v.), jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 891 og Peer Lorenzen m.fl., Den Europæiske Menneskerettighedskonvention med kommentarer, 3. udg., 2011, DJØF Forlag, s. 755.

Efter artikel 8, stk. 2, kan et indgreb i bl.a. retten til respekt for korrespondance retfærdiggøres, hvis tre betingelser er opfyldt. Indgrebet skal være foreskrevet ved lov (legalitetskrav), varetage et eller flere legitime formål og være nødvendigt i et demokratisk samfund for at opnå det eller de omhandlede formål (proportionalitet).

Kravet om, at indgrebet skal have hjemmel i national lovgivning, indebærer et krav om, at der skal findes nationale regler, der giver myndigheder ret til at foretage det pågældende indgreb, ligesom de nationale materielle og processuelle regler konkret skal være overholdt i forbindelse med indgrebet. Det formuleres på den måde, at indgrebet skal have "sufficient legal basis in domestic law". Hvis der ikke findes nationale regler, der regulerer og hjemler indgrebet, statueres krænkelse. Hvis indgrebet ikke har hjemmel i national ret, statueres ligeledes krænkelse. Hvis indgrebet ikke har fundet sted under overholdelse af national ret, statueres også krænkelse, jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 837 og 839.

Kravet om, at indgrebet skal være nødvendigt i et demokratisk samfund, indebærer et krav om, at indgrebet sker ud fra hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder. Der er tale om en udtømmende opregning af legitime formål, der skal fortolkes indskrænkende, jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 851.

Ved vurdering af, om et indgreb varetager et legitimt formål, skal der foretages en vurdering af formålet med den omhandlede lovgivning under hensyn til den måde, lovgivningen er blevet bragt i anvendelse i den konkrete sag, jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 851.

Kravet om, at indgrebet skal være "*nødvendigt i et demokratisk samfund*", indebærer et krav om, at indgrebet skal modsvare et presserende socialt behov ("a pressing social need"), og at indgrebet er proportionalt i forhold til det forfulgte legitime formål. Det er vigtigt at være opmærksom på, at stk. 2 i artikel 8-11 er undtagelsesbestemmelser, og at de derfor skal fortolkes indskrænkende, og at behovet for at gøre indgreb skal godtgøres på en overbevisende måde ("must be convincingly established"). Ved vurderingen af, om et indgreb er "nødvendigt", er det vigtigt at være opmærksom på, at begrebet "nødvendigt" ikke er lige så fleksibelt som udtryk som "hensigtsmæssig", "ønskelig" eller lignende formuleringer. Der henvises til Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 853.

Ved vurderingen af, om kravet om proportionalitet er opfyldt, er det af betydning, om de anvendte foranstaltninger er rimelige og egnede til at opnå det legitime formål. Hvis staten har holdt sig inden for disse grænser, er det ikke i sig selv afgørende, om der kan påvises alternative og mindre indgribende foranstaltninger, idet Domstolen ikke anser det for sin opgave at afgøre, om den valgte foranstaltning er udtryk for den bedste løsning ved behandling af det pågældende problem, eller om staten burde have udøvet sit skøn på en anden måde. Som udgangspunkt må det imidlertid være et krav, at der ikke findes andre og

mindre indgribende foranstaltninger, der er egnede til at opfylde det legitime formål, jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 854.

Ved vurderingen af, om et indgreb er nødvendigt i et demokratisk samfund, og dermed proportionalt, har medlemsstaterne en vis skønsmargin ("margin of appreciation") ved vurderingen af, om det er nødvendigt at gøre indgreb i en konventionssikret rettighed, samt ved valget af de midler, der skal bringes i anvendelse for at opnå det eller de anerkendelsesværdige formål.

Ved vurdering af omfanget af statens skønsmargin tillægges den nationale proces betydning, herunder lovgivningsprocessen og retsanvendelsen, og hvis det fremgår, at der er foretaget en grundig og indgående vurdering og afvejning af nødvendigheden, både generelt i forbindelse med lovgivningens tilblivelse og den konkrete anvendelse af reglerne, taler det for en større skønsmargin. Statens skønsmargin omfatter som udgangspunkt også valget af, om der ved lov skal indføres en generel foranstaltning eller ordning, eller om lovgivningen indebærer, at der skal foretages en konkret vurdering i det enkelte tilfælde.

Hvis de formål, medlemsstaterne forfølger, når de foretager indgreb, er beskyttelse af andre personers rettigheder og friheder, der er omfattet af konventionen, vil medlemsstaterne have en vid skønsmargin ved afvejningen af individers til dels modsatrettede interesser, da myndighederne er i en bedre position til at vurdere, om der er et "presserende socialt behov", der kan retfærdiggøre et indgreb i en af de rettigheder, der er beskyttet af konventionen, jf. Jon Fridrik Kjølbro, Den Europæiske Menneskerettighedskonvention for praktikere, 6. udg., 2023, DJØF Forlag, s. 854.

4.5 Reglerne om behandling af personoplysninger i databeskyttelsesforordningen og -loven

Databeskyttelsesforordningen finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. forordningens artikel 2, stk. 1.

Ved personoplysninger forstås efter artikel 4, nr. 1, enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Behandling defineres som enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks.

indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse, jf. artikel 4, nr. 2.

Der er ikke retlig tvivl om, at elektronisk behandling af oplysninger om fysiske personers afsendelse og modtagelse af e-mails, herunder elektronisk overvågning af eller søgning på oplysninger herom, udgør behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 2, stk. 1.

Det følger af databeskyttelseslovens § 3, stk. 3, at loven og databeskyttelsesforordningen ikke finder anvendelse på behandling af oplysninger, der foretages som led i Folketingets parlamentariske arbejde.

Omvendt finder loven og forordningen anvendelse på behandling af personoplysninger, når behandlingen ikke sker som led i parlamentarisk arbejde og betjening, jf. forslag nr. L 68 af 25. oktober 2017 til ny databeskyttelseslov, alm. bem., punkt 1.2.

Det anføres endvidere i de specielle bemærkninger til bestemmelsen, at i modsætning til persondataloven må forordningen antages at finde anvendelse for Folketinget og institutioner under Folketinget. Det anføres videre, at Justitsministeriet finder, at loven og databeskyttelsesforordningen skal finde anvendelse på Folketinget, når der ikke sker parlamentarisk arbejde og betjening. Videre anføres det, at Justitsministeriet foreslår, at lovforslaget og databeskyttelsesforordningen ikke finder anvendelse på den behandling af personoplysninger, der foretages som led i Folketingets parlamentariske arbejde, herunder den betjening af Folketingets medlemmer, som Folketingets Administration foretager. Der henvises i øvrigt til Justitsministeriets betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 32 og 948-958.

På betænkningens s. 32 anføres det, at i modsætning til persondataloven må forordningen antages at finde anvendelse for Folketinget og institutioner under Folketinget. For så vidt angår den behandling af personoplysninger, der foretages for Folketinget som led i det parlamentariske arbejde, herunder den betjening af Folketingets medlemmer, som Folketingets Administration foretager, må der imidlertid foretages en afgrænsning i forhold til informations- og ytringsfriheden, hvorom de nærmere grænser fastsættes ved lov, jf. forordningens artikel 85. Den nærmere afgrænsning må i øvrigt udfyldes i praksis.

På betænkningens s. 957 anføres det bl.a., at når Folketingets Administration bistår Folketingets medlemmer i deres funktion som folketingsmedlemmer, må behandling i Folketingets Administration også antages at kunne undtages fra forordningen.

Det anføres i Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., 2020, DJØF Forlag, s. 989 ff. bl.a., at den behandling af oplysninger, der foretages som led i Folketingets kontrol med regering og i form af medvirken til udarbejdelse af lovgivning mv. er undtaget fra loven og forordningen efter databeskyttelseslovens § 3, stk. 3. Det anføres endvidere, at undtaget efter bestemmelsen er først og fremmest de egentlige folketingsudvalg, herunder Udenrigspolitisk Nævn, jf. grundlovens § 19, stk. 3, parlamentariske kommissioner, jf. grundlovens § 51, og det i henhold til grundlovens § 71, stk. 7, nedsatte udvalg for tilsyn med personer, der er underkastet administrativ frihedsberøvelse. Det antages endvidere, at behandlingen af oplysninger som led i betjeningen af Folketingets Præsidium og ved borgerdrevne beslutningsforslag også er undtaget efter bestemmelsen.

Det anføres endvidere, at når Folketingets Administration bistår Folketingets medlemmer i deres funktion som folketingsmedlemmer, er Folketingets Administrations behandling af personoplysninger undtaget fra loven og forordningen. Som eksempler på behandling foretaget i Folketinget, der ikke sker som led i parlamentarisk arbejde, kan nævnes Folketingets personale- og bygningsadministration.

Endelig anføres det af forfatterne på s. 990 f., at databeskyttelseslovens § 3, stk. 3, ikke ændrer på, at loven og forordningen gælder for behandlingsaktiviteter, som udføres for politiske partier repræsenteret i Folketinget. Det antages, at den behandling af personoplysninger, som består i at videregive oplysninger til Folketinget m.v., ikke kan falde ind under undtagelsen i § 3, stk. 3, men er omfattet af loven og forordningen.

Der ses ikke at være offentliggjort praksis fra Datatilsynet eller de danske domstole vedrørende spørgsmålet om grænserne for databeskyttelseslovens § 3, stk. 3. Fra Folketingets Administration har jeg modtaget kopi af en anmeldelse af 20. juni 2023 til Datatilsynet efter databeskyttelsesforordningens artikel 33 vedrørende et brud på persondatasikkerheden. I sagen havde fire personer sendt et brev til Folketingets Sundhedsudvalg indeholdende bl.a. helbredsoplysninger om afsenderne. Henvendelserne blev af Folketingets Administration omdelt som et udvalgsbilag på sundhedsudvalgets sagsområde og blev ved en menneskelig fejl efterfølgende offentliggjort på folketingets hjemmeside www.ft.dk. Folketingets Administration trak efterfølgende anmeldelsen tilbage overfor Datatilsynet, da Folketingets Administration mente, at behandlingen af personoplysningerne fandt sted som led i Folketingets parlamentariske arbejde og dermed var omfattet af undtagelsesbestemmelsen i databeskyttelseslovens § 3, stk. 3. Datatilsynet er efter det oplyste ikke fremkommet med bemærkninger hertil.

Den dataansvarlige er defineret som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger, jf. databeskyttelsesforordningens artikel 4, nr. 7, 1. led.

Databehandleren er defineret som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne, jf. databeskyttelsesforordningens artikel 4, nr. 8.

Enhver behandling af personoplysninger skal leve op til en række principper for behandling af personoplysninger opregnet i databeskyttelsesforordningens artikel 5.

Det følger således af artikel 5, stk. 1, litra a, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«). Bestemmelsen antages at fastsætte en standard om god databehandlingsskik, som skal udfyldes af tilsynsmyndighederne, jf. Justitsministeriets betænkning 1565/2017, s. 92. Det fremgår af præambelbetragtning 39 bl.a., at enhver behandling af personoplysninger bør være lovlig og rimelig. Det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet. Dette princip om gennemsigtighed har sammenhæng med reglerne om oplysningspligt efter databeskyttelsesforordningens artikel 13-14.

Efter Datatilsynets praksis medfører princippet om god databehandlingsskik endvidere bl.a., at en behandling, der er i strid med anden lovgivning end databeskyttelsesforordningen, heller ikke lovligt vil kunne foretages efter databeskyttelsesforordningen, jf. f.eks. Datatilsynets afgørelse af 17. maj 2018 vedrørende SKAT's brug af ulovligt fremskaffede oplysninger (j.nr. 2018-32-0065).

Efter princippet om formålsbegrænsning skal personoplysninger endvidere indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål, jf. artikel 5, stk. 1, litra b, 1. led.

Personoplysninger skal endvidere være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«), jf. artikel 5, stk. 1, litra c.

Den dataansvarlige skal endvidere have hjemmel til behandlingen af personoplysninger efter databeskyttelsesforordningens og -lovens hjemmelsbestemmelser.

Oplysninger om identiteten på fysiske personer, der modtager e-mails, e-mailadresser, så vel som oplysninger om afsendelses- og modtagelsestidspunktet for e-mailen udgør ikke-følsomme personoplysninger omfattet databeskyttelsesforordningens artikel 6. Efter bestemmelsen kan en dataansvarlig lovligt behandle sådanne personoplysninger, hvis behandling er nødvendig af hensyn til udførelse af en opgave i

samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. artikel 6, stk. 1, litra e.

Behandling er endvidere lovlig, hvis behandlingen er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn, jf. artikel 6, stk. 1, litra f, der dog ikke gælder for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Fra dansk retspraksis kan der henvises til Højesterets dom af 4. februar 2015 i U 2015.1525 H, som er gennemgået ovenfor.

Datatilsynet har i tilsynets vejledning og praksis i flere tilfælde forholdt sig til spørgsmålet om overvågning af e-mails. Som det fremgår nedenfor, vedrører vejledning og praksis i langt overvejende grad spørgsmålet om, hvorvidt arbejdsgivere lovligt kan foretage overvågning af medarbejderes ind- og udgående e-mails som led i ansættelsesforholdet.

Kristian Korfits Nielsen og Anders Lotterup sammenfatter i Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., 2020, DJØF Forlag, s. 396 ff. retsstillingen vedrørende private arbejdsgiveres kontrol med medarbejdernes ind- og udgående e-mail. Det anføres – bl.a. på baggrund af Datatilsynets udtalelse i sagen j.nr. 2000-631-0001 (ÅB 2000, side 31-32) – at en privat virksomhed kan ud fra ledelses-, drifts- og sikkerhedsmæssige hensyn normalt foretage kontrol af, om fastsatte retningslinjer for brug af myndighedens eller virksomhedens it-systemer bliver overholdt, jf. forordningens artikel 5, stk. 1, litra b, og artikel 6, stk. 1, litra f. Kontrollen kan rette sig mod medarbejdernes adgang til hjemmesider og afsendelse og modtagelse af privat e-mail og kan omfatte en gennemgang af en eventuel sikkerhedskopi af ind- og udgående e-mail. Som udgangspunkt skal de ansatte på forhånd klart og tydeligt være gjort opmærksom på, at denne kontrol kan finde sted, jf. forordningens artikel 13-14 om oplysningspligt og artikel 5, stk. 1, litra a, om god databehandlingsskik. Ved kontrol med e-mail må virksomheden ikke læse indholdet af en e-mail, når denne er identificeret som privat, jf. herved også straffelovens § 263, stk. 2, nr. 1, om brevhemmelighed.

Det anføres endvidere, at Datatilsynets praksis skal ses i lyset af Den Europæiske Menneskerettighedsdomstols praksis i forhold til Den Europæiske Menneskerettighedskonventions artikel 8 om den enkeltes ret til respekt for bl.a. privatliv og korrespondance.

I Datatilsynets vejledning om databeskyttelse i ansættelsesforhold, marts 2023, fremgår det af afsnit 5.4 på s. 34 bl.a., at arbejdsgiveres registrering (logning) af medarbejdernes hjemmesidebesøg og efterfølgende gennemgang af registreringen ved mistanke om misbrug af internettet samt tilsvarende kontrol af

e-mails kan ske under visse betingelser. Hvis behandlingen ikke sker som led i en kontrolforanstaltning i henhold til en kollektiv aftale om kontrolforanstaltninger, vil behandlingsgrundlaget være databeskyttelsesforordningens artikel 6, stk. 1, litra e (offentlige arbejdsgivere) eller litra f (private arbejdsgivere). Det anføres endvidere, at medarbejderne skal på forhånd – på en klar og utvetydig måde – være informeret om, at registreringen/logningen finder sted, og at registrering af hjemmesidebesøg og brug af e-mails eventuelt vil blive gennemset som led i en kontrol ved mistanke om brug i strid med arbejdspladsens retningslinjer.

Der kan endvidere henvises til Artikel 29-Gruppens udtalelse 2/2017 om databehandling på arbejdspladsen af 8. juni 2017 (WP 249) samt Artikel 29-Gruppens Working document on the surveillance of electronic communications in the workplace af 29. maj 2002 (WP 55), der angår retsstillingen efter det nu ophævede databeskyttelsesdirektiv. Af sidstnævnte vejledning anføres på s. 4 bl.a. følgende:

> *"It should be clear that the simple fact that a monitoring activity or surveillance is considered convenient to serve the employer's interest would not solely justify any intrusion in worker's privacy. Before being implemented in the work place, any monitoring measure must pass a list of tests, which are extensively detailed in this working document.*
>
> *The following questions may summarise the nature of this assessment:*
>
> *a) Is the monitoring activity transparent to the workers?*
>
> *b) Is it necessary? Could not the employer obtain the same result with traditional methods of supervision?*
>
> *c) Is the processing of personal data proposed fair to the workers?*
>
> *d) Is it proportionate to the concerns that it tries to ally?"*

Der kan endelig henvises til Peter Blumes artikel "Ansattes e-post" i UfR 1999B.194 samt Peter Blume og Jens Kristiansen, Persondataret i ansættelsesforhold, 1. udg., 2011, DJØF Forlag, s. 173-184.

5. VURDERING

5.1 Straffeloven og EMRK

Det følger af straffelovens § 263, stk. 1, at den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem, straffes med bøde eller fængsel indtil 1 år og 6 måneder.

Det følger af forarbejderne til bestemmelsen, at beskyttelsen af datasystemer og data omfatter alle former for data, dvs. både programmer, indholdsdata og metadata. Det er således ikke alene indholdet af eksempelvis elektronisk kommunikation, der er beskyttet, men også eksempelvis oplysninger om afsender og modtager af en e-mail, antallet af udvekslede e-mails mellem bestemte personer, størrelsen af vedhæftede filer mv. Det følger videre, at elektronisk kommunikation er beskyttet både før afsendelsen, under forsendelsen (transmissionen) og efter modtagelsen, herunder efter at være blevet læst af rette modtager.

Det følger videre af forarbejderne til straffelovens § 263, stk. 1, at bestemmelsen angår den, der på en hvilken som helst måde uberettiget skaffer sig adgang til et datasystem eller data, jf. Folketingstidende 2018-19 (1. samling), tillæg A, lovforslag nr. L 20, som fremsat, s. 46. Det følger videre, at udtrykket "*en andens*" relaterer sig både til datasystem og data, og gerningsindholdet er således opfyldt, hvis man skaffer sig adgang til en andens data, uanset om systemet tilhører gerningsmanden eller en anden. Der vil således kunne foreligge en strafbar krænkelse ved brug af eget datasystem, hvis f.eks. udlejeren af et datasystem uberettiget skaffer sig adgang til lejerens data, som er indkodet i datasystemet.

Det følger også af forarbejderne til bestemmelsen, at der kan forekomme tilfælde, hvor man kun ved et konkret skøn kan afgøre, om en handling, der sprogligt omfattes af bestemmelsens ordlyd, skal anses som strafbar. Dette vil navnlig få betydning i forhold til personer, der har en berettiget adgang til et datasystem, men som anvender denne adgang til andre formål end dem, som adgangen er givet til.

Det fremgår videre af forarbejderne, at for så vidt angår en arbejdsgivers adgang til en medarbejders private oplysninger, som måtte være placeret i arbejdsgiverens datasystem, herunder navnlig private e-mails – må udgangspunktet være, at arbejdsgiveren ikke er berettiget til at tilgå en medarbejders private oplysninger, selv om disse findes i arbejdsgiverens datasystem. Det er imidlertid vanskeligt i generel form at fastslå, under hvilke omstændigheder dette udgangspunkt kan fraviges. Afgrænsningen af, hvornår arbejdsgiverens adgang er berettiget, må således bero på en konkret vurdering af sagens omstændigheder, herunder navnlig af hvad der eventuelt er aftalt mellem arbejdsgiveren og medarbejderen om brugen af arbejdsgiverens systemer til private formål.

Folketingets Administration foretog den 14. marts 2024 en søgning i spamfiltret efter e-mails ud fra et konkret afsendernavn og tidspunktet for modtagelsen af e-mailen og gjorde sig derved bekendt med, at 33 personer – heraf 17 folketingsmedlemmer og 16 ansatte i partierne – havde modtaget en e-mail fra en specifik borger. Ved søgningen fremkom følgende oplysninger:

- Mailens navn (emnefelt),
- afsenderen (e-mail/navn),
- modtageren (e-mail/navn),
- dato for e-mailens afsendelse,
- tidspunktet for e-mailens afsendelse, samt
- nogle tekniske felter.

Der er således tale om data, der er omfattet af beskyttelsen i straffelovens § 263, stk. 1.

Det er på baggrund af sagens oplysning herudover vores vurdering, at Folketingets Administration havde en klar formodning om det konkrete indhold af de 33 udsøgte e-mails henset til, at de anvendte søgekriterier skete med det formål at udsøge bestemte e-mails med et indhold svarende til den e-mail, som Folketingets Administration fik videresendt den 14. marts 2024 fra Formandens sekretariat, og som indeholdt navn og billede på en sigtet i en verserende straffesag om drabet på en 13-årig pige i Hjallerup.

Det forhold, at Folketingets Administration har anført i sine regler, at "*Folketinget betragter som udgangspunkt alle e-mail som tilhørende Folketinget, medmindre den i emnefeltet er mærket: "Personligt", "Privat" el.lign.*", ændrer ikke ved, at de udsøgte mails udgør privat korrespondance mellem en borger og et Folketingsmedlem/en ansat i partierne, som er beskyttet af straffelovens § 263 mod at andre end afsenderen og modtageren gør sig bekendte hermed.

Det skal hertil bemærkes, at det forhold, at de fremsendte e-mails efter det oplyste ikke var mærket "privat" eller lignende heller ikke ændrer på, at der er tale om privat korrespondance, og at Folketingets Administration forud for udsøgningen var bekendt med, at de e-mails, som Folketingets Administration udsøgte, udgjorde privat korrespondance fra en borger til medlemmer af Folketinget og ansatte i partierne uden relation til Folketingets Administration. Det bemærkes samtidig, at der var tale om indgående e-mails sendt til brugere af Folketingets IT-systemet, og at der derfor ikke kan stilles samme krav, om at borgere, der fremsender e-mails til Folketingets medlemmer eller ansatte i partierne er bekendte med, at private mails skal markeres med "privat" for at blive anset for private og ikke blive tilgået af Folketingets Administration.

Der foreligger i øvrigt ikke et arbejdsgiver/arbejdstager-forhold mellem Folketingets Administration og Folketingets medlemmer eller ansatte i partierne, hvor Folketingets Administration f.eks. har instruksbeføjelser over Folketingsmedlemmer eller de ansatte i partierne, og de modtagne e-mails kan således ikke tilhøre Folketingets Administration som arbejdsgiver.

Sagen adskiller sig på disse punkter også afgørende fra Højesterets dom gengivet i UfR 2015.1525 H, hvor det blev tillagt vægt, at der bestod en arbejdsgiver/arbejdstager-relation, herunder at der forelå en underskrevet ansættelseskontrakt om vilkår for anvendelse af arbejdsmailen, at medarbejderen selv havde fremsendt mailen uden at angive "privat" i emnefeltet, ligesom det ikke på forhånd var muligt at afgøre, om de pågældende e-mails havde et privat indhold, og at de pågældende e-mails både indeholdt private og arbejdsrelaterede meddelelser. Ingen af de nævnte omstændigheder er til stede ved Folketingets Administrations udsøgning af e-mails.

Det er på den baggrund vores vurdering, at det objektive gerningsindhold i straffelovens § 263 er opfyldt, for så vidt angår, at Folketingets Administration har skaffet sig adgang til andres data, som er bestemt til at bruges i et datasystem. Spørgsmålet er herefter alene om handlingen på andet grundlag kan anses for "berettiget".

Der foreligger efter det oplyste ikke samtykke fra de 33 personer til, at Folketingets Administration har gjort sig bekendt med indholdet af deres private korrespondance (såkaldt "diskulperende samtykke"). Spørgsmålet er herefter om Folketingets Administration på andet grundlag berettiget har skaffet sig adgang til de pågældendes private korrespondance.

Folketingets Administration var først i kontakt med politiet efter tidspunktet for udsøgningen af e-mails, og det fremgår af sagens oplysninger, at der ikke var drøftelser med politiet om udsøgningen af e-mails eller vejledning af Folketingets it-brugere, og udsøgningen af e-mails skete således ikke på grundlag af dialog eller opfordring fra politiet, men på Folketingets Administrations eget initiativ.

Når en domstol i straffesager nedlægger et navneforbud efter retsplejelovens § 31 indebærer dette ingen handlepligter for Folketingets Administration i relation til Folketingets Administrations udbud af mailservice til medlemmer af Folketinget eller ansatte i Folketingets partier.

Hvis Folketingets Administration bliver bekendt med et muligt strafbart forhold – som eksempelvis mistanke om overtrædelse af et navneforbud efter retsplejelovens § 31 – kan Folketingets Administration (på samme måde som alle øvrige borgere og virksomheder) anmelde forholdet til politiet i medfør af retsplejelovens § 742, hvorefter politiet efter anmeldelse eller af egen drift iværksætter efterforskning, når der er rimelig formodning om, at et strafbart forhold, som forfølges af det offentlige, er begået. Det følger

af politilovens § 2, nr. 3, at det er politiets opgave at bringe strafbar virksomhed til ophør, og de nærmere regler og processer herfor er fastsat i retsplejeloven.

Da Folketingets Administration således ikke har nogen retlige pligter i anledning af et nedlagt navneforbud i relation til Folketingets Administrations udbud af mailservice, er spørgsmålet, om det kan være berettiget på frivillig basis at skaffe sig adgang til andres data med henblik på at kunne yde dem vejledning om indholdet af en modtaget e-mail.

For at en sådan handling vil kunne anses for berettiget vil det efter vores vurdering som minimum kræve, at udsøgningen både var egnet, nødvendig og proportional til at opnå formålet. Da Folketingets Administration udsøgning skete med det formål at vejlede medlemmerne/de ansattes i partierne om et nedlagt navneforbud er spørgsmålet således, om det var påkrævet at foretage en søgning i medlemmernes/de ansattes i partierne modtagne e-mails, før en sådan vejledning kunne ydes.

Det er vores vurdering, at Folketingets Administration kunne have ydet den fornødne vejledning til brugerne af deres it-system, uden først at foretage søgning i privat korrespondance. Folketingets Administration kunne således have opnået vejledningsformålet ved at udsende en generel mail med oplysninger om, at der var nedlagt navneforbud i den verserende straffesag om drabet på en 13-årig pige i Hjallerup, og at Folketingets Administration var blevet gjort bekendt med, at der (evt. på en bestemt dato og tidspunkt) var blevet sendt oplysninger til visse af Folketingets it-brugere, som kunne udgøre en overtrædelse af navneforbuddet. Det var således efter vores vurdering hverken egnet, nødvendigt eller proportionalt at foretage søgning i brugernes e-mails for at kunne give denne vejledning.

Det skal dog samtidig fremhæves, at der foreligger en række formildende omstændigheder i sagen, som også kan tillægges vægt ved bedømmelsen af forholdet. Det må således tillægges en formildende omstændighed, at den valgte metode for udsøgningen af e-mails ikke gav mulighed for at åbne de pågældende e-mails, og at Folketingets Administration ikke har gennemgået meddelelser af privat karakter i videre omfang, end påkrævet for at kunne udskille den del af mailkorrespondancen, Folketingets Administration vurderede var relevant i forhold til undersøgelsens formål. Det må endvidere tillægges en vis vægt, at Folketingets Administration straks slettede søgningen efter at have identificeret modtagerne af de pågældende e-mails og også orienterede de berørte personer herom samt var i kontakt med politiet om indgivelse af en politianmeldelse. Det må ligeledes tillægges en vis formildende omstændighed, at medarbejderen, der foretog udsøgningen af e-mails, havde en berettiget adgang til spam-filtret og var sikkerhedsgodkendt og underlagt tavshedspligt. Det må også tillægges en vis formildende betydning, at der var fastsat retningslinjer om brugen af e-mails, og at it-brugerne var blevet gjort bekendt med, at Folketingets Administration ville kunne have adgang til e-mails under særlige omstændigheder, og at Folketingets Administration agerede i henhold hertil, om end de som nævnt efter vores vurdering ikke gav grundlag for at skaffe sig berettiget adgang til informationer om de 33 personers private e-mails.

Det bemærkes i den forbindelse, at vurderingen af, om et strafbart forhold er begået, udelukkende henhører under domstolene, og at det inden da også beror på, hvilke oplysninger der fremkommer under politiets efterforskning af et muligt strafbart forhold samt af politiets og anklagemyndighedens vurdering af forsætsgraden og sagens beviser på tidspunktet for eventuel anmeldelse, sigtelse og tiltalerejsning.

Da vi vurderer, at forholdet er omfattet af straffelovens § 263, stk. 1, er det ikke aktuelt at foretage en vurdering af en potentiel overtrædelse af straffelovens § 263, stk. 2, nr. 1, da denne er subsidiær i forhold til straffelovens § 263, stk. 1.

I forhold til spørgsmålet om overtrædelse af Den Europæiske Menneskerettighedskonventions (EMRK) artikel 8, stk. 1, om retten til respekt for sit privatliv og sin korrespondance, er det vores vurdering, at Folketingets Administrations udsøgningen af de 33 e-mails udgør et indgreb i Folketingsmedlemmernes og de ansatte i partiernes ret til privatliv og korrespondance. Som nævnt ovenfor er det endvidere vores vurdering, at udsøgningen ikke skete i overensstemmelse med straffelovens § 263, stk. 1, og at udsøgning dermed ikke var i overensstemmelse med loven, hvorfor kriteriet i artikel 8, stk. 2, om lovhjemmel ikke var opfyldt.

Det er tilsvarende vores vurdering, at udsøgningen ikke opfylder kravene i EMRK artikel 8, stk. 2, om at være nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder, idet udsøgningen af de 33 personers e-mails ikke var egnet, nødvendig eller proportional i forhold til, at Folketingets Administration kunne søge at yde vejledning til deres it-brugere om, at de kunne have modtaget en e-mail med oplysninger omfattet af et navneforbud.

Det er samlet set derfor vores vurdering, at Folketingets Administrations udsøgning af e-mails ikke var foreneligt med straffelovens § 263, stk. 1, eller med EMRK artikel 8.

5.2 Spørgsmålet om overtrædelse af reglerne om behandling af personoplysninger i databeskyttelsesforordningen og -loven

Der er ikke tvivl om, at Folketingets Administrations søgning på de indgående e-mails i sagen udgør en elektronisk behandling af personoplysninger, idet personoplysningerne udgøres af e-mailadresser og oplysninger om navn på afsender og modtagerne, der er fysiske personer.

Folketingets Administrations søgning på modtagerne af de omhandlede e-mails kan endvidere ikke anses for at være omfattet af undtagelsen i databeskyttelseslovens § 3, stk. 3, hvorefter loven og databeskyttelsesforordningen ikke finder anvendelse på behandling af oplysninger, der foretages som led i Folketingets parlamentariske arbejde. Det er således vores vurdering, at databeskyttelsesreglerne i databeskyttelsesforordningen og -loven finder fuldt ud anvendelse i sagen.

For så vidt angår personoplysningerne om de partiansatte og borgerens e-mail til disse finder loven og forordningen anvendelse i overensstemmelse med det almindelige udgangspunkt om, at loven og forordningen finder anvendelse på behandling af personoplysninger, når behandlingen ikke sker som led i parlamentarisk arbejde og betjening, herunder de behandlingsaktiviteter, som udføres for politiske partier repræsenteret i Folketinget. At databeskyttelsesforordningen og -loven finder anvendelse i forhold til de partiansatte, er også antaget af Folketingets Administration selv, der således har indgået en databehandleraftale med de pågældende partier efter databeskyttelsesforordningen.

For så vidt angår vurderingen i forhold til personoplysningerne om folketingsmedlemmerne må der lægges vægt på, at Folketingets Administrations søgning på de omhandlede e-mails ikke kan siges at ligge indenfor Folketingets Administrations opgaver – hverken som led i parlamentarisk arbejde eller i øvrigt – idet beslutningen om at gennemføre søgningen udgjorde en overtrædelse af straffeloven og EMRK. Det forhold, at folketingsmedlemmerne har modtaget de pågældende e-mails, der var genstanden for Folketingets Administrations søgning, fra en borger som led i parlamentarisk arbejde i deres egenskab af folketingsmedlemmer, kan ikke føre til et andet resultat.

Ved at have taget initiativ til og gennemført søgningen må Folketingets Administration anses for dataansvarlig for behandlingen. Det gælder også i forhold til de partiansatte, uanset at Folketingets Administration har indgået databehandleraftaler med de respektive partier, og hvorefter Folketingets Administration er databehandler. Der må lægges vægt på, at det ikke fremgår af databehandleraftalen, at Folketingets Administration instrueres i at foretage en sådan søgning, som sagen handler om. Ved således at have handlet uden for instruksen i databehandleraftalen, har Folketingets Administration handlet som selvstændig dataansvarlig.

Spørgsmålet er herefter, om Folketingets Administration havde hjemmel og overholdt de grundlæggende principper i databeskyttelsesforordningens artikel 5 ved søgningen. Efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, er behandling af ikke-følsomme personoplysninger lovlig, når behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Efter Datatilsynets praksis medfører princippet om god databehandlingsskik i databeskyttelsesforordningens artikel 5, stk. 1, litra a, bl.a., at en behandling, der er i strid med anden lovgivning end databeskyttelsesforordningen, heller ikke lovligt vil kunne foretages efter databeskyttelsesforordningen.

Som det er konstateret i gennemgangen ovenfor, udgjorde Folketingets Administrations søgning en overtrædelse af straffelovens § 263, stk. 1, og EMRK artikel 8 og dermed også en overtrædelse af god databehandlingsskik efter databeskyttelsesforordningens artikel 5, stk. 1, litra a.

Ved vurderingen af proportionaliteten af behandlingen efter databeskyttelsesforordningens artikel 5, stk. 1, litra c, må der – på samme måde som ved vurderingen efter straffelovens § 263, stk. 1 – navnlig lægges vægt på, at Folketingets Administration burde have søgt at bekræfte, hvorvidt der var nedlagt navneforbud i sagen, inden søgningen blev foretaget, samt at Folketingets Administration under alle omstændigheder kunne have sendt en e-mail tilsvarende advarselsmailen til alle folketingsmedlemmer og partiansatte med samme virkning, uden at det havde været nødvendigt at tilgå bestemte folketingsmedlemmer og partiansattes data. Hertil kommer det forhold, at Folketingets Administration først sendte advarselsmailen to dage (ca. 38 timer) efter modtagelsen af den oprindelige e-mail, hvilket også taler imod berettigelsen af søgningen. Efter vores vurdering var forløbet derfor tilrettelagt på en sådan måde, at der i hvert fald var en betydelig risiko for, at den oprindelige e-mail allerede var blevet læst af i hvert fald de fleste af modtagerne med den konsekvens, at formålet med stor sandsynlig ikke ville kunne opnås. Folketingets Administrations søgning var således ikke egnet, nødvendig eller proportional.

I formildende retning taler, *at* formålet med søgningen – at advare modtagerne af e-mailen – tjente et sagligt formål, idet Folketingets Administration befandt sig i en faktisk vildfarelse, *at* medarbejderen, der foretog udsøgningen af e-mails, havde en berettiget adgang til spam-filtret og var sikkerhedsgodkendt og underlagt tavshedspligt, *at* søgningen blev gennemført som en "nålestiksoperation", hvor der alene blev søgt på den pågældende e-mail og ikke bredt, og hvor Folketingets Administration ikke forsøgte eller fik adgang til modtagernes e-mailindbakker eller indholdet i de fremfundne e-mails, *at* Folketingets Administration straks slettede listen efter søgningen, *at* Folketingets Administration i to e-mails informerede modtagerne om søgningen og formålet hermed samme dag, som søgningen blev foretaget, *at* Folketingets Administration involverede politiet i sagen, samt *at* der var fastsat retningslinjer om brugen af e-mails, og at it-brugerne var blevet gjort bekendt med, at Folketingets Administration ville kunne have adgang til e-mails under særlige omstændigheder, og at Folketingets Administration agerede i henhold hertil, om end de som nævnt efter vores vurdering ikke gav grundlag for at skaffe sig berettiget adgang til informationer om de 33 personers private e-mails.

På denne baggrund er det vores vurdering, at Folketingets Administrations udsøgning af e-mails ikke skete i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra a, om god databehandlingsskik, artikel 5, stk. 1, litra c, om dataminimering samt databeskyttelsesforordningens artikel 6, stk. 1, litra e.

5.3 Sammenfatning og anbefalinger

Som begrundet ovenfor, er det samlet set vores vurdering, at Folketingets Administrations udsøgning af e-mails ikke var foreneligt med straffelovens § 263, stk. 1, eller med EMRK artikel 8.

Det er endvidere vores vurdering, at Folketingets Administrations udsøgning af e-mails ikke skete i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra a, om god databehandlingsskik, artikel 5, stk. 1, litra c, om dataminimering samt databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Som anført ovenfor gælder der en række formildende omstændigheder i sagen. Det er på denne baggrund ikke vores opfattelse, at Folketingets Administration har pligt til at politianmelde forholdet.

Vi anbefaler, at Folketingets Administration retter henvendelse til de implicerede folketingsmedlemmer og partiansatte, der var genstand for søgningen, og anfører, at søgningen på e-mails ikke var i overensstemmelse med gældende regler, som Folketingets Administration beklager. Meddelelsen skal endvidere indeholde de forhold, der er omfattet af oplysningspligten i databeskyttelsesforordningens artikel 14. Tilsvarende gælder i forhold til borgeren, der sendte e-mailen til de pågældende personer. Da Folketingets Administration har slettet listen fra søgningen over de omhandlede personers e-mailadresser, kan Folketingets Administration orientere om sagen ved at sende samtlige partiansatte og medlemmer af Folketinget samt borgeren en e-mail med de ovenfor angivne informationer.

[redacted] Der foreligger ikke i sagen informationer om, at hverken Folketingets Administrations direktion – defineret som direktøren og de to vicedirektører – eller Folketingets formand var vidende om eller involveret i selve fremsøgningen af de omhandlede e-mails eller har afgivet instruktioner herom. På denne baggrund er der ikke grundlag for et strafferetligt ansvar for denne personkreds, endsige ansættelsesretlige sanktioner.

Vi kan i øvrigt forstå, at Folketingets Administration allerede har iværksat arbejde med henblik på at revidere procedurer og arbejdsgange med henblik på at undgå lignende tilfælde fremadrettet.

Vi har ikke foretaget en vurdering af, hvorvidt Folketingets Administrations søgning udgjorde et brud på persondatasikkerheden, der skal anmeldes til Datatilsynet – og som de berørte registrerede skal underrettes om – efter de gældende regler herom i henholdsvis databeskyttelsesforordningens artikel 33-34.

København, den 18. april 2024

Martin Sønnersgaard
Partner, Advokat

Fra: Jonas Blegvad Jensen <jona@poulschmith.dk>
Sendt: 17. april 2024 16:47
Til: Lotte Spanggaard <lotte.spanggaard@ft.dk>
Cc: Anita Strauss Sørensen <asso@poulschmith.dk>
Emne: Lidt ekstra fakta - fortroligt

Kære Lotte

[redacted]

[redacted]

[redacted]

Du må endelig tage fat i mig, hvis du har spørgsmål.

Dbh

Jonas

Med venlig hilsen

JONAS BLEGVAD JENSEN
PARTNER, ADVOKAT

M +45 31 79 31 31
@ JONA@POULSCHMITH.DK
W POULSCHMITH.DK

Poul Schmith
KAMMERADVOKATEN

FOLKETINGET

Redegørelse om Folketingets Administrations overvågning af bl.a. folketingsmedlemmers mails i en konkret sag

April 2024

Indhold

1. Indledning

På baggrund af en konkret sag, hvor Folketingets Administration (herefter: administrationen) har foretaget en søgning på udvalgte folketingsmedlemmers og ansattes indgående mails, er det besluttet at udarbejde nærværende redegørelse om sagen til Folketingets Præsidium.

Redegørelsen er bygget op om tre afsnit:

For det første indledes med en beskrivelse af de generelle regler og procedurer, der i dag gælder for administrationens overvågning af mails, *jf. afsnit 2. Generelle regler og procedurer i dag*. Afsnittet har bl.a. til formål at beskrive, hvorfor der foretages overvågning, i hvilket omfang der overvåges, hvem der overvåger, samt hvad overvågningen indebærer.

For det andet gennemgås det konkrete sagsforløb, som har givet anledning til redegørelsen, *jf. afsnit 3. Beskrivelse af den konkrete sag*. Sagsforløbet gennemgås kronologisk og sammenholdes med Folketingets generelle regler og procedurer for at identificere, om der er sket overtrædelser af de gældende regler og om der kan ske opstramninger af de nuværende regelsæt og procedurer.

Endelig *for det tredje* afrundes redegørelsen med et afsnit, dels med en juridisk vurdering af den aktuelle sag, dels med forslag til anbefalinger om opstramninger af de gældende regler og procedurer som følge af den konkrete sag, *jf. afsnit 4. Fremadrettede opstramninger og procedurer*.

2. Generelle regler og procedurer for overvågning af mails i Folketinget

2.1. Om it i Folketinget

Administrationen stiller forskellige it-systemer til rådighed for både folketingsmedlemmer, ansatte i grupper og partier samt for administrationen selv. Folketingsmedlemmerne bruger bl.a. et mailsystem, som administrationen drifter på vegne af alle partigrupper. Medlemmer og ansatte er i kraft heraf også udstyret med en officiel mailadresse fra Folketinget og følger de it-regler, som til enhver tid er gældende for brugere i Folketinget.

Det er Folketingets it-afdeling (herefter ITS), der drifter Folketingets netværk og servere samt de programmer, som anvendes i det daglige arbejde, herunder mailsystemet. ITS stiller desuden udstyr (pc, iPhone og evt. iPad) til rådighed for alle it-brugere i huset.

2.2. It-sikkerhed i Folketinget

Folketinget prioriterer it-sikkerhed meget højt for at beskytte brugernes data og integritet. [redacted]

Som led i driften opretholder administrationen derfor til stadighed et højt informationssikkerhedsniveau på baggrund af det aktuelle trusselsbillede og risikovurderinger af Folketingets data og aktiver.

Informationssikkerhedsarbejdet i Folketinget følger – ligesom i staten – ISO-standarden 27001. Denne standard anviser en struktureret tilgang og "best practice" inden for it-sikkerhed.

For at opretholde et højt informationssikkerhedsniveau og beskytte medlemmers og Folketingets data, foretages der automatiske overvågninger, scanninger og logninger af alle data i Folketingets it-systemer. Det er her vigtigt at understrege, at administrationen i denne overvågning *ikke* overvåger enkeltmedlemmers eller –ansattes mailbokse, ligesom indholdet af mails ikke tilgås. Der er således fuld fortrolighed omkring det enkelte medlems og ansattes mailkorrespondancer.

Det er også vigtigt at understrege, at det alene er i helt særlige tilfælde af alarmer fra overvågningen eller ved anden mistanke, der indikerer tegn på aktive it-sikkerhedshændelser, at betroede og sikkerhedsgodkendte it-medarbejdere, der er underlagt tavshedspligt, foretager analyse af den pågældende datatrafik. Dette gøres for at forhindre potentielle cyberangreb eller andre hændelser, der kan skade it-brugerne eller Folketingets data og systemer. Det kan fx være afpresningsmails, ransomware (hvor data krypteres og der skal betales en løsesum for at få dem udleveret) eller spyware (skadeligt software, som installerer sig med det formål at overvåge og indsamle information om brugerens aktiviteter).

I tilrettelæggelsen og udviklingen af it-sikkerhedsarbejdet modtager administrationen løbende rådgivning fra CFCS og PET, ligesom administrationen i høj grad læner sig op ad de sikkerhedsanbefalinger, som gælder for Staten.

Det er særdeles sjældent, at ITS søger på indgående mails, og det sker altid på baggrund af en konkret sag eller henvendelse. [redacted]

[redacted]

Det er således meget sjældent, at administrationen tilgår mails, og som de konkrete tilfælde viser, så har det været i sager vedrørende datasikkerhed. Der er ikke nylige eksempler på, at der er foretaget en søgning som følge af kriminelle handlinger.

Folketinget prioriterer således it-sikkerhed meget højt med det klare formål at beskytte folketingsmedlemmerne mod spionage, kriminalitet og tyveri af data og personoplysninger. Som led heri er en løbende generel overvågning af datatrafik ind og ud af Folketingets systemer nødvendig, men uden at enkeltmedlemmers mails og deres indhold overvåges og tilgås. Overvågningen er automatiseret, og det sker meget sjældent, at ITS søger på indgående mails, og altid på baggrund af en konkret sag eller henvendelse.

2.3. Folketingets It-sikkerhedspolitik

Folketingets it-sikkerhedsarbejde er forankret i *Folketingets overordnede informationssikkerhedspolitik, jf. bilag 1*, som er godkendt af Præsidiet, og i

Folketingets regler for Informationssikkerhed og *Brug af Folketingets it-udstyr på rejser, jf. bilag 2*, som er godkendt af Direktionen.

Som nyvalgt folketingsmedlem skal man deltage i *Folketingets Introduktionskursus* (FTI) om sikkerhed, it og telefoni i Folketinget for at få udleveret it-udstyr. Dette foregår ved en mentorsamtale med en it-medarbejder. I forbindelse med udlevering af it-udstyr til nye medlemmer gennemgås og udleveres også *Folketingets overordnede informations-sikkerhedspolitik* og *Folketingets regler for Informationssikkerhed*.

Af *Folketingets regler for Informationssikkerhed* fremgår bl.a.:

"Privat brug af e-mail

...

Folketinget forbeholder sig ret til at skaffe sig adgang til data og e-mail hos medarbejdere, når dette sker af drifts- eller sikkerhedshensyn eller ved henvendelser fra politiet, PET og lignende myndigheder i forbindelse med opklaring af strafbare forhold eller i tilfælde, hvor Folketinget er retligt forpligtet til at udlevere det pågældende materiale til andre."
(Folketingets regler for Informationssikkerhed, side 6).

"Overvågning og begrænsning

Folketinget filtrerer og begrænser internetadgangen baseret på trusselsniveauet. Det betyder, at hjemmesider, der indeholder virus eller på andre måder udgør en sikkerhedstrussel, bliver blokeret af forskellige automatiske sikkerhedssystemer.

Monitorering

Folketinget har automatiseret overvågning af al ind- og udgående datatrafik for at forebygge it-sikkerhedshændelser. I tilfælde af alarmer fra

overvågningen eller ved anden mistanke, der indikerer tegn på aktive it-sikkerhedshændelser, tillades det at foretage en analyse af den pågældende datatrafik."
(Folketingets regler for Informationssikkerhed, side 10)

Folketingsmedlemmer og ansatte gøres således bekendt med, at Folketinget som led i it-sikkerhedsarbejdet løbende overvåger data- og mailtrafikken med mulighed for at foretage nærmere analyser af datatrafikken i helt særlige tilfælde.

Folketingets it-sikkerhedsregler er desuden tilgængelige på Nettinget https://nettinget.ft.dk/ It_sikkerhed?item=6609.

Der har hidtil hersket den praksis, at ITS i henhold til det regelsæt, som Præsidiet og direktionen har godkendt, kan foretage nærmere analyser af data- og e-mailtrafik uden inddragelse af direktionen, når det sker i forbindelse med forebyggelse af sikkerhedshændelser eller opklaring af strafbare forhold. Ledelsen informeres således ikke forud for igangsættelse af nærmere analyser på anmodning fra fx myndighederne, men orienteres i stedet efterfølgende i bl.a. statusopgørelser.

Folketingsmedlemmer gøres i forbindelse med udlevering af it-udstyr opmærksom på, at Folketinget i henhold til det gældende regelsæt foretager løbende overvågning af al ind- og udgående datatrafik for at forebygge it-sikkerhedshændelser. Det fremgår således af Folketingets it-sikkerhedspolitikker, at ITS i tilfælde af alarmer fra overvågningen eller ved anden mistanke, der indikerer tegn på aktive it-sikkerhedshændelser, kan foretage analyser af den pågældende datatrafik. It-sikkerhedsreglerne er tilgængelige på Nettinget for såvel medlemmer som ansatte.

3. Beskrivelse af den konkrete sag
I dette afsnit gennemgås den konkrete sag, der sammenholdes med de overordnede it-sikkerhedsregler som beskrevet i det foregående afsnit.

3.1. Den 12. marts 2024 modtager Formandskontoret en mail i Postkasse til Folketingets Formand fra et folketingsmedlem, som gør opmærksom på, at vedkommende har modtaget en mail vedrørende en verserende retssag. Det drejer sig om drabet på en 13-årig pige fra Hjallerup. Af mailen fremgår den sigtedes navn og billede. Samtidig nævner det pågældende folketingsmedlem, at der er nedlagt navneforbud i sagen.

3.2. Formandskontoret videresender den 14. marts 2024 mailen til ITS med henblik på at få undersøgt sagen. Formanden orienteres ikke om sagen, der betragtes som en ren administrativ sag.

3.3. [redacted] kontakter [redacted], som anbefaler, at der tages kontakt til Politiets efterforskningsvagt i Folketinget for en vurdering af mailen. [redacted] iværksætter herefter en søgning i mailtransportserveren for at undersøge, om mailen er sendt til flere modtagere, hvilket viser sig at være tilfældet. I henhold til praksis orienteres hverken vicedirektøren eller direktionen forud for igangsættelsen af søgningen. Herefter kontaktes politiet. I dialogen med politiet får administrationen desværre den fejlagtige opfattelse, at der er nedlagt navneforbud i sagen.

3.4. Som det fremgår af Folketingets it-sikkerhedspolitik, så kan ITS foretage en analyse af den pågældende datatrafik, der knytter sig til den konkrete sag, hvor Folketinget er retligt forpligtet til at udlevere det pågældende materiale til andre. Derfor samler ITS en liste over it-brugere i

Folketinget, som har modtaget den pågældende mail, som anses for at bryde med et navneforbud. 33 it-brugere havde modtaget mailen, heraf 17 folketingsmedlemmer.

3.5. Når ITS vælger at gå videre med sagen, så skyldes det altså hensynet til det enkelte folketingsmedlem, som måtte have modtaget mailen for at gøre opmærksom på, at der var mistanke om et strafbart forhold. Som bekendt viste det sig senere at være en fejlagtig opfattelse, at der var nedlagt et navneforbud i den konkrete sag.

3.6. Konkret foregår dette ved, at en betroet og sikkerhedsgodkendt medarbejder i ITS samlede navnene på en liste, som alene it-medarbejderen selv, en [redacted] medarbejder samt [redacted] har set. Listen er efterfølgende slettet efter at den har tjent sit konkrete formål.

3.7. Det er også vigtigt at understrege, at når der foretages en søgning på indgående mails, kan it-medarbejderen ikke læse indholdet af mailen. Søgningen foretages på en såkaldt mailtransportserver, hvor der alene kan ses følgende oplysninger om indgående mails: Dato, tidspunkt, afsender, modtager og emnefelt. Medarbejderen har således ikke tilgået eller set andre informationer eller læst indholdet af mailen og medarbejderen har ikke haft adgang til modtagernes postkasser på mailserveren.

3.8. Herefter sender ITS en mail til de 33 modtagere for at gøre opmærksom på, at de har modtaget mailen, som ITS har en opfattelse af bryder med et navneforbud, *jf. bilag 3*. I mailen beder en medarbejder fra ITS om, at man sletter mailen.

3.9. Efter at mailen er udsendt, kontaktes ITS af flere medarbejdere fra DF, der spørger til sagen og fremgangsmåden. Andre medarbejdere kvitterer og fortæller, at de har blokeret afsenderen.

3.10. ITS udsender herefter endnu en mail, hvor baggrunden forklares (at ITS reagerer på en henvendelse) og det understreges, at søgningen udelukkende er foregået på dato, tidspunkt og afsenderadresse, og at ITS ikke har tilgået brugernes indbakker og indholdet af mails.

3.11. [redacted] orienterer herefter den 14. marts om aftenen pr. mail vicedirektøren om, at der er foretaget en søgning som følge af en konkret sag.

3.12. Dagen efter den 15. marts 2024 fremsender MF Peter Kofod (DF) en klage til formanden med en række opklarende spørgsmål, *jf. bilag 4*. Hermed orienteres direktionen om den konkrete sag.

3.13. Da der ikke var udformet svar på klagen fra Peter Kofod på tidspunktet for præsidiemøde den 20. marts 2024, valgte administrationen ikke at nævne sagen på mødet. I stedet ville man afvente det endelige svar og orientere Præsidiet efterfølgende om administrationens svar på DF's klage. I lyset af det videre sagsforløb burde der have været orienteret om henvendelsen på præsidiemødet, hvilket administrationen skal beklage ikke skete.

3.14. Administrationen fremsender den 22. marts 2024 svar på Peter Kofods spørgsmål, *jf. bilag 5*. Samtidig orienteres Præsidiet om svaret.

3.15. Ekstra Bladet bringer den 23. marts 2024 en artikel om sagen, *jf. bilag 6*.

3.16. Ekstra Bladet bringer en ny artikel den 25. marts 2024 med gengivelse af administrationens svar til Peter Kofod, *jf. bilag 7.*

3.17. Ekstra Bladet bringer den 28. marts 2024 en ny artikel, hvoraf det fremgår, at der ikke er nedlagt navneforbud i sagen, *jf. bilag 8.* I artiklen undskylder administrationen for de fejlagtige oplysninger i svaret til Peter Kofod og bebuder en gennemgang og opstramning af de eksisterende procedurer. Det fremgår også af artiklen, at der er foretaget en anmeldelse til Københavns Politi for brud på brevhemmeligheden. Administrationen har dog endnu ikke hørt fra Københavns Politi. Præsidiet orienteres forud for artiklen om Folketingets svar til Ekstra Bladet.

3.18. Jyllands-Posten bringer den 30. marts 2024 også en artikel om sagen, *jf. bilag 9.* Ud over at gengive indholdet af Ekstra Bladets artikler, så indeholder artiklen også kommentarer til sagen fra henholdsvis SF og Enhedslisten. Præsidiet orienteres forud for artiklen om Folketingets svar til Jyllands-Posten.

3.19. Den 2. april 2024 briefes præsidiemedlemmerne mundtligt om sagen af vicedirektøren for Service- og Administrationsafdelingen.

3.20. Den 3. april 2024 sendes udkast til orienteringsmail af gruppeformændene til Præsidiet til orientering.

3.21. Senere samme dag sendes orienteringsmail til gruppeformænd om sagen, *jf. bilag* 10.

3.22. Vicedirektøren for Service- og Administrationsafdelingen giver UFO en orientering om sagen på dets møde den 10. april 2024.

4. Fremadrettede opstramninger og procedurer

4.1. Juridisk vurdering af sagen

Kammeradvokaten er bedt om at lave en juridisk vurdering af den konkrete sag, herunder om der er sket strafferetlige overtrædelser, om brevhemmeligheden er brudt, om hvilket arbejdsgiveransvar, der påhviler Folketinget som systemansvarlig, samt om der er sket brud på GDPR-reglerne.

Ifølge Kammeradvokatens vurdering foreligger der ikke i sagen informationer om, at hverken Folketingets Administrations direktion – defineret som direktøren og de to vicedirektører – eller Folketingets formand var vidende om eller involveret i selve fremsøgningen af de omhandlede e-mails eller har afgivet instruktioner herom. På denne baggrund er der ikke grundlag for et strafferetligt ansvar for denne personkreds, endsige ansættelsesretlige sanktioner.

Overordnet set konkluderer Kammeradvokaten følgende (af hensyn til personfølsomme oplysninger i redegørelsen, optrykkes Kammer-advokatens redegørelse ikke som bilag):

- Det er samlet set vurderingen, at Folketingets Administrations udsøgning af e-mails i den konkrete sag ikke var foreneligt med straffelovens § 263, stk. 1, eller med Den Europæiske Menneskerettighedskonventions (EMKR) artikel 8.
- Det er desuden vurderingen, at Folketingets Administrations udsøgning af e-mails ikke skete i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 1, litra a, om god databehandlingsskik, artikel 5, stk. 1, litra c, om dataminimering samt data-beskyttelsesforordningens artikel 6, stk. 1, litra e.

- Kammeradvokaten konkluderer også, at der gælder en række formildende omstændigheder i sagen: I formildende retning taler, at formålet med søgningen - at advare modtagerne af e-mailen - tjente et sagligt formål, idet Folketingets Administration befandt sig i en faktisk vildfarelse, at medarbejderen, der foretog udsøgningen af e-mails, havde en berettiget adgang til spam-filtret og var sikkerhedsgodkendt og underlagt tavshedspligt, at søgningen blev gennemført som en "nålestiksoperation", hvor der alene blev søgt på den pågældende e-mail og ikke bredt, og hvor Folketingets Administration ikke forsøgte eller fik adgang til modtagernes e-mailindbakker eller indholdet i de fremfundne e-mails, at Folketingets Administration straks slettede listen efter søgningen, at Folketingets Administration i to e-mails informerede modtagerne om søgningen og formålet hermed samme dag, som søgningen blev foretaget, at Folketingets Administration involverede politiet i sagen, samt at der var fastsat retningslinjer om brugen af e-mails, og at it-brugerne var blevet gjort bekendt med, at Folketingets Administration ville kunne have adgang til e-mails under særlige omstændigheder, og at Folketingets Administration agerede i henhold hertil, om end de som nævnt efter Kammeradvokatens vurdering ikke gav grundlag for at skaffe sig berettiget adgang til informationer om de 33 personers private e-mails.
- Det er på denne baggrund ikke Kammeradvokatens opfattelse, at Folketingets Administration har pligt til at politianmelde forholdet.
- Kammeradvokaten anbefaler, at Folketingets Administration retter henvendelse til de implicerede folketingsmedlemmer og partiansatte, der var genstand for søgningen, og anfører, at søgningen på e-mails ikke var i overensstemmelse med gældende regler, som Folketingets Administration beklager. Meddelelsen skal endvidere indeholde de

forhold, der er omfattet af oplysningspligten i databeskyttelses-forordningens artikel 14. Tilsvarende gælder i forhold til borgeren, der sendte e-mailen til de pågældende personer. Da Folketingets Administration har slettet listen fra søgningen over de omhandlede personers e-mailadresser, kan Folketingets Administration orientere om sagen ved at sende samtlige partiansatte og medlemmer af Folketinget samt borgeren en e-mail med de ovenfor angivne informationer.

[redacted]

- Kammeradvokaten anbefaler endelig, at Folketingets Administration reviderer sine procedurer og arbejdsgange med henblik på at undgå lignende tilfælde fremadrettet.

Nedenfor vil Kammeradvokatens vurderinger blive flettet ind i de konkrete anbefalinger og opstramninger, som sagen giver anledning til. Samlet set skal anbefalingerne dels tage hånd om de forhold, som Kammeradvokaten anfører ovenfor, og dermed skal de dels betrygge såvel folketingsmedlemmer som ansatte i, at en lignende sag ikke fremover bør eller kan forekomme. Det er vigtigt hensyn fra administrationens side, at det gode og tillidsfulde forhold til såvel medlemmer som ansatte hermed ønskes bevaret og styrket.

4.2. Juridiske anbefalinger

Anbefaling 1: Styrket DPO-aftale og samling af complianceområdet

Det er Kammeradvokatens opfattelse, at Folketingets Administration ikke har pligt til at politianmelde den konkrete sag. Det skyldes, at der gælder en række formildende omstændigheder i sagen: Bl.a. tjente søgningen et sagligt formål, medarbejderen, der foretog udsøgningen af e-mails, havde

en berettiget adgang til spam-filtret og var sikkerhedsgodkendt og underlagt tavshedspligt, søgningen blev gennemført som en "nålestiksoperation", hvor der alene blev søgt på den pågældende e-mail og ikke bredt, og hvor Folketingets Administration ikke forsøgte eller fik adgang til modtagernes e-mailindbakker eller indholdet i de fremfundne e-mails, Folketingets Administration slettede straks efter listen, Folketingets Administration informerede i to e-mails modtagerne om søgningen og formålet hermed samme dag, som søgningen blev foretaget, Folketingets Administration involverede politiet i sagen og endelig var der fastsat retningslinjer om brugen af e-mails, og at it-brugerne var blevet gjort bekendt med, at Folketingets Administration ville kunne have adgang til e-mails under særlige omstændigheder.

Der vil dog blive lagt op til opstramning og styrkelse af GDPR-området i Folketinget.

Det vil for det første ske i en ny aftale med et eksternt advokatfirma om at varetage DPO-rollen for Folketinget. I aftalen vil der være ekstraordinær fokus på en ansvarlig og korrekt overvågning af og tilgang til medlemmers og ansattes mails.

For det andet vil complianceopgaven på it-sikkerhedsområdet samles ét sted i administrationen, fremfor som nu to steder. Med den organisatoriske samling ét sted vil der ske en faglig styrkelse af området samtidig med, at der sker en ressourcemæssig opnormering.

Anbefaling 2: Henvendelse til de implicerede, der var genstand for søgningen

Folketingets Administration vil også rette henvendelse til de implicerede folketingsmedlemmer og partiansatte, der var genstand for søgningen.

Tilsvarende gælder i forhold til borgeren, der sendte e-mailen til de pågældende personer. I henvendelsen vil Folketingets administration beklage sagen.

Da Folketingets Administration har slettet listen fra søgningen over de omhandlede personers e-mailadresser, vil Folketingets Administration orientere om sagen ved at sende samtlige partiansatte og medlemmer af Folketinget samt borgeren en e-mail med de ovenfor angivne informationer.

Anbefaling 3: Personalemæssige konsekvenser drages

Selvom udsøgningen af de pågældende mails ifølge Kammeradvokaten ikke var foreneligt med bl.a. straffelovens § 263, stk. 1, så er det Kammeradvokatens vurdering, at Folketingets Administration ikke har pligt til at politianmelde forholdet.

[redacted]

4.3. Administrative anbefalinger

Det er overordentlig vigtigt, at folketingsmedlemmer og ansatte til enhver tid kan have tillid og tiltro til Folketingets Administration. Med henblik på at sikre denne tillid i forlængelse af den konkrete sag, vil der ud over de juridiske skridt også iværksættes en administrativ opstramning, der skal forhindre at lignende sager fremover opstår.

Anbefaling 4: Væsentlig styrkelse af de nuværende regler og procedurer
Det følger af redegørelsen, at administrationens forvaltning af it-sikkerheds-området er forankret i *Folketingets overordnede informationssikkerheds-politik, Folketingets regler for informationssikkerhed* samt *Brug af Folketingets it-udstyr på rejser*.

Det fremgår af reglerne for informationssikkerhedspolitik i hvilke situationer administrationen forbeholder sig ret til at skaffe sig adgang til data og e-mail hos medlemmer og medarbejdere. Dette kan ske af drifts- eller sikkerhedshensyn eller ved henvendelser fra politiet, PET og lignende myndigheder i forbindelse med opklaring af strafbare forhold eller i tilfælde, hvor Folketinget er retligt forpligtet til at udlevere det pågældende materiale til andre.

Fremadrettet skal det nuværende regelsæt strammes op, så det er klart i hvilke situationer administrationen kan tilgå bl.a. medlemmers mails. I dag kan to situationer udløse en tilgang til mails:

1. Ved henvendelser fra politiet i efterforskningssager;
2. Ved it-sikkerhedstrusler, hvor systemer, data og integritet skal beskyttes.

Det skal præciseres, at administrationen alene kan foretage en søgning, hvor det følger af EU-ret eller national ret og sager, hvor systemer og data er truet af akutte cyberhændelser. Administrationen skal således fremadrettet afskæres fra at kunne tage sager op af egen drift som i det konkrete eksempel.

Det er vigtigt at understrege, at Folketinget alene er databehandler og ikke dataansvarlig. Folketinget råder derfor ikke over den data som it-systemerne rummer. Det fremgår også af Kammeradvokatens juridiske vurdering, at der ikke foreligger et arbejdsgiver-/arbejdstagerforhold mellem Folketingets Administration og Folketingets medlemmer eller ansatte i partierne, hvor Folketingets Administration f.eks. har instruksbeføjelser over Folketingsmedlemmer eller de ansatte i partierne. De modtagne e-mails kan således ikke tilhøre Folketingets Administration som arbejdsgiver.

I forlængelse af den konkrete sag er det blevet klart, at administrationen *ikke* kan tilgå mails på baggrund af fx et angiveligt navneforbud eller mistanke om et strafbart forhold. I den konkrete sag konkluderer Kammeradvokaten, at det er uden betydning, om der har været nedlagt et navneforbud eller ej. Folketinget burde ikke af egen drift have tilgået medlemmers og ansattes mails. I stedet burde administrationen have undladt at gøre noget i den konkrete sag og have informeret generelt om den konkrete mail på Nettinget, og at det var op til det enkelte medlem eller den ansatte at håndtere mailen. I sin iver efter at servicere medlemmer og ansatte er man fra administrationens side derfor gået for vidt i den konkrete sag.

I forlængelse af anbefaling 1, vil der derfor sammen med det eksterne advokatfirma blive igangsat en opstramning og revision af de nuværende regler og procedurer, således det står klart i hvilke situationer administrationen kan tilgå medlemmers mails og hvad det kræver af forudgående information til medlemmer og ansatte. Retningslinjen vil som udgangspunkt her være, at det kun er i tilfælde, hvor EU-ret eller national ret tillader en søgning samt i situationer, hvor medlemmers data og integritet samt it-systemer skal beskyttes i tilfælde af akut cybersikkerhed, at der kan foretages en søgning.

Desuden vil det tydeliggøres og orienteres om på Nettinget og i databehandleraftaler i hvilke tilfælde, der kan forekomme overvågning af mails.

Anbefaling 5: Forudgående orientering af direktionen
Direktionen blev ikke orienteret på forhånd om den søgning, som ITS foretog i sagen. En forudgående orientering ville sandsynligvis have medført et andet hændelsesforløb, da der ville have været tid til at drøfte den konkrete sag og dens konsekvenser.

Derfor vil der blive indskrevet i retningslinjerne, at den ansvarlige vicedirektør eller direktionen skal orienteres forud for, at administrationen ønsker at foretage en søgning i it-systemerne.

Anbefaling 6: Øget ledelsesmæssig fokus på området
I lyset af den konkrete sag er det tydeligt, at der fremadrettet vil være behov for et øget ledelsesmæssigt fokus på området fra vicedirektørens side. Den ansvarlige vicedirektør vil derfor dække området tættere fremover.

Anbefaling 7: Orientering af medlemmer og Præsidium
På UFO-mødet var der et ønske om, at der fremadrettet er hurtig information i denne slags sager, der involverer medlemmers mails.

I arbejdet med en opdatering af regler og retningslinjer vil det derfor blive indskrevet, at administrationen løbende skal informere de direkte involverede folketingsmedlemmer og andre relevante parter i sagen. I nogle sager vil man dog ikke kunne involvere andre end det implicerede folketingsmedlem. I sager med en bredere offentlig interesse orienteres Præsidiet og UFO hurtigst muligt, hvis sagens karakter tillader det.

Bilag 3

Fra: Postkasse til Informationssikkerhed
Sendt: 14. marts 2024 12:47
Cc: IT-Hotline <3000@ft.dk>; [redacted]
Emne: Du har modtaget en mail med ulovligt indhold, der skal slettes.

Kære modtager af denne mail

Vi er blevet gjort opmærksom på, at du og flere andre har modtaget en e-mail, der indeholder grafik og informationer om en aktuel straffesag, hvor der er nedlagt navneforbud.

Vi skal bede dig om at slette den pågældende mail fra din Indbakke og dernæst fra din mappe til Slettet post.

Du kan kende mailen på afsenderen [redacted] samt at mailen er ankommet 12. marts kl. 22:35.

Hvis du har spørgsmål til dette, er du velkommen til at kontakte mig eller ringe til It-Hotline på tlf. 3000.

Med venlig hilsen

[redacted]

FOLKETINGET

It-systemer

Christiansborg

1240 København K

Tlf. +45 3337 5500

[redacted]

www.ft.dk

Bilag 4

Christiansborg, den 14. marts 2024

Kære Søren Gade,

Den 14. marts kl. 12.47 modtog flere personer tilknyttet Dansk Folkeparti på Christiansborg en henvendelse fra [redacted], der underskrev sig "[redacted]" i Folketinget.

Af mailen fremgik følgende tekst:

Kære modtager af denne mail

Vi er blevet gjort opmærksom på, at du og flere andre har modtaget en e-mail, der indeholder grafik og informationer om en aktuel straffesag, hvor der er nedlagt navneforbud.

Vi skal bede dig om at slette den pågældende mail fra din Indbakke og dernæst fra din mappe til Slettet post.

Du kan kende mailen på afsenderen >NN Borger> på nnadressen@xmail.dk (her har Folketinget angivet navn og mailadresse på mailens afsender) samt at mailen er ankommet 12. marts kl. 22:35.

Hvis du har spørgsmål til dette, er du velkommen til at kontakte mig eller ringe til It-Hotline på tlf. 3000. "

Det gjorde en af vores medarbejder og vedkommende fik af [redacted] oplyst, at der var en person, der havde vist mailen til Folketingets formand, og at Folketingets formand havde tilkendegivet, at han ikke ville have den slags i Folketingets system. Jeg kan så efterfølgende forstå på [redacted] mail til en anden medarbejder i Dansk Folkeparti, at Folketinget har kontaktet politiet og anmeldt afsenderen – må man antage – på vegne af den person, der har vist mailen til Folketingets formand.

Der er flere ting, der undrer i denne forbindelse.

For det første hvem er det, der har gjort Folketingets [redacted] opmærksom på, at personer tilknyttet Dansk Folkeparti og eventuelle andre har modtaget denne mail?

For det andet hvad giver Folketingets [redacted] ret til at påbegynde en søgning af hvilke mails folketingsmedlemmer og medarbejdere måtte have modtaget? Er dette ikke en krænkelse af brevhemmeligheden?

For det tredje hvilken ret har Folketinget til at beordre folketingsmedlemmer og ansatte til at slette mails, som de har modtaget?

For det fjerde hvem har taget initiativ til at [redacted] skulle rundsende en henvendelse med krav om sletning til modtagere af den pågældende mail?

For det femte kan formanden ikke godt se, at formanden med sin disposition om at få gennemtrawlet folketingsmedlemmernes mailkorrespondance og som medlem af et regeringsparti dermed reelt spionerer på oppositionens medlemmer?

For det sjette har Folketingets [redacted] eller andre ansatte i IT-afdelingen søgt på andre mails, som folketingsmedlemmer eller ansatte har modtaget?

For det syvende, er der lavet en liste over, hvem der har modtaget henvendelsen fra NN Borger i Folketinget? Hvem er i besiddelse af denne liste og hvem kender til indholdet heraf? Man må antage, at der er en liste, eftersom [redacted] udbakke kan vise, hvem der har modtaget mailen fra NN Borger, idet

det jo fremgår af hvem [redacted] har sendt sin mail til. Er det ikke bekymrende, at der dermed figurerer lister over, hvem der modtager korrespondance fra en specifik borger?

Endelig er der det helt principielle spørgsmål:

Vi arbejder i Danmarks parlament. Folketingsmedlemmerne må kunne forvente, at den e-post, som de modtager og udveksler ikke kan læses af andre end dem selv. Jeg bliver stærkt foruroliget over, at Folketinget iværksætter en proces, hvor man undersøger, hvilke medlemmer og ansatte, der har modtaget henvendelser fra bestemte personer. Folketingsmedlemmerne kan ikke udføre deres arbejde, hvis deres emailkorrespondance bliver overvåget fra formandskontoret.

I Dansk Folkeparti undrer vi os såre over denne sag.

Der er efter vores opfattelse gjort et indgreb i brevhemmeligheden. Folketinget har tilsyneladende på formandens foranledning undersøgt hvilke personer folketingsmedlemmer kommunikerer med. Hele processen er undergravende for folketingsmedlemmernes tillid til at de kan arbejde uden at være genstand for overvågning fra formandskontoret.

Dansk Folkeparti ønsker på denne baggrund, at sagen tages op i Folketingets præsidium.

Peter Kofod

Gruppeformand

Bilag 5

Kære Peter Kofod

Tak for din henvendelse til Folketingets Formand med spørgsmål til en mail, der indeholder informationer om en aktuel straffesag, hvori der er nedlagt navneforbud. Formanden har bedt Folketingets Administration om at besvare din henvendelse.

Jeg er selvfølgelig ærgerlig over, hvis der har været uklar kommunikation mellem Folketingets Administration og Dansk Folkeparti om sagen. Derfor vil jeg også kort redegøre for det faktiske forløb med henblik på at besvare de spørgsmål, som du har rejst i din henvendelse til formanden. Jeg har også rakt ud til jeres sekretariatschef Nicolai Kjær for at drøfte de stillede spørgsmål.

I forbindelse med den verserende sag om drabet i Hjallerup nedlagde politiet skærpet navneforbud i forhold til den 17-årige sigtede i sagen. Administrationen blev imidlertid den 14. marts 2024 gjort opmærksom på, at et medlem af Folketinget havde modtaget en mail, hvor den sigtedes både navn og billede fremgår. Folketingets Administration tog herefter kontakt til politiet med henblik på at vurdere, hvordan man skulle forholde sig til sagen. Da der var tale om en overtrædelse af det skærpede navneforbud, ville Politiet gerne efterforske sagen. På denne baggrund valgte Administrationen at rette henvendelse til de it-brugere, som måtte have modtaget mailen.

I henhold til Folketingets Informationssikkerhedspolitik kan Folketingets Administration i helt særlige tilfælde, navnlig i overtrædelses- og efterforskningssager, foretage søgninger i vores mailsystemer. Det fremgår af retningslinjernes side 6. Informationssikkerhedspolitikken og de tilhørende retningslinjerne er godkendt af Folketingets Direktion og Præsidium.

Det er vigtigt at understrege, at Folketingets Administration naturligvis aldrig på daglig basis, fremsøger eller tilgår medlemmers eller ansattes mails. Det sker kun helt undtagelsesvist som beskrevet ovenfor i overtrædelses- og efterforskningssager. Jeg har derfor forståelse for, hvis der i den konkrete sag kan have været skabt usikkerhed om, hvorvidt Folketingets Administration tilgår medlemmers og ansattes mails. Men her er det meget vigtigt for mig at slå fast, at dette *ikke* er tilfældet.

Søgningen i mailsystemet er konkret sket ved, at den ansvarlige it-medarbejder, der ligesom alle andre it-medarbejdere både er sikkerhedsgodkendt af PET og underlagt tavshedspligt, alene har søgt på det konkrete afsendernavn og tidspunkt for modtagelse. Medarbejderen har altså ikke hverken tilgået eller set andre informationer eller indhold af mails i it-systemerne. Der er derfor ikke tale om en gennemgang af mailkorrespondancer eller brud på brevhemmeligheden, men en søgning efter én specifik mail på en afsenderadresse. Jeg håber derfor at kunne berolige med at søgningen alene er afgrænset til én afsenderadresse.

For at kunne rette henvendelse til modtagerne af mailen, har en medarbejder i it-afdelingen samlet navnene på en liste, som alene personen selv, [redacted] samt afsenderen af mailen har set. Listen er omgående slettet efter at den har tjent sit konkrete formål.

For så vidt angår mailen til modtagerne af mailen, så er det vigtigt at understrege, at hverken folketingsmedlemmer eller partiansatte er blevet beordret til at slette mailen. Vi gjorde opmærksom på mailen og bad om, at den blev slettet pga. navneforbuddet. Hvis nogen har følt sig beordret til at slette mailen har det været utilsigtet, og det skal Folketingets Administration i så fald beklage.

Jeg håber, at jeg med dette svar har gjort det tydeligt, at ingen medarbejdere i Folketingets Administration har haft uberettiget adgang til jeres mails. Formålet har alene været at gøre modtagerne opmærksom på, at de har modtaget en mail, som bryder et navneforbud samt opfordre til, at mailen slettes.

Med venlig hilsen

Torben Skovgaard Andersen, Vicedirektør

Bilag 10

Fra: Magnus Jarl Brunés **På vegne af** Folketingets formand
Sendt: 3. april 2024 17:12
Til: [redacted]
Emne: Håndtering af medlemmernes mails

Kære kollega

Hen over påsken har både Ekstra Bladet og Jyllands-Posten bragt en historie om Folketingets håndtering af medlemmernes mails i en konkret sag. Med denne mail vil jeg gerne kort orientere jer om den konkrete sag.

I forbindelse med sagen om drabet på en 13-årig pige i Hjallerup blev Folketingets Administration gjort opmærksom på, at et medlem af Folketinget havde modtaget en mail, hvori den sigtedes både navn og billede fremgår. Administrationen tog herefter kontakt til politiet med henblik på at vurdere, hvordan man skulle forholde sig til sagen. Politiet ville gerne efterforske sagen, og i dialogen med politiet fik administrationen desværre den fejlagtige opfattelse, at der var nedlagt et navneforbud i sagen. På denne baggrund valgte administrationen at rette henvendelse til de it-brugere, som måtte have modtaget mailen.

I henhold til Folketingets Informationssikkerhedspolitik og regler, som findes på Nettinget, kan Folketingets Administration i helt særlige tilfælde, herunder når hensynet til politimæssig efterforskning og cybersikkerhed tilsiger det, anvende muligheden for at søge i indgående mails. På baggrund af den fejlagtige opfattelse af et navneforbud, besluttede administrationen derfor at foretage en søgning på, om andre ansatte eller medlemmer i Folketinget havde modtaget den pågældende mail. Den medarbejder, som har foretaget søgningen i mailsystemet, er både sikkerhedsgodkendt og underlagt tavshedspligt. Listen fra søgningen er omgående slettet efter at den havde tjent sit konkrete formål. Det er værd at bemærke, at medarbejderen alene har søgt på det konkrete afsendernavn og tidspunktet for modtagelsen. Medarbejderen har således ikke tilgået eller set andre informationer eller læst indholdet af mails. Efterfølgende har administrationen skrevet til de personer, som har modtaget den pågældende mail og opfordret til, at mailen slettes.

Dansk Folkeparti har efterfølgende rettet henvendelse til mig med en række opklarende spørgsmål til det konkrete sagsforløb. Dem har administrationen efterfølgende svaret på. Desværre blev det i svaret fra administrationen fejlagtigt oplyst, at der var nedlagt et navneforbud i sagen. Det har administrationen erkendt var en klar fejl og undskyldt over for Dansk Folkeparti.

Sagen har givet anledning til, at jeg har bedt administrationen give Præsidiet en redegørelse om sagsforløbet på næste møde. I redegørelsen vil der også blive inddraget ekstern bistand med henblik på at vurdere de juridiske aspekter.

Desuden har sagen ført til, at administrationen har besluttet at gennemgå sine nuværende regler og procedurer med henblik på, dels om en lignende sag kan undgås fremover, dels om der generelt kan strammes op og udvises yderligere forsigtighed med hensyn til medlemmernes mails. I dette arbejde vil det også indgå, om vi kan kommunikere bedre om politikker og regler på området.

Lad mig afslutningsvis pointere, at der selvfølgelig skal være fortrolighed om de mails, som MF'ere modtager og sender. Folketingets Administration kan dog ved sjældne lejligheder blive nødt til at gå på kompromis med dette princip for at opretholde et højt IT-sikkerhedsniveau for det mailsystem, vi drifter på vegne af alle medlemmer. Risikoen for cyberangreb og digital kriminalitet bliver desværre ikke mindre. Det er naturligvis vigtigt, at der er klare og velargumenterede rammer for Folketingets Administrations handlinger i denne sammenhæng.

Skulle I have yderligere spørgsmål til den verserende sag eller vores generelle it-sikkerhed er I velkomne til at kontakte vicedirektør Torben Skovgaard Andersen, som kan uddybe. I kan kontakte ham på telefonnummer [redacted] eller på torben.andersen@ft.dk.

Med venlig hilsen

Søren Gade

Søren Gade

Folketingets formand

FOLKETINGET

Medlem af Folketinget (V)

Christiansborg

1240 København K

Tlf. +45 3337 5500

Dir. [redacted]

Postformand@ft.dk

www.ft.dk