Digitale Archivering in Vlaamse Instellingen en Diensten

DAVID

Archiveren van e-mail

Filip Boudrez

Hannelore Dekeyser

Sofie Van den Eynde

2de herwerkte editie

FACULTEIT RECHTSGELEERDHEID – K.U.LEUVEN

INTERDISCIPLINAIR CENTRUM VOOR RECHT EN INFORMATICA

Stadsarchief Stad Antwerpen

Versie 2.0

Wettelijk depot D/2003/9.213/11

Antwerpen-Leuven, november 2003

E-mailadres: david@stad.antwerpen.be

Website DAVID-project: http://www.antwerpen.be/david

DAVID is een onderzoeksproject gefinancierd door het Fonds voor Wetenschappelijk Onderzoek in het kader van het Max Wildiersfonds

INHOUDSTAFEL

I. INLEIDING

E-mail heeft zich tijdens de jaren negentig ontwikkeld als een algemeen verspreide technologie, die heel wat aspecten van ons professioneel en persoonlijk leven ingrijpend veranderd heeft. Er zijn dan ook ontelbare studies verricht naar de juridische, sociale en ethische implicaties van e-mail en naar de voor- en nadelen van dit nieuwe communicatiemiddel. Ook de overheden in Vlaanderen worden in toenemende mate geconfronteerd met het fenomeen 'elektronische post'. In het streven naar een betere dienstverlening aan de burger spelen netwerken en elektronische post een belangrijke rol. Op dit moment worden er zowel op federaal als op Vlaams niveau ambitieuze e-government projecten uitgewerkt. Het is de bedoeling om via gebruiksvriendelijke portaalsites zowel de communicatie tussen burger en overheid, als de communicatie tussen de overheden onderling op een snelle en efficiënte manier te laten verlopen. Deze experimenten zijn ondenkbaar zonder elektronische post.

Overheidsadministraties zijn volgens de archiefwet verplicht de onder hen berustende informatie in goede, geordende en toegankelijke staat te bewaren. Ook archivarissen worden bijgevolg volop met dit nieuwe medium geconfronteerd. Naast de archiefwet regelen ook de openbaarheidswetgeving en de privacyreglementering hoe overheidsadministraties moeten omgaan met de door hun ontvangen en opgemaakte informatie. Zoals we verder in dit rapport zullen aantonen, vallen ook digitale gegevens, waaronder elektronische post, onder de toepassing van deze reglementeringen en moeten dus dienovereenkomstig behandeld worden.

Op juridisch vlak heeft vooral de terbeschikkingstelling van e-mail door de werkgever aan zijn werknemers heel wat vragen doen rijzen. Er bestaat immers grote rechtsonzekerheid over de vraag in welke mate het recht op privacy van de werknemer mag opzij gezet worden, opdat de werkgever zijn recht om toezicht te houden op de arbeidsprestaties kan uitoefenen[1]. Ook de archivaris dient de privacyreglementering te respecteren en moet zich afvragen in welke mate de elektronische postbus van de ambtenaar een glazen huis is. Zoals verder zal blijken, beperkt niet het briefgeheim, maar het telecommunicatiegeheim, de rechten van de archivaris in niet geringe mate. Verder bekijken we ook hoe de openbaarheidswetgeving een invloed heeft op het e-mailbeleid binnen Vlaamse administratieve overheden.

Voor de meeste juridische vragen omtrent privacy en openbaarheid bestaan er geen kant-en-klare antwoorden. Daarom is het van belang dat de Vlaamse overheden duidelijke richtlijnen uitwerken, zodat bestuurders, ambtenaren en netwerkbeheerders weten waar ze aan toe zijn en hun gedrag hierop kunnen

[1] Deze juridische vraag wordt voor het Belgisch recht uitvoerig bestudeerd in J. DUMORTIER , "Internet op het werk: controlerechten van de werkgever", *Oriëntatie*, februari 2000, 35-42 en J. DUMORTIER, "Little Brother is watching you: mag de werkgever het Internetgebruik van zijn werknemers controleren?" in X., *Liber Amicorum Prof. Dr. Roger Blanpain*, Brugge, Die Keure, 1999, 243-259.

afstemmen. Naar aanleiding van het toenemend gebruik van e-mail op de werkvloer en het gebrek aan wetgeving hieromtrent, zijn er in vele organisaties op dit moment 'e-mail policies' in de maak. Wat we echter vaststellen, is dat in de meeste van deze policies geen enkele richtlijn voorkomt over het beleid van de organisatie omtrent het archiveren van e-mails[2]. Ze handelen vooral over toegang tot het e-mailsysteem ten aanzien van categorieën van werknemers, het loyaal gebruik van e-mail door de werknemer (hoe moet een bericht opgesteld zijn, e-mail etiquette, verboden gebruik), de privacy-verwachtingen die werknemers mogen hebben of juist niet mogen hebben (vooral dit deel moet juridisch geëvalueerd worden), bescherming tegen virussen, richtlijnen in verband met auteursrecht enzovoort. In het eerste deel van dit rapport gaan we na hoe het juridisch kader in België er op dit moment uitziet omtrent (het archiveren van) e-mail, zodat hiermee rekening kan worden gehouden bij de ontwikkeling van een e-mail policy.

Het wijdverspreide gebruik van e-mail brengt voor de archivaris niet alleen juridische vragen met zich mee. Van hen wordt verwacht dat ze deze digitale archiefdocumenten in hun archief opnemen en dat het e-mailarchief in een goede, geordende en toegankelijke staat wordt bewaard. In het tweede deel van dit rapport komt daarom de problematiek van e-mailarchivering aan bod. Daarom bekijken we heel concreet welke pistes er in de praktijk kunnen gevolgd worden om e-mail te archiveren en geven we richtlijnen voor het uitwerken ervan in de praktijk. De evolutie in de richting van e-government en e-commerce onderstreept het belang en de potentiële archiefwaarde van e-mails des te meer.

Niettegenstaande dit gegeven zijn er nog maar weinig instellingen of organisaties met een coherent archiveringssysteem voor binnenkomende en uitgaande e-mailberichten. De ontwikkeling van een archiveringsbeleid dringt zich dus op.

Voortbouwende op de conclusies uit de juridische voorstudie, worden eerst de archiverings-mogelijkheden overlopen. Hierbij wordt aandacht besteed aan de keuze tussen afdrukken of digitale archivering, de metadata en de context van e-mails, de bijlagen, de digitale duurzaamheid, de integratie met gerelateerde documenten, de terbeschikkingstelling en de veilige bewaring. In dit stuk worden een aantal archivistische en technologische bouwstenen voor het archiveringssysteem voor e-mails aangereikt. Beiden zullen het archiveringsproces in grote mate beïnvloeden. Andere bepalende factoren zijn het e-mailbeleid en de organisatie van de archiefvormer. Een efficiënt archiveringssysteem moet hierop worden afgestemd. Aangezien het e-mailbeleid en de organisatie verschillen van instelling tot instelling zijn er uiteindelijk veel varianten van een goed archiveringssysteem mogelijk. Bij wijze van voorbeeld wordt een *best practice* in digitale archivering voorgesteld.

---

[2] Een voorbeeld van een 'telecommunications policy' die het record-keeping aspect van e-mail wel mee in overweging neemt, is het model dat wordt voorgesteld door WHITMAN, TOWNSEND en AALBERTS. M., WHITMAN, A., TOWNSEND and S., AALBERTS, 'Considerations for an Effective Telecommunications-Use Policy', *Communications of the ACM*, Vol. 42, June 1999. CARDEN toetst de *ABC telecommunications' Electronic Mail Policy*, die midden 1999 verscheen op de Intranet-site van ABC, aan het model, en stelt vast dat er ook hier niets is bepaald omtrent de bewaring van e-mails. Beschikbaar op: http://science.kennesaw.edu/csis/msis/stuwork/IS8070_pa.htm#policy

Een voorbeeld van een *e-mail policy* uit de publieke sector die geen enkele verwijzing bevat naar de behandeling van e-mail als officiële stukken, is de *Internet and E-mail policy* van Washtenaw County, Michigan.

Antwerpen - Leuven, oktober 2001

Dit is de tweede, herwerkte versie van het DAVID-rapport over e-mail archivering. Door de snelle veranderingen op dit domein, bleek het nu reeds, na amper 2 jaar, nodig om dit rapport bij te werken. Op juridisch vlak was er de controverse omtrent de uitoefening van controle door de werkgever op het gebruik dat werknemers maken van de internet- en e-mail faciliteiten van de organisatie. De sociale partners hebben dit probleem aangekaart in C.A.O. nr. 81 dat moet garanderen dat elk toezicht het recht op privacy respecteert. Ook de archivaris dient de privacyreglementering te respecteren en moet zich afvragen in welke mate de elektronische postbus van de ambtenaar een glazen huis is.

Daarnaast werden de resultaten van het pilootproject e-mailarchivering aan de stad Antwerpen verwerkt in dit rapport. Deze casus heeft ondermeer geleid tot een aanpassing van het e-mailsjabloon dat nog efficiënter en gebruikersvriendelijk gemaakt werd.

Het juridische deel werd in deze herwerkte versie onder handen genomen door Hannelore Dekeyser. Het archiefwetenschappelijke deel is nog steeds van de hand van Filip Boudrez.

Antwerpen-Leuven, november 2003

II. WAT IS EEN E-MAIL?

Bij wijze van inleiding is een korte uiteenzetting over het fenomeen 'elektronische post' op zijn plaats. De lezer die reeds vertrouwd is met e-mail bijvoorbeeld als dagdagelijkse gebruiker, kan dit deel overslaan, en onmiddellijk starten met deel III.

Met e-mail kan je snel en gemakkelijk berichten met andere Internetgebruikers uitwisselen, op voorwaarde dat zowel de zender als de ontvanger een e-mailadres en een internetaansluiting heeft. 'Electronic mail' of kortweg 'e-mail', is de Engelse term voor elektronische post. Met de term 'e-mail' wordt zowel het systeem bedoeld dat langs elektronische weg berichten transporteert, als de berichten zelf. In dit rapport verwijzen we met de term 'e-mailsysteem' naar mailserver(software). De term 'e-mail' gebruiken we hier als synoniem voor een elektronisch bericht.

A. HOE WERKT E-MAIL?

Op het Internet heeft iedereen een eigen adres, dat steeds dezelfde structuur heeft. Een e-mailadres bestaat uit twee delen, die gescheiden zijn door het teken '@', ook wel apestaartje genoemd, en uitgesproken als het Engelse 'at' = 'te'. Het gedeelte voor het apestaartje wordt de gebruikersnaam of de e-mailnaam genoemd. Het gedeelte achter het apestaartje, wordt het domein genoemd. Het domein wordt bepaald door de domeinnaam van de internet-provider[3]. Indien een ontvanger, Jan Janssens, een elektronische postbus heeft geopend bij Hotmail, dan zou zijn e-mailadres er bijvoorbeeld als volgt kunnen uitzien: 'Jan.Janssens@hotmail.com'. Er zijn heel wat internet-providers actief op het Internet, waardoor de concurrentie erg groot is.

Om het elektronisch berichtenverkeer in goede banen te leiden, installeert de internet-provider speciale software. Deze speciale software wordt 'mailserversoftware' genoemd (bijvoorbeeld Exchange Server, Domino Server). Er bestaan twee soorten 'mailservers': één voor het versturen van berichten (de SMTP-server) en één voor het ontvangen van berichten (de POP-server). De SMTP-server ('Simple Mail Transport Protocol') zorgt ervoor dat de berichten die de afzender verstuurt, naar de juiste bestemming gaan.[4] Dit kan men vergelijken met sorteerders in het postkantoor. Op het Internet zijn er geen buslichtingen: het bericht wordt onmiddellijk bezorgd. De POP-server (Post Office Protocol) neemt de berichten in ontvangst, en plaatst de berichten in de juiste elektronische postbus. Deze server vervult als het ware de functie van de postbode, die de brieven ook in de juiste brievenbus moet deponeren. De elektronische postbus is een voorbehouden directory op de mailserver van de internet-provider. Hierin blijven de e-mails staan totdat de ontvanger ze opvraagt. De toegang tot de elektronische postbus is

[3] De domeinnaam van de Internet-provider vindt je vaak terug in diens Internetadres, bijvoorbeeld www.hotmail.com; www.uunet.com

[4] SMTP is één van de protocollen die wordt gebruikt voor het verzenden van e-mails. Daarnaast is er bijvoorbeeld ook X.400 en X.500. Netwerken hebben andere configuraties dan het e-mailen via een inbelverbinding (IMAP).

beveiligd door een paswoord. Op die manier wordt er vermeden dat iedereen je postbus kan ledigen en je berichten kan lezen.

De ‘mail-client’ of het e-mailprogramma is het programma dat je gebruikt om je berichten te schrijven, de elektronische post te verzenden, je postvak te ledigen en berichten te lezen of te printen. Er bestaan veel verschillende e-mailprogramma's zoals Eudora, Outlook, Happymail enzovoort

Afbeelding 1 : voorbeeld van een e-mailprogramma

B. STRUCTUUR VAN EEN E-MAILBERICHT

Alle e-mailberichten hebben dezelfde structuur, ongeacht het e-mailprogramma dat men gebruikt.

From: Hier staat het e-mailadres van de afzender: afzender@provider.be

To : Hier staat het e-mailadres van de ontvanger: ontvanger@provider.be

Subject: Dit is het onderwerp van het elektronisch bericht

Cc: ‘Carbon Copy’. Hier kan de afzender het e-mailadres invullen van andere personen, die dan ook het bericht krijgen toegestuurd. De ontvangers kunnen van elkaar het e-mailadres lezen.

Bcc: ‘Blind Carbon Copy’. Hiervoor geldt hetzelfde als voor Cc, maar met dit verschil dat de ontvangers elkaars e-mailadres niet zien verschijnen, zodat ze van elkaar niet weten dat ze dezelfde e-mail hebben ontvangen.

Attached: Complexe elektronische documenten, zoals documenten opgemaakt met een tekstverwerkingsprogramma, een rekenprogramma of een tekenprogramma, zijn doorgaans als een ‘attachment’ aan de e-mail gehecht. Zelfs geluids- en beeldbestanden kunnen op die manier verzonden

worden. Het eigenlijke bericht is dan vaak niets meer dan enkele begeleidende woorden of zinnen. Een ‘attachment’ maakt integraal deel uit van het elektronisch bericht.

Al deze informatie staat in de ‘header’ van de e-mail. De meeste e-mailprogramma’s voorzien ook de mogelijkheid om in de ‘header’ aan te geven dat de e-mail moet beveiligd worden bijvoorbeeld door encryptie, of om duidelijk te maken dat de e-mail met voorrang moet behandeld worden door de ontvanger. De ‘body’ van de e-mail bevat dan de eigenlijke inhoud van het bericht.

C. VOORDELEN VAN E-MAIL

E-mail vervangt niet alleen een deel van de informele, mondelinge communicatie, maar verdringt ook een deel van de formele briefwisseling, die verloopt via de interne briefwisseling binnen een organisatie of via de gereglementeerde postdienst van ‘de Post’. Ten aanzien van een gewone brief, biedt het sturen van een e-mail heel wat voordelen:

1. Het sturen van een e-mail gaat veel sneller. Binnen enkele seconden tot enkele minuten na het verzenden, zit de e-mail al in de elektronische postbus van de bestemmeling.
2. Het sturen van een e-mail is veel goedkoper. Een e-mail sturen in plaats van een brief wordt vooral interessant wanneer men die brief wil sturen naar een bestemmeling die zich in een ander land bevindt. Een e-mail kost immers evenveel, of men hem nu stuurt naar zijn buurman, of naar iemand die zich aan de andere kant van de wereld bevindt.
3. Het versturen van een e-mail kan gebeuren op ieder tijdstip (e-mail wordt ook verzonden op zaterdag en zondag) en bovendien hoef je er de deur niet voor uit.
4. Naar hoeveel personen je een elektronisch bericht ook stuurt, het kost nauwelijks meer tijd.
5. E-mail kan je overal ter wereld en op ieder tijdstip lezen, als je verbinding hebt met het Internet. De elektronische postbus is overal en altijd toegankelijk.

III. WAAROM E-MAIL ARCHIVEREN?

Alvorens in te gaan op het juridisch kader, moeten we ons eerst afvragen waarom de vraag naar de archivering van e-mail op dit moment zo belangrijk is. Met andere woorden: waarom zou men deze relatief nieuwe vorm van digitale informatie gaan archiveren, terwijl het voor de elektronische documenten, die al veel langer geleden hun intrede hebben gedaan, nog helemaal niet duidelijk is hoe hun archivering precies moet verlopen. Bovendien heeft de invoering van applicaties zoals e-mail in organisaties geleid tot een toename van vastlegging van informatie[5]. Inderdaad, e-mail is niet alleen in de plaats gekomen van een aantal klassieke communicatiemiddelen, zoals de briefwisseling en het telefoongesprek; e-mail is vooral een extra communicatiemiddel dat ons ter beschikking wordt gesteld, en dat de bestaande communicatiemiddelen aanvult[6]. Dit heeft voor gevolg dat er nog meer informatie dan voordien zou moeten gearchiveerd worden in heel wat organisaties. Het ontkennen van het bestaan van e-mail door records managers en archivarissen zou echter verkeerd zijn.

A. E-MAIL ALS ARCHIEFSTUK

Wanneer men de vergelijking maakt met het telefoongesprek, ziet men onmiddellijk in dat een e-mail als een archiefstuk moet beschouwd worden. Een archiefstuk is *informatie die is vastgelegd op een drager, ongeacht haar vorm, naar haar aard bestemd om te berusten onder een persoon, groep personen of organisatie die het heeft opgemaakt of ontvangen uit hoofde van zijn of haar activiteiten, zijn of haar taken of ter handhaving van zijn of haar rechten*[7]. Uit de analyse van wat e-mail precies is en hoe het werkt, weten we dat e-mail perfect aan deze definitie voldoet.

- Een e-mail is vastgelegd op een drager, hetzij op de server van de internet-provider, hetzij op de harde schijf van de computer van de ontvanger. Hierin ligt het verschil met een telefoongesprek en het bezoek aan een website. Beiden zijn ook vormen van telecommunicatie, maar de inhoud van het telecommunicatiebericht wordt niet vastgelegd op een drager. Deze vormen van telecommunicatie zijn vluchtig.

---

5 HORSMAN, P., *Archivering van Elektronische Post. Methoden, meningen en alternatieven*, Amsterdam, Archiefschool Amsterdam, 1999, 9,
beschikbaar op http://www.digitaleduurzaamheid.nl/bibliotheek/docs/archelp.pdf.

6 WALLACE, D., *Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice*, paper prepared for the Annual Meeting of the Society of American Archivists, Orlando, Florida, September 3, 1998, beschikbaar op http://www.mybestdocs.com/wallace.html. Het zal verder ook blijken uit de analyse van de toepasselijke rechtsregels dat e-mail een apart juridisch statuut heeft gekregen.

7 Zie de woordenlijst die in het kader van het DAVID-project ontwikkeld wordt met het oog op het herdenken en, waar nodig, het herformuleren van de archiefterminologie vanuit een digitaal oogpunt.

- Opgemaakt. Op dit punt is er geen verschil met traditionele archiefstukken. Een e-mail die enkel nog maar opgesteld is, maar nooit verzonden (UNSENT), is een archiefstuk van diegene die de e-mail heeft opgesteld. In de papieren wereld worden stukken die binnen de organisatie ontstaan, 'interne stukken' genoemd. Een 'interne e-mail' is dus bijvoorbeeld een e-mail die werd verzonden naar een persoon van de eigen organisatie[8].
- Ontvangen. Hier is er een verschil met traditionele archiefstukken. In de papieren wereld is een stuk dat een organisatie ontvangt, een archiefstuk van de ontvangende organisatie, en niet meer van de verzender. Er zal enkel een archiefstuk bij de verzender achterblijven voor zover er een dubbel exemplaar of minuut werd opgemaakt en bewaard. Omwille van de relatief hoge kosten werd het bijhouden van een dubbel vaak achterwege gelaten. Dit bezwaar speelt niet bij e-mail. Verzonden e-mail kan automatisch bewaard worden in de elektronische postbus van de verzender. Het is dan een stuk dat is opgemaakt (en verzonden) door die organisatie, en behoort bijgevolg tot diens archief. De e-mail is dan uiteraard ook een deel van het archief van de ontvangende organisatie.
- Uit hoofde van de activiteiten van of ter handhaving van de rechten van de organisatie. Hier situeert zich het probleem van het dubbel gebruik van het e-mailsysteem dat de organisatie ter beschikking stelt van zijn werknemers. Veel werknemers gebruiken het e-mailsysteem ook in meerdere of mindere mate voor privé-doeleinden. Enkel de e-mails die voortvloeien uit het functioneren van de organisatie kunnen echter als archiefstuk bestempeld worden. Ook e-mails die niet uitdrukkelijk gericht zijn tot de organisatie en bij toeval of ongevraagd in diens elektronische postbus terecht komen, behoren niet tot het archief[9]. Het gaat hier bijvoorbeeld om 'spam'[10] of berichten afkomstig van elektronische mailinglijsten, waarin het e-mailadres van de organisatie toevallig is verzeild geraakt. Deze e-mails dienen te berusten in het archief van diegene die ze heeft verstuurd.

In 1998 verschenen de resultaten van een studie die werd uitgevoerd aan de *Graduate School of Library and Information Science* van de universiteit van Austin, Texas. De bedoeling van deze studie bestond erin om de stand van zaken te onderzoeken inzake het nadenken over en het ontwerpen van e-mail policies, en dit zowel in de publieke als in de private sector[11]. Voortbouwend op de resultaten van deze

---

8 Een e-mail die wordt verzonden naar een persoon binnen de organisatie, is uiteraard ook een archiefstuk.

9 Zie voor een treffende gelijkenis met papieren archiefstukken, het voorbeeld van reclamedrukwerk en verkiezingspropaganda dat COPPENS aanhaalt. H. COPPENS, *Archiefbeheer in gemeenten en O.C.M.W.'s*, Brussel, Algemeen Rijksarchief, 1997, 43.

10 Er zijn veel manieren om 'spam' te definiëren. Een algemene definitie is: 'Gegevens die naar meerdere ontvangers, voor wie de verzender een vreemde is, worden verzonden terwijl er niet om gevraagd is door de ontvanger.' De meeste 'spamming' gebeurt per e-mail. Art. 114 §8 2° van de Telecomwet voorziet een strafsanctie nl. een geldboete, voor de persoon die een telecommunicatienet of –dienst of andere middelen van telecommunicatie gebruikt om overlast te veroorzaken aan zijn correspondent of om schade te berokkenen. Wie ongevraagd commerciële e-mails wenst te versturen, zal een aantal regels moeten naleven, die we o.a. vinden in de E-commerce richtlijn. Artikel 7.1 van de E-commerce Richtlijn voorziet dat de Lidstaten in hun wetgeving moeten bepalen dat ongevraagde commerciële communicatie per e-mail bij de ontvangst ervan door de afnemer duidelijk en ondubbelzinnig als zodanig herkenbaar moet zijn. Dit is in België gebeurd in art. 23 5° lid 2 van de Wet Handelspraktijken. Op die manier hoeft de ontvanger de boodschappen niet te lezen, en kan hij ze zonder veel tijdverlies gewoon uitwissen.

11 De resultaten van deze studie '*Managing E-mail as Records*' werden gepubliceerd op volgende URL: http://www.gslis.utexas.edu/~scisco/lis389c.5/email/index.html

studie, heeft DAVID WALLACE een aantal e-mail policies onderzocht op hun 'archiefgehalte'. Voor een waaier van 38 e-mail policies van over heel de wereld ging hij na in welke mate er een beleid wordt uitgewerkt ten aanzien van het archiveren van e-mail. Om geen vertekend beeld te krijgen, is het van belang om te weten dat WALLACE de e-mail policies enkel selecteerde, voorzover reeds op voorhand duidelijk was dat het archiveringsvraagstuk een belangrijk onderdeel van de policy uitmaakte[12]. Ten aanzien van de doorsnee e-mail policy is de situatie dus helemaal niet zo optimistisch als met betrekking tot de onderzochte policies, hoewel ook voor deze policies de resultaten tegenvallen, zoals we verder zullen zien.

In slechts 60 % van de onderzochte policies wordt er iets gezegd over de status van een e-mail als archiefstuk. Hoewel de meeste policies niet erg expliciet zijn en enkel vermelden dat een e-mail een archiefstuk van de organisatie *kan* uitmaken, lijkt er toch een algemene consensus te bestaan over het feit dat e-mail geen louter informeel communicatiemiddel is, maar wel degelijk archiefstukken kan opleveren. Wat wel algemeen voorkomt in de policies die iets zeggen over de status van e-mail, is de bepaling dat de gebruikte technologie of het formaat van de e-mail irrelevant is en dat de criteria om uit te maken of een e-mail een archiefstuk is, dezelfde moeten zijn als voor papieren documenten. Slechts 60 % van de policies die iets zeggen over de status van e-mail, geven enige vorm van criteria om archief-stukken van niet-archiefstukken te onderscheiden. De bedrijfsactiviteit (bijvoorbeeld e-mails waarin een beslissing wordt genomen, e-mails die toelating geven tot iets) en de vorm van de e-mail (bijvoorbeeld briefwisseling, minuten van vergadering) zijn daarbij de meest voorkomende criteria. De andere policies laten het over aan de eindgebruiker om de e-mail te kwalificeren. De stelling dat e-mails waarvan de inhoud niets te maken heeft met de activiteit van de organisatie, en dat strikt persoonlijke e-mails geen archiefstukken zijn, wordt in deze policies wel algemeen teruggevonden.

Het feit dat e-mail een archiefstuk kan uitmaken, blijkt ook uit de 'e-mail etiquette regels', die overal op het Internet gepubliceerd zijn. Ze geven aan hoe je je in het elektronisch berichtenverkeer als een beschaafde e-burger moet gedragen. De meeste van deze gedragscodes bevatten richtlijnen over de samenstelling en de vorm van een e-mailbericht en ook over het sturen van attachments. Sommige wijzen er zelfs op dat het van belang is om de regels na te leven, precies omdat e-mails wel eens zouden kunnen gearchiveerd worden[13].

Nu we weten dat e-mails kennelijk als archiefstukken van de organisatie kunnen beschouwd worden voorzover zij tot stand zijn gekomen in het kader van diens werkzaamheden (= **functionele e-mail**), moeten we ons afvragen of deze nieuwsoortige archiefstukken ook een permanente archiefwaarde hebben. Immers, slechts een zeer klein deel van alle archiefstukken worden uiteindelijk bewaard. De regel is dat voor e-mails dezelfde principes gelden als voor alle andere archiefstukken. Dit heeft voor

[12] Voor een overzicht van alle bestudeerde e-mail policies, zie http://www.mybestdocs.com/wallace.html

[13] http://www.larrysworld.com/articles/emailete.html

gevolg dat ook slechts een klein percentage van alle e-mails zullen moeten bewaard blijven. We noemen hier twee voorbeelden, één uit de publieke sector en één uit de private sector[14].

B. ARCHIEFWETGEVING

De overheid heeft geen vrije keuze om haar archiefstukken te bewaren of te vernietigen. De archiefwet bepaalt dat de overheden (nl. de rechtbanken, de rijksbesturen (lees: en de gemeenschaps- en gewestbesturen), de Raad van State, de provincies, de gemeenten en de openbare instellingen) hun archiefstukken niet mogen vernietigen zonder toestemming van de algemene rijksarchivaris of van diens gemachtigden en dat de archiefstukken die door deze overheden bewaard worden, onder het toezicht staan van de algemene rijksarchivaris of diens gemachtigden[15].

Voor zover een e-mail een archiefstuk is van de genoemde overheden, is het dus eveneens onderworpen aan de archiefwet. De opvatting dat e-mail een louter informeel communicatiemiddel is voor persoonlijk gebruik, mist dus archiefwettelijke grond.

De meest in het oog springende discussie omtrent het statuut van e-mail als officieel overheidsdocument, ontstond in de Verenigde Staten in 1989 naar aanleiding van de bekende 'PROFS' en 'GRS 20' rechtzaken. De e-mail policy van de federale administratie legde op dat moment aan alle ambtenaren op om alle e-mails uit te printen die als een document in de zin van de *Federal Records Act* konden gekwalificeerd worden. Op een bepaald moment werd er de beslissing genomen dat de elektronische versie van alle e-mails moest vernietigd worden. De motivatie voor deze beslissing luidde dat de elektronische versie van e-mails louter extra kopies zijn en dus geen officiële overheidsdocumenten. De federale administratie was van mening dat zij haar plichten was nagekomen onder de *Federal Records Act* door enkel de papieren versie van de e-mail te bewaren en dat de elektronische versie zonder voorafgaande toelating van NARA[16] mocht vernietigd worden. De *Federal Records Act* legt immers enkel de verplichting op om overheidsdocumenten te bewaren.

Een aantal belangengroepen[17] daagden de federale administratie voor de rechter en kregen gelijk. Volgens Judge CHARLES RICHEY is de elektronische versie van e-mail wel degelijk een archiefstuk in de zin van de wet en mag deze niet zomaar vernietigd worden. De praktijk van de administratie om e-mail af te printen en als papieren archiefstuk te behandelen voldeed niet omdat de afgedrukte versie niet steeds alle informatie weergeeft zoals die in de elektronische versie voorkomt (nl. contextuele informatie zoals

---

[14] Voor een omvattend overzicht van de redenen waarom archiefstukken bewaard worden: zie S. VAN DEN EYNDE, *Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1*, Leuven, ICRI, 2001, 88 p.

[15] Art. 5 en 6 van de archiefwet (*B.S.* 12 augustus 1955).

[16] NARA (National Archives and Records Administration) is een federale dienst die bij wet het toezicht heeft gekregen over alle federale documenten in de Verenigde Staten. http://www.archives.gov/

[17] o.a. The Organization for American Historians, alsook individuele personen zoals schrijvers, onderzoekers en journalisten. Armstrong et al. v. Executive Office of the President et al. (90 F.3d 553, 319 U.S.App.D.C. 330)

de datum en het uur van ontvangst en de identiteit van de ontvanger staan vaak niet op het scherm, maar maken wel deel uit van het e-mailbericht). In deze omstandigheden is de administratie verplicht de originele archiefstukken te bewaren, m.a.w. e-mail moet in zijn originele, elektronische vorm bewaard blijven.

Het NARA paste zijn richtlijnen in 1995 aan deze uitspraak aan: zodra elektronische berichten gekopiëerd zijn naar een 'record keeping system', mogen de originele berichten gewist worden[18]. Hierbij kan het zowel om een papieren als een elektronisch 'record keeping system' gaan. Voorwaarde is dat alle transmissiegegevens mee gekopiëerd worden. Prompt werd het NARA door andere belangengroepen voor de rechter gedaagd[19]. Op 6 augustus 1999 deed het Court of Appeal van het district of Colombia een definitieve uitspraak[20] in deze zaak en gaf het NARA gelijk. De rechter erkent dat elektronisch archiveren veel voordelen biedt, maar toch mocht de archivaris beslissen dat elektronische archiefstukken in papieren vorm bewaard mogen worden, voor zover alle relevante gegevens afgedrukt worden.

De juridische waarde die deze zaken hebben voor Vlaanderen is weliswaar louter illustratief. Toch werpen ze een klare kijk op de inhoud van de discussie die aan de gang is omtrent het bewaren van e-mail, een discussie die in Vlaanderen nog maar nauwelijks wordt gevoerd en die we vanuit het DAVID-project willen aanwakkeren. Aansluitend bij de oorspronkelijke uitspraak van Judge CHARLES RICHEY zijn we de mening toegedaan dat e-mails best digitaal gearchiveerd worden, en niet als *hard copy*[21]. Een onweerlegbaar juridisch argument is hiervoor niet te vinden.

Artikel 7 van de Nederlandse archiefwet van 1995 bepaalt uitdrukkelijk dat de zorgdrager bevoegd is om archiefbescheiden te vervangen door reproducties en om de archiefbescheiden die op die manier vervangen werden, te vernietigen. Het oplossen van de problemen in verband met het gebrek aan opslagcapaciteit bij de rijksarchiefdienst, ligt aan deze bepaling ten gronde[22]. Microverfilming en scanning zijn ongetwijfeld de meest gekende voorbeelden van dergelijke substitutiemaatregelen. Maar zou deze bepaling ook mogen aangewend worden om de problemen rond digitale archivering te omzeilen? Mogen originele digitale stukken vernietigd worden ten voordele van papieren substituten? Artikel 5 van de Belgische archiefwet bepaalt dat voor de vernietiging van de archiefstukken door de overheid de toestemming nodig is van de algemene rijksarchivaris. Het is dus de algemene rijksarchivaris die de bevoegdheid heeft om in laatste instantie te beslissen of e-mails in hun originele, elektronische vorm moeten bewaard blijven, dan wel of een afdruk op papier volstaat voor bewaring op lange termijn. Hij is ook bevoegd om de voorwaarden vast te leggen waaronder de originele, elektronische versie eventueel mag vernietigd worden. Tot op heden werd er daarover nog geen uitspraak gedaan.

---

[18] Zie: http://www.archives.gov/records_management/records_schedules.html

[19] Public Citizen, Inc. et al. v. Carlin et al. (F.3d 900, 337 U.S.App.D.C. 320)

[20] Het Supreme Court weigerde in te gaan op het verzoek van de belangengroepen om over deze zaak een uitspraak te doen.

[21] Een 'hard copy' (letterlijk: een duurzame kopie) is een afdruk op papier of microfilm.

[22] Memorie van Toelichting bij de archiefwet, Kamerstukken II, 1992-1993, 22 866.

Niets belet uiteraard dat alle elektronische berichten van de ambtenaren ook worden afgedrukt en op papier worden bewaard, maar dit kan volgens ons louter als een additionele bewaringsmaatregel beschouwd worden. Er kunnen daarvoor drie argumenten aangehaald worden die men niet zomaar naast zich kan neerleggen. Het eerste is een fundamenteel argument: e-mails zijn per definitie elektronisch. Volgens de geest van de archiefwet is het de originele elektronische versie van een e-mail die moet gearchiveerd worden. Ten tweede zijn er ook praktische redenen om te zeggen dat bewaring op papier alleen uitgesloten is. Een aantal elementen uit de elektronische context kunnen niet zinvol mee overgenomen worden naar een papieren omgeving. Zo gaat een digitale handtekening verloren door de omzetting naar gedrukte tekst omdat deze techniek afhankelijk is van de bitreeks waaruit de e-mail bestaat. Tenslotte geldt ook het logisch argument dat we in een wereld van digitale informatie op zoek moeten gaan naar digitale archiveringsmethoden omwille van de voordelen die dit biedt.

Het formele karakter dat e-mail kan hebben, blijkt ook uit de discussie die er momenteel in Europa gevoerd wordt rond e-government, zowel op niveau van de Europese Unie als in de administraties van de lidstaten. E-government staat hoog op de politieke agenda. Tijdens het Belgisch voorzitterschap van de Europese Unie werd samen met de Commissie een ministeriële conferentie over e-governement toepassingen georganiseerd. Het doel van deze conferentie was vast te stellen hoe ver Europa in dit domein staat en om een blijvend kader te scheppen om e-government te stimuleren na afloop van het 2002 eEurope Actieplan[23]. In de toekomst moeten alle basistransacties met de Europese Commissie online afgehandeld kunnen worden (bijvoorbeeld financiering van onderzoeksprojecten, recrutering, aanbestedingen). De lidstaten hebben zich ertoe geëngageerd om belangrijke openbare dienstverlening langs elektronische weg toegankelijk te maken tegen eind 2002. De werkgroep eGovernment stelde een lijst op met 20 basisdiensten die vervolgens werd aangenomen door de Raad Interne Markt in maart 2001[24].

In het regeerakkoord en in de Septemberverklaring van 2000 heeft de Vlaamse regering een geïntegreerd elektronisch loket naar voren geschoven als een belangrijk instrument om de overheid klantvriendelijker te maken en om het democratisch gehalte van de samenleving te vergroten. Het e-loket moet de burger in staat stellen om zich formeel tot de overheid te richten. De Vlaamse regering engageerde zich in haar Septemberverklaring van 2001 om e-government in het jaar 2002 op te tillen tot de interactieve fase[25]. Een aantal wettelijke bepalingen werden trouwens reeds aangepast om elektronisch berichtenverkeer tussen de burger en de overheid mogelijk te maken[26]. In het tijdperk van de elektronische overheid is het inderdaad nog moeilijk vol te houden dat de informatie die de overheid ontvangt via de digitale snelweg, aan de toepassing van de archiefwet zouden ontsnappen. De overheid is niet voor niets op zoek naar afdoende beveiligingsmethoden: zowel de burger als de overheid wenst zekerheid over de authenticiteit en integriteit van elektronische berichten.

---

[23] Http://europe.eu.int/information_society/eeurope/2002/action_plan/egov/index_en.htm.

[24] Voor de officiële Belgische e-government site, zie http://www.government-online.be/, met interessante links naar e-government projecten binnen de andere lidstaten.

[25] http://www2.vlaanderen.be/ned/sites/overheid/beleidsdoc/septemberverklaring/septemberverklaring_2001.pdf

[26] Bijvoorbeeld art. 327 W.I.B. bepaalt dat de belastingplichtige de in het aangifteformulier gevraagde gegevens eveneens bij middel van elektronische informatiedragers kan verstrekken onder de door de Koning bepaalde voorwaarden. Dit K.B. is echter nog niet verschenen in het Belgisch Staatsblad.

C. GOEDE BEDRIJFSVOERING

E-mail is in alle gelederen van bedrijven, overheidsdiensten en instellingen doorgedrongen als communicatiekanaal dat zowel op een formele als op een minder formele manier gehanteerd wordt. Communicatie die vroeger telefonisch of per brief verliep, gebeurt nu via e-mail. Het verloop van een aantal processen en transacties binnen deze organisaties vindt dan ook zijn neerslag in elektronische berichten. Om deze processen en transacties later te kunnen reconstrueren, is het van belang dat deze elektronische berichten op een overzichtelijke en toegankelijke wijze bewaard worden. De inhoud van een e-mail kan de stand van zaken betreffende een bepaald dossier weergeven, het kan het verslag van een vergadering bevatten waarin belangrijke beslissingen werden genomen of waarin taken werden verdeeld, of het kan simpelweg informatie bevatten die later nog van belang kan zijn voor jezelf of een collega (zoals een weblink). Wanneer deze e-mails niet op een doeltreffende wijze worden geselecteerd voor bewaring of vernietiging, is dit nefast voor de efficiëntie van de bedrijfsvoering.

Een belangrijke reden voor veel organisaties om e-mail niet te archiveren, is gelegen in de juridische risico's die geassocieerd worden met het bijhouden van e-mails gedurende een te lange periode. De idee is dat e-mails kunnen gebruikt worden als bewijsmiddel in de procesvoering tegen een organisatie, en op die manier eerder een bedreiging vormen, dan dat ze bijdragen tot de stabiliteit binnen een organisatie. Dit ondervond een Amerikaans bedrijf naar aanleiding van een rechtzaak die een werknemer had aangespannen om zijn ontslag te betwisten. De officiële reden luidde dat hij niet voldeed. *Electronic Evidence Discovery Inc*.[27] kreeg toegang tot meer dan 750 000 e-mails die terug te vinden waren in de backups van het e-mailsysteem van het bedrijf, en die nog steeds de eerder door de werknemers gewiste e-mails bevatten. Deze e-mails toonden aan dat de werknemer inderdaad niet was ontslagen omdat hij niet voldeed. We denken echter dat de voordelen van het permanent blijven bewaren van e-mails opwegen tegen de eventuele nadelen ervan.

Nu we weten dat het in bepaalde gevallen van belang kan zijn dat de e-mails van een organisatie bewaard worden, rijst de vraag of er in zekere mate controle kan en mag uitgeoefend worden op de vernietiging van e-mails door de eindgebruiker. Het eigene van dit communicatiemiddel is immers dat de gebruiker de ingekomen en uitgaande e-mails volgens zijn eigen inzichten kan bewaren of uitwissen, zonder dat hij of zij zich daarvoor tot iemand moet wenden. E-mail verloopt niet meer volgens de traditionele en geformaliseerde informatiestromen binnen de organisatie, waardoor er 'informatie-eilanden' tot stand komen[28]. Zijn deze eilanden het privé-domein van de werknemer, of mogen archivarissen en recordmanagers er toch in zekere mate op toezien dat er geen e-mails ten onrechte worden gewist. Aansluitend daarbij moeten we ook de vraag behandelen of een werknemer strikt persoonlijke e-mails mag versturen en ontvangen.

---

[27] *Electronic Evidence Discovery* biedt diensten aan op het vlak van het opsporen van elektronisch bewijsmateriaal tijdens een proces, en op het vlak van het verminderen van het risico dat dergelijk bewijsmateriaal gevonden wordt vóór een proces. http://www.eedinc.com/

[28] C. TOMER, and R. COX, 'Electronic Mail: Implications and Challanges for Records Managers and Archivists', *The Records and Retrieval Report 8*, November 1992, No° 9, 3-4.

We bekijken nu verder welke rechtsregels van toepassing zijn op (de archivering van) e-mail. Uit de analyse die volgt, zal blijken dat sommige rechtsregels conflicteren met de praktijk van het archiveren van e-mail waarbij er controle wordt uitgeoefend door de personen die verantwoordelijk zijn voor de briefwisseling en voor het archief van de organisatie. Deze analyse moet ons toelaten om uit te maken onder welke voorwaarden het uitoefenen van controle op het bewaren en vernietigen van e-mails door de eindgebruiker geoorloofd is.

IV. DE JURIDISCHE WAARDE VAN E-MAIL

De vraag naar de juridische waarde van e-mail moet gesteld worden om een beleid te kunnen ontwikkelen op het vlak van het verzenden van formele e-mail. Formele e-mailberichten zijn archiefstukken in de zin van de archiefwet (dus functionele e-mail) die meestal zullen bewaard worden omdat de inhoud, hetzij (rechts)gevolgen heeft voor de overheid, hetzij een bewijs- of een verantwoordingsfunctie heeft of nog kan krijgen, hetzij van belang is voor de juiste interpretatie van andere gegevens. Alle andere e-mail is informele e-mail. De overheid moet in de e-mail policy bepalen of het elektronisch verzenden van formele post toegestaan wordt, dan wel of er een schriftelijk stuk moet verzonden worden.

E-mail is een nieuwsoortig communicatiemiddel. Om het juridisch statuut van een e-mail te bepalen, moeten we trachten aansluiting te vinden bij een bestaand communicatiemiddel. We kunnen e-mail het best vergelijken met een brief. Een brief wordt in Van Dale gedefinieerd als: "een geschrift in de vorm van een mededeling, een boodschap, tot één of meer afwezige personen gericht, om hem (hen) iets te doen weten, gesloten en van een adres voorzien verzonden." Volgens de heersende rechtsleer kunnen ook elektronische gegevens een geschrift uitmaken voorzover ze op een min of meer duurzame wijze vastgelegd zijn[29]. ovendien heeft de afzender van de e-mail steeds de bedoeling om een boodschap over te brengen aan personen die niet fysisch aanwezig zijn. E-mail is ook steeds van een (e-mail)adres voorzien en wanneer de e-mail geëncrypteerd werd, is de e-mail ook gesloten, zijnde niet toegankelijk voor derden tijdens de transfer.

De waarde van een e-mail wordt bepaald door diens inhoud. Er zijn twee mogelijkheden. De keuze voor twee categorieën gebaseerd op het onderscheid tussen het al dan niet in het leven roepen van rechtsgevolgen, is ingegeven door de toepasselijkheid van de gemeenrechtelijke bewijsregeling. Voor de eerste categorie van e-mails legt deze regeling bijzondere vormvereisten op.

A. DE E-MAIL ROEPT RECHTSGEVOLGEN IN HET LEVEN

De inhoud van de e-mail (of van de reeks opeenvolgende e-mails) kan erop gericht zijn rechtsgevolgen in het leven te roepen dwz. de rechtstoestand van de partijen (burger-overheid, overheid-overheid) wordt erdoor gewijzigd. De formele e-mail is dan een ondertekend stuk opgemaakt met de bedoeling om tot bewijs te strekken. Voor het bewijs van rechtshandelingen is het burgerlijk bewijsrecht van toepassing. Het bewijsrecht legt vaak vormvereisten op aan allerlei documenten, en zal dan ook doorslaggevend zijn voor de manier waarop deze documenten bewaard moeten worden. De handtekening is de meest voorkomende formaliteit en tot voor kort bestond er onzekerheid over of rechters elektronisch ondertekende documenten ook zouden aanvaarden.

---

[29] S. VAN DEN EYNDE, *Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1,* K.U.Leuven, ICRI, 2001, 55.

De Europese richtlijn 1999/93/EG[30] legt alle lidstaten op om zogenaamde 'gekwalificeerd elektronische handtekeningen' dezelfde juridische waarde te geven als een handgeschreven handtekening. Sinds de wet van 20 oktober 2000, die deze richtlijn omzet, kunnen e-mails elektronisch ondertekend worden waardoor ze de status van onderhandse akte krijgen. Voorwaarde is dat de elektronische handtekening aan een bepaalde persoon kan toegerekend worden en dat zij de integriteit van de inhoud van de onderhandse akte aantoont.

Andere formele vereisten die soms door de wet worden opgelegd, zijn de noodzaak van een geschrift of het voorkomen van een aantal verplichte vermeldingen in het document. De richtlijn elektronische handel (2000/31/EG)[31] verplicht de lidstaten alle juridische obstakels uit de weg te ruimen die het sluiten van contracten (inclusief het archiveren ervan) langs elektronische weg belemmeren. De wet op de elektronisch handel van 11 maart 2003[32] zet deze richtlijn om in het Belgisch recht. Contracten gesloten via e-mail zullen in de toekomst vaker voorkomen.

Toch zal dit type van e-mails zeer zelden voorkomen bij de overheid. De erkenning van de elektronische handtekening is immers beperkt tot het gemene verbintenissenrecht. Er is niet geraakt aan specifieke reglementeringen omtrent het bewijs of de vormvoorschriften. Voor de overheid is er echter meestal specifieke wetgeving van toepassing[33], waardoor het niet mogelijk is om onderhandse akten elektronisch en per e-mail tot stand te brengen. Ter wille van het bewijs zal er dus nog steeds een schriftelijk stuk moeten verzonden worden.

B. DE E-MAIL ROEPT GEEN RECHTSGEVOLGEN IN HET LEVEN

Dit maakt het leeuwenaandeel uit van de e-mails die door de overheid verzonden worden. Het gaat dan meestal om formele e-mail, waarop de vormvoorwaarden van het burgerlijk bewijsrecht niet van toepassing zijn wegens de afwezigheid van een rechtshandeling. De meeste formele e-mails bevatten rechtsfeiten (sensu stricto[34]). Dit zijn feiten met een juridische implicatie. Het kan bijvoorbeeld gaan om een antwoord op een vraag om inlichtingen waarmee de overheid haar aansprakelijkheid engageert. Feitelijke elementen mogen bewezen worden met alle middelen van recht. De e-mail zal in dit geval als een gewoon geschrift gekwalificeerd worden.

---

30 *B.*L13/12, 19 January 2000.

31 *P.B.* L178/1, 17 July 2000.

32 Wet van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij (*B.S.* van 17 maart 2003)

33 K.B. 8 januari 1996 betreffende overheidsopdrachten voor aanneming van werken, leveringen en diensten en de concessies voor openbare werken (*B.S.* 26 januari 1996).

34 Rechtshandelingen maken deel uit van de rechtsfeiten in ruime zin. Na uitsluiting van de rechtshandelingen uit die categorie blijven de rechtsfeiten in strikte zin over.

De reden om een boodschap eventueel niet elektronisch te versturen maar op papier, is dus gelegen in het feit dat de wet soms bijzondere vormvereisten stelt die enkel op papier kunnen vervuld worden. Alle andere boodschappen kunnen wel elektronisch verzonden worden. We zijn van mening dat dit zeker moet gebeuren wanneer de burger de overheid op eigen initiatief en op een reglementaire wijze gecontacteerd heeft via e-mail. De burger mag dan redelijkerwijze verwachten dat een overheid, die serieus werk maakt van haar elektronisch imago, elektronisch zal antwoorden.

V. OPENBAARHEID VAN BESTUUR

A. INLEIDING

Er bestaat echter ook nog een andere reglementering waarmee de Vlaamse overheden moeten rekening houden. Door enkel oog te hebben voor de archiefwetgeving, zou men er kunnen van uitgaan dat het bewaren van e-mails een lange termijn probleem is waar pas moet over nagedacht worden lang nadat de e-mails hun onmiddellijke nut voor de overheid verloren hebben. De administratie moet echter ook rekening houden met de openbaarheidswetgeving. Een e-mail geadresseerd aan of verzonden door de overheid kan immers in bepaalde gevallen een bestuursdocument uitmaken in de zin van de openbaarheidsreglementering. Deze e-mails moeten ten allen tijde ter beschikking worden gehouden van de burger die erom vraagt. De Vlaamse overheden moeten hun e-mails bijgevolg niet alleen ter beschikking kunnen stellen van de archivaris naar aanleiding van de overdracht, maar er moet ook een korte termijn beleid voor het dynamische en het semi-statische e-mailarchief worden gevoerd teneinde de openbaarheidsreglementering te kunnen respecteren. Het spreekt voor zich dat de archivaris een belangrijke rol te spelen heeft bij het uittekenen van dit beleid.

B. VLAAMSE ADMINISTRATIEVE OVERHEDEN EN HUN OPENBAARHEIDS-REGLEMENTERING

De regelgeving inzake de openbaarheid van bestuur in België is sterk versnipperd. Enerzijds bestaat er op elk niveau in België (federaal, regionaal, provinciaal en gemeentelijk) een specifieke wetgeving inzake de openbaarheid van bestuur en anderzijds wordt de reglementering inzake de toegang tot bestuursdocumenten vaak geïntegreerd in bestaande wetten[35] Op federaal niveau is de wet van 11 april 1994 (B.S. 30 juni 1994) van toepassing. In Vlaanderen wordt de openbaarheid van bestuur geregeld door het Vlaamse decreet van 18 mei 1999 (B.S. 15 juni 1999). Het is van toepassing op:

- De administratieve overheden van het Vlaams Gewest en de Vlaamse Gemeenschap (art. 41°)
- De andere administratieve overheden, doch slechts in zoverre dit decreet op gronden die tot de bevoegdheid van de Vlaamse Gemeenschap of het Vlaams gewest behoren, de openbaarheid van bestuursdocumenten verbiedt of beperkt (art. 42°)
- De verenigingen van provincies en gemeenten (art. 43°)
- De openbare centra voor maatschappelijk welzijn en de verenigingen bedoeld in hoofdstuk 12 van de organieke wet van 8 juli 1976 betreffende de openbare centra voor maatschappelijk welzijn (art. 44°)

[35] Bijvoorbeeld art. 120 lid 4 Provinciewet; art. 45 §1 B.W. inzake de akten van de burgerlijke stand.

Voor het gemeentelijke en provinciale bestuursniveau is de federale wetgever krachtens art. 162 van de grondwet bevoegd om een openbaarheidsregeling uit te werken. Deze bevoegdheid vertaalde zich in de wet van 12 november 1997 betreffende de openbaarheid van bestuur in de gemeenten en provincies (B.S. 19 december 1997).

C. E-MAIL ALS BESTUURSDOCUMENT

Dat e-mail in bepaalde gevallen een bestuursdocument kan uitmaken, lijdt geen twijfel. Het decreet definieert het begrip 'bestuursdocument' als 'de drager, in welke vorm ook, van informatie waarover een administratieve overheid beschikt'. Deze definitie sluit aan bij de ruime omschrijving die de grondwetgever, zowel wat de vorm als wat de inhoud betreft, heeft willen geven aan het begrip bestuursdocument.

De overheid moet zich ervan bewust zijn dat ook elektronische informatie een 'bestuursdocument' kan uitmaken. Tijdens de parlementaire voorbereiding van art. 32 van de grondwet werd er daarover het volgende gezegd[36]: 'De term bestuursdocument dient breed te worden opgevat. Het betreft alle beschikbare informatie, welke ook de informatiedrager is: schriftelijke stukken, geluids- en beeldopnamen met inbegrip van de gegevens vervat in de geautomatiseerde informatieverwerking, sommige notulen en processen-verbaal, statistieken, administratieve richtlijnen, omzendbrieven, contracten en vergunningen, registers van openbaar onderzoek, examencohiers, films, foto's enzovoort waarover een overheid beschikt, zijn in regel openbaar, behoudens wanneer een uitzonderingsgrond moet worden toegepast.'[37]. Hoewel het gebruik van e-mail in 1992 nog niet zo ingeburgerd was bij de overheid als nu, is het duidelijk dat het decreet ook e-mails viseert.

In Vlaanderen heeft men zich over de kwestie van e-mail als zodanig nog nooit formeel uitgesproken[38]. In de V.S. bepaalt de Freedom of Information Act Manual, dat een leidraad moet bieden aan ambtenaren van de US National Labor Relations Board inzake het openbaar maken van public records, dat alle documenten in elektronische vorm, inclusief e-mail en documenten die zijn gecreëerd met behulp van een tekstverwerkingsprogramma's, potentieel onderworpen zijn aan openbaarmaking en in overweging moeten genomen wanneer een verzoek tot openbaarmaking behandeld wordt[39].

---

[36] Vermits art. 32 van de Grondwet de openbaarheid van bestuur heeft verheven tot een grondwettelijk recht, stelde de Raad van State dat de decreetgever, die door diezelfde bepaling is gemachtigd om aspecten van het recht op openbaarheid nader uit te werken, is gehouden aan de door de grondwetgever beoogde begripsbepaling.

[37] *Gedr. St.*, Kamer, 1992-93, nr. 839/1, verklarende nota, 5.

[38] Naar aanleiding van haar interventie als co-rapporteur in het debat over de openbaarheid in de Europese Unie heeft de voorzitster van de Nederlandse CDA-delegatie van het Europees Parlement, Hanja Maij-Weggen, gesteld dat ook elektronische post tot de in principe openbare documenten van Europese instellingen. http://web.archive.org/web/20030205194600/http://www.maij-weggen.com/publicaties/openbaarheid.html

[39] Freedom of Information Act Manual, 8, http://www.nlrb.gov/foia/submanl.html

Het vorige openbaarheidsdecreet voor Vlaanderen sloot heel wat e-mails van de administratieve overheid uit van openbaarheid. Om van een bestuursdocument te kunnen spreken, moest er immers steeds een nauwe relatie bestaan met een bestuurshandeling of een handeling die ertoe heeft bijgedragen[40]. Een bestuurshandeling of een administratieve rechtshandeling is een beslissing die erop gericht is rechtsgevolgen tot stand te brengen. Het gebruik van e-mail bij de administratieve overheid zal echter in de meeste gevallen niet te koppelen zijn aan (de voorbereiding van) een bestuurshandeling. Meestal zal het e-mailverkeer tussen ambtenaren betrekking hebben op andere overheidsactiviteiten dan het voorbereiden van of het nemen van individuele of algemene eindbeslissingen. Denk aan het uitwisselen van verslagen van vergaderingen, van rapporten die in het kader van wetenschappelijke studies tot stand komen of gewoon e-mails met een vraag om inlichtingen.

Deze beperking is sinds 1999 weggevallen. Thans zijn quasi alle e-mails onderworpen aan het principe van openbaarheid. Het huidige Vlaamse openbaarheidsdecreet bepaalt dat openbaar is 'alle informatie waarover een administratieve overheid beschikt'.

In principe is dus alle informatie openbaar die is terug te vinden in e-mails en de bijhorende attachments en waarover de Vlaamse administratieve overheid beschikt. Het recht op openbaarheid is evenwel niet absoluut. De verschillende openbaarheidsreglementeringen erkennen dat andere belangen voorrang kunnen krijgen op de openbaarheid. De veiligheid van de bevolking, het recht op privacy van de betrokkenen, het strafrechterlijk onderzoek zijn slechts enkele voorbeelden hiervan. De persoonlijke e-mail van een ambtenaar is dus niet zonder meer aan de openbaarheid van bestuur onderworpen.

Wanneer een persoon zich tot deze overheid richt met de schriftelijke vraag tot openbaarheid van bestuursdocumenten betreffende een bepaald dossier, dan moet men ook rekening houden met de e-mails die hierop eventueel betrekking hebben. Het spreekt voor zich dat e-mails/bestuursdocumenten daarom zorgvuldig moeten bewaard worden. Hoewel de openbaarheidsreglementering op zich weliswaar geen bepalingen bevat over het bewaren en vernietigen van bestuursdocumenten, leggen de regels inzake (vooral de passieve) openbaarheid aan de overheid toch heel wat plichten op die vernietiging van bestuursdocumenten inclusief e-mails uitsluit. Veel minder dan voor de archivering is het hier nodig dat met de originele, elektronische versie wordt gewerkt.

Uit de administratieve praktijk in de meeste overheidsorganisaties blijkt dat het besef begint door te dringen dat e-mails ook bestuursdocumenten kunnen zijn. In de gemeente Kortenberg worden op dit moment alle officiële e-mails aan en van het schepencollege afgedrukt en opgenomen in het register van ingekomen en uitgaande post[41]. Om het geheim van de telecommunicatie te respecteren bepaalt het

---

[40] Art. 2 Decreet 23 oktober 1991 betreffende de openbaarheid van bestuursdocumenten in de diensten en instellingen van de Vlaamse Executieve (*B.S.* 27 november 1991): '*Voor de toepassing van dit decreet wordt verstaan onder: 1° bestuursdocument: alle beschikbare informatie in geschreven, visuele, auditieve of geautomatiseerde vorm waaruit hetzij een bestuursbeslissing blijkt, hetzij een handeling die tot een bestuursbeslissing heeft bijgedragen.*'

[41] Beslissing van de gemeenteraad van 26 maart 2001.

'Protocol Elektronische Post' van de stad Amsterdam dat de geadresseerde van de e-mail zelf een als eensluidend gewaarmerkt afschrift ter beschikking moet stellen van de afdeling DIV van zijn dienst[42].

Let wel dat het alleen de administratieve overheden zijn die met deze reglementering rekening moeten houden. Het e-mailverkeer van de decreetgevende overheid valt er niet onder[43]. Deze e-mails kunnen echter nog steeds als archiefstuk gekwalificeerd worden, wat voor gevolg heeft dat deze overheid ze eveneens niet zomaar mag vernietigen. Voor de gemeentelijke en de provinciale administratieve overheden is het begrip bestuursdocument dezelfde wijze gedefinieerd als voor de Vlaamse overheid[44].

D. REGISTRATIEPLICHT: OOK VOOR E-MAIL?

Een adequaat informatiebeleid is van wezenlijk belang, niet alleen voor een betere dienstverlening naar de burgers toe, maar ook voor intern gebruik, de informatievoorziening naar ambtenaren en bestuurders toe. Het zoeken en soms niet of slechts gedeeltelijk kunnen vinden van informatie is een belangrijke kostenpost[45]. Voor papieren briefwisseling wordt er daarom een register van de ingekomen en uitgaande briefwisseling bijgehouden. Voor de provincies is dit zelfs een wettelijke verplichting. Art. 65 bis van de Provinciewet bepaalt dat er een register van de ingekomen en uitgaande stukken moet worden bijgehouden door de diensten en instellingen van de provincie. Deze verplichting moet alle informatie die de overheid bereikt via de Post, beschikbaar en traceerbaar maken op het organisatieniveau. Bovendien zijn brieven die door de overheid worden verstuurd of ontvangen, in heel wat gevallen bestuursdocumenten die moeten geregistreerd worden teneinde het openbaarheidsrecht van de burger veilig te stellen.

De vraag rijst of de administratieve regels die verbonden zijn met formele post van de overheid, met name de registratieplicht, ook van toepassing zijn op elektronische post. Registratie van inkomende en uitgaande post is een oplossing die typisch is voor de papieren wereld. Dit register is de enige manier om bij te houden welke brieven de organisatie binnenkomen en verlaten, en vooral wie ervoor verantwoordelijk is. E-mail kan je daarentegen centraal op de server beheren. De administratie kan zijn mailserver zo instellen dat alle inkomende en uitgaande berichten bijgehouden worden. Een apart register met inkomende en uitgaande e-mail heeft dus weinig zin.

Het echte probleem is dat van toegang tot de informatie die in de e-mail vervat zit. E-mail wordt beschermd door het telecommunicatiegeheim, zoals brieven beschermd worden door het briefgeheim. Deze problematiek wordt verder besproken onder VI Privacyreglementering.

---

[42] http://digidiv.amsterdam.nl/handleidingen/e-mail/downloads/prot.doc

[43] Idem voor het e-mailverkeer van de rechterlijke overheden. Deze overheden laten we hier buiten beschouwing aangezien zij niet onder de bevoegdheid van Vlaamse archiefinstellingen vallen.

[44] Art. 2 2° Wet 12 november 1997.

[45] Handleiding archivering elektronische post, http://beens.fol.nl/zwgroep/pdf/HandleidingEmail.pdf

E. DE AANSPRAKELIJKHEID VAN DE AMBTENAAR

Wat gebeurt er als er informatie door de fout van de ambtenaar verloren gaat of als het e-mailsysteem door zijn fout niet meer naar behoren functioneert? Welke wetgeving er van toepassing is, is afhankelijk van de wijze waarop de eindgebruiker werd aangeworven. Voor gewone werknemers die werken onder een arbeidscontract, bepaalt art. 18 van de wet arbeidsovereenkomsten van 3 juli 1978 dat de werknemer enkel aansprakelijk is voor zijn bedrog en zijn zware schuld als hij bij de uitvoering van zijn arbeidsovereenkomst aan zijn werkgever schade heeft berokkend. Voor lichte schuld is hij enkel aansprakelijk als die bij hem eerder gewoonlijk dan toevallig voorkomt. Dit is een feitenkwestie die in dit geval moet beoordeeld worden volgens de informaticakennis van de werknemer.

Is de eindgebruiker aangeworven onder het statuut van het overheidspersoneel, dan situeert de aansprakelijkheid van de ambtenaar zich voornamelijk op het disciplinaire terrein. Voor de vergoeding van de schade, moet er toepassing gemaakt worden van de artikelen 1382 en 1383 van het Burgerlijk Wetboek[46]. De rechtspraak beperkt de aansprakelijkheid van de ambtenaar ten opzichte van de overheid tot de gevallen van zware fout of bedrog in hoofde van de ambtenaar, zoals voor werknemers is bepaald.

Wanneer er schade aan het e-mailsysteem en eventueel aan de rest van het informaticasysteem van de overheid wordt aangericht door een virus, dan zal hiervoor in principe de eindgebruiker niet strafbaar zijn, maar wel de persoon die het virus de wereld heeft ingestuurd. Deze persoon pleegt een misdrijf naar Belgisch recht door het verspreiden van een virus en zal kunnen gestraft worden met een gevangenisstraf van zes maanden tot drie jaar en/of met een geldboete van zesentwintig tot vijfentwintigduizend frank[47]. Wordt er door het virus effectief schade aangericht, dan zijn de straffen zelfs nog hoger. Interessant om weten: het ontwerpen van een virus is op zichzelf ook strafbaar, voorzover kan worden aangetoond dat dit met bedrieglijk opzet gebeurde.

---

[46] J. JACQMAIN, *Droit social de la fonction publique*, Brussel, Presses universitaires, 2000, 49.

[47] Zie het nieuwe artikel 550 ter van het Strafwetboek: "*Hij die, met het oogmerk om te schaden, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist, of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem verandert, wordt gestraft met een gevangenisstraf van zes maanden tot drie jaar en/of met een geldboete van zesentwintig tot vijfentwintigduizend frank.*"

VI. DE PRIVACYREGLEMENTERING

Dat het archiveren van e-mail een noodzaak is, daar twijfelt na het lezen van dit rapport hopelijk niemand meer aan. De overheid is wettelijk verplicht e-mail te archiveren, maar deze opgave maakt meer in het algemeen deel uit van een goede bedrijfsvoering.

Mag de records manager zomaar alle e-mail doornemen om de archiefstukken te selecteren zonder medeweten van de betrokkenen? Vaak vind je in e-mail etiquette regels de aanbeveling terug dat je dingen, waarvan je niet wil dat anderen ze weten, of die je niet in publiek zou zeggen, beter niet in een e-mail zet, maar dat je ze beter van persoon tot persoon of telefonisch afhandelt. E-mails zouden door je werkgever bekeken worden voor allerlei doeleinden, waaronder archivering. Deze gedragscodes trachten je ervan te overtuigen dat 'there is no such thing as a private e-mail'. Maar is dit wel zo? Is je elektronische postbus een soort glazen huis waar iedereen, die technisch gezien over de mogelijkheden beschikt, zich in mag begeven, of is de inhoud van een e-mail in principe geheim? De regels omtrent de bescherming van de persoonlijke levenssfeer behandelen deze vraag.

A. JURIDISCH KADER

De bescherming van de persoonlijke levenssfeer van eenieder is een fundamentele waarde in onze maatschappij en er bestaat een overvloed aan rechtsnormen die deze materie beheersen. De eerbiediging van de persoonlijke levenssfeer is eerst en vooral een grondrecht, zoals blijkt uit art. 12 van de Universele Verklaring van de Rechten van de Mens (10 december 1948), art. 8 van het Europees Verdrag van de Rechten van de Mens (4 november 1950, Rome), art. 17 van het verdrag inzake burgerrechten en politieke rechten (19 december 1966, New York), art. 7 van het Handvest van de Grondrechten van de Europese Unie (2000/C 364/01, P.B. C 364 18 december 2000, p. 1) en verschillende artikelen van de Belgische Grondwet (art. 22 en 29).

De Europese wetgever heeft dit grondrecht concreet uitgewerkt in de richtlijn over de verwerking van persoonsgegevens (1995/46/EG) en de richtlijn betreffende privacy en telecommunicatie/elektronische communicatie (1997/66/EG en 2000/58/EG).

In ons nationale recht zijn de privacywet, het telecommunicatiegeheim (art. 314bis SW en art. 109terD Telecomwet) en de C.A.O. nr. 81 van belang voor het archiveren van e-mail.

B. GRONDRECHTEN

B.1. E.V.R.M.

Art. 8 van het E.V.R.M. bepaalt:

1. *Eenieder heeft recht op eerbiediging van zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling.*
2. *Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, of voor de bescherming van de rechten en vrijheiden van anderen.*

Dit artikel beschermt enerzijds tegen inmenging door de overheid, anderzijds wordt algemeen aangenomen dat dit artikel directe derdenwerking heeft, m.a.w. particulieren moeten in hun omgang met elkaar de grondrechten respecteren.

B.1.1. Historische context

Het Europees Verdrag van de Rechten van de Mens werd gesloten in het kader van de Raad van Europa. Deze organisatie werd opgericht in 1949 te Londen door tien West-Europese staten en stelt zich tot doel het beleid van zijn lidstaten te harmoniseren en gemeenschappelijke normen en praktijken te doen invoeren. Hiertoe brengt de Raad op verschillende niveaus parlementariërs, ministers, overheidsdeskundigen, lokale en regionale vertegenwoordigers, jongerenorganisaties en INGO's (internationale niet-gouvernementele organisaties) bijeen om hun kennis en ervaringen uit te wisselen. Reeds meer dan 170 Europese verdragen verschaffen de lidstaten een basis om hun nationale wetgeving aan te passen en te harmoniseren. De verdragen behandelen zeer uiteenlopende onderwerpen: van bescherming van computergegevens, supportersgeweld en bescherming van de natuur tot sociale zekerheid, culturele samenwerking en het voorkomen van foltering.

Het Europees Verdrag tot Bescherming van de Rechten van de Mens heeft als doel om de principes vastgelegd in de Universele Verklaring voor de Rechten van de Mens een collectief afdwingbare status te geven. De Raad van Europa heeft een in de wereld unieke rechtsgang ontwikkeld, zodanig dat een lidstaat of een individuele burger bij het Europees Hof voor de Rechten van de Mens een klacht kan indienen tegen een lidstaat die dit verdrag, naar zijn mening, niet respecteert. In het kader hiervan kwam een omvangrijke rechtspraak tot stand van het Europees Hof voor de Rechten van de Mens.

In Europa gaat het telecommunicatiegeheim als een fundamenteel recht reeds een hele tijd terug. Het briefgeheim werd voor de eerste maal erkend in 1831 in de "Constitution of Hesse" van het Duitse vorstendom Hesse. Hoewel er in de tekst uitdrukkelijk wordt gerefereerd naar "das Briefgeheimnis", werden niet alleen brieven beschermd, maar de inhoud van alle verzendingen die per post gebeurden. De onschendbaarheid van het briefgeheim was in dit beginstadium weliswaar enkel van toepassing in de verhouding tussen de burger en de overheid. In de tweede helft van de negentiende eeuw werd de wetgever geconfronteerd met nieuwe communicatietechnieken, zoals de telegraaf en de telefoon. Nieuwe grondwetten die nadien in Europa tot stand kwamen, erkenden ook deze nieuwe communicatievormen.

In de U.S. daarentegen is het bestaan van een telecommunicatiegeheim het gevolg van de interpretatie van het *Fourth Amendment* als een bepaling die de bescherming van de privacy viseert. Het *Fourth Amendment* vrijwaart eenieders persoon, huis, documenten en bezittingen tegen onredelijke zoekingen, beslagnames of andere schendingen, buiten de gevallen waar een om gegronde reden een beperkt mandaat afgeleverd wordt [48]. Deze bepaling was een reactie op het verschijnsel van de algemene zoekingsmandaten (general search warrants) in het Amerika van de achttiende eeuw, een procedure die vaak gebruikt werd om bewijsmateriaal te vinden in de archieven van verdachten van politieke misdrijven.

De Amerikaanse rechtbanken hebben aan het *Fourth Amendment* naderhand een betekenis gegeven buiten deze specifieke omstandigheden. Door *alle onredelijke* zoekingen en beslagnames onder de toepassing te brengen van de Fourth Amendment, werd een algemeen grondrecht op privacy afgeleid uit deze bepaling[49]. Ook gevallen waarbij telecommunicatie werd onderschept, werden steeds voor de rechtbank gebracht als gevallen van onredelijke zoeking en beslagname[50]. De constitutionele bescherming van het telecommunicatiegeheim is dus tot stand gekomen als een aspect van het recht op privacy, en niet als een autonoom recht.

B.1.2. Draagwijdte van art. 8. E.V.R.M.

Artikel 8 E.V.R.M beschermt eenieder tegen elke ongerechtvaardigde inmenging in zijn briefwisseling. In het verdrag wordt het begrip "briefwisseling" ("correspondance" in het Engels en het Frans) echter niet nader uitgelegd. De doctrine legde het begrip gewoonlijk letterlijk uit. Enkel schriftelijke correspondentie viel in deze optiek onder art. 8 E.C.H.R.[51] Het Hof heeft echter in haar rechtspraak de term "correspondence" geïnterpreteerd als zijnde alle vormen van telecommunicatie[52]. In de zaak Klass

---

[48] The Fourth Amendment states that the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

[49] RUIZ, B., *Privacy in Telecommunications. A European and an American approach*, The Hague, Kluwer Law International, 1997, 86.

[50] Maryland Penitentiary v. Hayden, 387 US 294 (1967).

[51] FAWCETT, J., *The Application of the European Convention on Human Rights (Article 8)*, Oxford, Clarendon Press, 1987, 228.

[52] RUIZ, B., *o.c.*, 142.

v. Germany[53], stelde het Hof dat art. 8 zowel geschreven correspondentie als telefoongesprekken beschermt. Over e-mail heeft het Hof zich nog niet kunnen buigen, maar het standpunt over briefwisseling en telefoongesprekken kan ongetwijfeld doorgetrokken worden[54].

Het Hof beschermt communicatie op twee manieren: ten eerste is er de communicatievrijheid, ten tweede het communicatiegeheim. Beide zijn relevant voor het archiveren van e-mail binnen een organisatie.

B.1.2.1. Het recht op communicatievrijheid

Het dubbel gebruik van het e-mailsysteem door werknemers (nl. professioneel en privé) maakt het er voor de onderneming niet gemakkelijker op om de archiefstukken van de niet-archiefstukken te onderscheiden. Vanuit archivistisch oogpunt zou het wellicht veel beter zijn dat alle e-mail binnen de organisatie een louter professioneel karakter zou hebben. Dit kan bijvoorbeeld gerealiseerd worden door aan de werknemers te vragen om alle strikt persoonlijke e-mail zo veel mogelijk via een persoonlijk e-mailadres te laten verlopen, en niet via het e-mailadres dat aan de werknemer werd ter beschikking gesteld om zijn beroepsactiviteiten efficiënt te kunnen uitvoeren.

Dit betekent nochtans niet dat men de werknemer mag verbieden om het e-mailsysteem dat de werkgever ter beschikking heeft gesteld, voor persoonlijke doeleinden te gebruiken. Het feit dat een werknemer zich in een arbeidsverhouding bevindt, betekent niet dat zijn communicatievrijheid verloren gaat. De communicatievrijheid is immers een grondrecht dat wordt beschermd door art. 8 E.V.R.M [55], en houdt in dat men moet worden vrij gelaten om al dan niet communicatie aan te gaan of te ontvangen. Dit principe werd voor het eerst verwoord in het arrest NIEMITZ van het Europees Hof voor de Rechten van de mens: "*respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.*" De heer NIEMITZ was een advocaat in Duitsland die klacht indiende tegen de Duitse staat omdat die zijn kantoor had doorzocht met de bedoeling om brieven te vinden die een andere persoon konden incrimineren, zonder het telecommunicatiegeheim, gegarandeerd door art. 8 E.C.H.R., te respecteren.

---

53 *KLASS v. Germany*, ECHR, 6 September 1978, Series A, No. 24, para. 41.

54 Online Rights for Online Workers in Member States of the European Union, Report on a Research Project for UNI Europa, European Commission, 15 November 2000, http://www.union-network.org/uniibits.nsf/172541a5444b8445c1256811002a0302/061b38ba2eca776dc1256a2b0048e644?OpenDocument

55 BURGHARTZ, E.H.R.M. 22 februari 1994, Serie A, Vol. 280-B, § 36 : "private life conceived of as including, to a certain degree, the right to establish and develop relationships with other human beings, in professional or business contexts as in others." Art. 8 E.V.R.M. omvat enkel een recht op vrijheid van communicatie, voorzover de communicatie kan geacht worden privé-communicatie te zijn. Verder zullen we echter zien dat elektronische berichten bijna altijd kunnen geacht worden privé-communicatie te zijn. Iedere communicatie die niet is bestemd om door iedereen te worden gehoord of gelezen, is immers privé.

Communicatievrijheid impliceert ook de vrijheid om van de ter beschikking zijnde communicatiemiddelen gebruik te maken[56]. Het argument dat de werkgever eigenaar is van de telecommunicatiemiddelen, wordt in de rechtsleer terecht bekritiseerd[57]. Precies omwille van het feit dat de werkvloer de uitgelezen plaats is om contacten met collega's, en zelfs met buitenstaanders, te onderhouden, maakt dat werkgevers een zekere tolerantie moeten tonen ten aanzien van privé-communicatie die wordt gevoerd met hun communicatiemiddelen. Dat dit voor de selectie en de bewaring van e-mails extra problemen met zich brengt, kan geen afbreuk doen aan dit grondrecht.

De werknemer moet echter ter beschikking staan van de werkgever tijdens de arbeidstijd om zijn taken uit te voeren. De communicatievrijheid van de werknemer binnen de organisatie is dus niet onbeperkt. Privé-communicatie door de werknemer mag de goede uitvoering van de arbeidsovereenkomst niet in het gedrang brengen.

B.1.2.2 Het telecommunicatiegeheim

Zelfs wanneer duidelijk is dat alle e-mails in de elektronische postbus van de werknemer verzonden en ontvangen zijn uit hoofde van zijn beroepsactiviteit, blijft het de vraag of de records manager deze e-mails op eigen initiatief en zonder medeweten van de werknemer, mag overhevelen naar het archiefbeheerssysteem.

Uit het hierboven geciteerde arrest NIEMITZ blijkt dat professionele communicatie evenzeer binnen de persoonlijke levenssfeer valt. Het Hof bevestigde zijn rechtspraak in de zaak HALFORD, waarin het Verenigd Koninkrijk aangeklaagd werd door een voormalig politie-officier wiens privé telefoongesprekken op het werk afgeluisterd werden. Het Verenigd Koninkrijk argumenteerde dat art. 8 niet van toepassing was, aangezien de telefoontjes van op het werk gevoerd werden. Het Hof verwierp deze stelling en oordeelde dat een werknemer redelijkerwijs mag verwachten dat zijn privacy gerespecteerd zal worden, zeker in gevallen waar hij vooraf niet geïnformeerd wordt over de mogelijkheid dat hij afgeluisterd kan worden[58].

De nationale rechtbanken uit verschillende landen delen het standpunt van het Hof. Het Franse Hof van Cassatie oordeelde in 2001 dat een werkgever niet zomaar de e-mail van zijn werknemers mag lezen[59]. Dit principe geldt zelfs wanneer de werkgever privé-gebruik van het bedrijfsnetwerk verbiedt. Het Hof verwijst in zijn arrest uitdrukkelijk naar artikel 8 E.V.R.M. Dit arrest verhindert niet dat bedrijven in sommige omstandigheden toch toegang krijgen tot e-mail van werknemers, op voorwaarde dat dit geen schending van de privacy inhoudt. Een werkgever die e-mail van werknemers wil inkijken moet op voorhand duidelijk stellen wanneer hij dit zal doen en om welke reden, bijvoorbeeld om berichten te archiveren. Daarom kan je als werkgever best een e-mail policy opstellen die de regels voor het gebruik

---

56 F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 182.

57 P. DE HERT, "Schending van het (tele)communicatiegeheim in het beroepsleven", *T.S.R.*, 1995, 213.

58 HALFORD v. UK, ECHR, 25 June 1997, No. 73, para. 45.

59 Cour de Cassation (Fr.), Nikon France v. Onos, 2 October 2001, Arrêt No. 41-64.

van e-mailsystemen duidelijk voorop stelt. De werknemers moeten weten in hoeverre ze een redelijke verwachting van privacy mogen koesteren.

Het Europese Hof voor de Rechten van de Mens heeft in zijn rechtspraak een sterke bescherming van correspondentie. De huidige Amerikaanse rechtspraak daarentegen laat het rechtmatig belang van het bedrijf om e-mail van werknemers de doorzoeken meestal zwaarder doorwegen dan de werknemers verwachting van privacy. Het principiële recht op privacy, zoals dat uit het Fourth Amendment wordt afgeleid, wordt door de rechters toegepast op de louter privaatrechtelijke arbeidsrelatie. In de zaak MCLAREN v. Microsoft Corporation (28 mei 1999), oordeelde een rechter dat een werknemer die e-mail verstuurde via het bedrijfsnetwerk en bewaarde in persoonlijke folders toch geen redelijke verwachting van privacy kon hebben tegenover deze berichten. Het feit dat de U.S. nooit een expliciet grondwettelijk recht op bescherming van het telecommunicatiegeheim gekend hebben, en het feit dat het een "afgeleid recht" is, zijn hier wellicht niet vreemd aan.

B.1.2.3 Uitzonderingen

Archiveren van e-mail impliceert de kennisname van de inhoud ervan. Zelfs als de archivering automatisch gebeurt op de e-mailserver, houdt de werkgever zich in elk het geval het recht voor om het archief te openen op een later tijdstip. Dit staat haaks op het geheime karakter van e-mail. Maar grondrechten gelden niet absoluut, art. 8 E.V.R.M. voorziet zelf dat uitzonderingen mogelijk zijn onder strenge voorwaarden. De rechtspraak ziet in dit artikel drie voorwaarden: het legaliteitsbeginsel, het finaliteitsbeginsel en het proportionaliteitsbeginsel.

Het legaliteitsbeginsel stelt dat een inmenging in de persoonlijke levenssfeer van een ander enkel mag als de betrokkene dit kon verwachten. De overheid moet zich kunnen baseren op een regel uit het recht, maar alleen rechtregels die voldoende duidelijk en toegankelijk zijn voor de burgers tellen mee. Tussen particulieren geldt hetzelfde principe onder de noemer van het transparantiebeginsel, wat aanduidt dat de privacyverwachting[60] van de betrokkene beïnvloed kan worden door duidelijke afspraken vervat in een contract, een reglement of een dienstvoorschrift. In een arbeidsverhouding verwacht de werknemer wel dat de werkgever een zekere controle zal uitoefenen, maar daarom niet dat elke e-mail die hij schrijft ingekeken en gearchiveerd wordt. Daarom is het van groot belang dat het archiveringsbeleid klaar en duidelijk uitgelegd wordt.

Het finaliteitsbeginsel bepaalt dat inmenging enkel kan ter bescherming van een gerechtvaardigd belang. Tussen particulieren zal vooral de "bescherming van rechten en vrijheden van anderen"[61] een rol spelen. De werkgever put onder andere een recht op gezag en controle uit de arbeidsovereenkomst, hij heeft er een rechtmatig belang bij om bijvoorbeeld misbruik van communicatiemiddelen op te sporen of aan kwaliteitscontrole te doen[62]. De werkgever heeft er ook belang bij dat zakelijke communicatie bewaard

[60] F. HENDRICKX, *Privacy en arbeidsrecht,* Brugge, die Keure, 1999, p. 51 e.v.

[61] Art. 8 lid 2 E.V.R.M.

[62] F. HENDRICKX, *Privacy en arbeidsrecht,* Brugge, die Keure, 1999, p. 210 e.v.

blijft, eventueel als bewijs van transacties of om know-how op te bouwen. Een archief van e-mails met zakelijke inhoud aanleggen maakt deel uit van een goede bedrijfsvoering.

Bovendien moet elke inmenging in een grondrecht proportioneel zijn aan het vooropgestelde doel. Concreet moet het inkijken en opslaan van e-mails noodzakelijk zijn en er mag geen minder ingrijpend middel zijn om het doel te bereiken. Vooral de manier waarop het archief wordt opgebouwd zal hier van belang zijn: kiest de werknemer zelf welke e-mails hij in het archief klasseert of gebeurt dit automatisch op de server?

Het uitgangspunt is dus dat e-mails confidentieel zijn. Archiveren van e-mails door de werkgever is een inmenging in de privacy van de werknemer. Deze inmenging is enkel aanvaardbaar als voldaan is aan de voorwaarden van de legaliteit, de finaliteit en de proportionaliteit. Telkens moet in concreto nagekeken worden of het archief conform de voorwaarden van art. 8 E.V.R.M. wordt opgebouwd en beheerd.

B.2. De Belgische Grondwet

Het recht op bescherming van de persoonlijke levenssfeer en in het bijzonder van communicatie is vastgelegd in art. 22 (privé- en gezinsleven) en art. 29 (briefgeheim) van de Grondwet.

B.2.1 Het briefgeheim

Voor de toepassing van het briefgeheim wordt een e-mail door velen ten onrechte beschouwd als een brief. Het briefgeheim ligt vervat in artikel 29 van de Grondwet (G.W.)[63]. Het briefgeheim bestaat hierin dat iedereen het recht heeft om te eisen dat het geheim van de boodschappen (brieven, postkaarten, drukwerk enzovoort) die hij aan de openbare dienst der posterijen toevertrouwt, door de Staat wordt geëerbiedigd[64]. Zo geformuleerd, is de onschendbaarheid van het briefgeheim enkel van toepassing in de verhouding tussen de burger en de overheid. De grondwettelijke bescherming van het briefgeheim geldt echter ook in de relatie tussen particulieren[65].

Uit het tweede lid van art. 29 G.W., dat zegt dat de wet bepaalt welke agenten verantwoordelijk zijn voor de schending van het geheim der aan de post toevertrouwde brieven, wordt wel eens afgeleid dat het

---

[63] Art. 29 Grondwet: "*Het briefgeheim is onschendbaar. De wet bepaalt welke agenten verantwoordelijk zijn voor de schending van het geheim der aan de post toevertrouwde brieven*."

[64] A. MAST en J. DUJARDIN, *Overzicht van het Belgisch grondwettelijk recht*, Brussel, Story-Scientia, 1987, 541, nr. 470.

[65] F. HENDRICKX, *o.c.*, 206; R. SENELLE, *Commentaar op de Belgische Grondwet*, Brussel, Ministerie van Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking, 1974, 53, aangehaald door J. VANDE LANOTTE *Overzicht Publiek Recht*, Brugge, Die Keure, 2001, 392. Art. 8 E.V.R.M. bepaalt dat eenieder recht heeft op de eerbiediging van zijn briefwisseling, zonder te specifiëren ten aanzien van wie deze bescherming geldt.

briefgeheim enkel grondwettelijke bescherming geniet gedurende de periode dat de brief aan de post is toevertrouwd. Met deze toevoeging heeft men voor de wetgever echter enkel de mogelijkheid willen voorzien om de overheidsorganen aan te duiden die het geheim van aan de post toevertrouwde brieven in bepaalde omstandigheden wel mogen schenden[66]. Het briefgeheim geldt dus voor alle brieven, zoals brieven toevertrouwd aan privé-koeriers, of brieven in iemands brievenbus of postvakje, of nog brieven die in iemands huis of kantoor worden gevonden. Het briefgeheim geldt niet alleen voor brieven die men ontvangen heeft, maar eveneens voor uitgaande brieven die nog niet verstuurd of bezorgd werden. De schending van het briefgeheim wordt gesanctioneerd met burgerrechtelijke sancties.

Het briefgeheim is niet alleen grondwettelijk beschermd, maar ook strafrechtelijk[67]. Het wegmaken of openen van een brief is slechts strafbaar wanneer dit gebeurt in de periode dat de brief aan de post is toevertrouwd. De strafrechtelijke bescherming van het briefgeheim is dus zeer beperkt.

B.2.2. Het briefgeheim en de werkplaats

Het briefgeheim is zoals gezegd onschendbaar, en iedere uitzondering moet bij wet zijn vastgelegd. Nergens bepaalt de wet echter dat werkgevers de bevoegdheid hebben om binnenkomende correspondentie te openen, ook niet voor archiveringsdoeleinden.

De grondwettelijke bescherming van het briefgeheim geldt ook voor de briefwisseling die men ontvangt in de onderneming. Zelfs de briefwisseling die gevoerd wordt op kosten van de werkgever behoudt zijn privé-karakter[68]. In dit verband is het interessant om te wijzen op de parlementaire vraag die werd gesteld op initiatief van de Vereniging van Steden en Gemeenten naar aanleiding van het bestaan van onderrichtingen in sommige administraties volgens welke alle binnenkomende correspondentie moet worden geopend door de daartoe aangestelde personeelsleden[69].

Volgens de Vereniging van Steden en Gemeenten moet een brief op naam van een personeelslid van een gemeente of OCMW, die noch de vermelding ‘vertrouwelijk’, noch de vermelding ‘persoonlijk’ draagt, beschouwd worden als een brief die bestemd is voor de ‘ambtenaar’ en niet voor de ‘persoon’ aan wie hij

---

66 Zo werd het Bestuur der posterijen bevoegd gemaakt om onbestelbare brieven te openen. Hetzelfde geldt voor brieven waarvan vermoed wordt dat ze verboden waarden of verboden voorwerpen bevatten (art. 2 en art. 32 lid 5 Wet 26 december 1956 op de postdient, *B.S.* 30-31 december 1956). De inbeslagneming en opening van aan de post toevertrouwde brieven in het kader van de opsporing, is geregeld in de ‘Algemene Onderrichting betreffende de werking der posterijen’, die niet openbaar is gemaakt. Deze situatie is onverenigbaar met de legaliteitseis uit de Grondwet. Zie voor de inhoud van de Onderrichting: P DE HERT, “Bedrijf mag post werknemers niet zomaar open maken”, *Juristenkrant*, 2001, afl. 21, 6.

67 Art. 460 Sw.: “*Hij die schuldig bevonden wordt aan het wegmaken van een aan de post toevertrouwde brief of aan het openen van een zodanige brief om het geheim ervan te schenden, wordt gestraft met gevangenisstraf van acht dagen tot een maand en met geldboete van zesentwintig tot tweehonderd frank of met een van die straffen alleen, onverminderd zwaardere straffen, indien de schuldige een ambtenaar of een agent van de Regering of van de posterijen is.*”

68 F. HENDRICKX, *o.c.*, 206-207.

69 Parl. Vr. nr. 71 van CARDOEN, 26 februari 1987, *Vr. en Antw.*, Senaat, 1987-1988, afl. 1, 4.

geadresseerd is. Een dergelijke brief zou enkel betrekking hebben op de werking van de administratie en niet op het privé-leven van het betrokken personeelslid. De bezorgdheid van de steden en gemeenten was vooral gelegen in het feit dat een te strak standpunt omtrent het briefgeheim tot gevolg zou hebben dat alle brieven die de naam van de behandelende ambtenaar bevatten, niet meer centraal zouden mogen ingeschreven worden, maar rechtstreeks aan deze ambtenaar zouden moeten bezorgd worden. Zeker nu de openbaarheidsreglementering in het kader van de actieve openbaarheid oplegt dat elke briefwisseling uitgaande van een federale, gemeentelijke of provinciale administratieve overheid[70] de naam, de hoedanigheid, het adres en het telefoonnummer moet vermelden van degene die meer inlichtingen kan verstrekken over het dossier, komt er immers heel wat briefwisseling op naam toe bij de administratie. De steden en gemeenten argumenteerden dat de noodzaak van een ordevolle, administratieve organisatie, een inbreuk op de grondwettelijk gewaarborgde onschendbaarheid van het briefgeheim rechtvaardigt.

De Minister van Justitie was het niet eens met deze redenering, waaromtrent ook Senator CARDOEN zijn bezorgheid uitdrukte. De Minister is van mening dat *de onderrichtingen die in sommige administraties zouden bestaan volgens welke ook de correspondentie die op naam van een ambtenaar is gestuurd, moet geopend worden door de daartoe aangestelde personeelsleden, strijdig zijn met het fundamenteel beginsel van de onschendbaarheid van het briefgeheim zoals voorzien in art. 22* (nu 29) *van de Grondwet en in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden* en dat *zelfs het argument van een betere werking van de dienst* (een efficiënte dossiervorming met het oog op de bewaring?) *geen afwijking op dit essentieel beginsel toelaat*. Er mag met andere woorden geen onderscheid worden gemaakt tussen brieven met de vermelding 'vertrouwelijk' of 'persoonlijk' en brieven waarop deze vermelding niet voorkomt. Het briefgeheim is van toepassing op alle nominatim geadresseerde brieven, ook indien men deze brieven ontvangt in de organisatie en niet op zijn privé-adres[71].

Uit het voorgaande leiden we af dat de persoon, die in de organisatie verantwoordelijk is voor de dossiervorming en de bewaring van deze dossiers, dus zal moeten wachten tot de geadresseerde de brief aan een dossier heeft toegevoegd, alvorens men de brief kan gaan selecteren voor archivering. Aangezien er ten aanzien van brieven een zeker automatisme bestaat om hen aan het juiste dossier toe te voegen, zal de records manager, en later de archivaris, deze brief wellicht aantreffen, zodat hij een professioneel oordeel kan vellen over de bewaring op lange termijn.

---

[70] Art. 2 3° Wet 11 april betreffende de openbaarheid van bestuur (*B.S.* 30 juni 1994) en art. 3 3° Wet 12 november 1997 betreffende de openbaarheid van bestuur in de provincies en gemeenten (*B.S.* 19 december 1997); Het Vlaams decreet van 23 oktober 1991 bevat geen dergelijke bepaling. Aan de hand van het Internet kan de burger echter heel snel terugvinden welke ambtenaar instaat voor welke aangelegenheid. Zie http://www.vlaanderen.be/ned/sites/adressen/Gids2001MVG.pdf

[71] Zie ook een recentere vraag over deze kwestie gesteld aan Minister KELCHTERMANS door de Vereniging van Steden en Gemeenten: M. SUYKENS, "Briefgeheim bij openbare besturen", *De Gemeente*, 1995, nr. 4, 182. De Minister zegt dat hij begrip kan opbrengen voor de bezorgdheid van de steden en gemeenten omtrent de eventuele moeilijkheden m.b.t. het centraal inschrijven van ingekomen briefwisseling (selecteren van briefwisseling voor archivering?). Zie ook nog in verband met deze problematiek: J.M. LEBOUTTE, "De wettelijke bescherming van het briefgeheim", *De gemeente*, 1988, 369-371 en E. VAN VAERENBERGH, "Wettelijke bescherming van het briefgeheim", *De gemeente*, 1989, 165-166.

B.2.3. Wordt e-mail beschermd door het briefgeheim?

Ten aanzien van e-mail bestaat er (nog) geen automatisme om de berichten toe te voegen aan de dossiers van de organisatie. In vele organisaties bestaat er dus een grote ongerustheid over de manier waarop werknemers omgaan met de ingekomen en de uitgaande e-mails. Heel wat e-mails worden ongetwijfeld willekeurig gewist worden door de werknemers. De vraag is dus of de records manager van de organisatie de elektronische postbus van de werknemer mag bekijken, de inhoud van de elektronische berichten mag controleren en het elektronisch bericht mag registreren en eventueel kopiëren, zodat de bewaring ervan later, indien nodig, verzekerd is.

Als een e-mail voor de toepassing van het briefgeheim als een brief zou kunnen beschouwd worden, dan zouden de hierboven geschetste regels van toepassing zijn met betrekking tot het openen door derden van brieven. In België zijn er echter andere regels van toepassing op e-mail.

B.2.4. Het telecommunicatiegeheim

Door de wet van 13 oktober 1930 werd een gelijkaardige bescherming als het briefgeheim geregeld voor het domein van de telegraaf- en de telefoonverbinding[72]. Deze wet kan beschouwd worden als de eerste wet die het zogenaamde 'telecommunicatiegeheim' beschermt. Met het oog op het uitbreiden van het briefgeheim tot nieuw ontdekte vormen van communicatie is art. 29 G.W. opgenomen in de verklaring tot herziening van de Grondwet van 5 mei 1999[73]. Nochtans geniet het telecommunicatiegeheim reeds de grondwettelijke bescherming van art. 22, aangezien privé-communicatie een element van de persoonlijke levenssfeer is. De omgang met e-mail zal daarom bekeken worden aan de hand van de regels over de bescherming van de persoonlijke levenssfeer uitgewerkt in verschillende Europese richtlijnen en nationale wetten.

C. EUROPESE RICHTLIJNEN

De Richtlijn 95/46 EG betreffende de verwerking van persoonsgegevens stelt de algemene regels vast voor de omgang met persoonsgegevens. De impact van deze richtlijn op het archiveren van e-mail wordt verder besproken bij de Belgische wet op de bescherming van de persoonlijke levenssfeer van 8 december 1992.

Het telecommunicatiegeheim wordt op Europees niveau beschermd door Richtlijn 97/66 EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (Richtlijn Privacy en Telecommunicatie). Deze richtlijn werd vervangen door Richtlijn 2002/58 EG betreffende de verwerking van persoonsgegevens en de bescherming van de

---

[72] Wet 13 oktober 1930 tot samenordening der verschillende wetsbepalingen op de telegrafie en de telefonie met draad, *B.S.* 20-21 oktober 1930.

[73] B.S. 5 mei 1999.

persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn Privacy en Elektronische communicatie). De lidstaten hebben tot 31 oktober 2003 om deze richtlijn om te zetten. Wat betreft archiveren van e-mail is er weinig veranderd.

Beide richtlijnen hebben als voornaamste doel de bescherming van de persoonsgegevens en van de persoonlijke levenssfeer van abonnees en gebruikers van telecommunicatiediensten en is voor ons onderzoek van belang in het kader van het gebruik dat wordt gemaakt van telecommunicatiediensten voor het uitwisselen van elektronische berichten.

Art. 5 lid 1 van beide richtlijnen bepaalt dat de lidstaten in hun nationale reglementering het vertrouwelijk karakter garanderen van oproepen via het openbare telecommunicatienetwerk en via algemeen beschikbare telecommunicatiediensten[74]. Zij moeten met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van gesprekken door anderen dan de gebruikers verbieden, indien de betrokken gebruikers daarmee niet hebben ingestemd. De lidstaten kunnen uitzonderingen op het vertrouwelijk karakter invoeren om bepaalde openbare belangen te beschermen[75].

Beide richtlijnen voorzien in een uitzondering voor zakelijke communicatie[76]. Deze uitzondering kwam er op aandrang van de financiële sector, die telefoongesprekken met klanten opneemt als bewijs voor de gesloten transacties. De bewoording van het artikel is erg ruim gesteld zodat ook het archiveren van zakelijke e-mail eronder valt. Het begrip 'zakelijke communicatie' wordt niet gedefiniëerd, maar het is duidelijk de bedoeling een onderscheid te maken tussen professionele communicatie en persoonlijke communicatie. De registratie is enkel toegelaten in het kader van 'legaal zakelijk verkeer', een voorwaarde die op het eerste zicht niet zo duidelijk is. De Engelse terminologie '*in the course of lawful business practice'* en de Franse uitdrukking *'usages professionnels licites*' lijken te verwijzen naar de regelgeving over de handelspraktijken. De kwestie is dan niet zozeer of het een legale onderneming betreft, maar of de opnames kaderen in een legitieme handelspraktijk. Als laatste voorwaarde geldt dat de wet het registreren moet toestaan. Het Europees parlement wilde hiermee verzekeren dat het nationaal parlement over het toepassingsgebied van deze uitzondering zou waken[77]. Een expliciete toelating in de wet lijkt dus noodzakelijk om van deze uitzondering gebruik te kunnen maken. De bewoording van het artikel laat een wat lossere interpretatie wel toe, een impliciete toelating in de wet zou kunnen volstaan.

---

[74] Er is een terminologisch verschil tussen beide richtlijnen die de verbreding van het toepassingsgebied weerspiegelt, i.p.v. over telecommunicatie gaat het telkens over elektronische communicatie.

[75] "De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6 en in artikel 8, leden 1 tot en met 4, bedoelde rechten en plichten, indien dit noodzakelijk is voor het vrijwaren van de veiligheid van de staat, de landsverdediging, de openbare veiligheid, alsmede voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het telecommunicatie-systeem als bedoeld in artikel 13, lid 1 van Richtlijn 95/46/EG" Art 14 lid 1 van Richtlijn 97/66/EG. Deze bepaling werd in een licht gewijzigde vorm overgenomen in art. 15 lid 1 van Richtlijn 2002/58/EG.

[76] Art. 5 lid 2 van Richtlijn 97/66/EG en Richtlijn 2002/58/EG.

[77] Report on the joint text, approved by the Conciliation Committee, for a European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector (c4-0571/97 – 00/0288(COD)), PE A4-0361/97, Publicatieblad C371 8 december 1997, p. 4

Valt e-mail uitgaande van een ambtenaar onder de uitzondering van art. 5 lid 2? De bewoording van art. 5 lid 2 is toegespitst op de privé-sector[78], maar wil eigenlijk een onderscheid maken tussen professionele communicatie en persoonlijke communicatie. Binnen de professionele communicatie nog het onderscheid tussen publieke sector en private sector maken is arbitrair, aangezien deze scheidingslijn in alle lidstaten anders ligt.

Professionele e-mails van ambtenaren zijn bovendien onderworpen aan de nationale regels in verband met openbaarheid van bestuur. De Richtlijnen Privacy en Telecommunicatie respectievelijk Elektronische Communicatie kunnen en willen de openbaarheid van bestuur niet inperken. Het Europees Hof van Justitie erkent de openbaarheid van bestuur als grondrecht van alle burgers[79] en de richtlijnen moeten grondrechtsconform geïnterpreteerd worden. De lidstaten kunnen dus ook een uitzondering voorzien voor professionele e-mail in de publieke sector.

D. BELGISCH RECHT

D.1. Het telecommunicatiegeheim

Het telecommunicatiegeheim wordt in België strafrechtelijk beschermd in twee afzonderlijke wetten: enerzijds door de artikelen 109terD en 109terE van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven[80], en door de artikelen 259bis en 314bis van het Strafwetboek[81] anderzijds.

Art. 109terD: “Behoudens toestemming van alle andere personen, die rechtstreeks of onrechtstreeks betrokken zijn bij de hierna bedoelde informatie, identificatie of gegevens, is het iedereen verboden zelf of door toedoen van een derde:

1. met bedrieglijk opzet kennis te nemen van het bestaan van met telecommunicatie overgebrachte tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, die herkomstig zijn van en bestemd zijn voor andere personen.
2. met bedrieglijk opzet de in 1° bedoelde informatie met gelijk welk technisch procédé te wijzigen of weg te laten of de andere personen te identificeren.
3. met opzet kennis te nemen van gegevens inzake telecommunicatie, die betrekking hebben op een ander persoon.

---

[78] De verschillende taalversies hebben het over: 'zakelijke communicatie', '*business communication*', '*communication commerciale*', '*geschäftlichen Nachricht*'.

[79] Nederland v. Raad EU, C-58/94, EHJ I-2169.

[80] Deze wet wordt ook wel de Belgacomwet of de Telecomwet genoemd.

[81] Ingevoegd in het Strafwetboek door de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en –telecommunicatie, *B.S.* 24 januari 1994.

4. de in 1°, 2° en 3° bedoelde informatie, identificatie en gegevens die met of zonder opzet werden bekomen, kenbaar te maken, deze te wijzigen of ze te vernietigen.

Art. 109terE §1: "De bepalingen van artikel 109terD van deze wet en van de artikelen 259bis en 314bis van het Strafwetboek zijn niet van toepassing:

1. wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt.
2. wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een telecommunicatiedienst te garanderen.
3. wanneer de handelingen worden gesteld om de interventie van hulp- en nooddiensten mogelijk te maken die antwoorden op aan hen gerichte verzoeken om hulp.
4. wanneer de handelingen worden gesteld in het kader van de algemene opdracht inzake toezicht en controle die aan het Instituut is toegekend bij artikel 75, § 3 van deze wet. De door het Instituut gevraagde inlichtingen kunnen slechts betrekking hebben op de identiteit en het adres van een houder van een telefoonnummer, alsook op de referenties van de opgeroepen nummers en de boekhoudkundige gegevens met betrekking tot de facturatie.

Art. 314bis Sw. §1 Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd frank tot tienduizend frank of met een van die straffen alleen wordt gestraft hij die:

1. ofwel, opzettelijk, met behulp van enig toestel, privé-communicatie of –telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie
2. ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen

§2 Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd frank tot twintigduizend frank of met een van die straffen alleen wordt gestraft hij, die wetens, de inhoud van privé-communicatie of –telecommunicatie die onwettig afgeluisterd of opgenomen is of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.

Met dezelfde straffen wordt gestraft hij die, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van een wettig gemaakte opname van privé-communicatie of –telecommunicatie

Telecommunicatie wordt in de Telecomwet omschreven als 'elke overbrenging, uitzending of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, *per draad, radio-elektriciteit, optische seingeving of een ander elektromagnetisch systeem.*'[82] Telecommunicatie wordt heel ruim opgevat en omvat niet alleen telefonie, maar ook telex, telefax, mobilofonie, telebanking, e-mail, surfen

[82] Art. 68 4° Telecomwet.

op het Internet enzovoort Alle moderne vormen van telematica aan de hand waarvan communicatie kan verlopen, worden beschermd[83]. Van zodra het bericht dat gecommuniceerd wordt, vervat zit in een geschreven stuk, is echter het briefgeheim van toepassing. Wanneer een e-mail afgedrukt is, kan het afgedrukte stuk beschouwd worden als een geschreven stuk en is het briefgeheim van toepassing. De elektronische versie van de e-mail blijft beschermd door het telecommunicatiegeheim[84].

Wat houdt dat telecommunicatiegeheim nu precies in en wat zijn de gevolgen voor de bewaring van e-mails in de organisatie?

D.1.1. Kennisnemen van de inhoud van e-mails

De *inhoud* van telecommunicatie wordt beschermd door de artikelen 259bis en 314bis van het Strafwetboek. Deze twee artikelen bevatten dezelfde misdrijven, maar art. 259bis is van toepassing wanneer het misdrijf wordt gepleegd door 'een openbaar officier of ambtenaar, drager of agent van de openbare macht', terwijl art. 314bis wordt toegepast indien het misdrijf wordt gepleegd door andere personen dan deze vermeld in artikel 259bis. Het enige verschil is dat de straffen zwaarder zijn indien het misdrijf wordt gepleegd door een openbaar ambtenaar. Het kennisnemen van de inhoud van e-mails wordt dus potentieel zwaarder gestraft wanneer dit gebeurt door een ambtenaar bij een overheidsinstelling.

Wat staat er nu precies in art. 314bis Sw.? Elke vorm van kennisname van privé-communicatie of -telecommunicatie wordt gestraft, voorzover dit gebeurt met behulp van enig toestel en voorzover dit gebeurt tijdens de overbrenging van de communicatie. Er moeten dus enkele voorwaarden voldaan zijn opdat er van een misdrijf sprake zou zijn.

Om strafbaar te zijn, moet degene die kennisneemt van de inhoud van een telecommunicatiebericht, dit doen met behulp van enig toestel. Welk toestel er wordt gebruikt, speelt geen rol. De records manager zal minstens een computer nodig hebben om de e-mail berichten van de werknemers in te kijken.

Bovendien moet het gaan om privé-telecommunicatie. Telecommunicatie is privé wanneer ze niet bestemd is om door iedereen gehoord te worden, en dit ongeacht de plaats waar ze plaatsvindt[85]. Communicatie blijft privé, ook al nemen meer dan twee personen er aan deel. Dat is bijvoorbeeld het geval met een e-mail met meerdere bestemmelingen (To:) of een e-mail waarvan een *Carbon Copy* werd verzonden aan andere personen dan de geadresseerde (Cc:). Dit kan een probleem opleveren wanneer er een *Blind Carbon Copy* werd verzonden (Bcc:). Het strafbaar karakter vervalt immers wanneer de dader

---

83 *Parl. St.*, Senaat, 1992-1993, nr. 843/1, 3.

84 *Parl. St.*, Kamer, 1989-1990, nr. 1287/10, 173: voor de fax wordt er gepreciseerd dat deze als een geschreven stuk kan beschouwd worden dat beschermd wordt door de wet op het briefgeheim, zodra de fax uit het apparaat komt. In tegenstelling tot de e-mail bestaat de fax slechts tijdelijk in een elektronische versie nl. tijdens de overbrenging.

85 *Parl .St.*, Senaat, 1992-1993, nr. 843/1, 6-7 en nr. 843/2, 10.

de toestemming heeft van alle deelnemers aan de communicatie. Een *Blind Carbon Copy* geeft echter niet prijs welke personen er allemaal een kopie ontvingen.

Professionele e-mail die in het kader van de organisatie werd ontvangen of verzonden, heeft in principe ook een privé-karakter[86]. Een e-mail die via het intern netwerk van de organisatie werd verstuurd, is eveneens privé. Volgens BLANPAIN[87] vertegenwoordigt de werknemer zijn werkgever wanneer hij in het kader van zijn werk met anderen communiceert en is er dus geen sprake van privé-communicatie. Deze interpretatie druist in tegen de gangbare definitie van privé-communicatie. Bovendien wordt de relatie tussen een werknemer en een werkgever in het algemeen niet als een vertegenwoordiging aanzien[88]. Vertegenwoordiging is er slechts wanneer de werknemer in naam en voor rekening van zijn werkgever rechtshandelingen stelt. Uiteraard kan dit via e-mail en internet ook gebeuren, maar dit zal slechts een fractie uitmaken van de totale elektronische communicatie van een werknemer. Zelfs als er sprake is van vertegenwoordiging maakt dit van de werkgever niet automatisch een deelnemer aan het gesprek.

Het kennisnemen van de telecommunicatie moet met opzet gebeuren d.w.z. wetens en willens[89]. Maar het is niet nodig dat de dader met kwade bedoeling handelt, bijvoorbeeld met het doel schade te veroorzaken of om iemand te bedriegen. Loutere nieuwsgierigheid kan dus bestraft worden. Alleen iemand die per ongeluk een e-mail bericht onderschept en kennisneemt van de inhoud, is niet strafbaar.

Tenslotte is het noodzakelijk dat er van het telecommunicatiebericht kennis werd genomen 'tijdens de overbrenging ervan'. Indien de records manager de e-mail onderschept tijdens de route tussen de verzender en de ontvanger is hij strafbaar[90]. De records manager zal echter vooral geïnteresseerd zijn in de elektronische postbus van de werknemer. Daar vindt hij alle e-mailberichten die de werknemer die dag heeft verzonden en ontvangen[91]. Het lezen van een bericht dat in de elektronische postbus van de werknemer is opgeslagen, kan niet gekwalificeerd worden als het kennisnemen van de inhoud van een e-mail tijdens de overbrenging ervan[92]. Dit geldt ook wanneer het e-mailbericht nog is opgeslagen bij de dienstenvertrekker en dus nog op de server staat. Het maken van een kopie van de inhoud van de berichten in de elektronische postbus, zonder van de inhoud kennis te nemen, is evenmin strafbaar onder art. 314bis Sw.

---

86 F. HENDRICKX, *o.c.*, 190 en 195, VAN EECKE, P., "Call centers en de Belgische afluisterwet: een pijnlijke confrontatie", *Computerrecht*, 1997, afl. 1, p. 8.

87 R. BLANPAIN, M. VAN GESTEL, *Gebruik en controle van e-mail, intranet en internet in de onderneming*, Praktijk en Recht, Brugge, Die Keure, 2003, nr. 252 en 254.

88 W. VAN EECKHOUTTE, *Arbeidsrecht*, Antwerpen, Kluwer, 2000, nr. 360.

89 Wetens en willens is een term uit het strafrecht en wil zeggen dat de persoon die het misdrijf pleegt op de hoogte is van het feit dat hij een strafbaar feit pleegt (hier speelt het adagium: iedereen wordt geacht de wet te kennen) en dat hij, goed wetende waar hij mee bezig is, de feiten heeft willen plegen.

90 O. RIJCKAERT maakt een verschil tussen e-mailberichten die in de postbus van de werknemer staan en de reserve copie gemaakt door bijvoorbeeld de bedrijfsserver in het kader van de overbrenging van e-mail, zie O. RIJCKAERT, "Le contrat de travail face aux nouvelles technologies", *Orientations*, 2000, p. 208.

91 In veel organisaties worden 's nachts de e-mailberichten die de werknemer gewist heeft, ook effectief verwijderd.

92 J. DUMORTIER, "Internet op het werk: controlerechten van de werkgever", *l.c.*, 40.

Dit levert een vreemde situatie op: het briefgeheim verbiedt dat er van de inhoud van een brief kennis wordt genomen, ook wanneer die brief zich niet meer in de overbrengingsfase bevindt, bijvoorbeeld wanneer de brief zich niet meer in handen van de Post bevindt, maar zich reeds in de brievenbus van de bestemmeling bevindt. Wanneer dezelfde inhoud echter per e-mail zou worden verstuurd en zich in de elektronische brievenbus bevindt, dan verbiedt het telecommunicatiegeheim niet dat er van de inhoud van die e-mail kennis wordt genomen.

Toch ontsnapt de records manager niet aan bestraffing, wanneer hij de hierboven beschreven handelingen zou stellen. Hij neemt daardoor dan immers kennis van of registreert het bestaan van e-mails. Dit is het terrein van art. 109terD van de Telecomwet.

D.1.2. Kennisnemen van het bestaan van e-mails

Art. 109terD van de Telecomwet handelt enkel over het kennisnemen, registreren enzovoort van *het bestaan* van een telecommunicatiebericht of van gegevens over de communicatie, zoals de naam van de correspondenten, het onderwerp, het tijdstip of de duur. Wie echter op een onwettige, of zelfs op een wettige wijze kennis neemt van de inhoud van een e-mailbericht, kan dit onmogelijk doen zonder tegelijk kennis te nemen van het bestaan van die e-mail en van de gegevens betreffende die e-mail. Een records manager die een e-mail leest of registreert, of die een kopie maakt van de e-mails voor bewaring, zal dus steeds strafbaar zijn onder art. 109terD van de Telecomwet.

Art. 109terD 1° verbiedt het kennisnemen van *het bestaan* van telecommunicatieberichten. Aangezien voor deze eerste strafbaarstelling bedrieglijk opzet[93] vereist is, zal een records manager die de e-mails wil controleren voor bewaringsdoeleinden wellicht niet het misdrijf plegen dat hier wordt geviseerd. Dat element van bedrieglijk opzet ontbreekt echter in art. 109terD 3°, dat verbiedt om met (gewoon) opzet kennis te nemen van gegevens inzake telecommunicatie die betrekking hebben op een andere persoon. Met ‘gegevens inzake telecommunicatie die betrekking hebben op een andere persoon’ wordt bedoeld ‘de individuele gegevens welke betrekking hebben op een persoon die gebruik maakt van diensten voor telecommunicatie, beperkt tot het gedeelte dat tot de telecommunicatie behoort.’[94] Het gaat dus niet om algemeen bekende gegevens, zoals iemands e-mailadres, maar wel het onderwerp van de communicatie, het tijdstip van verzenden enzovoort. De vermelding van een e-mailadres in een e-mail, is wel een gegeven inzake telecommunicatie, voorzover men daaruit kan afleiden naar wie of door wie er een e-mail werd verstuurd.

Een records manager zal dus in zijn speurtocht naar e-mails die niet mogen gewist worden, zeer snel aan de kwalificatie van dit misdrijf voldoen. Ten aanzien van e-mails gaat het bijvoorbeeld om gegevens

---

93 Soms vereist de strafwet dat de dader de feiten pleegde met een bijzonder oogmerk, opdat er van een misdrijf sprake zou zijn. Bedrieglijk opzet is het oogmerk om aan zichzelf of aan anderen een onrechtmatig voordeel te verschaffen dat van eender welke aard kan zijn en dat men niet had verkregen, als men het misdrijf niet had gepleegd.

94 *Parl. St.*, Kamer, 1990-1991, nr. 1287/10, 173.

zoals de bestemmeling of de afzender van het bericht, het onderwerp van de e-mail, het al dan niet toegevoegd zijn van een 'attachment', de voorrang waarmee een e-mailbericht moet behandeld worden enzovoort. Al deze zaken zijn natuurlijk van groot belang om de archiefwaarde van een e-mail te bepalen. Volgens de wet mag er echter geen kennis van worden genomen door personen die niet bij de communicatie betrokken zijn.

Merk op dat het erg onduidelijk is waarin het verschil is gelegen tussen *kennis nemen van gegevens inzake telecommunicatie, die betrekking hebben op een andere persoon* (art. 109terD 3°) en *kennis nemen van het bestaan van met telecommunicatie overgebrachte tekens of gegevens, die herkomstig zijn van of bestemd zijn voor andere personen* (art. 109terD 1°)[95]. De records manager zal in principe alleen het eerst genoemde misdrijf plegen, aangezien bedrieglijk opzet normaal zal ontbreken.

Art. 114 §2 van de Telecomwet bestraft een overtreding van artikel 109terD met een geldboete van 50 tot 50 000 EUR. Geldboetes bepaald in strafwetten moeten steeds worden vermenigvuldigd met een factor vijf[96]. Het schenden van het telecommunicatiegeheim kan de records manager dus een boete van 250 000 EUR opleveren. Dit moet wel enigszins gerelativeerd worden in die zin dat sinds de wet van 4 mei 1999 tot invoering van de strafrechtelijke verantwoordelijkheid van rechtspersonen (*B.S* 22 juni 1999) ook de organisatie (mee) kan veroordeeld worden.

Ook in de Telecomwet is bepaald dat de strafbaarstelling vervalt wanneer de records manager de toestemming zou hebben van alle deelnemers aan de communicatie. Het is echter moeilijk in te zien hoe men de toestemming van de communicatiepartners kan verkrijgen. Vaak kent de werknemer deze personen niet zo goed, en soms is niet duidelijk wie de communicatiepartners bij een e-mail zijn. Er kan gedacht worden aan een vaste clausule onderaan de e-mail die aan de communicatiepartners dat de e-mail voor archiveringsdoeleinden kan ingekeken of gecontroleerd worden. Dit biedt echter geen oplossing voor de archivering van e-mails die men ontvangt[97].

Er is opnieuw een groot verschil met het briefgeheim: het kennisnemen van het bestaan van brieven en zelfs het registreren ervan is toegelaten, zolang de brief maar niet geopend wordt en mits men voldoet aan de regels betreffende de verwerking van persoonsgegevens[98]. Ten aanzien van e-mails is dit dus zoals gezegd verboden.

---

95 J. DUMORTIER, *Informatica- en telecommunicatierecht*, Leuven, Acco, 2001, 107.

96 De omzetting van geldboeten in euro werd geregeld in de wet van 26 juni 2000 (*B.S. 29 juli 2000)*, zie ook www.just.fgov.be "Justitie en de euro".

97 Voor het registreren van het Internetverkeer ligt dat anders: als iemand surft op het Internet, zijn daar in principe geen derden bij betrokken. De toestemming van de eindgebruiker is dan ook voldoende om van het bestaan van deze vorm van communicatie kennis te mogen nemen.

98 Zie verder.

D.1.3. Uitzonderingen op het telecommunicatiegeheim

Art. 109terE van de Telecomwet bevat vier uitzonderingen op het telecommunicatiegeheim. Art. 109terE 3° (hulpdiensten) en 4° (toezicht BIPT) zijn niet relevant in deze context. Art. 109terE 2° laat logging van ingekomen en uitgaande e-mails toe wanneer het tot doel heeft om de goede werking van het netwerk na te gaan en de goede uitvoering van de telecommunicatiedienst te garanderen[99]. Logging wil zeggen dat men bestanden aanlegt die o.a. de datum en het tijdstip van verzending, de afzenders, de geadresseerden en de bestandsgrootte van de ingekomen en uitgaande e-mails en van de eventuele attachments bevatten. De *serverlogfiles* bevatten dus gegevens inzake telecommunicatie. Het argument van technische supervisie kan echter bezwaarlijk worden ingeroepen door een werkgever, een records manager of een systeembeheerder om het e-mailverkeer te screenen op zijn archiefwaarde. Bovendien mogen de logs overeenkomstig de privacywetgeving slechts zolang worden bijgehouden als nodig is om de controle uit te oefenen.

Alleen art. 109terE 1° is mogelijks van toepassing op archivering. Volgens deze bepaling zijn art. 109terD Telecomwet en 314bis Sw. niet van toepassing wanneer de wet het stellen van bedoelde handelingen toestaat of oplegt. Deze bepaling drukt uit dat er andere gerechtvaardigde belangen zijn die het telecommunicatiegeheim kunnen inperken. Deze uitzondering doelt in eerste instantie op de wettelijke bepalingen die het parket of de onderzoeksrechter expliciet toelaten om het telecommunicatiegeheim te doorbreken in het kader van het onderzoek. Een voorbeeld is art. 88 bis Wetboek van Strafvordering dat bepaalt dat de onderzoeksrechter de oproepgegevens kan doen opsporen van telecommunicatiemiddelen van waaruit of waarnaar oproepen worden of werden gedaan, en dat hij de oorsprong of de bestemming van telecommunicatie kan laten lokaliseren, wanneer hij van oordeel is dat er omstandigheden zijn die het doen opsporen van communicatie noodzakelijk maken om de waarheid aanhet licht te brengen[100].

Andere conflicterende belangen komen tot uiting in het arbeidsrecht, de regelgeving omtrent de openbaarheid van bestuur en de archiefwet[101]. Een expliciete uitzondering bestaat voor deze belangen niet, maar de bewoording van art. 109terE is ruim genoeg om ook impliciete uitzonderingen toe te laten. De voorbereidende werken geven geen enkele aanwijzing over de precieze reikweidte van het telecommunicatiegeheim en de uitzonderingen erop[102]. Ook de rechtspraak biedt weinig houvast, omdat dergelijke gevallen zelden voorkomen. De arbeidsrechtbanken kregen enkele zaken voorgeschoteld en

---

[99] Art. 109terD 2° Telecomwet.

[100] Andere voorbeelden zijn art. 46bis Wetboek van Strafvordering en art. 90ter wetboek van Strafvordering omtrent het gerechtelijk afluisteren.

[101] Voor een analyse van de verhouding tussen de regelgeving over de openbaarheid van bestuur en de archiefwetgeving: F. SCHRAM, "Openbaarheid en Archiefwetgeving" in A.-M. DRAYE (ed.), *Openbaarheid van bestuur in Vlaanderen, België en de europese instellingen*, Leuven, Instituut voor administratief recht, 1996.

[102] Doc. Kamer, 1287/1 zitting 89/90, p. 67-68.

probeerden telkens een evenwicht te zoeken tussen de belangen van de werkgever en die van de werknemer[103].

De werkgever heeft het recht gezag en toezicht uit te oefenen over zijn werknemers gebaseerd op art. 17 2° van de arbeidsovereenkomstenwet (AOW). Hierin ziet de rechtsleer[104] een uitzondering op het telecommunicatiegeheim, zodat de werkgever misbruik van internet en e-mail kan controleren, maar ook zakelijke communicatie kan archiveren. Art. 17 2° AOW op zich biedt de werknemers geen enkele indicatie over hoe de werkgever dit recht kan en mag uitoefenen, en voldoet niet aan de kwaliteitseisen voorzienbaarheid en toegankelijkheid van het E.V.R.M. Natuurlijk moet de werkgever zich nog steeds aan de privacywet houden. Alle normen samen gezien voldoen dus wel aan de kwaliteitseisen van het E.V.R.M. Deze interpretatie lijkt ook aan de grondslag van CAO nr. 81 te liggen[105].

Ook het recht op openbaarheid van bestuur komt in conflict met de strenge formulering van het telecommunicatiegeheim. Art. 32 G.W. bepaalt: *"Ieder heeft het recht elk bestuursdocument te raadplegen en er een afschrift van te krijgen, behoudens in de gevallen en onder de voorwaarden bepaald door de wet, het decreet of de regel bedoeld in artikel 134."* Dit artikel heeft direkte werking, iedereen kan dit recht afdwingen bij de rechter. De voorbereidende werken definiëren een bestuursdocument als *"alle informatie, in welke vorm ook, waarover de administratieve overheden beschikken"*. E-mail geschreven of ontvangen door een ambtenaar in het kader van zijn functie valt duidelijk onder deze beschrijving en zal dus soms openbaar moeten gemaakt worden. Art. 32 van de G.W. kan dus gezien worden als een wet die handelingen in strijd met het telecommunicatiegeheim toestaat. In hoeverre een bericht ook effectief openbaar mag gemaakt worden, hangt af van de concrete belangenafweging die moet gemaakt worden tussen het recht op privacy en het recht op toegang tot bestuursdocumenten[106]. Zowel de wet op de privacy als de reglementering omtrent de openbaarheid van bestuur leggen een dergelijke belangenafweging op[107].

De archiefwet verbiedt om archiefstukken (e-mails) te vernietigen zonder toelating van de rijksarchivaris of diens gemachtigde, bijgevolg moeten e-mails met archiefwaarde door de overheid ingekeken of geregistreerd worden om willekeurige vernietiging tegen te gaan. Net als in de vorige twee gevallen, kan deze wet gezien worden als een uitzondering op het telecommunicatiegeheim. De naleving van de privacywet zal het respect van art. 8 E.V.R.M. moeten garanderen.

---

[103] Arbeidsrechtbank Brussel, 2 mei 2000, beschikbaar op www.droit-technologie.org; Arbeidsrechtbank Brussel, 6 juni 2001, J.T.T., 2002, p. 52-55; Arbeidsrechtbank Brussel, 22 juni 2000, Computerrecht, 2001, p. 311-313; Arbeidshof Gent, 4 april 2001, J.T.T., 2002, p. 49-52.

[104] J. DUMORTIER, "Little brother is watching you: mag de werkgever het internetgebruik van zijn werknemers controleren?", in *Liber Amicorum Roger Blanpain*, 1998, die Keure, Brugge, p. 254-255. F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, die Keure, 1999, p. 198 e.v.

[105] Zie verder.

[106] Minister VAN GREMBERGEN stelt dat het belangenconflict tussen het recht op privacy van de ambtenaren en het inzagerecht van raadsleden in bestuurlijke e-mails moet opgelost worden aan de hand van de concrete afweging uit de wet op de privacy. Omzendbrief BA 2002/10 van 28 juni 2002 (B.S. 29 juli 2002).

[107] Zie bijvoorbeeld art. 4 lid 2 en 6 § 2 1° federale wet 11 april 1994, art. 5 lid 2 federale wet 12 november 1997 ove r de openbaarheid van bestuur in de provincies en gemeenten, art. 7 §1 lid 3-4 en art. 8 §3 2° decreet Vl. Gem. van 18 mei 1999.

Een voor de hand liggende kritiek op deze interpretatie van art. 109terE 1° is dat het telecommunicatiegeheim uitgehold wordt. Naast de genoemde gevallen, zijn er nog andere tegengestelde belangen, zoals bijvoorbeeld het recht op vrije nieuwsgaring door journalisten. De correspondent van een ambtenaar of werknemer verliest ook plots de bescherming van het telecommunicatiegeheim. Maar de inperking van het telecommunicatiegeheim maakt het onderscheppen van andermans e-mail niet zomaar legaal. Zoals reeds aangehaald zijn er nog andere regels die de privacy beschermen. De CBPL[108] heeft bij de invoering van het telecommunicatiegeheim dergelijke problemen al voorzien, en stelde voor het telecommunicatiegeheim een plaats te geven in de privacywet zodat een concrete belangenafweging mogelijk is.

D.2. Privacywetgeving

De archiefvormer zal zich bij de behandeling van e-mail moeten oriënteren aan de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

D.2.1 Toepassingsgebied

De privacywet is van toepassing op de verwerking van persoonsgegevens. Een persoonsgegeven wordt omschreven als ‘iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. E-mail is een persoonsgegeven voor zover het aan één of meerder personen kan toegeschreven worden. De eerste aanwijzing voor de identiteit van de verzender en/of de ontvanger(s) is uiteraard het e-mail adres. De e-mail adressen voor professioneel gebruik identificeren de gebruiker vaak onmiddellijk en eenduidig (bijvoorbeeld Hannelore.Dekeyser@law.kuleuven.ac.be). Private e-mail adressen daarentegen bevatten vaak pseudoniemen. Zelfs e-mailadressen die niet onmiddellijk toelaten de eigenaar ervan te identificeren, kunnen persoonsgegevens zijn. Om te bepalen of een persoon identificeerbaar is, moet immers worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door diegene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren. Vaak zal de leverancier van de e-maildienst in staat zijn de gebruiker van een bepaald e-mail adres te identificeren. Andere aanwijzingen vindt men meestal in de inhoud van het elektronisch bericht, zoals een automatisch bericht van ondertekening of een digitale handtekening vergezeld van een certificaat.

Eenzelfde e-mail zal meestal een persoonsgegeven zijn zowel met betrekking tot te verzender als de ontvanger. Dit is uiteraard niet zo wanneer het gaat om automatisch gegenereerde e-mailberichten, de verzender is dan geen natuurlijke persoon. Berichten verstuurd naar het algemene adres van een organisatie (bijvoorbeeld info@domeinnaam.be) zijn op hun beurt geen persoonsgegevens ten aanzien van de ontvanger. De archivaris zal de rechten van zowel de verzender als de ontvanger moeten

[108] Advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, nr. 23 14 december 1993, overweging 10-12.

respecteren bij het verwerken van e-mail. Waneer de inhoud van de e-mail bovendien persoonsgegevens bevat over een derde, moeten ook zijn rechten gerespecteerd worden.

De term 'verwerking' is erg ruim en omvat alle bewerkingen die een records manager met de e-mails zou uitvoeren. Het raadplegen, registreren, ordenen, bewaren enzovoort zijn allemaal verwerkingen in de zin van de wet. Opdat de wet van toepassing zou zijn, is het niet vereist dat de verwerking op een geautomatiseerde manier gebeurt. Ook een niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen, zoals een schriftelijk register van briefwisseling, valt onder de wet.

Het is de verantwoordelijke voor de verwerking die moet toezien op de naleving van de regels vastgelegd in de wet. Dit is de persoon die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. De organisatie die beslist een e-mail archief aan te leggen, beslist meteen over het doel en de middelen voor de verwerking van e-mail.

D.2.2. Welke regels zijn van toepassing op de verwerking van persoonsgegevens?

Volgens de wet mogen persoonsgegevens enkel worden verwerkt in een aantal limitatief opgesomde gevallen, onder meer na toestemming van de betrokkene, voor de uitvoering van een overeenkomst, of voor de uitvoering van een wettelijke verplichting, of in het belang van de verwerker tenzij het grondrecht van de betrokkene zwaarder weegt. De wetgeving rond de openbaarheid van bestuur en de archiefwetgeving maken de verwerking van persoonsgegevens noodzakelijk voor de overheid. De werkgever heeft duidelijk een belang bij de verwerking van zakelijke e-mail. De verwerking van gegevens betreffende de werknemers en het overheidspersoneel gebeurt in het kader van een contractuele of statutaire relatie.

Ten slotte moet er rekening worden gehouden met het finaliteitsprincipe: de persoonsgegevens mogen enkel verwerkt worden voor een welbepaald en uitdrukkelijk omschreven, gerechtvaardigd doel en enkel in de mate waarin dit nodig is, rekening houdend met dit doel. Concreet betekent dit dat e-mail met professionele inhoud soepeler verwerkt mag worden dan e-mail met een privé inhoud.

Om de rechten van alle betrokkenen te waarborgen moet de verantwoordelijke van de verwerking informatie verstrekken o.a. over wie hij is, welke gegevens hij verwerkt en met welk doel. Deze verplichting vervalt wanneer de verwerking gebeurt op wettelijk voorschrift of wanneer dit onevenredig veel moeite kost. Het volstaat om aan elke uitgaande e-mail deze informatie toe te voegen. Voor inkomende e-mail ligt dit moeilijker, al zijn technische oplossingen wel mogelijk.

De betrokkene heeft ook steeds het recht om de verwerkte gegevens te raadplegen en indien nodig te verbeteren.

D.3. C.A.O. nr. 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens

C.A.O. nr. 81 probeert het kluwen van regels te ontwarren en de werkgever concrete richtlijnen te geven voor de omgang met o.a. e-mail. De sociale partners beklemtonen in de toelichting dat de C.A.O. uitsluitend de bestaande regels interpreteert en toepast in de specifieke context van de arbeidsrelatie. De derden die corresponderen met werknemers genieten enkel de bescherming van de wet op de privacy.

De werkgever moet de persoonlijke levenssfeer van zijn werknemers respecteren, maar hij behoudt zijn recht van toezicht en controle binnen de perken uitgestippeld door de C.A.O.[109] De C.A.O. formuleert regels enerszijds over de installatie van controlemechanismen in het bedrijf en anderszijds over op individuele werknemers gerichtte controles. Controlemechanismen mogen slechts voor vier opgesomde doeleinden geïnstalleerd worden: het voorkomen van ongeoorloofde en lasterlijke feiten, het beschermen van vertrouwelijke bedrijfsgegevens, de bescherming van het netwerk en ten slotte ter controle van de regels die het bedrijf heeft opgesteld omtrent het gebruik van e-mail. Verder moet de inmenging in de persoonlijke levenssfeer van de werknemers tot het minimum beperkt blijven en de werknemers moeten op voorhand individueel en collectief ingelicht worden. Op regelmatige basis moeten de controlemechanismen geëvalueerd worden in overleg met de werknemers. Controles gericht op individuele werknemers mogen in principe slechts volgens een bepaalde procedure gebeuren.

D.3.1. Archiveren van e-mail in een onderneming

Wat betekent dit nu voor de archivering van e-mail binnen een bedrijf? De C.A.O. heeft een andere impact naargelang de gekozen archiveringsstrategie: archiveert de werknemer zelf de e-mail of gebeurt dit centraal op de server?

D.3.1.1. De werknemer archiveert zelf

Deze oplossing is vanuit privacy oogpunt het minst problematisch. De werknemer selecteert zelf welke e-mails een archiefwaarde hebben en voegt ze toe aan het relevante dossier of speelt ze door aan de records manager. De werkgever stelt best duidelijke richtlijnen op over de selectie van e-mail voor het archief om zijn werknemers te helpen. De opbouw van het archief houdt geen controle in van elektronische on-line communicatiegegevens.

De werkgever kan eventueel een mechanisme opzetten dat de naleving van deze richtlijnen controleert. De regels van de C.A.O. moeten daarbij gerespecteerd worden, de werknemers moeten geïnformeerd worden en de inmenging in de persoonlijke levenssfeer moet beperkt blijven tot het minimum.

[109] Art. 3 C.A.O. nr. 81.

Indien onregelmatigheden vastgesteld worden - een werknemer gooit belangrijke zakelijke e-mail weg - moeten de richtlijnen in eerste instantie opnieuw uitgelegd worden aan de werknemer(s). Pas wanneer opnieuw gelijkaardige onregelmatigheden opduiken, mag de werkgever ingrijpen. Deze indirecte procedure vermindert de doeltreffendheid van de controle op het archiefbeleid enigszins, aangezien belangrijke zakelijke e-mail zo toch kan verdwijnen. De tussenkomst van een vertrouwenspersoon kan hier eventueel een oplossing bieden. Bij een eerste onregelmatigheid schotelt de vertrouwenspersoon de e-mail in kwestie opnieuw ter beoordeling voor aan de werknemer en verduidelijkt tegelijk de relevante bedrijfsregels. De nieuwe beslissing van de werknemer is definitief, aangezien de werkgever pas bij een volgende gelijkaardige onregelmatigheid kan optreden. De tussenkomst van de vertrouwenspersoon moet strikt vertrouwelijk blijven. Op deze manier kunnen vergissingen rechtgezet worden. De wettelijkheid van een dergelijk systeem zal afhangen van de concrete omstandigheden in de onderneming.

D.3.1.2. De archivering gebeurt centraal op de server

De werkgever kan ervoor kiezen zijn archiefbeleid zelf te implementeren. De opbouw van het archief houdt dan op zich al een vorm van controle in op de communicatie die werknemers voeren. Vandaar moeten de regels van de C.A.O al in dit stadium nageleefd worden.

De opbouw van het archief gebeurt in uitvoering van de gebruiksregels binnen de onderneming, conform art. 5 §1 4° C.A.O. nr. 81. De werknemers moeten op voorhand ingelicht worden over het archiefbeleid in al zijn aspecten, in het bijzonder over het controlebeleid, de duur en de plaats van de bewaring van gegevens en het permanente karakter van de controle[110].

Heel de regeling omtrent controle van elektronische online communicatiegegevens in twee fases houdt geen steek wanneer het gaat om de opbouw van een e-mailarchief. De werkgever die centraal vanop de server e-mail overhevelt naar het archief is niet bezig met een globale en anonieme verwerking van gegevens. Integendeel, elke e-mail bevat het e-mail adres van verzender en bestemmeling(en). De raadpleging van individuele gegevens in het archief komt neer op de individualisering van elektronische on-linecommunicatiegegevens en in principe en in principe zou de indirecte procedure gevolgd moeten worden. De gebruiksregels moeten eerst opnieuw uitgelegd worden en pas bij een volgende onregelmatigheid mag de dader geïdentificeerd worden, maar de regels werden helemaal niet overtreden en er is dus ook geen onregelmatigheid.

Eén categorie gegevens mag zonder enige procedure ingekeken worden, namelijk de gegevens waarvan het beroepsmatige karakter door de werknemer niet in twijfel wordt getrokken. De enige manier om dit te weten is aan de werknemer te vragen. Bij het raadplegen van de e-mail is het te laat, want dan zou men de gegevens eerst moeten individualiseren met de procedure om te weten te komen of men ze mag individualiseren zonder procedure. Daarom moet men de werknemer vragen de e-mail te klasseren bij het opstellen of het ontvangen ervan.

[110] Art. 7-9 C.A.O. nr. 81.

E-mail die door de werknemer als privé aangemerkt wordt, mag de werknemer niet archiveren voor verder gebruik in het bedrijf. Controleren op misbruik en eventueel individualiseren volgens de voorziene procedure kan uiteraard wel.

D.3.2. Archiveren van e-mail binnen de overheid

C.A.O. nr. 81 werd bij koninklijk besluit algemeen verbindend verklaard en is dus van toepassing voor heel de private sector in België, maar niet op de publieke sector. Een gelijkaardige tekst zou best ook uitgewerkt worden voor de publieke sector, zodat ook ambtenaren weten waar ze aan toe zijn. Zolang er geen algemene tekst is voor de overheidssector, stellen de besturen best zelf een intern document op. C.A.O. nr. 81 kan hierbij als inspiratie dienen. Bij de doelstellingen die een inmenging in het privé-leven rechtvaardigen vermeldt men best expliciet ook de naleving van de regels omtrent de openbaarheid van bestuur en de archiefwetgeving.

Minister Van Grembergen stelde reeds een omzendbrief op over dit thema toegespitst op het inzagerecht van leden van gemeenteraden, politieraden, provincieraden en de raden voor maatschappelijk welzijn met betrekking tot bestuurlijke e-mailberichten[111]. E-mailberichten vallen in principe onder de persoonlijke levenssfeer van de ambtenaar en blijven in principe vertrouwelijk[112]. Binnen de perken van de privacywet moet het inzagerecht in bestuurlijke e-mail toch gerespecteerd worden. De minister vraagt de verschillende raden en besturen concrete regels uit te werken met het proportionaliteits- en finaliteitsbeginsel uit de privacywet in het achterhoofd en geeft in zijn omzendbrief slechts wat suggesties.

E. BESLUIT

Archiveren van e-mail mag met mate. Als uitgangspunt geldt dat e-mail confidentieel is, uitzonderingen moeten gebaseerd zijn op duidelijke regels, moeten een gerechtvaardigd doel hebben en strikt noodzakelijk zijn om dit doel te bereiken.

Het archiveren van professionele e-mail is een gerechtvaardigd doel. Voor de publieke sector blijkt dit uitdrukkelijk uit de archiefwetgeving en de regels omtrent openbaarheid van bestuur. Privé e-mail daarentegen moet buiten het archief gehouden worden.

De wet op de privacy geeft het finaliteits- en proportionaliteitsbeginsel concreet vorm. Elke organisatie moet zijn e-mailbeleid hierop afstemmen, zowel ten aanzien van het personeel als ten aanzien van alle

---

[111] Omzendbrief BA 2002/10 van 28 juni 2002 (B.S. 29 juli 2002).

[112] De minister baseert zich, volgens ons ten onrechte, op het briefgeheim en zwijgt over het telecommunicatie-geheim.

derden. De privé-sector kan zich daarnaast oriënteren aan de C.AO. nr. 81 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens. Binnen de overheidssector worden ook best concrete afspraken gemaakt over het archiveren van e-mail.

Het minst problematisch is de selectie van te archiveren e-mails volledig over te laten aan de eindgebruiker[113]. De organisatie kan de eindgebruiker bijstaan door richtlijnen op te stellen over de selectiecriteria en voorbeelden te geven. De naleving van deze richtlijnen mag door de organisatie centraal gecontroleerd worden, met respect voor de persoonlijke levenssfeer uiteraard.

Wil men als organisatie het archiefbeleid centraal implementeren dan moet men de selectieprocedure erg zorgvuldig ontwerpen, zodat enkel professionele e-mail in het archief terechtkomt. Het onderscheid maken tussen professionele en persoonlijke e-mail is een teer punt. De eindgebruiker is het best geplaatst om deze scheiding door te voeren, hetzij door verschillende e-mail adressen te gebruiken, hetzij door de berichten die hij stuurt en ontvangt te classificeren. Zonder de medewerking van de eindgebruiker is het erg moeilijk het onderscheid correct te maken. Privé e-mail inkijken gaat te ver en filters zijn niet waterdicht. De records manager zal bij het op eigen houtje scheiden van e-mail bijna automatisch de privacy schenden.

De ontwikkeling van het archiefbeleid vergt van de records manager een delicate evenwichtsoefening tussen enerzijds de rechtmatige belangen van de eindgebruiker en anderzijds de rechtmatige belangen van de organisatie en in het geval van de overheid daarbovenop het publieke belang.

[113] Zelfs de meest strenge interpretatie van het telecommunicatiegeheim laat dit toe, aangezien deelnemers aan het gesprek vrij mogen beschikken over 'wettig gemaakte opnames' van telecommunicatie.

VI. ARCHIVEREN VAN E-MAILS: DE OPTIES

A. DE UITDAGINGEN VOOR DE ARCHIVARIS

Ondanks het feit dat het gebruik van e-mail al volop is ingeburgerd, zijn er nog maar weinig instellingen met een coherent archiveringssysteem voor hun ontvangen of uitgaande e-mailberichten. De administratie wordt aan zijn lot overgelaten, archiveert volgens eigen goeddunken en is zich vaak niet bewust van de archiefwaarde van e-mails. Dit leidt tot parallelle circuits waarbij dezelfde informatie in papieren en digitale vorm aanwezig is of tot onrechtmatige vernietigingen. Een duidelijk en coherent archiveringssysteem voor de e-mails van de organisatie vermijdt dit in de toekomst en leidt er toe dat e-mails met archiefwaarde worden gearchiveerd en raadpleegbaar zijn. E-mail-archivering is een uitdaging, want het confronteert archivarissen met de belangrijkste vraagstukken die met het beheer van digitale archiefdocumenten gepaard gaan.

Het archiveren van e-mails vraagt een serieuze inspanning op het vlak van intellectueel archiefbeheer. Het e-mailsysteem is immers een informatiesysteem dat losstaat van het archiveringssysteem voor (digitale) archiefdocumenten. Omwille van toegankelijkheid en interpreteerbaarheid wordt het e-mailbericht op de één of andere manier aan de structuur en de context van het archief gerelateerd. De band tussen het e-mailbericht, de bijlagen, de andere samenhangende stukken en het werkproces moet op één of andere manier in het archiveringssysteem worden opgenomen. Immers, voor redenen van latere raadpleging en interpretatie moet duidelijk zijn in welk werkproces de e-mails werden gecreëerd of gebruikt en wat hun relatie is tot de andere archiefdocumenten. Het belang van de archivalische band mag niet onderschat worden: de archivalische band geeft een document de status van archiefstuk[114]. De archivering van de context is ook belangrijk om de authenticiteit en betrouwbaarheid van archiefbescheiden aan te tonen. Terwijl de archivalische band in een papieren omgeving overwegend op een fysieke wijze wordt vastgelegd, kan dit bij digitale archiefdocumenten enkel op een logische of intellectuele manier gebeuren[115]. De e-mailcontext is niet in het verstuurde of ontvangen bericht zelf aanwezig. Afzender en geadresseerde kennen de context wel en moeten die op de één of andere manier expliciet vastleggen. Zowel bij papieren als digitale archivering zal op het tijdstip van de creatie of de ontvangst de nodige contextuele gegevens aan de berichten toegevoegd worden. De courante e-mailsystemen beschikken standaard echter niet over de functionaliteit om de relatie met het werkproces en andere documenten vast te leggen, zodat hiervoor ad hoc oplossingen nodig zijn.

Aan de andere kant moet men bij de uitwerking van een archiveringsstrategie ook rekening houden met de technologische infrastructuur waarover de organisatie beschikt. Binnen de ene organisatie zal het mogelijk zijn om een bijkomende computertoepassing voor e-mailarchivering in te schakelen, in de andere zal men enkel over een standaard e-mailpakket beschikken. In dit laatste geval zal het er op aan

---

[114] L. DURANTI, "The archival bond", p. 216.

[115] T. THOMASSEN, "Een korte introductie in de archivistiek", p. 14-16.

komen om de e-mailarchivering binnen het bestaande e-mailprogramma in te passen. Ook binnen dezelfde organisatie is de technologische infrastructuur niet noodzakelijk overal dezelfde kunnen er zich verschillende situaties voor doen. Niet elke dienst bijvoorbeeld zal een documentbeheerssysteem of hetzelfde e-mailpakket gebruiken.

Het archiveren van e-mails is ook een schoolvoorbeeld van het *records-continuum* principe[116]. Vanwege de nood aan selectie en expliciete contextualisering kan men niet anders dan vanaf de creatie of de ontvangst actief met het archiveringsproces te starten. De archivaris is verplicht om als het ware als records manager op te treden en met het archiveringssysteem in de administratie te duiken.

Gelet op de omvang aan e-mails verloopt de archivering best zoveel mogelijk automatisch en wordt de menselijke inbreng tot een minimum beperkt. Aan de andere kant moet er ook selectie mogelijk zijn, want het bewaren van e-mails zonder enige archiefwaarde is onnodig.

Tenslotte moeten e-mails op een duurzame wijze worden gearchiveerd, waarbij eveneens de authenticiteit en integriteit is gegarandeerd. De e-mails met archiefwaarde worden met zoveel mogelijk garanties inzake leesbaarheid op lange termijn opgeslagen.

De uitdagingen voor archivarissen zijn dus legio. Het archiveringssysteem voor e-mails moet voor elk van deze uitdagingen een oplossing bieden.

B. KWALITEITSVEREISTEN VOOR HET ARCHIVEREN VAN E-MAILS

De archivering van e-mailberichten moet aan de volgende vereisten voldoen:

- de gearchiveerde e-mails zijn volledig. De inhoud, de structuur en de context van de e-mailberichten wordt gearchiveerd[117]. De presentatie en het gedrag[118] van e-mails wordt niet gearchiveerd. E-mails hebben geen vaste verschijningsvorm, want hun opmaak is mede afhankelijk van de gebruikte e-mail clientprogrammatuur. E-mails zijn na verzending of ontvangst statisch.
  - ► *inhoud*: naast het eigenlijke bericht, bevat de gearchiveerde e-mail ook alle essentiële transmissiegegevens. Dit zijn de naam van de afzender, de naam van de

[116] S. FLYNN, "The records continuum model in context and its implications for Archival Practice", in *Journal of the Society of Archivists*, vol. 22, nr. 1, 2001, p. 79-93.

[117] *Guide for managing electronic records from an archival perspective*, p. 10; K. THIBODEAU, *Preservation and migration of electronic records: the state of the issue*. De structuur van een archiefdocument is de relatie tussen de elementen waaruit het bestaat. De context van een archiefdocument is de archivalische band met de gerelateerde stukken.
http://www.archives.gov/electronic_records_archives/papers/preservation_and_migration.html

[118] Gedrag in de zin van "functionaliteiten" bijvoorbeeld het dynamisch ophalen van gegevens of het genereren van een index.

geadresseerde(n), het onderwerp, de ontvangers van de kopie(ën), de datum en het tijdstip van verzending en de datum en tijdstip van ontvangst. Ontbreekt één van deze gegevens, dan kunnen we niet spreken van een volledig en authentiek bericht. De bijlage wordt ook bij de inhoud van de e-mail gerekend.

- ► *structuur*: de onderlinge relatie tussen de elementen die een e-mail vormen, wordt gearchiveerd. De vaste elementen van een e-mail zijn een header, een body met het eigenlijke bericht en de eventuele bijlage(n).
- ► *context*: de e-mails worden binnen hun context gearchiveerd. Een verwijzing naar het werkproces waarbinnen het bericht werd gecreëerd, ontvangen of gebruikt, wordt samen met de e-mail gearchiveerd. Ook de band tussen e-mail en gerelateerde documenten zoals de bijlagen moet bij latere raadpleging duidelijk zijn[119].

- ❑ de inhoud van het bericht, de transmissie- en de contextuele gegevens van elke gearchiveerde e-mail zijn (onlosmakelijk) met elkaar verbonden. Al deze elementen en de band die hen verbindt, moet bij digitale archivering op een duurzame en platformonafhankelijke wijze gearchiveerd worden.
- ❑ de e-mails met archiefwaarde worden in het archiveringssysteem van de organisatie opgenomen. Het archiveringssysteem is beveiligd en voorkomt dat gearchiveerde e-mails gewijzigd of gemanipuleerd kunnen worden. Het archiveringssysteem helpt mee de authenticiteit en de betrouwbaarheid van gearchiveerde e-mails te verzekeren. De gearchiveerde e-mails zijn echt en onvervalst.
- ❑ de gearchiveerde e-mails zijn raadpleegbaar. Bij digitale archivering worden de e-mails in een geschikt archiveringsformaat bewaard. Het bestandsformaat is duurzaam, leesbaar en gebruikersvriendelijk.
- ❑ de gearchiveerde e-mails zijn geordend en toegankelijk. Het (computer)systeem dat de gearchiveerde e-mails beheert, moet ze kunnen terugvinden op basis van de inhoud, de headergegevens en de context.

C. DE ARCHIVERINGSSTRATEGIEËN VOOR E-MAILS

Er zijn verschillende manieren waarop men e-mails kan archiveren. Hier worden de mogelijke archiveringsstrategieën één voor één besproken. Elke strategie wordt getoetst aan de vooropgestelde kwaliteitsvereisten.

[119] De verplichte vermelding van deze gegevens is onder meer opgenomen in de Amerikaanse DoD 5015.2 standaard (zie C2.2.3: Filing Electronic Mail Messages).

C.1. Hard Copy

In de *hard copy* piste worden e-mails afgedrukt en op papier, microfilm of microfiche bewaard. Eigenlijk betekent dit dat men e-mails niet in hun primaire vorm archiveert, maar vervangt door afdrukken op papier of microfilm/fiche. Met het vervangen van de originele digitale e-mails gaan een aantal voordelen van digitale informatie verloren: er is meer opslagruimte in het archiefmagazijn vereist, de e-mails zijn slechts op één lokatie raadpleegbaar, simultaan gebruik is niet mogelijk en de gearchiveerde e-mails kunnen niet snel doorzocht, gesorteerd of geïndexeerd worden.

Toch is de afdrukoptie niet zonder belang voor het archiveren van e-mails. De wijdverspreide commerciële e-mailsystemen voldoen immers niet aan de archivistische noden. Digitale archivering van e-mails vraagt in veel gevallen een gecustomiseerde oplossing, die soms technisch complex is, waar soms geen off-the-shelf producten voor bruikbaar zijn en waar dan ook een groot prijskaartje aan vasthangt. De National Archivist van de Verenigde Staten argumenteerde in de GRS20-zaak dat het gedecentraliseerd bijhouden van e-mails in persoonlijke postbussen of op verschillende werkstations zeker niet beantwoordt aan de eisen inzake bewaring in geordende en toegankelijke staat. Bij *hard copy* archivering kan gemakkelijker aan deze eisen worden voldaan zodat opname in een papieren archiveringssysteem te verantwoorden is. Archivering op papier heeft onrechtstreeks nog een aantal bijkomende voordelen: het bericht wordt naar een meer duurzame drager overgezet en het probleem van het bestandsformaat en de leesbaarheid op lange termijn wordt vermeden.

Het voornaamste argument voor een *hard copy* archivering is de afwezigheid van een doeltreffend digitaal archiveringssysteem. Beter de berichten op papier te archiveren in een goede, geordende en toegankelijke staat, dan digitaal te archiveren in slechte staat[120]. In administraties met een overwegend papieren dossiervorming vermijdt men zo ook een hybride informatiesysteem. Men moet wel oppassen met dit laatste argument. Informatie is alsmaar meer in digitale vorm aanwezig. De keuze voor papieren e-mailarchivering zou dus wel eens kunnen betekenen dat er op termijn toch een papieren én digitaal informatiesysteem ontstaat. Eigenlijk dringt een archiveringssysteem voor digitale archiefdocumenten zich op en kan papieren archivering enkel als korte termijnoplossing dienen. Van zodra dit voor handen is, zou men naar digitale e-mailarchivering moeten overschakelen. In afwachting van de ontwikkeling en implementatie van een digitaal archiveringsproces kunnen e-mails op papier worden gearchiveerd.

Een goede archivering van e-mails op papier is relatief gemakkelijk te realiseren. Net zoals bij de klassieke briefwisseling kunnen de nodige registratiegegevens op de afdruk worden geplaatst. Door de afgedrukte e-mail in de map betreffende het onderwerp of de zaak op te bergen, bewaart men het bericht samen met de andere gerelateerde stukken die binnen dezelfde context werden gevormd. Op die manier wordt de archivalische band grotendeels fysiek vastgelegd. Dit laatste gaat echter niet op wanneer de gearchiveerde e-mails als één doorlopende serie op microfilm worden geplaatst. De bijlagen bij e-mails

[120] In die zin is bijvoorbeeld in Australië, in de Verenigde Staten en in Nederland de archivering van e-mails op papier een geldige optie (Australië: http://www.naa.gov.au/recordkeeping/er/elec_messages/policy.html; VS: GRS20-zaak; Nederland: P. HORSMAN, *Archivering van elektronische post. Methoden, meningen en alternatieven*, p. 15).

kan men afdrukken en in dezelfde dossier- of onderwerpsmap opbergen, al zijn niet alle types bijlagen afdrukbaar (geluid, bewegend beeld). Tot op de dag van vandaag hanteren veel archiefinstellingen deze archiveringsstrategie. Zij hebben nog geen archiveringssysteem voor digitale archiefdocumenten en passen dus hun archiveringssysteem voor papieren archiefdocumenten op e-mails toe.

Vooraleer er met de toepassing van deze archiveringsstrategie kan worden gestart, zijn er nog enkele aandachtspunten. Vooreerst is er de kwaliteitsvereiste dat de afgedrukte e-mail alle inhoudelijke en transmissiegegevens moet bevatten. De courante e-mailsystemen bevatten voor het afdrukken van e-mails een aantal standaardopmaakstijlen. In deze opmaakstijlen is vastgelegd welke headergegevens worden afgedrukt. Niet alle vereiste velden worden automatisch mee afgedrukt. In het algemeen worden enkel de gegevens afgedrukt die op het scherm staan. Zo wordt in de memostijl van MS Outlook de datum en tijd van ontvangst niet standaard afgedrukt. Dit gebeurt wel in de tabelstijl, maar hier ontbreekt dan de datum en tijd van verzending. Nochtans zijn deze data en tijdstippen voor elke e-mail in het e-mailsysteem aanwezig. De afdrukstijl of het formulier voor ontvangen e-mails moet dus eventueel worden aangepast (zie verder)[121]. Zo voorkomt men dat bij het afdrukken transmissiegegevens verloren gaan en bijgevolg de volledigheid en de authenticiteit van e-mails als archiefdocumenten in gevaar komt. De gegevens met betrekking tot de archivalische band kan men op dezelfde manier aan het e-mailbericht toevoegen of men kan die met de hand en stempel op de afdruk aanbrengen. Ten tweede houdt *hard copy* archivering in dat de digitale e-mails vernietigd (moeten) worden. Hiervoor is de goedkeuring van de Algemene Rijksarchivaris of diens gemachtigde vereist. Vernietigt men de digitale e-mails niet, dan ontstaat er een parallel circuit voor dezelfde informatie. De digitale e-mails worden niet in een gecontroleerde omgeving bewaard. Ze kunnen dan toch niet meer gebruikt worden als verantwoordings- of bewijsstuk. Om dit mogelijk te maken moet er ten derde ook een duidelijke procedure zijn voor het afdrukken van de e-mails zodat ook de authenticiteit en integriteit van de berichten op papier of op microfilm verzekerd is.

[121] In de Verenigde Staten heeft een rechtbank in 1993 geoordeeld dat de papieren afdruk van een e-mail niet zomaar identiek is aan de digitale versie (*Armstrong vs Executive Office of the President*, ook de *PROFS*-zaak genoemd). De afdruk bevat immers minder gegevens dan de e-mail die binnen het e-mailsysteem wordt bewaard. Het bewaren van de tekst van het bericht was niet voldoende. Ook de transmissiegegevens en de bijlagen maken deel uit van een e-mailbericht. De Amerikaanse overheid reageerde op deze uitspraak door de administraties op te leggen dat afdrukken ook alle transmissiegegevens moeten bevatten (http://www.gcn.com/archives/gcn/1998/February9/gellm.htm). In het arrest van het Hof van Beroep van 6 augustus 1999 argumenteerde de rechtzoekende *Public Citizin* ondermeer dat papieren afdrukken van e-mails geen identieke vervangingen van de originele digitale versies zijn. In de GRS20-standaard, d.i. een algemene selectielijst van het NARA, werd onder nr. 14 nochtans expliciet vastgelegd dat men bij archivering op papier of microfilm ervoor moet zorgen dat deze gegevens mee buiten het e-mailsysteem worden getransporteerd. Alhoewel het NARA en het Hof van Beroep van oordeel zijn dat digitale archivering primeert op papieren archivering, was men in het arrest van 6 augustus 1999 van oordeel dat digitale archivering niet kan verplicht worden en dat adequate papieren versies de digitale originelen mogen vervangen. Zie eerder: deel III B, p. 13 e.v.

Filip Boudrez

Van:	Filip Boudrez
Verzonden:	donderdag 30 augustus 2001 10:31
Aan:	Willem Vanneste
CC:	David
Onderwerp:	E-mailarchivering
Ontvangen:	30/08/01 10:31:03

Afbeelding 2: Voorbeeld van een e-mailheader op papier waarbij alle transmissiegegevens automatisch in de hoofding worden afgedrukt.

C.2. Digitaal archiveren

C.2.1. Archiveren van op de mailserver of door de betrokken administratieve medewerker?

Technisch is het perfect mogelijk om van op de mailserver een kopie te archiveren van elke ontvangen en uitgaande mail, al dan niet samen met de verstuurde bijlagen. Hierdoor zou geen enkele e-mail aan archivering ontsnappen en hoeft de administratie geen actieve rol in het archiveringsproces te spelen. In de internationale literatuur wordt deze aanpak als een mogelijke archiveringsstrategie voorgesteld[122]. Peter Horsman vraagt zich in zijn richtinggevende brochure ook af of een dergelijke verzameling e-mails in de toekomst niet van grote waarde kan zijn. Immers, zo'n verzameling e-mails kan informatie bevatten die niet in andere documenten voorkomt of kan een beeld geven van het gebruik van dit medium wat dan weer van belang is om het handelen van een organisatie te reconstrueren[123]. Het rechtstreeks archiveren vanop de mailserver stoot echter op een aantal juridische en archivistische belemmeringen.Vanuit archivistisch standpunt kan men opmerken dat een bulkverzameling veel e-mails zal bevatten die helemaal geen archiefstuk zijn of archiefwaarde hebben, wat vragen doet oprijzen over de functie en de kwaliteit van de gearchiveerde e-mails. Selectie dringt zich bovendien ook op vanwege de toegankelijkheid en de hoge kostprijs. Ook voor het bewaren van de context zou deze optie moeilijkheden opleveren. Aan verzonden e-mails zou men wel een verwijzing naar de context kunnen toevoegen, maar ontvangen e-mails zouden zonder archivalische band worden gearchiveerd.

Vanuit juridisch[124] en archivistisch standpunt zijn de opties bij digitaal archiveren dus eigenlijk beperkt tot archivering mits tussenkomst van de afzender of de geadresseerde. Dit biedt aan de ene kant een meerwaarde. De afzender of geadresseerde zijn het best vertrouwd met de inhoud of de functie van berichten. Beide factoren zijn belangrijk om e-mails met de status van archiefstuk te onderscheiden van

---

[122] Bijvoorbeeld STATE RECORDS NEW SOUTH WALES, *Managing the message-Guidelines on managing electronic messages as records. 5. Capturing electronic messages into recordkeeping systems.* In de V.S. werd naar aanleiding van de PROFS- en GRS20zaak duidelijk gemaakt dat werknemers geen privacyrechten kunnen laten gelden wanneer ze e-mails verzenden of ontvangen via het e-mailsysteem dat door hun werkgever ter beschikking wordt gesteld.

[123] P. HORSMAN, *Archiveren van elektronische post*, p. 12.

[124] Zie hiervoor het stuk over het telecommunicatiegeheim in deel VI DPrivacyreglementering van dit rapport.

e-mails zonder deze status[125]. Van de afzender of geadresseerde wordt ook verwacht dat hij de e-mail in zijn context plaatst en de archivalische band toekent. De keerzijde is natuurlijk dat het slagen van het archiveringsproces afhankelijk zal zijn van de toepassing in de praktijk door de administratieve medewerkers. Coaching en vorming van de administratie zullen belangrijk zijn om de archivering te doen slagen.

C.2.2. Digitaal archiveren binnen het e-mailsysteem

Om een goede digitale archivering mogelijk te maken, is de eerste vereiste dat e-mails worden gearchiveerd in de context waarbinnen ze werden verstuurd, ontvangen of gebruikt. Zonder die context zijn e-mails niet toegankelijk of interpreteerbaar. In een digitale omgeving kan men dit via twee pistes bereiken: het bewaren van de e-mails binnen een logisch geordende mappenstructuur en het toevoegen van een dossiernummer of classificatiecode aan elke e-mail.

Het bewaren van computerbestanden binnen een logisch geordende mappenstructuur is de geijkte methode om digitale archiefdocumenten die bij elkaar horen te groeperen en context aan de e-mails toe te voegen. De courante e-mailpakketten laten toe dat e-mails in on line en off line mappen worden bijgehouden. De ontvangen en verstuurde e-mails worden normaliter in de persoonlijke postbus op de mailserver bewaard. De persoonlijke postbus staat in een afgeschermde map op de mailserverschijf waarvan de toegang beschermd wordt door een gebruikersaccount en een paswoord. Vanuit de persoonlijke postbus kan de ontvangen of verstuurde e-mail naar on line en off line mappen worden versleept. De on line mappen staan op de harde schijf van de mailserver en zijn toegankelijk voor iedereen die de nodige toegangsrechten heeft. Zo kan er een openbare map gemaakt worden voor een hele dienst of voor de medewerkers die aan hetzelfde project werken. De off line mappen (bijvoorbeeld MS Outlook; *.pst-bestanden, Lotus Notes: *.nsf-bestanden, Eudora: POP mail folders *.mbx) staan best op een harde schijf die geen deel uitmaakt van de e-mailserver. Dit is bij voorkeur geen lokale harde schijf, maar een serverschijf waarvoor veiligheidsmaatregelen bestaan (o.a. back-up). Vanuit het e-mailclientprogramma kunnen e-mails in on line of off line mappen worden beheerd. De on line en off line mappen bevatten naast de berichten ook de bijlagen. De mappen kunnen bijgevolg al snel een grote bestandsomvang bereiken. Veel netwerkbeheerders stellen een maximale bestandsomvang voor de on line mappen in. E-mailgebruikers dienen dus regelmatig hun on line postbus op te ruimen. Om de mailserver niet overmatig te belasten, wordt de voorkeur gegeven aan het zoveel mogelijk off line bewaren van e-mails met archiefwaarde. Alle mappen, e-mails en bijlagen die in één off line map worden geplaatst, worden in één computerbestand opgeslagen.

Net zoals op een harde schijf kan er binnen de on line of off line map een structuur worden aangebracht waarbinnen de e-mails met archiefwaarde worden opgeborgen. Het uitwerken van een mappenstructuur laat een ordening per dossier of onderwerp toe. Aangezien het archief als functie heeft de werkprocessen te ondersteunen, te documenteren en te bewijzen, wordt deze doelstelling het best gerealiseerd wanneer

[125] In een poging om hiervoor een oplossing te bieden, werd in een oude versie van de Australische richtlijnen gesuggereerd dat de afzender vastlegde of de e-mail al dan niet een archiefstuk is vooraleer hij het bericht verzond. Dit moest selectie door het computersysteem op basis van de status van de berichten toelaten. Dit is echter alleen maar bruikbaar voor de afzender en biedt de geadresseerde geen oplossing.

de mappenstructuur een weerspiegeling is van de werkprocessen en meer bepaald van de functies, taken en activiteiten van de archiefvormer. De mappenstructuur wordt dan ook bij voorkeur hiërarchisch van algemeen naar bijzonder ingedeeld. De algemene functies van de archiefvormer vormen de hoofdtakken. Voor elke taak of activiteit wordt een submap binnen die hoofdtakken gemaakt. Desgewenst kunnen deze mappen nog verder opgesplitst worden per subtaak of subactiviteit. Op het laagste niveau wordt voor elk onderwerp of elk dossier een map voorzien waarin de e-mails worden geplaatst. Op die manier weerspiegelt de mappenstructuur de logische structuur van het archief en de context van de archiefbestanddelen. Door codes vooraan de mapnamen te plaatsen kan een hiërarchie worden aangebracht en kan de structuur worden opgebouwd volgens de archivistische principes (intern → extern, algemeen → bijzonder) Een dergelijke indeling heeft veel weg van een archiefschema of ordeningsplan en integreert de archiefdocumenten met het werkproces waarbinnen ze werden gecreëerd of ontvangen. In veel gevallen zal de mappenindeling ook overeenstemmen met de ordening van het papieren archief, wat dan weer belangrijk is voor de integratie van papieren en digitale informatiestroom.

Afbeelding 3: Een mappenstructuur voor een dienst Burgerlijke Stand & Bevolking bij een gemeentebestuur binnen het e-mailsysteem. Voor de hele dienst wordt binnen één openbare map ('E-mailarchief') een hiërarchische mappenstructuur uitgewerkt. De functies van de dienst vormen de hoofdmappen. De hoofdmappen zijn verder opgesplitst in taken en activiteiten. Op het laagste niveau wordt voor elk dossier of onderwerp een aparte map gemaakt.

Het eindresultaat moet een logische en heldere mappenstructuur zijn die elke e-mail al voor een stuk in zijn archiefcontext situeert. Verwarring, onduidelijkheid of meerdere mappen voor hetzelfde bericht moeten ten alle prijze worden vermeden. Voor het welslagen van de archiveringsprocedure is het belangrijk dat de gebruikers weten in welke map ze e-mails en bijlagen plaatsen en later terugvinden. Zo niet blijven e-mails in persoonlijke postbussen of mappen bewaard. Voor het uitwerken en toepassen van

een goede mappenstructuur worden best binnen de organisatie een aantal regels gehanteerd.[126] Deze kunnen betrekking hebben op[127]:

- de mapnamen: de mapnamen moeten uniek, duidelijk en semantisch (zelfbeschrijvend) zijn. Afkortingen moeten voor iedereen van de organisatie duidelijk zijn.
- het aanmaken van nieuwe mappen: de hoofdstructuur ligt bij voorkeur vast en wordt enkel door de systeembeheerder in overleg met de records manager of archivaris aangepast. Administratieve medewerkers maken enkel mappen aan op dossier of onderwerpsniveau.
- het afstemmen van de mappenstructuren op de gedeelde serverschijf, binnen het e-mailsysteem en eventueel het papieren klassement: een gebruik van een identieke mappenstructuur maakt een integratie van de gerelateerde archiefdocumenten mogelijk.

De e-mails kunnen ook aan hun context gekoppeld worden door een dossiernummer of classificatiecode aan de e-mails toe te voegen. Door dit gegeven aan een e-mail toe te kennen, legt men de archivalische band met de context vast. In de standaard e-mailsystemen is hiervoor niet de nodige plaats voorzien[128]. Courante e-mailsystemen zoals MS Outlook of Lotus Notes beschikken wel over de functionaliteit om dit mogelijk te maken. Het aanpassen van de sjablonen voor ontvangen en uitgaande e-mails lijkt hiervoor de aangewezen optie. In de sjablonen worden de nodige velden voorzien waarin de geadresseerde en/of de afzender een verwijzing naar de context en de gerelateerde documenten kan toevoegen. Men kan extra velden voorzien in de standaard e-mailheader of de body zodanig dat al in elke uitgaande of ontvangen e-mail de nodige plaats wordt voorzien. Op die manier wordt het *encapsulation*principe toegepast en worden de metadata die de archivalische band weergeven een onlosmakelijk onderdeel van het e-mailbericht. Dit betekent op zijn beurt dat e-mails later ook op basis van dit gegeven teruggevonden kunnen worden (bijvoorbeeld een dossiernummer). De sjablonen voor ontvangen én uitgaande e-mails worden aangepast.

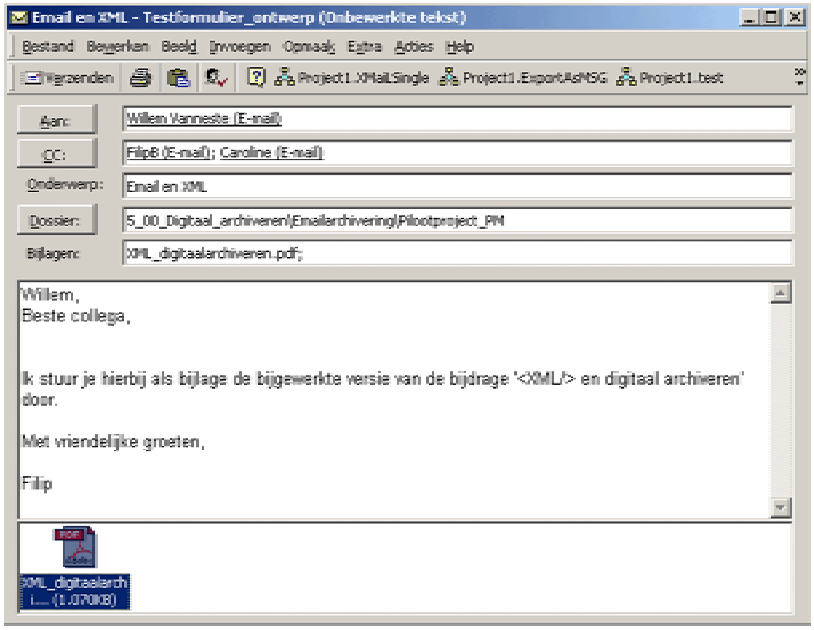
Vervolgens installeert men deze sjablonen op de mailserver zodat ze voor iedereen van de organisatie beschikbaar zijn. Een centrale ter beschikkingstelling is belangrijk voor de schaalbaarheid van de archiveringsoplossing. Het handigste is dat iedereen binnen de organisatie met dezelfde sjablonen werkt. Zo verzekert men er zich van dat iedereen goed gestructureerde e-mails creëert die naar hun context verwijzen. De sjablonen zullen dat mee bewerkstelligen. Zo kan men de e-mails van de organisatie overigens een huisstijl geven. Het invullen van de extra velden zal een automatisme worden zoals het invullen van de gegevens ‘Ons kenmerk’ en ‘Uw kenmerk’ in de klassieke briefhoofding.

---

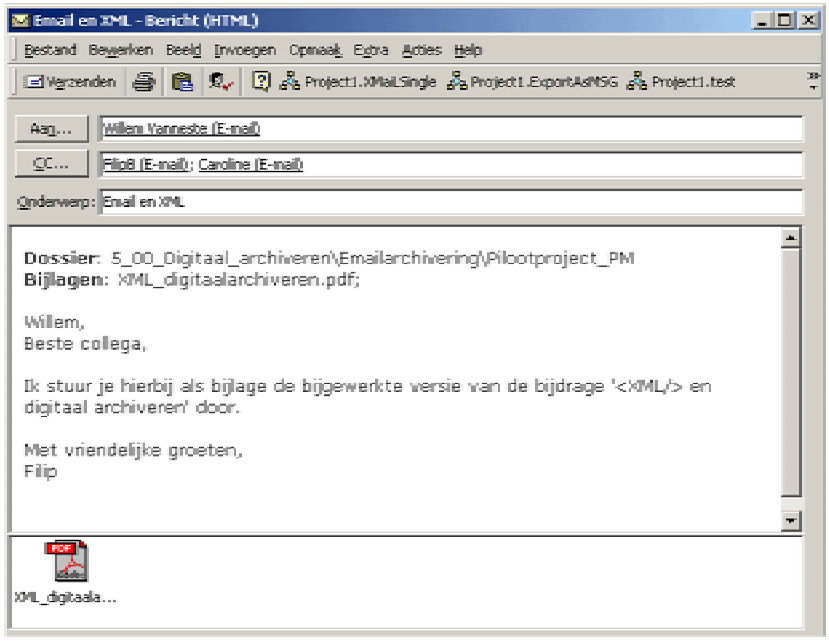
[126] Op de website van het stadsarchief Antwerpen is een richtlijn voor het uitwerken van een mappenstructuur beschikbaar (http://stadsarchief.antwerpen.be → Werking archieftoezicht → Archiefbeheer → Digitale Archivering).

[127] Digitaal ArchiVeren. rIchtlijn & aDvies, nr. 3 bevat praktische richtlijnen en aanbevelingen voor het uitwerken van mappenstructuren.

[128] Een aantal auteurs stelden voor om eventueel dit gegeven in het vak ‘onderwerp’ te noteren. Dit zou enkel werken bij de archivering van uitgaande e-mails. Voor de archivering van ingekomen e-mails zou dit betekenen dat de oorspronkelijke inhoud van het veld ‘onderwerp’ wordt gewijzigd.



Afbeelding 4: De nodige extra velden worden in de header voorzien.



Afbeelding 5: In het sjabloon van de body worden standaard twee velden voorzien voor het contextualiseren van de e-mail. Bij het openen van concept worden deze drie velden automatisch in de body vermeld.

De e-mails met archiefwaarde worden dus binnen het e-mailsysteem aan hun context gekoppeld. De clientmailprogramma's beschikken over een aantal zoek- en sorteermogelijkheden zodat gearchiveerde e-mails op een geautomatiseerde wijze kunnen teruggevonden worden. Daarnaast kan er ook gebladerd worden in de mappenstructuur.

Het permanent bewaren van de e-mails binnen het e-mailsysteem heeft echter een aantal belangrijke nadelen waardoor deze optie niet volstaat voor archivering op lange termijn.

- e-mailsystemen zijn in de eerste plaats informatiesystemen en geen document- of archiefbeheerssystemen. E-mailsystemen beschikken niet over de essentiële

functionaliteiten voor document- en archiefbeheer (o.a. beschrijving van de context, integratie met het bedrijfsproces, vernietiging, enzovoort). Bovendien staan ze buiten de systemen die deze functies wel vervullen. Net zoals de andere archiefdocumenten (bijvoorbeeld brieven of faxen) moeten de e-mails in het archiefbeheerssysteem worden opgenomen.

- e-mailsystemen zijn niet ontworpen om alle bij elkaar horende documenten te groeperen. Binnen het e-mailsysteem worden enkel de berichten en hun bijlagen met betrekking tot één zaak bijgehouden die via mail worden verzonden. Andere stukken die niet via het e-mailsysteem werden verstuurd of ontvangen, maken geen deel uit van het dossier binnen het e-mailsysteem. De dossiervormingsmogelijkheden binnen e-mailsystemen zijn beperkt tot de stukken die via mail worden verstuurd.
- de e-mails worden niet in een toegankelijke staat in de archivistische betekenis bewaard. De toegang tot postbussen en openbare mappen is beschermd door gebruikersnamen, bijhorende paswoorden en toegangsrechten. E-mails in mappen met beperkte toegangen of op lokale harde schijven, zijn van weinig nut voor de archiefvormer en latere onderzoekers. De gearchiveerde e-mails zijn verspreid over verschillende mappen en computerbestanden.
- de e-mailsystemen zijn niet geschikt om grote hoeveelheden e-mails te bewaren en te centraliseren. Het langdurig bewaren van e-mails binnen het e-mailsysteem levert opslagproblemen op en hypothekeert de performantie van de mailservers.
- de e-mails en de mappen worden in een software afhankelijk formaat vastgelegd. De e-mails kunnen slechts met de overeenstemmende computerapplicatie worden bekeken. Bij elke vervanging of versieverhoging van het e-mailsysteem bestaat de kans dat alle gearchiveerde e-mails omgezet moeten worden. De 'archiverings'-functies voorzien in een aantal e-mailsystemen (opslag in mini-databanken of gecomprimeerde bestanden) zijn evenmin digitaal duurzaam en bovendien niet betrouwbaar[129]. Deze functionaliteiten dienen in de eerste plaats de mailservers te ontlasten.

Kortom, archivering binnen e-mailsystemen voldoet niet aan de kwaliteitsvereisten. De e-mails met archiefwaarde mag men hoogstens tijdelijk binnen het e-mailsysteem bijhouden. De courante e-mailsystemen schieten te kort als definitieve bewaaromgeving voor archiefdocumenten. Hetzelfde geldt voor back-ups van de postbussen op de mailserver. Dit neemt niet weg dat ze wel een belangrijke functie kunnen vervullen binnen het globale archiveringsproces. Aangepaste sjablonen voor uitgaande en ontvangen e-mails helpen de creatie van goed gestructureerde e-mails en laten toe dat de afzender of geadresseerde op het tijdstip van verzending of ontvangst een verwijzing naar de context in de vorm van een dossiernummer of classificatiecode toevoegt. Het onderbrengen van e-mails met archiefwaarde in de overeenstemmende mappen gebeurt best al binnen het e-mailsysteem. Het archiveringsproces mag hier niet ophouden, maar de e-mails met archiefwaarde moeten buiten het e-mailsysteem worden geëxporteerd en in een archiveringssysteem worden opgenomen. Al naargelang de voorkeur of de mogelijkheden van een organisatie, kan dit een papieren of een digitaal archiveringssysteem zijn.

[129] Pst-bestanden zijn vaak corrupt.

C.2.3. Digitaal archiveren buiten het e-mailsysteem

Kiest men voor een digitale archiveringsstrategie, dan moeten de e-mails buiten het e-mailsysteem geëxporteerd worden en naar een geschikt archiveringsformaat worden omgezet. De courante e-mailsystemen beschikken standaard over een functionaliteit om e-mails buiten het e-mailsysteem te plaatsen. In MS Outlook wordt deze functionaliteit 'archiveren' genoemd, in Lotus Notes 'exporteren'. Men kan de e-mails per map of afzonderlijk exporteren. Alle e-mails binnen één map naar hetzelfde computerbestand wegschrijven is echter niet aangewezen vanwege de identificatie van de archiefstukken en hun toegankelijkheid. Men archiveert de e-mails beter als afzonderlijke bestanden. De e-mailclientprogramma's bieden standaard de keuze tussen een aantal bestandsformaten: het clientprogramma eigen bestandsformaat (bijvoorbeeld *.msg van MS Outlook, *.vew van Novell Groupwise), Excel, Acces, HTML, RTF, Lotus 1-2-3 of Unicode. De eerste vier formaten zijn helemaal niet geschikt als archiveringsformaat, want migraties zullen heel frequent nodig zijn. Unicode biedt meer garanties inzake leesbaarheid op lange termijn. Onze voorkeur gaat echter uit naar XML (eXtensible Markup Language).

XML-bestanden zijn even duurzaam als Unicodebestanden en zijn uitermate geschikt om de inhoud en de structuur van een e-mail te archiveren[130]. XML benadert het best het ideaal van *Persistent Object Preservation*. De *Persistent Object Preservation* methode is de object-georiënteerde archiveringsstrategie die het Amerikaanse San Diego Supercomputer Center momenteel in samenwerking met het NARA aan het ontwikkelen is voor een heel digitaal archief. Aan de basis van deze opslagmethode ligt de opvatting dat bestaande opties voor de archivering van digitale archiefdocumenten (bewaren van de originele hard- en software, migratie, emulatie) allemaal hun zwakke punten hebben en dus op lange termijn ontoereikend of onefficiënt zijn. De onderzoekers willen computerbestanden zodanig opslagen dat ze gedurende 300 tot 400 jaar (!) leesbaar blijven en geen wijzigingen moeten ondergaan. Om hieraan te kunnen voldoen moeten de gearchiveerde bestanden aan volgende eisen voldoen[131]:

- opslag in een technologisch neutraal bestandsformaat.
- raadpleegbaar op toekomstige heterogene platformen zonder conversie of migratie. Op die manier worden mogelijke bedreigingen voor schending van de authenticiteit en betrouwbaarheid tot een minimum herleid.
- uitbreidbaar en aanpasbaar aan toekomstige noden.

---

[130] Zie F. BOUDREZ, *<XML/> en digitaal archiveren*, Antwerpen, 2002 voor meer informatie over de toepassingsmogelijkheden van XML voor archiefdiensten.

[131] Op de website van het NARA (http://www.archives.gov) zijn diverse artikelen en presentaties van K. THIBODEAU over de *Persistent Object Preservation* methode beschikbaar (*Building the Electronic Records Management Information Infrastructure*; *Persistent Object Preservation: Advanced Computing Infrastructure for Digital Preservation; Preservation and migration of electronic records: the state of the issue*). De onderzoekers van het San Diego Supercomputer Center publiceerden artikels over deze opslagmethode in D-Lib Magazine (*Collection-Based Persistent Digital Archives*, deel 1 en 2) en op de website van hun instelling. Bij de vooropgezette levensduur van 300 tot 400 jaar moet men wel de bedenking maken dat XML-bestanden maar bruikbaar zijn zolang computers Unicode-karakters kunnen inlezen. Men gaat er echter vanuit dat Unicode de basis voor nieuwe karaktertabellen blijft. Wanneer XML in onbruik raakt of zijn de facto status van standaard verliest, hoeven de XML-bestanden niet omgezet te worden maar meent men dat een aangepaste interface (bijvoorbeeld webbrowser) volstaat om de bestanden te lezen.

- zelfbeschrijvend.

De *Persistent Object Preservation* methode vertrekt vanuit een selectie van de elementen die het archiefdocument vormen. De elementen die een computerbestand de status van archiefstuk geven, worden gearchiveerd. Algemeen is men het over eens dat de inhoud, de structuur en de context van een archiefbescheid essentieel zijn. In een aantal gevallen moet de verschijningsvorm en het gedrag daar aan worden toegevoegd, maar dit is niet het geval voor het archiveren van e-mails.

De digitale archiefdocumenten worden als XML-bestanden opgeslagen. XML is immers platformonafhankelijk, (semi-) zelfbeschrijvend, uitbreidbaar, leesbaar mits een minimale tussenkomst van hard- en software en gestandaardiseerd. De structuur van de archiefdocumenten of van een archiefbestand wordt in de DTD's of XML Schemas vastgelegd. Hierin worden de geselecteerde elementen en hun onderlinge relatie formeel gedefinieerd[132]. Door de XML-bestanden te *parsen* controleert men de geldigheid van de XML-bestandsstructuur tegenover de formele structuur in de DTD of XML Schema. Dit is perfect toepasbaar op e-mails. Binnen dezelfde organisatie wordt best een vaste structuur voor de e-mails vastgelegd (cfr. gebruik van sjablonen). Hierdoor hoeft er maar in één omzettingsprocedure naar XML-bestanden worden voorzien.

De *Internet Engineering Task Force (IETF)* werkt momenteel aan een standaard XML-structuur en bijhorende DTD voor e-mails (zgn. 'Email+XML bericht formaat')[133]. Een e-mail als XML-bestand is in deze standaard in de eerste plaats bedoeld als uitwisselingsformaat tussen verschillende programma's van e-mails en gegevens over de e-mails. De e-mail als XML-bestand zou ook rechtstreeks als dusdanig kunnen opgeslagen worden. Hierdoor worden omzettingsoperaties vermeden.

Door de headergegevens van een e-mail als afzonderlijke elementen in de XML-bestanden op te nemen, kunnen e-mails gemakkelijk op basis hiervan worden opgezocht of gesorteerd. Een tweede voordeel is dat bij opname in het document- of archiefbeheerssysteem van de archiefdienst de metadata uit de header kunnen worden overgenomen. Op die manier is automatische beschrijving van de e-mails mogelijk. Voor het opzoeken van e-mails zijn dan meerdere mogelijkheden: gestructureerd zoeken op de inhoud van de e-mailheaders, full-text zoekopdrachten op de inhoud van de berichten of een combinatie van beide.

De meeste e-mailberichten bevatten geen opmaakgegevens en kunnen dus als gewoon plat tekstbestand worden opgeslagen. Een aantal mailclientprogramma's laten het opmaken van een e-mailbericht toe. Hiervoor wordt gebruik gemaakt van HTML-pagina's en stylesheets. Clientprogramma's die dit niet ondersteunen, krijgen het e-mailbericht als plat tekstbestand te zien. Mocht de archivering van de verschijningsvorm belangrijk zijn dan kan er aan het XML-bestand een stylesheet worden gekoppeld.

---

[132] Deze archiveringsmethode werd door het stadsarchief Antwerpen al toegepast bij de digitale archivering van de digitale kiezersregisters van 1994, 1995, 1999 en 2000 en van gegevens uit het bevolkingsregister. Meer informatie over deze cases is beschikbaar op de DAVID website. Op voorhand werd bepaald welke elementen al dan niet werden gearchiveerd. De digitale archiefdocumenten werden als XML-bestanden bewaard en hun structuur werd in bijhorende DTD's vastgelegd.

[133] http://web.archive.org/web/20011224185049/http://www.ietf.org/internet-drafts/draft-klyne-message-rfc822-xml-02.txt. Deze draft maakt een onderscheid tussen de e-mailheader en het e-mailbericht. Dit laatste kan een tekstbericht als onderdeel van de e-mail of een bijlage zijn.

Een andere optie zijn *Multi-Valent Documents* waarbij een bitmap van het origineel document als een laag aan het computerbestand wordt toegevoegd.

PDF (Portable Document Format) van Adobe is een tweede bestandsformaat dat in aanmerking komt als archiveringsformaat voor e-mails. In plaats van op papier af te drukken wordt het e-mailbericht naar een PDF-bestand buiten het e-mailsysteem weggeschreven. Het gebruik van het PDF-formaat heeft als voordeel dat de migratie eenvoudig en snel kan worden gerealiseerd. Men dient enkel te beschikken over het Acrobat-softwarepakket, dat off-the-shelf kan worden geïnstalleerd. Via Acrobat Distiller of Acrobat Writer kunnen de e-mails als afzonderlijke PDF-bestanden buiten het e-mailsysteem worden geplaatst. De laatste PDF-versie (1.4) maakt een gestructureerde gegevensopslag mogelijk. PDF heeft vanuit archiveringsstandpunt de algemene nadelen dat specifieke software nodig is voor raadpleging, de status heeft van producentgebonden de facto standaard en de opslag van karakters niet op Unicode is gebaseerd. Momenteel wordt gewerkt aan het vastleggen van een PDF subset voor archiverings- en lange termijn bewaringsdoeleinden als standaard (PDF/A)[134]. HTML (HyperText Markup Language) zou als een derde mogelijkheid kunnen beschouwd worden, al is de archivering van puur tekstuele documenten in HTML niet gebruikelijk. HTML heeft wel de status van officiële standaard.

Bij de keuze van het archiveringsformaat moet men de voor- en nadelen van elk formaat goed tegen elkaar afwegen. In vergelijking met XML hebben e-mails opgeslagen als PDF- of HTML-bestanden een aantal belangrijke nadelen. In PDF- of HTML-bestanden zijn enkel full text zoekopdrachten mogelijk. Gearchiveerde e-mails opgeslagen als XML-bestanden zijn ook opzoekbaar of sorteerbaar op basis van hun gestructureerde headergegevens. Het archiefbeheerssysteem kan de inhoud voor zijn metadatavelden voor e-mails niet automatisch van PDF- of HTML-bestanden overnemen. De structuur van de e-mails in PDF of HTML wordt evenmin op een formele wijze vastgelegd. XML heeft als belangrijkste nadeel dat het nog niet geïmplementeerd is in de recentste versies van de courante e-mailsystemen. Voor een export als XML-bestanden moet het e-mailsysteem dus aangepast worden. Opslag als PDF- of HTML-document is gemakkelijker te realiseren. HTML-opslag is doorgaans standaard voorzien in de e-mailsystemen, voor een bewaring als PDF-bestanden dient men enkel over het Acrobatprogramma van Adobe te beschikken. In ieder geval zijn zowel XML, PDF als HTML een betere optie dan e-mails in het bestandsformaat van het e-mailsysteem bewaren.

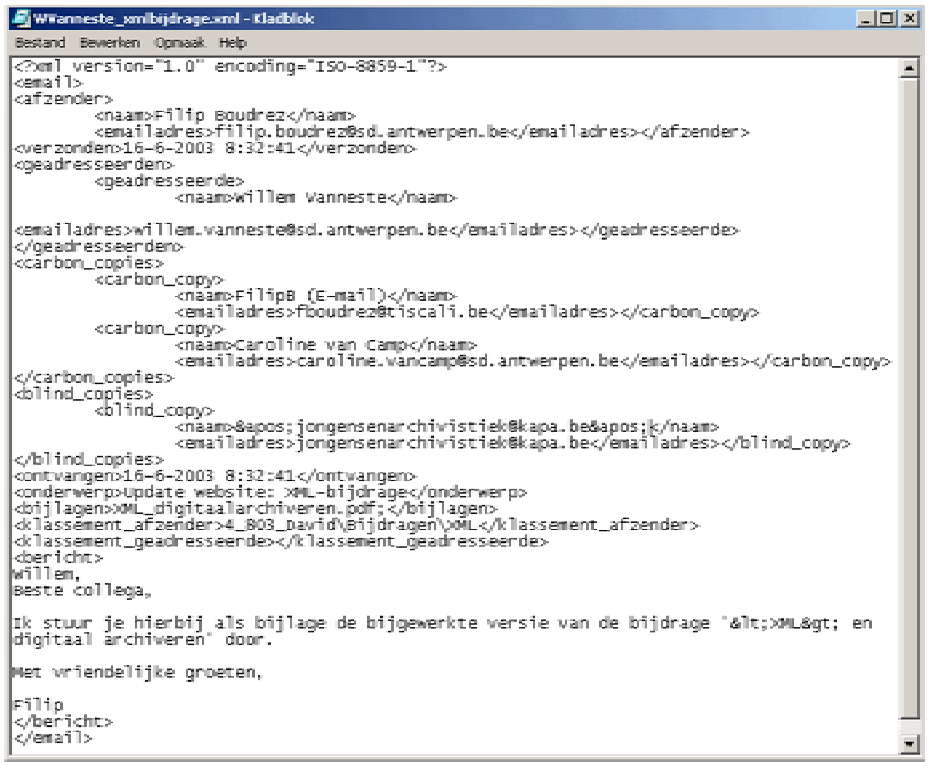
Na de export buiten het e-mailsysteem en de omzetting naar een geschikt archiveringsformaat, wordt er best een controlefase voorzien. Men moet er zich van verzekeren dat de e-mails tijdens de omzettingsoperatie niet gewijzigd zijn of dat er geen informatie verloren is gegaan. In de meest optimale situatie zou elke gemigreerde e-mail gecontroleerd worden. Het is echter de vraag of dit mogelijk zal zijn. Anders zullen logbestanden van de omzettingsprocedure of steekproeven moeten volstaan. In het geval van XML zou men de bestanden kunnen *parsen* tegen een DTD, of beter een XML Schema.[135] In

[134] Voor meer informatie over PDF/A: F. BOUDREZ, *Standaarden voor digitale archiefdocumenten* (http://www.antwerpen.be/david → standaarden)

[135] Een moeilijkheid is wel het vinden van een geschikte opslagplaats voor de DTD of het XML Schema. Elke e-mail opgeslagen als XML-bestand kan in principe naar dezelfde DTD of hetzelfde XML Schema verwijzen. Alleen moet men de passende locatie voor dit bestand vinden. Deze locatie moet overal toegankelijk zijn en mag eigenlijk nooit veranderen. Anders moet in elke e-mailheader de padaanduiding worden gewijzigd. Het Internet lijkt op het eerste zicht de meest aangewezen oplossing (bijvoorbeeld onmiddellijk achter de URL van

beide gevallen wordt de structuur van de XML-bestanden op zijn geldigheid getest. Een XML Schema laat ook een controle van het soort en aantal karakters toe. Een echte inhoudelijke controle is dit echter niet. *Parsing* zal bijvoorbeeld de inhoudsomwisseling van de velden 'afzender' en 'geadresseerde' niet aan het licht brengen. Zoals elke migratie zal ook de export buiten het e-mailsysteem en de omzetting naar een archiveringsformaat gedocumenteerd moeten worden.

Bij het exporteren dient men er ook voor te waken dat alle e-mailgegevens mee buiten het systeem worden geplaatst. Wanneer men met aangepast e-mailheaders werkt, dient men doorgaans expliciet op te geven dat de toegevoegde velden mee worden afgedrukt of geëxporteerd. Een bijzondere aandacht moet uitgaan naar de adresgegevens van afzender en geadresseerde (naam + e-mailadres) en eventueel de samenstelling van verzendlijsten.



Afbeelding 6: Een e-mail opgeslagen als een XML-bestand. De header- of contextuele gegevens van de e-mail worden als afzonderlijke elementen opgeslagen. De gearchiveerde e-mails kunnen later op de inhoud van deze velden worden opgezocht. Deze e-mail is aan een stylesheet gekoppeld. Hoe de e-mail in een webbrowser gepresenteerd wordt, ziet u in afbeelding 11. De structuur van deze e-mail is uitgebreider dan de standaardstructuur in e-mailclientprogramma's. De uitbreiding van de structuur is een gevolg van de aanpassing van de headers in de e-mailformulieren of -sjablonen (zie verder).

Wanneer de e-mails buiten het e-mailsysteem worden geplaatst, krijgen ze ook een bestandsnaam. Dit is doorgaans standaard de inhoud van het veld 'onderwerp', maar dit kan gewijzigd worden. Hierbij moet men ervoor zorgen dat de e-mails een unieke bestandsnaam krijgen. Computerbestanden met dezelfde naam die in dezelfde map terechtkomen overschrijven elkaar. Een unieke bestandsnaam is ook belangrijk om de bijlage naar de overeenstemmende e-mail te laten verwijzen.

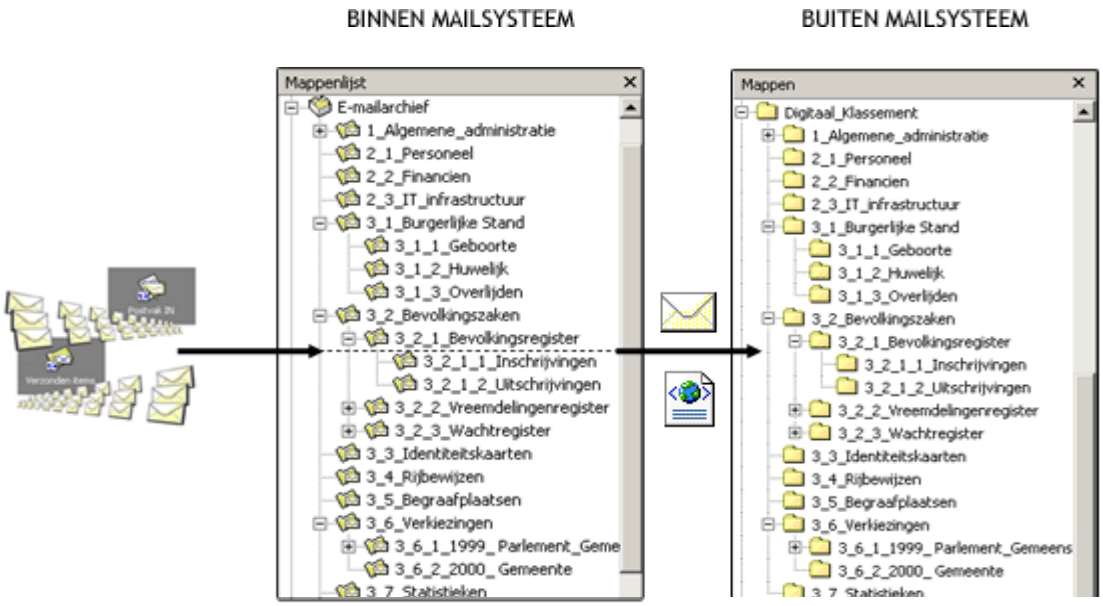
De e-mails worden buiten het e-mailsysteem bewaard in een mappenstructuur die een onderdeel is van het archiveringssysteem. Deze mappenstructuur is bij voorkeur identiek aan die binnen het e-mailsysteem. De geëxporteerde e-mails komen als afzonderlijke bestanden in dezelfde map te staan als

---

de eigen organisatie). Andere opties zijn het gezamenlijk bewaren van DTD of XML Schema in elke map (geen pathaanduiding nodig, enkel een bestandsnaam) of een interne DTD.

binnen het e-mailsysteem. De indeling in mappen maakt dossiervorming en integratie met de gerelateerde digitale archiefdocumenten mogelijk. Daarom is het van belang om de mappenstructuur binnen het e-mailsysteem af te stemmen op de globale mappenstructuur van de gedeelde werkruimte op de serverschijf. Op het moment van de export van e-mails en bijlagen buiten het e-mailsysteem vindt dan de integratie met de andere digitale documenten met betrekking tot dezelfde zaak of hetzelfde onderwerp plaats. Zo kunnen alle archiefdocumenten die bij elkaar horen gegroepeerd worden: de interne digitale documenten die op de gedeelde werkruimte stonden, de e-mails en de ontvangen bijlagen. Het resultaat is dan een elektronisch dossier.

Ten laatste op het ogenblik van de export buiten het e-mailsysteem worden e-mail en bijlage van elkaar gescheiden. In de metadata van beide digitale documenten moet naar elkaar worden verwezen, zodat de band behouden blijft. Voor de bijlagen wordt dan de archiveringsstrategie gevolgd die het best bij dat type document past. Aangezien de bijlagen veelal de meeste schijfruimte op de mailserver in beslag nemen, kan het ook aangewezen zijn om deze bestanden onmiddellijk na ontvangst buiten het e-mailsysteem te plaatsen. De bijlagen die men zelf verstuurt, maken doorgaans al deel uit van de gedeelde schijfruimte en staan al in de corresponderende map.



Afbeelding 7: De mappenstructuur binnen en buiten het e-mailsysteem worden best op elkaar afgestemd. Bij export buiten het e- mailsysteem komen de e-mails in dezelfde mappenstructuur terecht zodat alle gerelateerde digitale documenten gegroepeerd worden. De bijlagen kunnen onmiddellijk na ontvangst in de externe map geplaatst worden of samen met de e-mails geëxporteerd worden.

De groepering van e-mails, bijlagen en andere gerelateerde archiefdocumenten in mappen biedt de mogelijkheid tot selectie op dossier- of onderwerpsniveau na het verstrijken van de administratieve bewaartermijn.

Om onrechtmatige wijzigingen, vernietigingen of verplaatsingen te voorkomen moet de mappenstructuur buiten het e-mailsysteem beveiligd zijn. De beveiliging moet niet alleen zorgen voor een toegangscontrole en bescherming tegen onrechtmatige manipulaties, maar ook voor een bescherming tegen virussen. Op de meeste mailservers zal wel een antiviruspakket actief zijn, maar alvorens de e-mails en hun bijlagen aan het digitaal archief toe te voegen is het aangewezen om voor alle zekerheid nog een nieuwe controle op virussen uit te voeren.

De opname van de mappenstructuur in het document- of archiefbeheerssysteem is aangewezen. De laatste stap in het archiveringsproces is dan de vernietiging van de e-mailversies binnen het e-mailsysteem. De omgezette e-mails zijn voortaan de authentieke versies.

C.2.4. Archivering buiten het e-mailsysteem: gevolgen voor het authenticiteitsbewijs

Uit de beschrijving en evaluatie van de mogelijke archiveringsstrategieën blijkt duidelijk dat de e-mailberichten het best in een digitale vorm buiten het e-mailsysteem worden bewaard. De e-mails worden afgedrukt en in de respectieve dossiers opgeborgen (*hard copy*), of ze worden in een geschikt archiveringsformaat (XML, PDF, HTML) buiten het e-mailsysteem in een mappenstructuur opgeslagen. Beide opties hebben belangrijke gevolgen voor het verzekeren van de authenticiteit en betrouwbaarheid van de gearchiveerde e-mail. In een digitale omgeving kan men de digitale handtekening gebruiken om een handtekening in juridische zin te plaatsen. Een (digitale) handtekening heeft drie functies: identificatie van de afzender, verificatie of de boodschap van het verstuurde en ontvangen bericht wel identiek is en de afzender kan niet ontkennen dat hij het bericht heeft verstuurd. De digitale handtekening kan enkel maar gebruikt worden als alternatief voor de handgeschreven handtekening op voorwaarde dat men op gelijk welk moment na de archivering in staat is om de verificatie opnieuw uit te voeren. De geadresseerde kan die verificatie wel uitvoeren op het moment van ontvangst, maar na archivering is dit op basis van de originele digitale handtekening niet meer mogelijk. In de *hard copy* optie is de digitale versie van het bericht niet meer voor handen. Bij digitale archivering is het e-mailbericht naar een ander bestandsformaat gemigreerd en voegt de geadresseerde op zijn minst ook registratiegegevens toe. De bitreeksen - waarop de digitale handtekening van de afzender is berekend - worden dus danig gewijzigd zodat de digitale handtekening van de afzender de gearchiveerde e-mail niet meer kan valideren. Hoe de authenticiteit en integriteit dan wel wordt gegarandeerd, is nog geen uitgemaakte zaak. Hierover dient nog nader onderzoek te gebeuren.

VII. E-mailarchivering in de praktijk

A. INLEIDING

Elke instelling kiest de archiveringsstrategie voor e-mails die het best bij haar organisatie, informatica-infrastructuur en e-mailbeleid past. De hierboven beschreven opties kunnen op uiteenlopende manieren en in verschillende combinaties worden toegepast. Er zijn diverse voorbeelden voor handen. De *National Archives* van Nieuw Zeeland geeft de voorkeur aan de archivering van e-mails op papier[136]. De provincie Zeeland drukt de e-mails op papier af en bewaart haar e-mails niet digitaal[137]. In de Amerikaanse GRS20-standaard werden aanvankelijk de twee opties naast elkaar gebruikt. E-mails met archiefwaarde op korte termijn blijven binnen het e-mailsysteem bewaard. E-mails met een archiefwaarde op lange termijn werden afgedrukt en bij de dossiers gevoegd. In zijn huidige versie laat de GRS20-standaard digitale en *hard copy* (papier, microfiche) archivering toe[138]. De nationale dienst voor statistiek in Canada laat haar medewerkers de e-mails met archiefwaarde naar een centrale postbus sturen, waar records managers ze klasseren, linken en archiveren. Het Nederlandse Ministerie van Binnenlandse Zaken past binnenkort een gelijkaardige aanpak toe.

Bij wijze van voorbeeld wordt hieronder een *best practice* uitgewerkt. De doelstelling is een digitale archiveringsstrategie die aan de vooropgestelde kwaliteitsvereisten voldoet. Digitale archivering wordt hier verkozen boven afdrukken op papier omdat e-mails in primaire vorm digitaal zijn en vanwege de voordelen die aan digitaal archiveren verbonden zijn: geautomatiseerde zoek-, sorteer- en indexeringsopdrachten, centraal beheer en decentrale terbeschikkingstelling, simultaan gebruik, enzovoort

De technologische infrastructuur is een belangrijke factor waarmee men bij het uittekenen van een archiveringsstrategie moet rekening houden. De beschikbare computerprogrammatuur zal in belangrijke mate bepalen hoe het archiveringsproces er uit zal zien. Niet elke Vlaamse instelling of dienst beschikt over de mogelijkheid om zijn computerprogrammatuur aan de archiveringsstrategie aan te passen. Er werd met dit gegeven rekening gehouden door bij het uitwerken van deze modeloplossing een oplossing te zoeken die zoveel mogelijk binnen wijdverspreide en verschillende computertoepassingen toepasbaar is.

---

[136] http://www.archives.govt.nz/statutory_regulatory/er_policy/chapter_5_frame.html

[137] J. JONKERS, "Zeeland gaat digitaal: studiedag over elektronisch documentmanagement", in: *Od*, september 2001, nr. 9, p. 349.

[138] http://www.archives.gov/records_management/ardor/grs20.html

De *best practice* bestaat uit het archiveren van de e-mails als afzonderlijke XML-bestanden in een mappenstructuur buiten het e-mailsysteem en binnen het archief- of documentbeheerssysteem van de organisatie[139]. Het archiveringsproces verloopt in verschillende stappen:

- STAP 1: identificatie van de archiefstukken en registratie van contextuele en transmissiegegevens.
- STAP 2: groeperen van e-mails en bijlagen per zaak of onderwerp in een mappenstructuur.
- STAP 3: omzetting naar geschikte archiveringsformaten en opname in het archiefbeheerssysteem.

B. BEST PRACTICE

B.1. Stap 1: Identificatie van de archiefstukken en registratie van contextuele en transmissiegegevens

In een eerste stap wordt ervoor gezorgd dat alle e-mails met de status van archiefstuk expliciet alle transmissiegegevens en een verwijzing naar de context bevatten. Zoals hierboven al werd aangehaald, dient dit ook geverifieerd te worden wanneer de *hard copy* piste wordt gevolgd.

Vanwege juridische en archivistische redenen bepaalt de verzender of ontvanger van e-mails zelf welke e-mails worden gearchiveerd en welke niet. Maw, het komt aan de administratieve medewerker toe om te beslissen welke e-mails belangrijk zijn voor het werkproces van zijn organisatie. Van de e-mails met de status van archiefstuk wordt verwacht dat ze worden voorzien van de een klassementscode en dat ze naar de overeenstemmende map worden verplaatst. Het welslagen van de archiveringsprocedure is afhankelijk van de zorgvuldigheid van de administratieve medewerker. Dit houdt natuurlijk een aantal risico's in: onrechtmatige vernietigingen, het onvoldoende navolgen van de archiveringsprocedure, het aanleggen van een eigen "archiefje" buiten het officiële archiveringssysteem van de organisatie, enzovoort. Training en opleiding zijn bijgevolg onmisbaar zodat de archiefvormers zelf een onderscheid kunnen maken tussen e-mails met de status van archiefstuk en e-mails zonder die status. De (administratieve) medewerkers zullen in de praktijk voortdurend een selectie uitvoeren en het moet dan ook duidelijk zijn welke e-mails bijgehouden worden, en welke niet. Een deel van de e-mails wordt onmiddellijk vernietigd. Dit zijn in de eerste plaats de e-mails zonder de status van archiefstuk. Voorbeelden hiervan zijn persoonlijke e-mails of louter informatieve e-mails waarvan de inhoud zich niet richt op de archiefvormer. In deze fase worden best ook afspraken gemaakt over het bijhouden van interne algemeen verspreide e-mails door de afzender of de geadresseerde. E-mails die dienen als algemene kennisgevingen binnen de eigen organisatie worden best door de afzender bewaard. De richtlijn zegt best ook iets over de zogenaamde "reply-mails". Hier heeft men de keuze tussen het archiveren van de laatste mail (die ook alle voorgaande bevat) of het archiveren van elke e-mail als een afzonderlijk e-mail. Bij de implementatie van de archiveringsstrategie besteedt men best voldoende aandacht aan dit onderscheid.

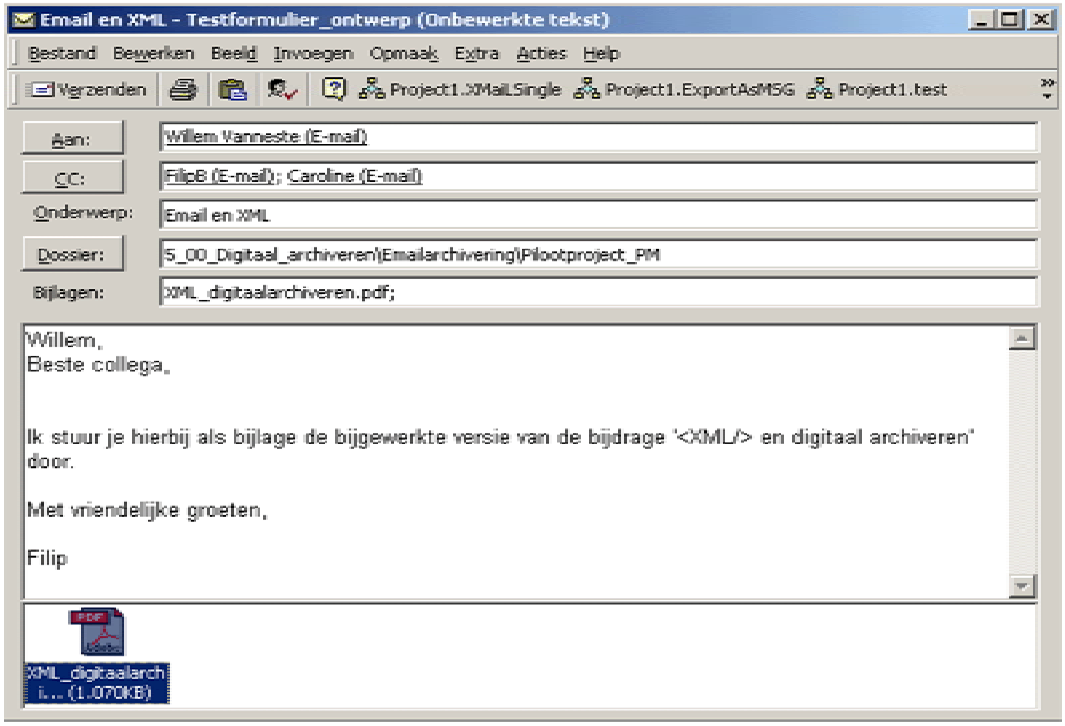
[139] Deze *best practice* zal in de praktijk worden gezet door het stadsarchief Antwerpen bij het archiveren van de e-mails van de Antwerpse stadsadministratie.

Een organisatie archiveert zowel uitgaande als ontvangende e-mails. Beide soorten e-mails moeten alle transmissiegegevens en een verwijzing naar de context bevatten. Om dit te bekomen, past men best de e-mailsjablonen aan. In de meeste e-mailsystemen wordt voor de e-mails in de mappen 'Postvak In' (ontvangen berichten) en 'Verzonden Items' (uitgaande berichten) hetzelfde sjabloon gebruikt, namelijk dat van de ontvangen e-mails[140]. In dit sjabloon ontbreekt standaard meestal de datum en het tijdstip van ontvangst. De andere transmissiegegevens (naam afzender, naam geadresseerde, ontvangers van de kopie(ën), onderwerp, datum en tijdstip van verzending) maken in de courante e-mailsystemen al deel uit van het sjabloon van ontvangen e-mails. In wijdverspreide e-mailclientprogramma's zoals MS Outlook en Lotus Notes is het mogelijk om de sjablonen aan te passen. Door een veld voor de datum en het tijdstip van ontvangst aan de e-mailheader toe te voegen, verzekert men zich ervan dat dit gegeven mee deel uitmaakt van de gearchiveerde e-mail. Bij het toevoegen van een dergelijk nieuw veld aan de e-mailheader moet men soms expliciet opgeven dat het veld mee wordt afgedrukt of geëxporteerd.

In de standaardsjablonen is evenmin plaats voorzien om een verwijzing naar de context van het e-mailbericht toe te voegen. Die context heeft betrekking op het werkproces en de gerelateerde documenten. Naar de samenhang met een bepaald werkproces kan het best door middel van een klassementscode of een dossiernummer worden verwezen. In het sjabloon voor uitgaande e-mails wordt een veld voorzien waarin de afzender zijn klassementsgegevens noteert[141]. In onderstaand voorbeeld is dit het veld 'Dossier'. De inhoud van dit veld verwijst naar de zaak of het dossier waarbinnen de e-mail moet gesitueerd worden. Voor de verwijzing naar de bijlagen bij het e-mailbericht wordt een gelijkaardige oplossing toegepast. In dit zelfde sjabloon worden hiervoor een bijkomend veldtoegevoegd: 'Bijlage'. In dit veld worden de bestandsnamen van de bijlagen geregistreerd. Op die manier wordt er in het e-mailbericht een koppeling met de bijlagen opgenomen. Tijdens het archiveringsproces worden berichten en bijlagen immers op een bepaald moment van elkaar gescheiden en door expliciet vast te leggen welke bijlagen bij het bericht werden verstuurd, wordt de relatie behouden.

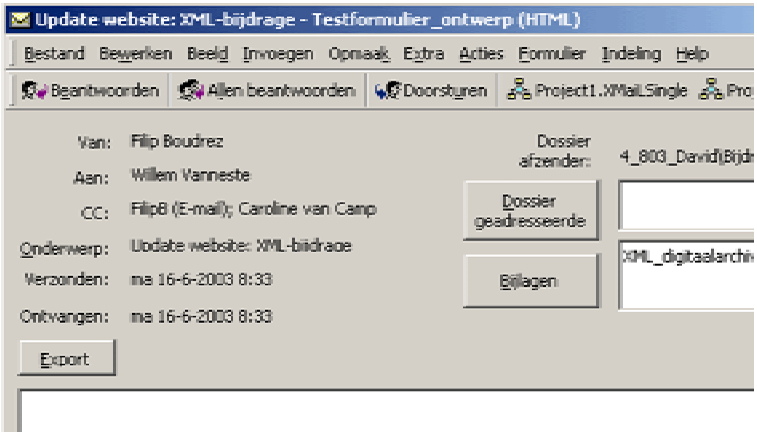
[140] De courante clientmailprogramma's kunnen zo ingesteld worden dat ze een automatisch een kopie van elke uitgaande e-mail in de map verzonden (items) bewaren.

[141] Het zou ook mogelijk zijn om de klassementsgegevens in het veld 'Onderwerp' in te vullen. Voor de geadresseerden zou dit echter inhouden dat ze e-mails ontvangen met een nietszeggende onderwerpsomschrijving. Bovendien moet er toch plaats worden voorzien voor de klassementskenmerken van de geadresseerde.



Afbeelding 8: Het aangepaste formulier voor de uitgaande e-mails. De gebruiker kan in de header opgeven In het veld 'Dossier' hoeveel en welke bijlagen hij bij de e-mail heeft gevoegd. kan hij de klassementsgegevens van zijn uitgaande e-mail noteren.

Het aanpassen van het sjabloon voor uitgaande e-mails is eigenlijk enkel van belang om de afzender toe te laten de nodige contextuele informatie expliciet vast te leggen. Zijn uitgaande e-mails komen immers in het sjabloon van ontvangen e-mails in de map 'Verzonden items' terecht. Het sjabloon voor ontvangen e-mails moet dus ook aangepast worden. Hiervoor wordt dezelfde werkmethode toegepast. In de e-mailheader worden een aantal bijkomende velden opgenomen. Een eerste extra gegeven is de datum en het tijdstip van ontvangst. Ook de velden 'Dossier afzender', 'Bijlagen' en worden in de header opgenomen. Dit is van belang voor de archivering van uitgaande e-mails. Het veld 'Dossier afzender' is read-only. De twee velden met betrekking tot de bijlagen kunnen indien nodig aangepast worden. Immers, het gebeurt niet zelden dat een bijlage vergeten wordt of dat er al een bijlage met die bestandsnaam is. Tenslotte wordt deze header uitgebreid met een veld waarin de geadresseerde zijn eigen klassementsgegevens kan invullen: 'Dossier geadresseerde' Bij de archivering van uitgaande e-mails blijft dit veld leeg.



Afbeelding 9: Om de archivering van ingekomen en uitgaande e-mails met de nodige transmissie-en contextuele gegevens mogelijk te maken, werd de standaardheader voor ingekomen e-mails uitgebreid met de volgende velden: de datum en het tijdstip ontvangst, de klassementsgegevens van de afzender en geadresseerde, en de bijlagen

Voor de archivering van uitgaande e-mails behoeft de e-mail zoals die in de map 'Verzonden items' terecht komt geen aanpassing. De afzender heeft in de header voor uitgaande berichten al de verwijzing naar de context en de samenhang met eventuele bijlagen vastgelegd. Bij de archivering van ontvangen e-mails moet de geadresseerde in het veld 'Dossier geadresseerde' nog de archivalische band door middel van een klassementskenmerk vastleggen. Vervolgens slaat hij de e-mail op. De inhoud van dit veld wordt hierdoor aan de ontvangen e-mail toegevoegd.

Door de e-mailsjablonen aan te passen, voorziet men de mogelijkheid dat de archiefvormer onmiddellijk bij verzending of ontvangst contextuele metadata aan de e-mail toekent. De archiefvormer kent de context van het document het best, en is bijgevolg de meest geschikte persoon om de contextuele gegevens aan de archiefdocumenten toe te voegen. Als dit niet onmiddellijk bij ontvangst of verzending gebeurt, is de kans groot dat dit in de toekomst niet meer op een goede manier wordt uitgevoerd. Bovendien kan men dan vragen stellen bij de kwaliteit of haalbaarheid van dergelijke retro-actieve operaties. Door deze functionaliteit te voorzien binnen de bestaande e-mailprogrammatuur kan de gebruiker binnen zijn vertrouwde omgeving blijven werken.

Het aanpassen van het e-mailsjabloon, en meer bepaald de header, biedt ook de mogelijkheid om een bepaald documentmodel met vaste structuur op te leggen vanaf het moment van creatie. Dit biedt de garantie dat er goed gestructureerde ('archiveerbare') documenten worden gecreëerd, waardoor latere omzettingen naar een geschikt archiveringsformaat gemakkelijker zijn. Het toevoegen van een verwijzing naar de bijlagen en context heeft het voordeel dat deze essentiële informatie een onlosmakelijk onderdeel van het e-mailbericht wordt. Door de transmissiegegevens expliciet in de e-mailheaders op te nemen, vindt er automatisch een registratie van deze gegevens plaats. Dit is een toepassing van het *encapsulation*principe waarbij de nodige metadata in het digitale archiefdocument zelf worden opgenomen. Deze gegevens kunnen op die manier perfect binnen een bestaand e-mailsysteem worden beheerd. De bijkomende velden kunnen in theorie zowel in de header als in de body worden opgenomen, maar de voorkeur gaat naar de e-mailheader uit. Het gaat niet alleen om een soort metadata, maar het toevoegen van deze gegevens aan de header maakt een duidelijk gestructureerde opslag mogelijk. Gearchiveerde e-mails kunnen dan later op basis van deze gegevens worden opgezocht of gesorteerd. De transmissie- en contextuele gegevens worden later als onderdeel van het e-mailbericht naar XML omgezet. Hierdoor worden deze gegevens meteen ook op een duurzame, platformonafhankelijke en raadpleegbare wijze gearchiveerd.

B.2. Stap 2: Groeperen van e-mails en bijlagen per zaak of onderwerp in een mappenstructuur

De e-mails met archiefwaarde worden uit de mappen ‘Postvak In’ en ‘Verzonden items’ verplaatst naar de map waarin de e-mails met betrekking tot die zaak of dat onderwerp worden bewaard.

De e-mails met archiefwaarde worden verplaatst naar de overeenstemmende onderwerps- of dossiersmap. Alle e-mails betreffende hetzelfde onderwerp of dezelfde zaak komen zo samen te staan. De mappenstructuur is belangrijk vanwege het situeren van de e-mails binnen het werkproces en de koppeling met gerelateerde documenten. Die gerelateerde documenten zijn niet alleen de bijlagen bij de e-mails, maar ook andere papieren of digitale documenten die binnen de organisatie werden gecreëerd. Voorwaarde is wel dat de mappenstructuur binnen het e-mailsysteem afgestemd is op het klassement van de papieren bescheiden en op de mappenstructuur voor digitale documenten op de gemeenschappelijke werkschijven.

Afhankelijk van de werkorganisatie en de technologische infrastructuur kan men e-mails en bijlagen tijdelijk bewaren in een mappenstructuur binnen het e-mailsysteem of onmiddellijk exporteren naar een mappenstructuur buiten het e-mailsysteem. Deze laatste optie verdient aanbeveling omdat op die manier e-mails en bijlagen onmiddellijk gerelateerd worden aan andere digitale documenten met betrekking tot dezelfde zaak of onderwerp. Bovendien wordt binnen de organisatie de vindplaats van digitale informatie beperkt tot één mappenstructuur. Het bestandsformaat waarin de e-mails worden weggeschreven is afhankelijk van de toekomstige functionaliteit van e-mails. Zo kan men ervoor opteren om e-mails tijdelijk in het clientprogramma eigen bestandsformaat weg te schrijven zodat geëxporteerde e-mails opnieuw beantwoord of doorgestuurd kunnen worden.

Het bewaren van e-mails in een mappenstructuur vertoont veel gelijkenissen met het bijhouden van een papieren klassement of het efficiënt beheren van gemeenschappelijke werkschijven. De administratie heeft hier dus al enige ervaring mee. Toch is het raadzaam om hiervoor de nodige richtlijnen te geven. In de richtlijn kan een antwoord gegeven worden op volgende vragen: Wanneer wordt er best een openbare map gebruikt en wanneer een off line map? Hoe wordt de mappenstructuur het best uitgebouwd? Hoeveel niveau’s mag de structuur tellen? Wie bepaalt of wijzigt de hoofdstructuur? Een aantal goede voorbeelden kunnen als leidraad dienen. Medewerkers zullen e-mails en bijlagen maar naar mappen verplaatsen als ze weten in welke mappen de documenten thuis horen en waar ze ze achteraf gemakkelijk kunnen terugvinden.

B.3. Stap 3: Omzetting naar geschikte archiveringsformaten en opname in het archief-beheerssysteem

Voor de e-mails met archiefwaarde mag het archiveringsproces niet stoppen bij stap 2. De opname van e-mails in een archief- of documentbeheerssysteem is van essentieel belang omwille van de toegankelijkheid, raadpleegbaarheid en integratie met de gerelateerde archiefdocumenten.

In de archiveringsstrategie zullen er vervolgens archiveringsmomenten worden ingelast. Het is het meest aangewezen om dit archiveringsmoment zo dicht mogelijk te laten aansluiten bij het tijdstip van ontvangst of verzending. In de praktijk zal dit veeleer het tijdstip zijn waarop een dossier wordt afgesloten, waarop een map of postbus een bepaalde bestandsgrootte heeft bereikt of wanneer een bepaalde periode is verstreken. Het is van belang dat tijdens deze operatie de archivalische band bewaard blijft en de authenticiteit niet in gevaar komt. De e-mails die gearchiveerd worden, moeten in hun map blijven en moeten alle headergegevens (o.a. transmissie gegevens en verwijzing naar bijlagen) bevatten.

Voor het uitvoeren van de archivering zijn verschillende scenario's mogelijk. Het ware wenselijk dat dit proces zoveel mogelijk geautomatiseerd verloopt. Het exporteren van een map met alle e-mails als afzonderlijke XML-bestanden zal ongetwijfeld de snelste oplossing zijn. Deze functionaliteit is echter niet standaard aanwezig in de courante e-mailsystemen, ook niet in de recentste versies (MS Outlook 2002, Lotus Notes 5[142]). Rekening houdende met de groeiende XML-implementatie in softwarepakketten, is het niet denkbeeldig dat toekomstige versies standaard over deze functionaliteit beschikken. Om de XML-export in de bestaande e-mailsystemen mogelijk te maken zal er een ad hoc oplossing moeten worden uitgewerkt. Eén mogelijkheid is een plug-in (bijvoorbeeld een VBA-macro of Com Addin) die elke e-mail als een afzonderlijk Unicode-bestand buiten het e-mailsysteem plaatst, het bestand tagt en bewaart als een XML-bestand. Een andere mogelijkheid is een batchprocedure die autonoom functioneert en die de off line bestanden (*.pst, *.nsf) omzet.

Beide oplossingen vragen programmeerwerk. Hetzelfde resultaat kan met eenvoudige middelen, op een weliswaar meer arbeidsintensieve manier, worden bekomen. Op de doellocatie maakt men dezelfde mappenstructuur zoals binnen het e-mailsysteem aan. De e-mails worden één voor één als een Unicodebestand in de corresponderende map geplaatst. Vervolgens worden de e-mails naar XML omgezet. Het enige wat hiervoor moet gebeuren, is het toevoegen van een XML-header en het taggen van de elementen die samen de e-mail vormen. Aangezien alle e-mails toch een vaste structuur hebben, kan hiervoor gemakkelijk een macro binnen een teksteditor of tekstverwerker worden gebruikt.[143] Hetzelfde resultaat kan bekomen worden met een XML-editor. De getagde e-mails worden als XML-bestand bewaard. Het e-mailarchief kan op een harde schijf of op een externe drager worden geplaatst.

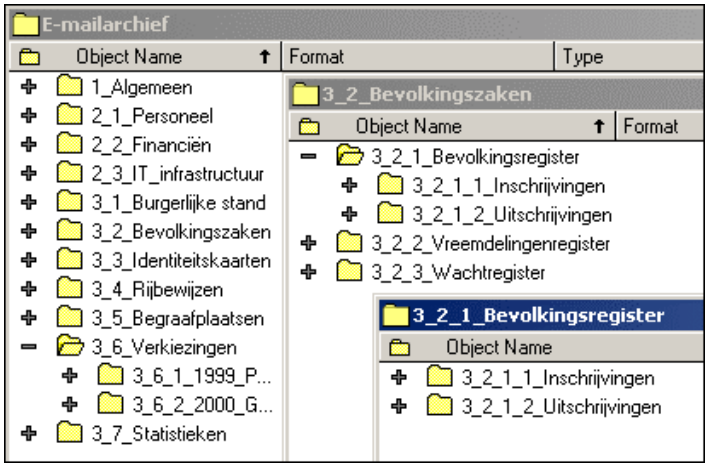
---

[142] MS Outlook 2002 biedt enkel de mogelijkheid om individuele e-mails in ASCII-, RTF- of Outlookbestand (*.msg) off line te plaatsen. Lotus Notes kan e-mails bewaren als ASCII-, Lotus Ami Pro-, Word-, WordPerfect-, TIFF- en RTF-bestand.

[143] Het enige waarin de structuur van e-mails verschillen is dat lege headerelementen niet worden opgeslagen in het platte tekstbestand. De macro voor de omzetting naar XML moet hierop voorzien zijn.

Op het ogenblik van de omzetting naar XML worden e-mails en bijlagen van elkaar gescheiden. De technologische band tussen e-mail en bijlage verdwijnt na de omzetting naar XML. XML is het beste archiveringsformaat voor de e-mails zelf. De bijlagen kunnen zowel tekstueel, grafisch als audio-visueel zijn. Voor elke type is er een gepaste archiveringsstrategie. De bijlagen zijn geen onderdeel meer van de e-mails, maar zijn afzonderlijke bestanden die in dezelfde map als de e-mails en gerelateerde digitale archiefdocumenten staan. Op die manier ontstaat er de facto een dossier waarbij e-mails en bijlagen met betrekking tot dezelfde zaak of hetzelfde onderwerp samen worden bewaard. Het spreekt voor zich dat ook de e-mailbijlagen met archiefwaarde naar een passend archiveringsformaat worden omgezet[144].

De laatste stap is de opname van de gearchiveerde e-mails in het document- of archiefbeheerssysteem van de organisatie. Het volstaat niet dat de e-mails in een mappenstructuur op een harde schijf of een externe drager staan[145]. De gearchiveerde e-mails moeten deel uitmaken van het globale archiverings-systeem van de instelling waarbinnen de samenhang en de context van de archiefbescheiden wordt bijgehouden. In het geval van het stadsarchief Antwerpen worden de gearchiveerde e-mails in het documentsbeheerssysteem opgenomen. Er werd een nieuw object 'e-mail' aangemaakt, met als attributen de metadata of de headervelden. Gelet op de grote omvang van te archiveren e-mails moet bulkopname mogelijk zijn. Binnen het documentbeheerssysteem wordt opnieuw dezelfde mappenstructuur aangebracht.



Afbeelding 10: De mappenstructuur voor gearchiveerde e-mails en de e-mails als XML-bestanden in het documentbeheerssysteem va het stadsarchief Antwerpen. De mappenstructuur is identiek aan de tijdelijke mappenstructuur in het e-mailsysteem (zie afbeelding 3). In de afbeelding zijn in het e-mailarchief de hoofdmappen 'bevolkingszaken' en 'verkiezingen' geopend (functies). Beide mappen bestaan uit submappen (taken) die op hun beurt nog in andere mappen zijn opgesplitst (activiteiten). In de map 'Kiezerslijsten' staan drie e-mails met dezelfde bestandsnaam. Om te voorkomen dat de e-mails elkaar overschrijven bij opname in de docbase werden ze genummerd zodat ze een unieke bestandsnaam hebben.

[144] Voor een overzicht van geschikte archiveringsformaten voor alle types bijlagen: Digitaal ArchiVeren. rIchtlijn & aDvies, nr. 4: *Standaarden voor bestandsformaten*.

[145] In Australië bijvoorbeeld hecht de Nationale Archiefdienst hier bijzonder veel belang aan. De keuze voor digitale archivering is er enkel verantwoord op voorwaarde dat de gearchiveerde e-mails in een archiefbeheerssysteem wordt opgenomen. Bij ontstentenis van een archiefbeheerssysteem wordt aangeraden de hard copy piste te volgen (Archives advice, nr. 20).

C. IMPLEMENTATIE IN DE PRAKTIJK

De beschreven *best practice* is toepasbaar binnen verschillende organisatiestructuren en verschillende technologische infrastructuren. Het doet er niet toe of gemeenschappelijke, persoonlijke e-mailadressen of een combinatie van beide worden gebruikt. De courante e-mailsystemen bieden de nodige functionaliteiten om de creatie van gestructureerde en gecontextualiseerde e-mails mogelijk te maken of te begeleiden. Ten aanzien van het e-mailsysteem zijn de voornaamste eisen de mogelijkheid om de sjablonen aan te passen en een mappenstructuur aan te leggen. De wijdverspreide e-mailpakketten bieden ook een aantal zoekmogelijkheden.

Eens de krachtlijnen van het archiveringssysteem vastliggen, kan met de uitvoering in de praktijk worden gestart. De implementatie van een e-mailarchiveringsstrategie zal best wat tijd in beslag nemen. De eerste twee stappen in deze *best practice* zijn in principe relatief snel uitvoerbaar. Het verdient zelfs aanbeveling om er zo vroeg mogelijk mee van start te gaan. Van zodra de sjablonen zijn aangepast en er een mappenstructuur uitgewerkt is, kan de archiefvorming op een gestructureerde en gecontextualiseerde wijze beginnen. Ondertussen kan er gezocht worden naar een manier om de derde stap in de praktijk om te zetten.

Een succesvolle toepassing zal in grote mate afhangen van de administratie. In de Vlaamse administraties is er geen traditie van records managers of documentaire informatievoorzieners. De administratie zal dus zelf verantwoordelijk zijn voor het toepassen van de eerste stappen in het archiveringsproces: vastleggen van de context door doeltreffend de headervelden in te vullen, selectie, organisatie en beheer van de mappen. Het spreekt voor zich dat deze acties enige vorming en coaching zullen vragen. Eén dienstnota met een algemene beschrijving van de procedure, zal onvoldoende zijn. De administratie heeft nood aan zo concreet mogelijke richtlijnen en voorbeelden. Bij de stad Antwerpen worden cursussen over e-mailarchivering gegeven en op de intranetsite zijn diverse handleidingen en richtlijnen beschikbaar. Eén richtlijn beschrijft de algemene archiveringsprocedure, een andere bevat tips en richtlijnen voor een goede mappenstructuur. De archivaris treedt hier best op als coach en staat mee in voor de nodige opleiding.

Binnen de meeste organisaties zal de archivaris voor de e-mailarchivering functioneren als de architect van het archiveringssysteem. Een goede samenwerking met de informaticaverantwoordelijke(n), in het bijzonder de beheerder(s) van het netwerk en de e-mailserver, is onontbeerlijk.

De krachtlijnen van het beschreven archiveringsproces kunnen ook aangewend worden om retroactief e-mails in een archiveringssysteem op te nemen. Het San Diego Supercomputer Center heeft bij wijze van experiment op één dag 1 miljoen e-mails gearchiveerd. De archivering hield in: tagging van de berichten, opname in het archiefbeheerssysteem, indexering en beschrijving[146]. Retro-actieve contextualisering is echter een ander paar mouwen. De e-mails verstuurd of ontvangen voor de ingebruikname van aangepaste headers zullen meestal standaardheaders zijn en geen verwijding naar de

[146] R. MOORE, e.a, "Collection-Based Persistent Digital Archives - Part 2".

context bevatten. Contextualisering is nog mogelijk door de e-mails in de overeenstemmende map te plaatsen en een referentie naar de context aan de e-mailbody toe te voegen.

XIII. Algemeen besluit

Deze case toont duidelijk de noodzaak aan om bij de archivering van digitale archiefdocumenten zo vroeg mogelijk in hun levensproces op te treden. Van bij de creatie worden er acties ondernomen om efficiënte e-mailarchivering mogelijk te maken. Het archiveringsproces pas starten met de overdracht aan de archiefdienst zou archivering in goede, geordende en toegankelijke staat zwaar hypothekeren. De selectie en contextualisering van de gearchiveerde e-mails zou een onmogelijke opdracht worden.

Het archiveren van e-mails brengt een grote verantwoordelijkheid mee voor de administratie. De administratie is verantwoordelijk voor de selectie en het contextualiseren van de verstuurde en ontvangen e-mails. De administratie heeft hiervoor behoefte aan duidelijke regels, zo concreet mogelijke richtlijnen en opleiding. Als architect van het archiveringssysteem is de archivaris hiervoor mee verantwoordelijk.

Hoe e-mails nu uiteindelijk worden gearchiveerd, zal verschillen van archiefvormer tot archiefvormer. Het afdrukken van e-mails is een valabele optie. Deze archiveringswijze houdt geen technologische moeilijkheden in en de archivalische band met de context wordt door de fysieke plaats van de afdruk vastgelegd. De vraag kan wel gesteld worden hoe lang het houdbaar is om afdrukken te archiveren en of afdrukken geen tussentijdse oplossing is tijdens de overgang van analoog naar digitaal. Belangrijk is dat men erover waakt dat de afgedrukte e-mail alle metadata bevat. Dit kan eenvoudig gerealiseerd worden door alle metadata als afzonderlijke velden in de header van de e-mailformulieren of -sjablonen op te nemen.

Bij digitale archivering van e-mails gaat men bij het aanpassen van de e-mailheaders nog een stap verder. Aangezien de context enkel op een logische of intellectuele manier kan worden vastgelegd, voorziet men in de header best de nodige velden waarin men de band met de bijlagen en het dossier aanduidt. De e-mails kunnen tijdelijk in een off line mappenstructuur binnen het e-mailsysteem worden bijgehouden. In een volgende fase worden de e-mails in een geschikt archiveringsformaat buiten het e-mailsysteem geplaatst en vervolgens in het document- of archiefbeheerssysteem opgenomen.

Welke optie er ook wordt gekozen, het is van groot belang dat de privacyreglementering gerespecteerd wordt bij het archiveren van e-mails. Niet het briefgeheim, maar wel het telecommunicatiegeheim is van toepassing op het kennisnemen en het registreren van (de inhoud van) e-mails. Ook al is deze reglementering (nog) niet aangepast aan de dagelijkse praktijk, de archivaris moet er rekening mee houden en moet ervoor zorgen dat het registreren van e-mails zoveel als mogelijk conform de wet verloopt. Bij de afweging tussen het privacybelang van de werknemer en het belang van de organisatie om over een behoorlijk archief te beschikken, moet steeds het principe van “de redelijke verwachting van privacy” gelden. Deze verwachting moet aan alle belanghebbenden zeer duidelijk kenbaar gemaakt worden. De e-mailpolicy moet deze problematiek op een ondubbelzinnige wijze behandelen.

Bibliografie

WET- EN REGELGEVING

BOEKEN

BLANPAIN, R., VAN GESTEL, M., *Gebruik en controle van e-mail, intranet en internet in de onderneming*, Praktijk en Recht, Brugge, Die Keure, 2003, 264 p.

COPPENS, H., *Archiefbeheer in gemeenten en O.C.M.W.'s*, Brussel, Algemeen Rijksarchief, 1997, 448 p.

DUMORTIER, J., *Informatica- en telecommunicatierecht*, Leuven, Acco, 2001, 226 p.

VAN EECKHOUTTE, W., *Arbeidsrecht*, Antwerpen, Kluwer, 2000, 487 p.

HENDRICKX, F., *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, XXI, 358 p.

JACQMAIN, J., *Droit social de la fonction publique*, Brussel, Presses universitaires, 2000, 49.

MAST, A. en DUJARDIN, J., *Overzicht van het Belgisch grondwettelijk recht*, Brussel, Story-Scientia, 1987, XXVII, 617 p.

NOUWT, S., *Toepassing van privacyregels op elektronische berichten: Privacyregels voor internetberichten; Privacyregels voor EDI-berichten*, Deventer, Kluwer, 1999, 227 p.

VANDE LANOTTE, J., *Overzicht publiek recht*, Brugge, Die Keure, 2001, XLIX, 1291 p.

VAN DEN EYNDE, S., *Digitale archivering: een juridische stand van zaken vanuit Belgisch perspectief. Deel 1*, Antwerpen - Leuven, Stadsarchief Antwerpen – ICRI K.U.Leuven, 2001, 88 p.

ARTIKELS

DE HERT, P., "Bedrijf mag post werknemers niet zomaar open maken", *Juristenkrant*, 2001, afl. 21, 5-6.

DE HERT, P., "Schending van het (tele)communicatiegeheim in het beroepsleven", *T.S.R.*, 1995, 213-293.

DUMORTIER, J., "Little Brother is watching you: mag de werkgever het Internetgebruik van zijn werknemers controleren?" in X., *Liber Amicoruum Prof. Dr. Roger Blanpain*, 1999, 243-259.

DUMORTIER, J., "Internet op het werk: controlerechten van de werkgever", *Oriëntatie*, februari 2000, 35-42.

HORSMAN, P., Archivering van Elektronische Post. Methoden, meningen en alternatieven, Archiefschool Amsterdam, 1999, 9, beschikbaar op http://www.digitaleduurzaamheid.nl/bibliotheek/docs/archelp.pdf

KUITENBROUWER, F., "Inzage e-mailberichten politie-ambtenaren door werkgever", noot onder Registratiekamer, brief d.d. 14 oktober 1997, kenmerk 97\0578.1, *Computerrecht*, 1998, nr. 5, 253-254.

LEBOUTTE, J.M., "De wettelijke bescherming van het briefgeheim", *De Gemeente*, 1988, 369-371.

RIJCKAERT, O., "Le contrat de travail face aux nouvelles technologies", *Orientations*, 2000, p. 208.

SCHRAM, F., "Openbaarheid en Archiefwetgeving" in A.-M. DRAYE (ed.), *Openbaarheid van bestuur in Vlaanderen, België en de europese instellingen*, Leuven, Instituut voor administratief recht, 1996, 153-207.

SUYKENS, M., "Briefgeheim bij openbare besturen", *De Gemeente*, 1995, nr. 4, 182-184.

VAN EECKE, P., "Call centers en de Belgische afluisterwet: een pijnlijke confrontatie", *Computerrecht*, 1997, afl. 1, p. 8-11

VAN VAERENBERGH, E., "Wettelijke bescherming van het briefgeheim", *De Gemeente*, 1989, 165-166.

WALLACE, D., Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice, paper prepared for the Annual Meeting of the Society of American Archivists, Orlando, Florida, September 3, 1998, beschikbaar op http://www.mybestdocs.com/wallace.html

DIGITAAL ARCHIVEREN

Archives advice 20. E-mail is a record!

Beschikbaar op: http://www.naa.gov.au/recordkeeping/rkpubs/advices/advice20.html

BOUDREZ, F., *<XML/> en digitaal archiveren*, Antwerpen-Leuven, Stadsarchief Antwerpen – ICRI K.U.Leuven, 2002, 24p.

BOUDREZ, F., *Standaarden voor digitale archiefdocumenten*, Antwerpen-Leuven, Stadsarchief Antwerpen – ICRI K.U.Leuven, 2003, 76 p.

DURANTI, L., "The archival bond", in *Archives and museum informatics*, 1997, nrs. 3-4, p. 213-218.

E-mail http://www.nla.gov.au/padi

E-mail policies in the government of Canada. A directory. Ottawa, 1996.

FLYNN, S., "The records continuum model in context and its implications for Archival Practice", in *Journal of the Society of Archivists*, vol. 22, nr. 1, 2001, p. 79-93.

Guideline for Managing E-mail, Kansas, 2000.

Handleiding archivering elektronische post, Amsterdam, 2000.

JANSEN, D., *Archiving E-Mail & Public Records: Challenges, Strategies, & NARA's Electronic Records Archives.* Beschikbaar op

http://www.archives.gov/electronic_records_archives/presentations_by_nara_staff.html

J. JONKERS, "Zeeland gaat digitaal: studiedag over elektronisch documentmanagement", in: *Od*, september 2001, nr. 9, p. 349.

KLYNE, G., *An XML format for mail and other message*.
Beschikbaar op:
http://web.archive.org/web/20011224185049/http://www.ietf.org/internet-drafts/draft-klyne-message-rfc822-xml-02.txt

Managing electronic messages as e-mails. Guidelines
http://www.naa.gov.au/recordkeeping/er/elec_messages/contents.html

Managing electronic messages as e-mails. Policy.

Beschikbaar op: http://www.naa.gov.au/recordkeeping/er/elec_messages/contents.html

Managing electronic messages as records

Beschikbaar op: http://www.gslis.utexas.edu/~scisco/lis389c.5/email/index.html

Managing e-mails as record. Website van het Managing eletronic records seminar, technologisch zomerkamp aan de universiteit van Texas,
Beschikbaar op: http://www.gslis.utexas.edu/~scisco/lis389c.5/email

MOORE, R., e.a., "Collection-Based Persistent Digital Archives-Part 1", in: *D-LIB Magazine*, maart 2000.
Beschikbaar op: http://www.dlib.org

MOORE, R., e.a, "Collection-Based Persistent Digital Archives - Part 2", in: *D-LIB Magazine*, april 2000.

THIBODEAU, K., MOORE, R. en BARU, C., "Persistent Object Preservation: Advanced Computing Infrastructure for Digital Preservation", in *Proceedings of the DLM Forum on electronic records. European citizens and electronic information: the memory of the Information Society*, Brussel, 1999, p. 113-120.

THIBODEAU, K., *Preservation and Migration of Electronic Records: The State of the Issues.*
Beschikbaar op:
http://www.archives.gov/electronic_records_archives/papers/preservation_and_migration.html

THIBODEAU, K., "Building the Archives of the Future", in *D-Lib Magazine*, februari 2001.

THOMASSEN, T.H.P.M., "Een korte introductie in de archivistiek", in P.J. HORSMAN, F.C.J. KETELAAR, THOMASSEN, T.H.P.M., *Naar een nieuwe paradigma in de archivistiek*, 's Gravenhage, 1999, p. 11-20.

TOMER, C., COX, R., "Electronic Mail: Implications and Challanges for Records Managers and Archivists", *The Records and Retrieval Report 8*, November 1992, No° 9, 3-4.

WHITMAN, A., TOWNSEND and S., AALBERTS, "Considerations for an Effective Telecommunications-Use Policy", *Communications of the ACM*, Vol. 42, June 1999.

X., *Van digitale vluchtigheid naar digitaal houvast*, Testbed Digitale Bewaring, Den Haag, 2003. http://www.digitaleduurzaamheid.nl/bibliotheek/docs/bewaren_van_email.pdf

Bijlage 1: E-MAIL POLICY

Bij de implementatie van elektronische post binnen de overheid, zijn niet alleen de laatste technologische ontwikkelingen van belang, maar ook en vooral heldere procedures die de verschillende functies die een overheid te vervullen heeft, in ogenschouw nemen. Het gebrek aan een e-mail policy binnen de overheid of het bestaan van een e-mail policy die geen aandacht heeft voor het bewaringsaspect van e-mail, zou er wel eens de oorzaak van kunnen zijn dat ambtenaren e-mail nog steeds als een informeel communicatie-middel beschouwen, en niet als een archiefstuk dat eventueel moet bewaard worden. Ook voor het leeuwendeel van de Vlaamse overheden is dat nog steeds zo. In dit deel gaan we na welke aspecten met betrekking tot archivering een e-mail policy best behandelt. Deze richtlijnen moeten de Vlaamse administraties helpen bij het uittekenen van hun eigen e-mail policy. Het uitgangspunt is niet het invoeren van belemmeringen, maar het streven naar een zorgvuldig communicatie- en informatiebeleid binnen de overheid.

Het opstellen van een e-mail policy wordt vaak ten onrechte toevertrouwd aan de juridische dienst van de organisatie in kwestie. De policy moet uiteraard door juristen nagekeken worden, om er zeker van te zijn dat hij in overeenstemming is met de juridische regels ter zake. Deze controle is echter slechts een laatste stap in de ontwikkeling van een e-mail policy[147]. Bovenstaande juridische analyse moet dan ook als een aanvulling bekeken worden op de policy zoals die voor de organisatie in concreto ontwikkeld werd. Het is in ieder geval een must dat archivarissen en record keepers eraan meewerken. Het is ook van belang dat ze nadien aan hun collega's in de organisatie op een overtuigende wijze uitleggen waarom de policy op een bepaalde manier werd opgesteld, voorzover dit uit de policy zelf nog niet voldoende zou blijken. Regels worden beter opgevolgd als ook duidelijk is waarom ze gelden.

De e-mail policy van een willekeurige Vlaamse administratie, moet aandacht besteden aan de volgende aspecten betreffende archivering:

1. <u>Het statuut 'archiefstuk'</u>

Een e-mail policy moet niet alleen bepalen dat een e-mail een archiefstuk van de administratie kan zijn, maar ook onder welke voorwaarden men te maken heeft met een functionele e-mail. Het moet duidelijk zijn wanneer de organisatie de e-mail als een archiefstuk zal beschouwen. Deze bepalingen zullen dwingender en begrijpbaarder zijn voor de eindgebruiker wanneer de policy archiefstukken definieert in termen van bedrijfsactiviteiten en de vorm van de e-mail, maar eveneens concrete voorbeelden geeft, die in de organisatie teruggevonden worden.

[147] DUMORTIER, J., Regulating and monitoring communications in the enterprise: guidelines for the development of an effective usage policy, paper voorbereid naar aanleiding van de Online Rights Conference.

Bepaal ook duidelijk welke functionele e-mail formeel is en daarom niet mag worden vernietigd door de eindgebruiker zonder voorafgaande toelating van de bevoegde personen binnen de administratie. Het is immers niet omdat een e-mail een archiefstuk is, dat hij ook moet bewaard worden. Verwijs eventueel ook naar de bepalingen of reglementeringen die de bewaring van bepaalde archiefstukken opleggen. Zo is het voor de eindgebruiker ook duidelijk waarom hij sommige e-mails niet zomaar mag wissen. Openbare besturen kunnen in hun e-mail policy bijvoorbeeld verwijzen naar de archiefwet en de openbaarheidswetgeving.

2. Beschikbaarheid van e-mailfaciliteiten en gebruik voor persoonlijke doeleinden

Richtlijnen over het persoonlijk gebruik van het e-mailsysteem komen reeds vaak voor in de bestaande e-mail policies. Zij beperken het gebruik van persoonlijk e-mailverkeer of sluiten het zelfs helemaal uit. Deze policies zijn meestal bezorgd om de rentabiliteit van de organisatie en willen daarmee onproductief e-mailverkeer uit de organisatie bannen. Zorg dat deze richtlijnen ook aandacht besteden aan het archiveringsaspect, bijvoorbeeld door te bepalen dat persoonlijk e-mailverkeer in principe via een apart e-mailadres dient te verlopen. Om de telecommunicatievrijheid van de eindgebruiker te respecteren, is het aan te bevelen om een terughoudend gebruik van e-mailfaciliteiten voor privé-doeleinden toe te laten, maar dat in dat geval toch alle e-mails in de elektronische postbus als functionele e-mail zal beschouwd worden.

Binnen een administratie moet er niet alleen bepaald worden voor wie en onder welke voorwaarden e-mailfaciliteiten beschikbaar zijn, maar ook dat een eindgebruiker die de beschikking heeft over e-mailfaciliteiten, verplicht is om zijn elektronische postbus regelmatig op ontvangen berichten te controleren. Op die manier kan er bekomen worden dat briefwisseling binnen een redelijke termijn behandeld wordt. De Europese Code van goed administratief gedrag bepaalt dat er voor iedere brief die de administratie ontvangt, binnen de twee weken een ontvangstbewijs moet gestuurd worden.

3. De redelijke verwachting van privacy

Uit het voorgaande blijkt dat men hier te maken heeft met twee conflicterende belangen nl. recht op privacy in hoofde van de eindgebruiker en het recht (en vaak ook de plicht) van de organisatie om over een goed geordend en volledig archief te kunnen beschikken. Er zal dus hoe dan ook aan de privacy van de eindgebruiker geraakt worden. De e-mail policy moet duidelijk aangeven hoe de privacy van alle betrokkenen zal gerespecteerd worden. De wet op de privacy is hiervoor maatgevend.

De organisatie moet zijn archiefbeleid duidelijk uit de doeken doen. Indien de eindgebruiker zelf de te archiveren e-mails selecteert, moet de organisatie selectiecriteria aanreiken in richtlijnen en voorbeelden geven. Controles op de naleving van het archiefbeleid moeten eveneens op voorhand aangekondigd worden, net zoals eventuele gevolgen van niet-naleving. Verkiest de organisatie om het archiefbeleid zelf te implementeren, dan moet de e-mail policy duidelijk aangeven dat alle e-mail permanent gefilterd zal worden om archiefstukken op te sporen

De e-mail policy moet vermelden dat elke betrokkene het recht heeft de verwerkte gegevens te raadplegen en indien nodig te verbeteren. De organisatie geeft best aan hoe dit recht in de praktijk kan uitgeoefend worden.

Zonder medewerking van de eindgebruiker zal de organisatie het erg moeilijk hebben om de privacy van alle betrokkenen te respecteren. De e-mail policy moet vermelden welke plichten de eindgebruiker heeft om dit doel te bereiken. Een belangrijk punt is de plicht private e-mail van professionele e-mail te onderscheiden, de verschillende opties werden hierboven aangehaald. De eindgebruiker moet ook meewerken om de privacy van zijn correspondenten te beschermen, bijvoorbeeld door een vaste clausule toe te voegen aan alle uitgaande e-mail of door correspondenten die zich spontaan en voor het eerst tot de organisatie wenden van de privacy policy op de hoogte te brengen.

4. Registratie van e-mails

Net zoals voor brieven, geldt voor e-mail de regel dat ingekomen e-mail niet centraal mag geopend en gelezen worden. De registratie het bestaan van e-mail mag onder dezelfde voorwaarden gebeuren als het archiveren ervan. De eindgebruikers moeten geïnformeerd worden over deze registratie en opnieuw moeten privé e-mails zoveel mogelijk buiten deze registratie gehouden worden. De privacy policy bestemd voor derden moet deze registratie ook vermelden.

Als er gebruik gemaakt wordt van een algemeen e-mail adres van het type 'naam_dienst@naam_administratie.be' (noot) mogen deze e-mails in principe wel centraal geopend en gelezen worden, aangezien ze niet toekomen in de elektronische brievenbus van een individuele ambtenaar. Deze werkwijze vergemakkelijkt de registratie aangezien het probleem van privé e-mail zich normalerwijze niet stelt.

Deze werkwijze kan in het kader van de openbaarheidswetgeving naar de burger toe afgedwongen worden door het algemene e-mailadres op de briefwisseling te vermelden, en ook door formele e-mails vanaf dit e-mailadres te zenden.

5. Versturen van formele e-mail

Nu de juridische status van een e-mailbericht in het huidige juridische kader min of meer geregeld is, en men kan uitmaken waarvoor e-mail kan gebruikt worden op een correcte wijze, moet de e-mailpolicy duidelijk bepalen welke formele boodschappen er elektronisch kunnen verzonden worden en welke niet. Hiervoor schakelt men best de juridische dienst in, die een analyse moet maken van alle mogelijke uitgaande stukken van de administratie.

6. Manier van bewaring

Hier legt men vast op welke wijze de administratie de e-mails bijhoudt. Er zijn verschillende opties: afdrukken van de e-mails en de print-outs toevoegen aan de papieren dossiers, de e-mails met archiefwaarde voor registratie en bewaring naar een centraal e-mailadres doorsturen, de e-mails bijhouden in off line bestanden, enzovoort. De richtlijn legt ook vast wat er gebeurt met de e-mails binnen het e-mailsysteem nadat ze werden afgedrukt of doorgestuurd naar een centrale postbus.

7. Ordenen van e-mails

Het is natuurlijk de eindgebruiker zelf die best weet wat de inhoud van de e-mails is, welke e-mails bij elkaar horen of welke e-mails aan welk dossier moeten toegevoegd worden. Daarom moet er vooraf afgesproken worden dat de eindgebruiker verantwoordelijk is om zijn elektronische postbus 'op orde' te houden. Dit kan gebeuren aan de hand van mappen die een bepaalde ordeningsmethode weerspiegelen. Elke medewerker of elke dienst zal hiervoor een eigen mappenstructuur uitwerken. Hier kan bijvoorbeeld worden verwezen naar een handleiding voor het aanleggen van een mappenstructuur.

8. Hoe attachments behandelen

De attachments bij e-mails belasten het e-mailsysteem en zijn meestal gevaarlijk voor de verspreiding van virussen. Welke soorten attachments zijn toegelaten? Hoe groot mogen de verstuurde attachments zijn? Bij een aantal bedrijven mag de geadresseerde de bijlage niet openen, vooraleer de informaticaverantwoordelijke het computerbestand op virussen heeft gescand. De policy moet ook een antwoord geven op de vraag hoe attachments met archiefwaarde worden gearchiveerd. Bij papieren archivering kunnen de bijlagen eveneens worden afgedrukt en bij de dossier- of onderwerpsmap worden gevoegd. Bij digitale archivering is er de keuze tussen tijdelijke bewaring binnen het e-mailsysteem en onmiddellijke bewaring buiten het e-mailsysteem.

9. Bewaringstermijn

Hier zal men meestal kunnen volstaan met een verwijzing naar de bewaringstermijnen van de papieren archiefstukken.

10. Hoe wordt encryptie behandeld?

De e-mail policy moet vanuit archivistisch oogpunt ook iets zeggen over de houding van de organisatie tegenover encryptie. Encryptie kan gebruikt worden om een elektronische handtekening toe te voegen aan een e-mail. In dat geval zal de inhoud van de e-mail de bestemmeling meestal in leesbare vorm bereiken. Het is echter ook mogelijk dat de communicatiepartners ervoor kiezen om de boodschap zelf te

versleutelen om zo de confidentialiteit van de boodschap te verzekeren[148]. Hier moet er een afweging gemaakt worden tussen leesbaarheid en confidentialiteit van het e-mailverkeer. Archivarissen zullen eerder de nadruk leggen op de leesbaarheid en daarom misschien wat afkerig zijn tegenover de versleuteling van e-mail. Hierbij moet dan wel opgemerkt worden dat de wet uitgaat van de principiële vertrouwelijkheid van e-mail. Men mag alle geoorloofde maatregelen nemen om deze vertrouwelijkheid tijdens de overbrenging te verzekeren. En ook al heeft men verzaakt aan zijn recht op privacy van zijn elektronisch berichtenverkeer tegenover de werkgever, dan nog gaat het volgens ons te ver om te beweren dat de administratie mag verbieden om e-mail te encrypteren. Bovendien kan dit soms in het voordeel zijn van de administratie bijvoorbeeld voor de communicatie van vertrouwelijke informatie.

11. Verantwoordelijkheid

In de e-mail policy wordt er best een referentiepunt bepaald waar men terecht kan als er problemen zijn bij de toepassing van de policy. Er hoeft niet noodzakelijk één aanspreekpunt te zijn voor de hele policy. Voor problemen met bewaring van e-mails is de records manager het aangewezen aanspreekpunt.

12. Sancties

Er moet duidelijk omschreven worden welke de sancties zijn als de policy niet wordt nageleefd. Hierdoor krijgt de policy een meer afdwingbaar karakter. De sanctie kan erin bestaan om de betrokkene de toegang te ontzeggen tot alle informatietechnologie binnen de organisatie. Merk op dat in België noch de archiefwet, noch de openbaarheidswetgeving, een sanctie bepaalt ten aanzien van personen die overheidsdocumenten, incl. e-mail vernietigen[149]. De Canadese *Freedom of Information and Protection of Privacy Act* bepaalt dat het een misdrijf is om opzettelijk documenten, inclusief e-mail en veiligheidskopieën, te vernietigen met de bedoeling om een verzoek om toegang tot deze documenten, uitgaande van een publieke instelling, af te wenden.

---

[148] Dit betekent praktisch dat de afzender de boodschap versleutelt met de publieke sleutel van de bestemmeling, zodat alleen de bestemmeling in staat is om de boodschap te ontsleutelen met zijn eigen private sleutel.

[149] Er is wel het art. 241 Strafwetboek dat alle openbare officieren of ambtenaren en alle met een openbare dienst belaste personen die akten of titels waarvan zij in die hoedanigheid de bewaarders zijn kwaadwillig of bedrieglijk vernietigen of wegmaken (bedoeld worden notarissen en hypotheekbewaarders, maar ook archivarissen in overheidsdiensten), straft met opsluiting van vijf tot tien jaar en met een geldboete van vijftig tot duizend euro (te vermenigvuldigen met 5).

BIJLAGE 2: DTD schema & XML schema voor e-mails

Voor de archivering van e-mails als XML-bestanden is er strikt genomen geen DTD of XML Schema vereist. Wie de migratie naar XML toch wil checken, kan toch een parsing inbouwen. Onderstaande DTD en XML Schema bevatten de elementen die een gearchiveerde minstens moet bevatten. De *Internet Engineering Task Force* werkt momenteel aan een standaard XML-formaat voor e-mails[150].

A. DTD

<!ELEMENT email (afzender, verzonden, geadresseerden, carbon_copies, blind_copies, ontvangen, onderwerp, bijlagen, klassement_afzender, klassement_geadresseerde, bericht, msg_stream?)>

<!ATTLIST email

bestandsnaam CDATA #REQUIRED

MD5_checksum CDATA #IMPLIED>

<!ELEMENT afzender (naam, emailadres)>

<!ELEMENT verzonden (#PCDATA)>

<!ELEMENT geadresseerden (geadresseerde*)>

<!ELEMENT geadresseerde (naam, emailadres)>

<!ELEMENT naam (#PCDATA)>

<!ELEMENT emailadres (#PCDATA)>

<!ELEMENT carbon_copies (carbon_copy*)>

<!ELEMENT carbon_copy (naam, emailadres)>

<!ELEMENT blind_copies (blind_copy*)>

<!ELEMENT blind_copy (naam, emailadres)>

<!ELEMENT ontvangen (#PCDATA)>

<!ELEMENT onderwerp (#PCDATA)>

<!ELEMENT bijlagen (#PCDATA)>

<!ELEMENT klassement_afzender (#PCDATA)>

<!ELEMENT klassement_geadresseerde (#PCDATA)>

<!ELEMENT bericht (#PCDATA)>

<!ELEMENT msg_stream (#PCDATA)>

<!ATTLIST msg_stream

[150] KLYNE, G., *An XML format for mail and other message*.

bestandsnaam CDATA #REQUIRED

encoding CDATA #REQUIRED>

B. XML SCHEMA

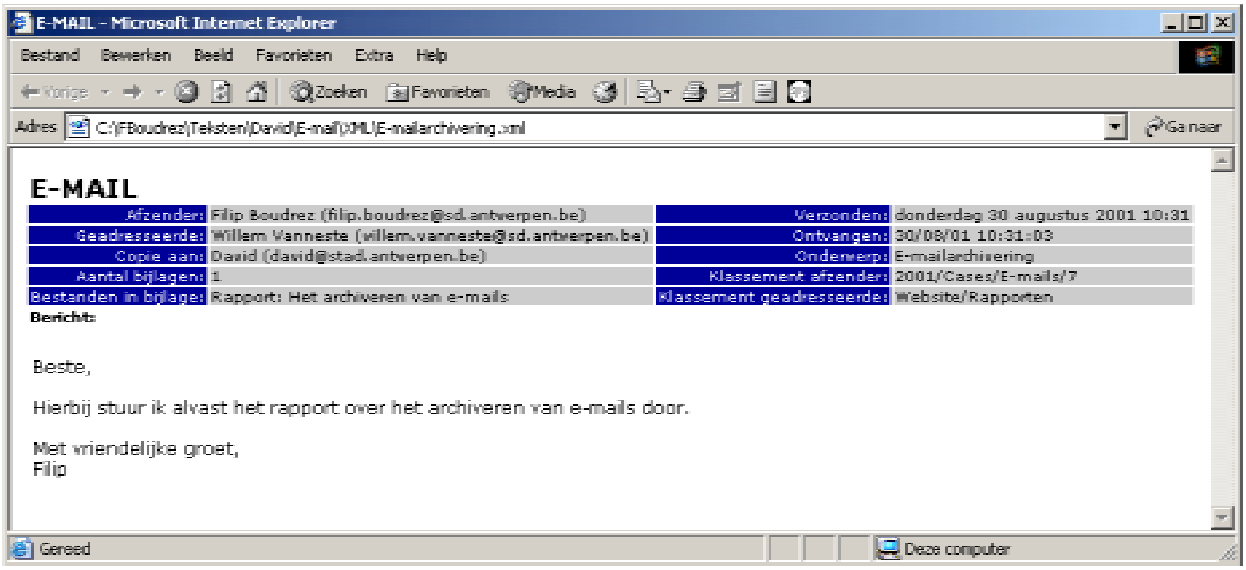
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
 - <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  - <xs:element name="email">
   - <xs:complexType>
    - <xs:sequence>
     - <xs:element name="afzender" minOccurs="1" maxOccurs="1">
      - <xs:complexType>
       - <xs:sequence>
          <xs:element name="naam" type="xs:string" />
          <xs:element name="emailadres" type="xs:string" />
        </xs:sequence>
      </xs:complexType>
    </xs:element>
   <xs:element name="verzonden" type="xs:string" minOccurs="1" maxOccurs="1" />
-  <xs:element name="geadresseerden" minOccurs="1" maxOccurs="1">
  - <xs:complexType>
   - <xs:sequence>
    - <xs:element name="geadresseerde" minOccurs="0" maxOccurs="unbounded">
     - <xs:complexType>
      - <xs:sequence>
         <xs:element name="naam" type="xs:string" />
         <xs:element name="emailadres" type="xs:string" />
       </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
```

```
  </xs:element>
- <xs:element name="carbon_copies" minOccurs="1" maxOccurs="1">
   - <xs:complexType>
     - <xs:sequence>
       - <xs:element name="carbon_copy" minOccurs="0" maxOccurs="unbounded">
         - <xs:complexType>
           - <xs:sequence>
               <xs:element name="naam" type="xs:string" />
             <xs:element name="emailadres" type="xs:string" />
           </xs:sequence>
         </xs:complexType>
       </xs:element>
     </xs:sequence>
   </xs:complexType>
 </xs:element>
- <xs:element name="blind_copies" minOccurs="1" maxOccurs="1">
    - <xs:complexType>
        - <xs:sequence>
          - <xs:element name="blind_copy" minOccurs="0" maxOccurs="unbounded">
            - <xs:complexType>
              - <xs:sequence>
                  <xs:element name="naam" type="xs:string" />
                  <xs:element name="emailadres" type="xs:string" />
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="ontvangen" type="xs:string" minOccurs="1" maxOccurs="1" />
    <xs:element name="onderwerp" type="xs:string" minOccurs="1" maxOccurs="1" />
    <xs:element name="bijlagen" type="xs:string" minOccurs="1" maxOccurs="1" />
    <xs:element name="klassement_afzender" type="xs:string" minOccurs="1" maxOccurs="1" />
```

```
    <xs:element name="klassement_geadresseerde" type="xs:string" minOccurs="1" maxOccurs="1" />
    <xs:element name="bericht" type="xs:string" minOccurs="1" maxOccurs="1" />
  - <xs:element name="msg_stream" minOccurs="0" maxOccurs="1">
     - <xs:complexType>
       - <xs:simpleContent>
         - <xs:extension base="xs:string">
            <xs:attribute name="bestandsnaam" type="xs:string" use="required" />
           <xs:attribute name="encoding" type="xs:string" use="required" />
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
   <xs:attribute name="bestandsnaam" type="xs:string" use="required" />
   <xs:attribute name="MD5_checksum" type="xs:string" use="optional" />
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Bijlage 3: Stylesheet voor e-mails

In een stylesheet kan gedefinieerd worden hoe de webbrowser de e-mail opgeslagen als een XML-bestanden presenteert.



Afbeelding 11: Voorbeeld van de wijze waarop een e-mail bericht, opgeslagen als XML-bestand en gekoppeld aan een stylesheet, in een webbrowser wordt weergegeven. Dit is dezelfde e-mail als in de afbeeldingen 6, 8 en 9.

De stylesheet voor de gearchiveerde e-mail in afbeelding 11 en op onze website is de volgende:

Zie http://www.antwerpen.be/david/downloads/david_emailsjabloon.zip

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns=" http://www.w3.org/TR/xhtml1/strict"
xmlns:xsl="http://www.w3.org/TR/WD-xsl"
xmlns:fo="http://www.w3.org/1999/XSL/Format">>
<xsl:template match="/">
    <html>
      <!-- stylesheet voor e-mails, geschreven door Filip Boudrez voor DAVID
(27 augustus 2001)-->
      <head>
        <title>E-MAIL</title>
        <style>body {}
          Table.e-mailstyle { font-size: 18; font-family: Verdana; line-
height: 1;text-align:left;}
            TD.e-mailstyle_EVEN { font-size:10; background-color: CCCCCC;}
```

```
         TD.e-mailstyle_ONEVEN { font-size:10; color:FFFFFF; background-
color: 000099 ;   text-align: right;}
         TD.e-mailstyle_tekstbericht { font-size:12; color: blue; }
         TD.bericht { font-size:10; color: # FFFFFF; font-weight: 700; }
         p.bericht { font-size:12; color: # FFFFFF; font-family: verdana;
margin-left: 5; white-space:pre;}
     </style>
      </head>
      <body class="Main">
        <xsl:apply-templates select="/e-mail"/>
      </body>
    </html>
  </xsl:template>
<xsl:template match="/e-mail">
    <xsl:for-each select="/e-mail">
      <TABLE WIDTH="100%" HEIGHT="10%" class="e-mailstyle">
        <TR>
          <TH colspan="4">
          E-MAIL
          </TH>
        </TR>
        <TR>
          <TD class="e-mailstyle_ONEVEN">
              Afzender:
              </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="afzender/naam"/> (<xsl:value-of
select="afzender/adres"/>)
              </TD>
          <TD class="e-mailstyle_ONEVEN">
              Verzonden:
              </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="verzonden"/>
          </TD>
        </TR>
        <TR>
          <TD class="e-mailstyle_ONEVEN">
              Geadresseerde:
              </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="geadresseerde/naam"/> (<xsl:value-of
select="geadresseerde/adres"/>)
              </TD>
          <TD class="e-mailstyle_ONEVEN">
              Ontvangen:
              </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="ontvangen"/>
          </TD>
        </TR>
        <TR>
          <TD class="e-mailstyle_ONEVEN">
              Copie aan:
              </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="copie_aan/naam"/> (<xsl:value-of
select="copie_aan/adres"/>)
```

```
            </TD>
          <TD class="e-mailstyle_ONEVEN">
              Onderwerp:
              </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="onderwerp"/>
          </TD>
        </TR>
        <TR>
       <TD class="e-mailstyle_ONEVEN">
              Aantal bijlagen:
          </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="bijlagen/aantal_bijlagen"/>
          </TD>
    <TD class="e-mailstyle_ONEVEN">
              Klassement afzender:
              </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="context/klassement_afzender"/>
          </TD></TR>
    <TR>
          <TD class="e-mailstyle_ONEVEN">
              Bestanden in bijlage:
          </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="bijlagen/bestanden_in_bijlage"/>
          </TD>
          <TD class="e-mailstyle_ONEVEN">
              Klassement geadresseerde:
          </TD>
          <TD class="e-mailstyle_EVEN">
            <xsl:value-of select="context/klassement_geadresseerde"/>
          </TD>
        </TR>
        <TR>
          <TD class="bericht">
              Bericht:
              </TD>
        </TR></TABLE>
    <pre><p class="bericht"><xsl:value-of select="bericht"/></p></pre>
     </xsl:for-each>
   </xsl:template>
</xsl:stylesheet>
```